VMware Workspace ONE Launcher

VMware Workspace ONE UEM

vmware®

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

Contents

VMware Workspace ONE Launcher Details

1

Workspace ONE Launcher is an app launcher that enables you to lock down Android devices for individual use cases and customize the look and behavior of managed Android devices. The Workspace ONE Launcher is pushed with Workspace ONE UEM powered by AirWatch and replaces your device interface with one that is custom- tailored to your business needs.

Note Workspace ONE Launcher only supported in Android 6.0+ Work Managed Device enrollment mode. Workspace ONE Launcher is not supported in Work Profile enrollment.

The biggest advantage of Workspace ONE Launcher is that it can give administrators complete control over mobile use without using the OEM-specific MDM APIs.

Configuring Workspace ONE Launcher settings in the VMware Workspace ONE UEM™ console tailors devices for deployment in any number of situations, such as:

- **Retail** – Lock each device into a single app with no access to other features or settings. Customers can browse store products or place food orders without employee interaction.
- **Education** – Load a single education or research app for students to use while in class. Students are unable to surf the Web or download more apps onto devices.
- **Healthcare** – Loan out devices with whitelisted apps for patient-use, such as games and entertainment apps. Enable phone features and customize an address book with important hospital contact information.

Supported OS Versions

Workspace ONE Launcher only supported in Android 6.0+ Work Managed Device enrollment mode. Workspace ONE Launcher is not supported in Work Profile enrollment.

Workspace ONE Launchersupports the following OS versions:

- 4.4.X
- 5.0.X
- 6.0.X
- 7.0.X
- 8.0.X

- 9.0.X
- 10.0.X

Consider viewing the tutorial that launches when you first open the Launcher profile in the Workspace ONE UEM console. The tutorial introduces the seven elements or steps to configure as you customize your Launcher profile. You can exit the tutorial and return later by selecting the question mark icon in the top right corner if you need to review.

Workspace ONE Launcher Profile 2

Locking down your devices with Workspace ONE Launcher includes the configuration of a profile and the deployment of the application to your device fleet. This profile allows complete customization of the look and feel of the device, and access to important settings and native applications depending on the app mode selected.

Workspace ONE Launchercan be configured in one of three app modes. **Single App** mode enables you to lock each device into a single app and prevent access to other features or settings on the device. You can provide access to dependent apps, set as hidden apps. **Multi App** mode enables you to restrict the Launcher profile to a limited set of whitelisted apps and customize the layout. **Template Mode** enables you to customize the entire user interface of the Launcher app such as app spaces, images, and text.

Using Workspace ONE Launcher with Android versus Android (Legacy)

How you use Workspace ONE Launcher depends on how you've configured setup in the Workspace ONE UEM console and the version of your Android devices:

- If you have completed Android EMM Registration and are using Android 6.0+ Work managed devices:
  - Deploy Workspace ONE Launcherusing the Android profile. Using Workspace ONE Launcher with the Android profile configures devices for a single purpose such as kiosk mode by whitelisting supported internal and public applications. This hides certain settings on the device to prevent users from exiting from the Workspace ONE Launcher app. For more information on Workspace ONE UEM integration with Android, see the VMware AirWatch Android Platform Guide.
- If you opted out of Android EMM Registration with Google:
  - Deploy Workspace ONE Launcher using the Android (Legacy) method.

    For more information on Workspace ONE UEM integration with Android (Legacy), see the VMware AirWatch Android (Legacy) Platform Guide.

After you configure all desired settings for your organization and selected app mode, determine what version of Workspace ONE Launcher you are pushing to our device fleet. You can control which devices receive the Workspace ONE Launcher by configuring the smart group assignment within the General profile when creating the Launcher profile.

Workspace ONE Launcher can be provisioned and deployed as a seeded application, internal application, or pushed through Product Provisioning. Depending on the use case for your device fleet, push the profile accordingly.

This chapter includes the following topics:

Configure Workspace ONE Launcher Profile

Locking down your devices with Workspace ONE Launcher includes the configuration of a profile and the deployment of the application to your device fleet.

You can deploy Workspace ONE Launcher to be used on Android 6.0+ Work managed devices for Android or Android (Legacy) if you've opted out of Android EMM registration with Google. Workspace ONE Launcher is not supported in Work Profile enrollment.

Procedure

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

  Alternatively, select **Android (Legacy)** to configure the Launcher profile if you've opted out of Android EMM registration.

2 Configure the **General** profile settings as desired.

3 Select the **Launcher > Configure**.

4 Configure devices with your custom home-screen by selecting an app mode: **Single App**, **Multi App**, or **Template Mode**.

5 Configure **Layout** elements such as the icon grid and orientation preference.

   You can upload images to customize the Launcher with your unique brand look and feel as allowed by the selected app mode. For the available layout settings, please see Layout Settings.

6 Determine if your devices need to be used in **Offline Mode**.

   Offline mode is used when devices are being used in check-in check-out mode. It allows users to continue their work even when they are unable to log in as themselves or are in areas where network connectivity is unstable.

   This setting should be applied to both the end-user and staging user or an organization group that includes both. Assigning to all users ensures the offline mode profile is present when moving between users.

7 Move to the **Apps** section and use the drop-down menu to select Public, Internal, or Miscellaneous or to add Bookmarks.

   To learn more about bookmarks, see Bookmarks for Workspace ONE Launcher.

8 Organize the Launcher Canvas with apps, view **App Attributes**, remove apps, and create folders for apps to group apps together.

   View the available Canvas settings on Canvas Settings for Workspace ONE Launcher View available App Attributes on App Attributes for Workspace ONE Launcher.

9 Configure **Hidden Apps**, if needed.

   Find out how to add hidden apps on Add Hidden Apps .

10 Click the **Settings** button to configure device settings and utilities to be allowed and to configure the admin passcode.

   To see available settings, please see Settings for Workspace ONE Launcher.

11 Select the **Preview** button to view how the configuration will appear on the user's device.

12 Select **Save** to add the profile to the Workspace ONE UEM console or **Save & Publish** to add the profile and immediately deploy it to applicable Android devices.

Results

After the profile is created and deployed to devices, the Device Details page shows the status of the Launcher as "Launcher is the home app." If install was not successful or Workspace ONE Launcher is not the default app, the status shows " Launcher is not set at the home app or is not installed."

What to do next

Configure Launcher version settings which determines which version of the Workspace ONE Launcher is pushed to you devices.

Custom XML for Workspace ONE Launcher

This topic covers the available Custom XML to be implemented with Workspace ONE Launcher for Android in each version.

Configure Custom XML for Launcher

The **Custom Settings** payload can be used when new Android functionality releases or features that Workspace ONE UEM console does not currently support through its native payloads. Use the **Custom Settings** payload and XML code to manually enable or disable certain settings.

Be sure you are using the right characteristic type for your profile type:

- For Android profiles, use characteristic type = "com.airwatch.android.androidwork.launcher".
- For Android (Legacy) profiles, use characteristic type = "com.airwatch.android.kiosk.settings".

To configure the custom XML:

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

2 Configure the profile's **General** settings,

3 Configure the applicable payload (for example, Restrictions or Passcode).You can work on a copy of your profile, saved under a "test" organization group, to avoid affecting other users before you are ready to Save and Publish.

4 **Save**, but do not publish, your profile.

5 Select the radio button from the **Profiles List View** for the row of the profile you want to customize.

6 Select the **XML** button at the top to view the profile XML.

7 Find the section of text starting with <characteristic> ... <characteristic> that you configured previously, for example, Restrictions or Passcode. The section contains a configuration type identifying its purpose, for example, restrictions.

> **Note** Be sure to always modify at least one number or character in the UUID before pasting into the UEM console. The UUID values are a sequence of values within 0-9 and a-f. Any one value can be changed to another within these ranges to distinguish this from the base UUID in this docs page. This helps avoid issues when using multiple profiles with the same UUID.

8 Copy this section of text and close the XML View. Open your profile.

9 Select the **Custom Settings** payload and select **Configure**. Paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from <characteristic> to <characteristic>.

   a This XML should contain the complete block of code as listed for each custom XML.

   b Administrators should configure each setting from <true /> to <false /> as desired.

   c If certificates are required, then configure a Certificate payload within the profile and reference the PayloadUUID in the Custom Settings payload.

10 Remove the original payload you configured by selecting the base payload section and selecting the minus [-] button. You can now enhance the profile by adding custom XML code for the new functionality.Any device not upgraded to the latest version ignores the enhancements you create. Since the code is now custom, you should test the profile devices with older versions to verify expected behavior.

11 Select **Save & Publish**

Use the sections below to find the custom XML.

Offline Mode for CICO (Beta)

Available in Workspace ONE Launcher 21.04

Offline mode allows employees can continue their work even when they are unable to log in due to network issues. You can designate a Launcher profile as an offline mode profile which can only be accessed when the device is offline.

To Beta offline mode, enroll your device into a UAT environment that has data-driven UI enabled, such as CN135.

Push the following custom XML to your organization group to enable offline mode:

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
 <parm name="EnableOfflineMode" value="True"/>
 </characteristic>
```

Disable FocusMonitoring API

Available in Workspace ONE Launcher 4.8

On Samsung devices, Launcher defaults to using the Samsung Focus Monitoring API. This allows Launcher to automatically foreground applications without the user having to grant the Android Usage Access Permission. The admin can disable this feature using the following custom XML. Disabling this feature on Samsung devices will require users to grant the usage access permission on the first launch of Launcher.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="DisableFocusMonitoring" value="True"/>
</characteristic>
```

Show Popup Notifications

Available in Workspace ONE Launcher 4.8

Admins can generate popup notifications regardless of channel priority using this custom XML. To show popups, the notification bar cannot be disabled. Admins can create popups regardless of how the app sending the notification prioritizes its notification channel.

After Android O, popups will only show if the app sending the notification sets a notification channel to show popups, but this custom XML bypasses that behavior.

For generating popup for all allowed apps:

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="ShowPopupNotification" value="True"/>
</characteristic>
```

For generating popup for specific apps:

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="ShowPopupNotification" value="com.application1.package,
com.application2.package"/>
</characteristic>
```

Hide Enable Notifications Button

Available in Workspace ONE Launcher 4.8

Admins can hide the “Enable Notifications” button from the Launcher dropdown menu by using the following custom XML.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="AllowEnableNotification" value="False"/>
</characteristic>
```

Disable Sensor Orientation

Available in Workspace ONE Launcher 4.8

Use this setting to prevent the device from switching to reverse portrait mode or reverse landscape orientation.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="DisableSensorOrientation" value="True"/>
</characteristic>
```

Speed Lockdown

Available in Workspace ONE Launcher 4.7

Use this custom XML to block device access when exceeding a specified speed threshold.

```
<parm name="SpeedLockdownSettings" value="{&quot;speed&quot;:&quot;20&quot;,
&quot;unit&quot;:&quot;0&quot;, &quot;timeThreshold&quot;:&quot;10000&quot;,
&quot;troubleshootPasscode&quot;:&quot;1234&quot;, &quot;headerText&quot;:&quot;Too
Fast&quot;, &quot;messageText&quot;:&quot;Stop to unlock&quot;}" />
```

The default values are as followed:

- Unit = 1 (m/h)
- TimeThreshold = 5000 (5 seconds)
- HeaderText = "Device Locked"
- MessageText = "Come to a complete stop to unlock device"

The accepted values are as followed:

- Speed > 0
- Unit = 0 - km/h , 1 - m/h (default = m/h)
- TimeTheshold > 0 (in milliseconds)
- TroubleshootPasscode (length > 0)
- HeaderText (length > 0 chars < 15 chars)
- MessageText (length > 0 chars < 30 chars)

Runtime Permissions

Available in Workspace ONE Launcher 4.6

Use this custom XML if you want to enable the Runtime Permissions prompt for end users.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
                    <parm name="RunTimePermissionSetting" value="0"/>
                    </characteristic>
```

The value can be one of the following :

- "0": Runtime permission prompt displays and the user cannot continue until all the permissions are granted. (Required)
- "1": Runtime permission screen displays but is not mandatory to grant all the permissions. (Optional)
- "2": Runtime permission screen is not displayed. (Not Required)

Write Settings Permission

Available in Workspace ONE Launcher 4.6

You can enable the 'Write Permissions' prompt during Launcher setup which allows users to change system settings inside the Launcher profile. When users go to configure settings inside the Launcher, for example, if the user wants to change screen brightness or change auto-rotate settings from inside the Launcher, they are no longer prompted to allow the permission at that time as the permission was granted during setup.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
                    <parm name="WriteSecurePermissionSettings" value="True"/>
                    </characteristic>
```

Skip overlay permission screen

Available in Workspace ONE Launcher 4.6

Use this custom XML to over to skip the 'Draw over other apps permission" which is used for adding overlays and blacklisting apps. This permission displays during initial Launcher setup.

```
 <characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
                <parm name="SkipOverlayPermissionScreen" value="True"/>
                </characteristic>
```

Actionbar Settings

Available in Workspace ONE Launcher 4.6

If you want to set a default action bar title to display during Check-in/Check-out (CICO) screen, this custom XML lets you configure Launcher to always retain the action bar title.

Since this XML is applicable for CICO, it should be pushed for the staging user. If the retainChildTitle is set to false or ignored, the defaultTitle will always be used in CICO action bar. If the child user has lookup values like username or email and retainChildTitle is set to true, that title will be retained, i.e. the email of the last user will appear in the CICO screen. During Launcher first configuration, it uses the default title.

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
                    <parm name="ActionBarSettings"
value="{&amp;quot;retainChildTitle&amp;quot;:&amp;quot;True&amp;quot;, &amp;quot;defaultTitle&amp;quot;:&amp;quot;Vmware
- Airwatch&amp;quot;}" />
                    </characteristic>
```

Wallpaper Scale Type

Available in Workspace ONE Launcher 4.5+

When using an image in Launcher settings, changing the device orientation can change the scaling of the image. For example, if you use a square image in Portrait mode and the rotate the device to Landscape mode, it changes to fit the entire screen instead of maintaining the square scaling.

If you want to set the scale type of the wallpaper to remain the same for different screen orientations, the following custom XML can be used:

```
<chara:teristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="WallpaperScaleType"
value=" {&quot;portraitScaleType&quot;:&quot;FIT_CENTER&quot;,
&quot;landscapeScaleType&quot;:&quot;FIT_XY&quot;}"/>
</characteristic>
```

App Pinning

Available in Workspace ONE Launcher 4.5+

App pinning allows you to pin icons at the bottom of the Workspace ONE Launcher screen similar to how any native launcher functions. The icons are placed in a bottom bar and remain pinned to the screen as users swipe through different screens. The basic custom XML is a JSON array of items that are to be added to the bottom bar:

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="HotSeatBarSettings" value="{&quot;HotSeatBarSettings&quot;: [
{&quot;pName&quot;: &quot;com.android.chrome&quot;,&quot;title&quot;:
&quot;GoogleChrome&quot;,&quot;applicationType&quot;: &quot;misc&quot;,&quot;position&quot;:
&quot;1&quot;} ]}"/>
</characteristic>
```

The parameters to add an application:

- **pName** - Indicates the package name of the application that has to be added. If an admin has not mentioned the package name, the application is not added to the bottom bar. This field is required.
- **title** - Indicates the application name that has to be displayed on the screen. This field is required.
- **position** - Indicates the position of the application to be added to the bottom bar. Position attribute is 0 indexed.

  The application is not added to the bottom bar if the admin :

  - Has not added the position attribute.
  - If the position is greater than the number of columns that are configured in the Launcher profile.
- **applicationType** - This attribute indicates the type of shortcut that has to be added to the bottom bar. This field is required. The value should be one of the following:
  - **Misc** - Miscellaneous application
  - **Public** - Public application
  - **Internal** - Internal application

    - **Bookmarks** - Bookmark
- **folderName** - indicates whether the application has to be added in a folder.

  Note If you want to add multiple applications to the same folder, then the folder name for all those applications should be the same and the position of all the applications should also be the same.

- **URL** - Indicates the URL that the bookmark has to load. The field us required if **applicationType** is set to **Bookmarks**.
- **subPackageNames** - Specifies which activities should be added in case of multi-launch application. Activity names must be comma-separated as shown in the above XML.

- **LaunchAppOnStartup** - Specifies whether the application should be launched as soon as the profile is loaded.

Note If a dynamic application (application with * in package name) is added to the bottom bar, then a folder is created with the name equal to the value of the "title" attribute and all the applications included in the subpackage will be added to that folder.

Use Case	Custom XML
Add an application to bottom bar	Miscellaneous `<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="HotSeatBarSettings" value="{"HotSeatBarSettings": [ {"pName": "com.android.chrome","title": "GoogleChrome","applicationType": "misc","position": "1"}]}"/></characteristic>` Public `<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="HotSeatBarSettings" value="{"HotSeatBarSettings": [ {"pName": "com.android.chrome","title": "GoogleChrome","applicationType": "public","position": "0"}]}"/></characteristic>` Internal `<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="HotSeatBarSettings" value="{"HotSeatBarSettings": [ {"pName": "com.android.chrome","title": "GoogleChrome","applicationType": "internal","position": "1"}]}"/></characteristic>`
Add a bookmark to the bottom bar	`<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="HotSeatBarSettings" value="{"HotSeatBarSettings": [ {"url": "https://www.google.com","title": "Google","applicationType": "bookmarks","position": "1"}]}"/>`

Staging Admin Passcode

Available in Workspace ONE Launcher 4.4.1+

Users can exit the Workspace ONE Launcher from the check-in/check-out screen by entering the password specified in the custom XML. After checkout, the staging admin passcode will be replaced by the end user profile admin passcode. Since the admin icon must be displayed in the check-in/check-out screen, the custom XML must be pushed for the staging user. Use this custom XML to enable an admin icon in the login screen:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="StagingAdminPasscode" value="1234"/>
</characteristic>
```

Allow Staging Activities

Available in Workspace ONE Launcher 4.4+

You can allow activities or Package Names for end users after devices have been checked out. This custom setting can be used in following scenarios:

- Allow activities or package names at parent Organization Group.
- Allow activities before end user profile lands on the device.

Use this custom XML to allow activities in the check in/check out screen:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="AllowStagingActivities" value="{&quot;AllowStagingActivities&quot;:
[ {&quot;pName&quot;: &quot;com.android.settings&quot;,&quot;cName&quot;:
&quot;com.android.settings.LanguageSettings&quot;},
{&quot;pName&quot;: &quot;com.android.settings&quot;,&quot;cName&quot;:
&quot;com.android.settings.WifiPicketActivity&quot;} ]}"/>
</characteristic>
```

Allow Log Collection

Available in Workspace ONE Launcher 4.4+

If admin wants to collect logs for a certain use case or in certain scenarios, use this Custom XML and request the debug logs from the Workspace ONE UEM console:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec"><parm name="AllowLogCollection" value="True"/></characteristic>
```

Allow Staging Profile

Available in Workspace ONE Launcher 4.2.1+

If the customer assigns a single profile to all the users at the parent Organization Group level, then use this custom XML:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="AllowStagingProfile"
        value="True"/></characteristic>
```

Settings Overlay for Android Tablet

Available in Workspace ONE Launcher 4.2+

This overlay can be used with allow list custom settings areas for users on Android tablets to prevent the user from accessing settings outside of the Launcher interface. To implement an overlay, use the following Custom XML:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="TabletOverlaySettings"
value="{&quot;activityNames&quot;:&quot;com.android.settings.Settings$lockAndsecuritySettingsA
ctivity,com.sonyericsson.setupwizard,com.honeywell.systemtools.autoinstall&quot;,&quot;potrait
Percentage&quot;:
&quot;60&quot;,&quot;transparency&quot;:&quot;100&quot;,&quot;landscapePercentage&quot;:
&quot;50&quot;}"/characteristic>
```

The above custom setting has multiple parameters:

- `activityName`: When this parameter is added the overlay appears only when the settings are accessed through the particular activity.
- `portraitpercentage`: This parameter configures the overlay percentage in portrait mode.
- `transparency`: This parameter configures the overlay transparency in terms of percentage.
- `landscapePercentage`: This parameter configures the overlay percentage in landscape mode.

Force Reset Launcher Layout on Profile Update

Available on Workspace ONE Launcher 4.2+

Through use of Workspace ONE Launcher if given the ability, users can move folders and application around to their preference. Normally these rearrangements are maintained when profiles or the Launcher are updated. To revert to the original configuration, this custom XML can ignore the user preference and go back to the original layout:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
 <parm name="AllowProfileReset" value="True"/>
 </characteristic>
```

Set Launcher as Default after Reboot

Available on Workspace ONE Launcher 4.2+

Currently, when a user exits Workspace ONE Launcher using admin passcode and reboots the device, Workspace ONE Launcher is not set as the default launcher. To set Workspace ONE Launcheras the default launcher for the device, the profile must be pushed again.

This setting is used in cases where an environment administrator exits Workspace ONE Launcherand forgets to reenter the secure launcher after completing their tasks. This feature works only on select Android devices, namely, Honeywell, Zebra and Samsung.

In cases where the launcher opens after a delay, the length of time can be defined in seconds in the XML below:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
 <parm name="AllowLaunchOnReboot" value="5"/>
 </characteristic>
```

Allow Staging Settings

Available in Workspace ONE Launcher 4.1+

In Workspace ONE Launcher, the option of toggling Wi-Fi is only available in the staging screen. If a user wants to configure Wi-Fi settings, long press on the Wi-Fi icon to launch the native Wi-Fi settings. Since this setting has to be accessed in the staging screen, the below custom xml must be pushed for the staging user (parent organization group). This can be configured by using below flag:

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="AllowStagingSettings" value="True"/></characteristic>
```

Floating Home Button Setting

Available with Workspace ONE Launcher4.0 +

In COSU mode, the HOME and RECENTS buttons are disabled making it hard for a user to switch between the applications. Workspace ONE Launcher provides a way to have a similar home screen experience by adding a Floating Home button.

Functionalities of the Floating Home button:

- The Floating Home button is shown on top of any application. Clicking the Floating Home button launches the home screen which is Workspace ONE Launcher since it is the default home application.
- The Floating Home button can be moved across any part of the screen.
- The Floating Home button, if not touched for a particular amount of time, fades so that it allows to read the content below it.
- The Floating Home button becomes active again when the user touches it back.

Note: By default the Floating Home button is added in Multi-App and Template modes.

The Floating Home button can be configured by using the below setting:

```
<characteristic
          type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="HomeFloatingButtonSetting"
value="{&quot;Size&quot;:&quot;Small&quot;,&quot;Color&quot;:

&quot;#F377F7&quot;,&quot;TimeToFade&quot;:&quot;5&quot;,&quot;FadeValue&quot;:&quot;3&quot;}"
/></characteristic>
```

Things that can be configured for the Floating Home button:

- `Size`: Indicates the size of the Floating Home button. The possible values: Small, Medium, Large.
- `TimetoFade`: Indicates the time in seconds for Floating Home button to fade away.
- `Color`: Indicates the color of the Floating Home button. color must be specified in a Hex code Eg: #F377F7.
- `FadeValue`: Indicates the amount of fading required.

Remove Floating Home Button Setting

Available with Workspace ONE Launcher 4.0+

In COSU mode the Home and Recents buttons are disabled making it hard for a user to switch between the applications. Workspace ONE Launcher provides a way to have a similar home screen experience by adding a Floating Home button.

The floating home button can be removed by using the below setting:

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="RemoveHomeFloatingButtonSetting" value="True"/></characteristic>
```

Allow Home Floating Setting

Available with Workspace ONE Launcher 4.0+

The Floating Home button is enabled for Android compliant devices only. On some devices, the default home button may be inaccessible. This is applicable only for non-Android devices and only in MULTIAPP and TEMPLATE modes. If an admin wants the Floating Home button functionality, use the below Custom XML.

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="AllowHomeFloatingSetting"
value="True"/></characteristic>
```

Single App Floating Button Setting

Available with Workspace ONE Launcher 4.0+

In Single application mode launcher provides a Floating action button for users to access different launcher settings. This button can be configured by using the below setting:

```
<characteristic
          type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec"><parm name="SingleAppFloatingButtonSetting"
value="{&quot;Size&quot;:&quot;Small&quot;,&quot;TimeOut&quot;:
          &quot;2&quot;,&quot;FixPosition&quot;:&quot;true&quot;}"/></characteristic>
```

Things that can be configured for floating action button:

- `Size`: Indicates the size of the floating action button. Possible values: Small, Medium, Large.
- `Timeout`: Indicates the time in seconds for floating button to fade away. Should be an integer only.
- `FloatingTimeoutValue` custom flag is now deprecated from version 4.0 instead we should use this flag.
- `FixPosition`: When enabled, the user cannot move the floating action button. It is positioned at the right end corner. This setting replaced the `FixSettingsPosition` from previous versions.

Allow Localized App Names

Available with Workspace ONE Launcher 4.0+

Currently in Launcher application names are displayed according to the names that are set on the console. Admin can use this flag to display application names according to the language set on the device:

```
<characteristic
          type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="AllowLocalizedAppNames"
value="True"/></characteristic>
```

Extra Lock Task Packages

Available with Workspace ONE Launcher 4.0+

This setting specifies the packages that are allowed to be launched but are not on the allow list.By default launcher automates the process of allowlist settings and other application ,but in any case if some application cannot be launched then we can use this flag.Note: This is only for troubleshooting purposes.

```
<characteristic
          type="com.airwatch.android.androidwork.launcher"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="ExtraLockTaskPackages"
          value="com.android.settings,com.google.android.chrome/></characteristic>
```

Skip Usage Access Permission

Available with Workspace ONE Launcher 4.0+

In case the customer has no use case of using usage access permission they can use the below custom profile to skip this permission being asked from launcher during configuring.

```
<characteristic
          type="com.airwatch.android.androidwork.launcher"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="SkipUsageAccessPermission"
value="True"/>
      </characteristic>
```

Skip CosuSetup - COSU

Available with Workspace ONE Launcher 4.0+

Launcher 4.0 uses new native Android APIs for Google EMM Registered enrollments in the standard Android profile. These new APIs fall under the umbrella of Corporate-Owned Single-Use (COSU) mode. Some features are removed while using COSU mode, this is purposeful to be able to drastically increase the security of the Launcher application. Please see the drawbacks and benefits below, use this custom XML tag to skip COSU mode setup.

```
<characteristic
          type="com.airwatch.android.androidwork.launcher"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="SkipCosuSetup"
value="True"/></characteristic>
```

When in COSU mode (Lock Task mode), devices running versions of Android older than 9.0 will see some features disabled by default. Impacted features include the removal of the Notification / Status Bar at the top of the screen, and the Home & Recent Task soft keys at the bottom of the screen.

By using COSU mode (default), the level of security is greatly improved within the Application.

In DO mode COSU will be configured by default, In case the customer's use cases are not satisfied then they can disable COSU setup.

Display Lock Screen Message

Available with Workspace ONE Launcher 3.3+

The Lock Screen message displays a custom message on the lock screen. You can customize the message with the following attributes:

- `Message` - Indicates the text to be displayed on the lock screen. If a message is not included in the XML, then the checked-out user name is displayed instead.
- `Position` - Indicates the position of the text on the lock screen.

  Values = topLeft, topRight, topCenter, bottomLeft, bottomRight, bottomCenter and center. If position is not included in the XML, the position defaults to topCenter.
- `TextSize`- Indicates the size of text in sp units.

- `TextColor` - Indicates the color of the text in hexadecimal format.

To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="eadfebd8-7f4c-4837-b9dd-dfcf31bd84e6">
<parm name="DisplayLockScreenMessage"

value="{&amp;quot;message&amp;quot;:&amp;quot;AirWatch&amp;quot;,&amp;quot;position&amp;quot;:&amp;quot;topRight&amp;quot;,&amp;quot;textSize&amp;quot;:&amp;quot;20&amp;quot;,
          &amp;quot;textColor&amp;quot;:&amp;quot;#4E993E&amp;quot;}"/> </characteristic>
```

Hot Swap Profile Caching

Available with Workspace ONE Launcher 3.3+

As check-in/check-out is common, users often check out the same device but have to wait a considerable amount of time for profiles to be a. As a result, AirWatch has enhanced the Hot Swap functionality to limit the number of profiles that are cached during check-in/check-out.Profiles are cached for the value specified in the custom setting. If a new profile is added to the cache and the number of cached profiles exceeds the specified value, the most recent specified number of profiles are cached and the initial profiles are deleted. Additionally, the title bar icons of the profiles are cached, but not the wallpapers.To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="MaxProfilesAllowed"
value="Value"/></characteristic>
```

Restrict Power Off/Restart/Safe Mode Options

Available with Workspace ONE Launcher 3.3+

Users can easily exit secure launcher by rebooting into safe mode. To enter into safe mode:

1 Press and hold power button on the device.

2 On the screen, touch and hold Power off.

3 The "Reboot to Safe mode" dialog displays.

To prevent this, AirWatch has an API to disable the power off button on SAFE devices; For non-SAFE devices admins can use the following Custom XML profile. To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="DismissSafeRebootDialog"
value="True"/></characteristic>
```

When users press and hold the power button, the power dialog displays. To dismiss this dialog, use the following custom XML - the dialog is dismissed after a one second delay. To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="DismissPowerOffDialog"
value="True"/></characteristic>
```

Selective App Cache Clearing

Available with Workspace ONE Launcher 3.3+

The Workspace ONE UEM console setting labeled "Clear App data on logout" will clear the data of all the assigned allowed application after logging out. Admins can provide a set of applications for which the data should not be cleared between check-in/check-out by using the following XML:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="DonotClearAppDataSet"
          value="com.airwatch.browser,com.android.testapplication"/></characteristic>
```

For each package ID included in the data set, the App Cache will not be cleared on check-in/ check-out.

Restrict Folder Renaming

Available with Workspace ONE Launcher 3.3+

By default, AirWatch Launcher allows end users to rename folders as a part of the customization options. Administrators can now disable folder renaming. To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
          uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec"><parm name="DisableFolderRename"
value="True"/></characteristic>
```

Usage Access

Available with Workspace ONE Launcher 3.2+

Sent from the console to allow the user to navigate to Usage access settings.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="UsageAccess"
        value="True"/>
</characteristic>
```

Floating Button Timeout

Available with Workspace ONE Launcher 3.2+

Used to set the timeout value of the Floating Button in Single App Mode. Should be an integer only. If this is not sent from the Console, Launcher uses a default value of 10 seconds.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="FloatingTimeoutValue"
        value="15"/>
</characteristic>
```

Fix Floating Button Position

Available with Workspace ONE Launcher 3.2+

When enabled, the user will not be able to move the floating action button. It will be positioned at right end corner.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="FixSettingsPosition"
        value="True"/>
</characteristic>
```

Dynamic Whitelisting of Settings

Available with Workspace ONE Launcher 3.2+

This setting allows you to assign an allowlist of certain native setting which may not have been included in Launcher settings or it can be a native setting screen specific to OEM.

Details needed to allow a setting:

- `SettingName` to be displayed on Launcher settings screen.
- `Packagename` and `classname` or `Action name` of that particular native setting to launch.

If only Action is used:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CustomSettings"
        value="{&amp;quot;CustomSettings&amp;quot;: [
{&amp;quot;name&amp;quot;: &amp;quot;Location
        Settings&amp;quot;,&amp;quot;action&amp;quot;:
        &amp;quot;android.settings.LOCATION_SOURCE_SETTINGS&amp;quot;}
]}"/></characteristic>
```

If packageName and class name is used:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CustomSettings"
        value="{&amp;quot;CustomSettings&amp;quot;: [
{&amp;quot;name&amp;quot;: &amp;quot;Manage Applications
```

```
        Settings&quot;,&quot;pName&quot;: &quot;com.android.settings&quot;,&quot;cName&quot;:
        &quot;android.settings.MANAGE_APPLICATIONS_SETTINGS&quot;}
]}"/>
</characteristic>
```

For additional information, please see the Android Developer Settings page.

Launcher Branding

Available with Workspace ONE Launcher 3.2+

Provides a proper combination of Action Bar color and Status Bar color (Light and dark) as recommended by Google. You may set different colors according to you company's brand colors .

Auto Branding: If you do not want to specify individual colors you can use this flag. In order for this to work, title bar icon (logo) must be present.The extracted colors for branding are from the company logo.

To enable and implement this feature the below flag must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="eadfebd8-7f4c-4837-b9dd-dfcf31bd84e6">
<parm name="AllowAutoBranding"
        value="true" />
</characteristic>
```

To personalize, then you can specify the title bar color, title text color, primary accent color, status bar color, and highlight color. Colors must be specified in hexadecimal color format:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="eadfebd8-7f4c-4837-b9dd-dfcf31bd84e6"><parm name="AllowBranding"
        value="
{&quot;titleColor&quot;:&quot;#FC002E&quot;,&quot;titleTextColor&quot;:

&quot;#F377F7&quot;,&quot;accentColor&quot;:&quot;#36E712&quot;,&quot;highlightColor&quot;:&qu
ot;#4E993E&quot;,&quot;statusBarColor&quot;:&quot;#FC002E&quot;}"/>
</characteristic>
```

Dynamic Whitelisting of Activities

Available with Workspace ONE Launcher 3.2+

To allow a particular activity , specify a list of activities with package names in the below flag. These activities will not be visible on the Launcher settings screen.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CustomActivities"
        value="{&quot;CustomActivities&quot;: [
{&quot;pName&quot;:
        &quot;com.example.demoapplication&quot;,&quot;cName&quot;:
```

```
        &amp;quot;com.example.demoapplication.MainActivity&amp;quot;},
{&amp;quot;pName&amp;quot;:
        &amp;quot;com.example.demoapplication&amp;quot;,&amp;quot;cName&amp;quot;:
        &amp;quot;com.example.demoapplication.Main2Activity&amp;quot;}
]}"/>
</characteristic>
```

Remove Welcome Screen

Available with Workspace ONE Launcher 3.2+

Currently, Launcher displays a welcome screen when it is pushed to the device. This can be removed by clicking the “Dismiss” (Cancel) button on the right lower corner. The below flag can be used to remove the Welcome screen.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="RemoveWelcomeScreen"
        value="True"/>
</characteristic>
```

Clear Application Data

Available with Workspace ONE Launcher 3.2+

Basically, in multi-user mode with checkin/checkout and Launcher, a user's data is cached/saved even after that user checks the device in.

Using OEM APIs that support it, Launcher will call Agent SDK API to clear the application data for all application that Launcher has allowed for a specific user if we use the below flag.

Workspace ONE does not clear application data for Anchor applications (Agent, Launcher, OEM Services).

To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="ClearAppData"
        value="True"/>
</characteristic>
```

Inactivity Timer

Available with Workspace ONE Launcher 3.2+

Specify an amount of time in which the device will automatically lock the Launcher screen and require the previously signed in user to re-enter their password to re-access the Launcher screen. In addition, if there is a user that has currently locked the Launcher screen, there needs to be a mechanism/option to force sign out the user and return the Launcher to the initial login screen where a different/new user can then log into that device. Note, this feature is not compatible with Workspace ONE Access.

To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="InActivityLock"
        value="True"/>
</characteristic>
```

If admin wants to specify the timeout value he can do so using the below flag . It must be an integer.The timeout value is in minutes.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="InActivityLock"
        value="True"/>
<parm name="InActivityTimeout"
        value="10"/>
</characteristic>
```

Hot Swap Profile Caching:

Available with Workspace ONE Launcher 3.2+

As check in/check out is done frequently, users often check out the same device but have to wait for a considerable amount of time for the profile to get applied after checking out. Workspace ONE can expedite this by caching profile per user when the user checks out that particular device for the first time.

To enable and implement this feature, the setting must be pushed down through the custom settings payload:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CacheProfile"
        value="True"/>
</characteristic>
```

Allow WebView inside Launcher:

Available with Workspace ONE Launcher 3.2+

Disable the WebView that is built into Workspace ONELauncher. If there is no Browser installed on the device, web clips will not open. WebView will be `disabled` by default if admins want it enabled then they can do so by using the below flag:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="AllowBuiltInBrowser"
        value="True"/>
</characteristic>
```

Notification Access in Launcher:

Available with Workspace ONE Launcher 3.2+

Workspace ONE Launcher is capable of catching and displaying notifications to devices, but you need to enter the Admin mode on the device through password and enable it. End users cannot do it themselves. This flag will prompt end users to enable notifications while configuring Launcher.

For Phone:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="AllowNotificationPermission"
        value="True"/>
</characteristic>
```

For tablets, you will need to use another flag in conjunction with the above flag, because in some tablets the notification settings can be opened in fragmented view. If 'canLaunchNativeSettings' is already used then there is no need for this flag:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="AllowNotificationPermission"
        value="True"/>
<parm name="ForceTabletNotificationPermission"
        value="True"/>
</characteristic>
```

or

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="AllowNotificationPermission"
        value="True"/>
<parm name="CanLaunchNativeSettings"
        value="True"/>
</characteristic>
```

Dynamically add shortcuts to Launcher screen:

Available with Workspace ONE Launcher 3.2+

Similar to adding of a setting to Launcher settings, you can add a shortcut to Launcher home screen by using the below flag by mentioning "shortcut name, package name, activity name" or "shortcut name, action name".

```
<characteristic type="com.airwatch.android.kiosk.settings" uuid="568bc89d-1df8-4ce9-a041-
e5a24acdb7ec">
<parm name="CustomShortcuts" value="{&quot;CustomShortcuts&quot;:
[{&quot;name&quot;:&quot; Manage Applications
Settings&quot;,&quot;pName&quot;:&quot;com.android.settings&quot;,&quot;cName&quot;:
&quot;com.android.settings.Settings$DateTimeSettingsActivity&quot;},
```

```
{&quot;name&quot;: &quot;Locale Settings&quot;,&quot;pName&quot;:
&quot;com.android.settings&quot;,&quot;cName&quot;:
&quot;com.android.settings.Settings$LocalePickerActivity&quot;}]}"/>
</characteristic>
```

Open Native settings in tablets:

Available with Workspace ONE Launcher 3.2+

In some of the tablets, native settings such as Wi-Fi, Bluetooth, Language etc. are opened in a fragmented view which allows users to access other settings as well, in such a case user can easily get out of launcher. So, by default, Launcher does not allow users to open settings unless they use the below flag. If the admin thinks that it is safe to open native settings in that particular tablet then he can use this flag and all the native settings which are allowed can be accessed. This is usually used along with dynamically allowed list settings flag (CustomSettings), custom shortcuts, custom activities and for notification access.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CanLaunchNativeSettings"
        value="True"/>
</characteristic>
```

If you on want a particular native setting to be accessed and not other settings, use the flag: `forceLaunch`. This flag is used individually with each setting. If admin uses the flag: `canLaunchNativeSettings`,then all the allowed native settings can be accessed. If you want a particular setting, use the `forceLaunch flag`. This is usually used along with dynamically allow list setting flag(CustomSettings), custom shortcuts, custom activities and for notification access.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CustomShortcuts"
        value="{&quot;CustomShortcuts&quot;: [
{&quot;name&quot;: &quot;Manage Applications
        Settings&quot;,&quot;forceLaunch&quot;: &quot;true&quot;,&quot;pName&quot;:
        &quot;com.android.settings&quot;,&quot;cName&quot;:
        &quot;com.android.settings.Settings$DateTimeSettingsActivity&quot;},
{&quot;name&quot;:
        &quot;Locale Settings&quot;,&quot;pName&quot;:
        &quot;com.android.settings&quot;,&quot;cName&quot;:
        &quot;com.android.settings.Settings$LocalePickerActivity&quot;}
]}"/></characteristic>
```

In the above XML (Customshortcuts) both Manage Applications and Locale Settings shortcuts will be visible on the Launcher screen, but users can only access Manage Application settings since it uses the `forceLaunch flag`.

The flags`forceLaunch` or `canLaunchNativeSettings` must be present for custom settings to be visible on Launcher settings screen.

Clear Application Defaults

Available with Workspace ONE Launcher 3.2+

If there is no default set, then Android presents a dialog with all the applications which support that particular format. If a user chooses an application as the default application for any file, then that file is always opened in the same application until the user clears the default manually. Since there is no access to native settings inside Launcher, the user cannot clear the defaults.

The Clear Application defaults commands displays the Clear Application Default in Launcher Settings. All commonly used application types (PDF, Excel, Browsers, Images etc.) will be listed where users can clear defaults. The API to clear application defaults may not work on some OEMs, so Workspace ONE has made this as a configurable setting.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="AllowClearAppDefaults"
        value="True"/>
</characteristic>
```

In some devices, Workspace ONE cannot clear application defaults automatically. For these devices you can send the below flag in which case when the user tries to clear default, they are navigated to application details settings screen where they can do it manually.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CannotClearAppDefaults"
        value="True"/>
</characteristic>
```

Cannot Clear Home Defaults (in some devices)

Available with Workspace ONE Launcher 3.2+

In some devices it is not possible to clear home defaults. For those devices, use the following flag to present the user with a clear default screen from which they can navigate to the native settings and clear the defaults manually:

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="CannotClearDefaults"
        value="True"/>
</characteristic>
```

Boot Up Launchers

Available with Workspace ONE Launcher 3.2+

There are some boot up application which run after the device is restarted. These boot up applications are getting allowed even though they are not allowed on the UEM console. Workspace ONE maintains a list of allowed applications in the Launcher profile, but after reboot Workspace ONE Launcher takes some time to load this profile.

To prevent the application from being allowed, you can provide the package name of all the boot up application which are to be allowed.

```
<characteristic type="com.airwatch.android.kiosk.settings"
        uuid="568bc89d-1df8-4ce9-a041-e5a24acdb7ec">
<parm name="BootupLauncher"
        value="com.sonyericsson.initialbootsetup, com.sonyericsson.setupwizard,
        com.honeywell.systemtools.autoinstall/>
</characteristic>
```

Allow Status Bar

Available with Workspace ONE Launcher 3.2+

This feature provides the administrator with the ability to enable or disable the status bar on the device.

```
<characteristic type="com.airwatch.android.androidwork.launcher" uuid="568bc89d-1df8-4ce9-
a041-e5a24acdb7ec">
<parm name="AllowStatusBar" value="True"/>
</characteristic>
```

Configure Launcher Version Settings

Determine which version of Workspace ONE Launcher is pushed to devices with the Launcher Version setting.

Procedure

1 Navigate to **Devices > Device Settings > Android > Service Applications**.

2 Configure the applicable settings.

Setting	Description
Always use the Latest Version of Workspace ONE Launcher	If this setting is enabled, the latest version of the app automatically pushes to devices when it becomes available. Once this setting is enabled, it applies across all devices you have enrolled into Workspace ONE UEM using Launcher.
Workspace ONE Launcher Version	If this setting is enabled, manually choose the version you want to deploy from the drop-down menu. Select **Upload** to add a new Launcher version to be seeded into the environment. Once uploaded, the Workspace ONE Launcher APK shows in the dropdown so you can select it immediately. **Note** Only upgrade across one version at a time as updating many versions at a time can cause issues.

3 Select **Save**.

Workspace ONE Launcher Status

The Device Details page in the console displays the status of Workspace ONE Launcher on a device which helps you quickly and easily view and check the Launcher status on multiple devices.

When the Workspace ONE Launcher is pushed to devices under a standard Android deployment, the Launcher is set as the default with no additional steps required from the user. For Android (Legacy), most OEMs will push the Launcher automatically with the help of the signed service such as the Platform OEM Service (POEM.

The Launcher status only displays when the following criteria is met:

- User is multi-user staging user
- Launcher payload is assigned to the device through Profiles or Products.

The status will show as follows:

Table 2-1. Workspace ONE Launcher Status Descriptions

Status	Description
Launcher is the Home App	Workspace ONE LauncherWorkspace ONE Launcher is set at the default launcher for the devices.
Launcher is not set as the home app or is not installed	This status indicates the profile push failed, did not install, or is not set as the default launcher on the selected device. If Launcher fails, you can check the network requirements for CDN to make sure it is up to date.

Layout Settings

Layout lets you control design elements such as icon grid and orientation preference, as well as upload images to customize the Launcher with your unique brand look and feel. The available settings depends on the mode.

Table 2-2. Layout Settings Descriptions

Setting	Description
Manufacturer	Select from Generic, Samsung, or Nexus as the device types. Available on Multi App and Template Mode.
Model	Select whether the Launcher profile is being pushed to a phone or to a tablet. Available on Multi App and Template Mode.
Orientation	Allows you to select the preview of the Workspace ONE LauncherWorkspace ONE Launcher in **Portrait** or **Landscape** view for all app modes. The Preview window adjusts according to selection depending on the app mode. Caution If you change the orientation while configuring Template mode, all settings are lost and you have to start your configuration over.
Lock	Enable this text box to lock the device into a single orientation.

Table 2-2. Layout Settings Descriptions (continued)

Setting	Description
Grid	Select the grid size from the drop-down menu to specify how the icons appear with the specified numbers of grid rows and columns. Select Hide to remove the grid lines on the canvas. Available on Multi App mode only. You can select **Hide** to hide the gridlines in the layout.
Minimize Title Bar	Select to hide the title bar on the user's device.The user van still swipe down on the screen to access the title bar and additional settings.
Add Row for Pinned Apps	Select to create a bottom bar in the launcher configuration to pin application icons that will remain visible on every screen. **Multi App mode only.**
Title Bar Icon	Upload a customized icon to appear in the title bar. Available on Multi App Mode only.
Wallpaper	Upload a custom wallpaper to display in the background of the Launcher setup. Available on Multi App mode only.

Apps for Workspace ONE Launcher

Workspace ONE UEM classifies applications as internal, public, and miscellaneous and you upload applications depending on the type.

Public and internal apps are pulled from your managed apps list from Apps & Books menu in the Workspace ONE UEM console. These apps are not whitelisted through Miscellaneous apps. Miscellaneous apps are only used for native device apps. You will need the **Application Name** and **Application ID** to whitelist miscellaneous apps.

Note When deploying Workspace ONE Launcher with Android for Work, make sure apps are approved for Android. For more information on approving apps for Android for Work, see Approve Applications for Android

Approve Applications for Android

Approve applications for integration so that you can upload them to the Workspace ONE UEM console.

Procedure

1. Navigate to Google Play for Work, https://play.google.com/work.
2. Login to the site using an Enterprise account for Google Play for Work.
3. Search for applications you want to add to the integration and select the **Approve** option.
4. View the permissions for the applications and follow the prompts to confirm approval. Check to make sure the application has been imported after approval.

Bookmarks for Workspace ONE Launcher

Bookmarks provide users a simple way to access a URL directly from the Workspace ONE Launcher home screen. The end-user sees the bookmark icon and title similar to any other app on the Launcher home screen. When a user taps on a bookmark icon, Launcher navigates to the specified URL.

In addition to navigating to any webpage, you can use these icons to connect to internal content repositories or login screens without having to open a browser and type out a long URL.

Adding bookmarks differ based on the enrollment method of your device fleet.

How to Add Bookmarks for Android

You can add bookmarks for through **Web Links** in the UEM console. To add bookmarks:

1 Navigate to **Resources > Apps > Native > Public > Add Application** and select **Android** from the **Platform** field.

2 Select **Next**. The Google Play store appears.

3 Once the Google Play store opens, add a web app by using the plus sign in the bottom right.

4 Complete the app details, select **Next**, then click on the icon for the web app you just created.

5 Assign the web app as you would any other native application.

6 To add it to the Launcher screen, navigate to the **Native** tab in the Launcher configuration screen and drag this icon to the home screen.

Note The native web app is only accessible through Google Chrome so be sure to add Google Chrome to the home screen or as a hidden app.

Canvas Settings for Workspace ONE Launcher

Use the **Canvas** tab to organize the Launcher layout by adding apps, creating folders, and determining the position of apps on the Launcher.

Table 2-3. Canvas Settings Descriptions

Setting	Description
Title Bar	Customize the title bar within the Launcher to support device-specific or user-specific names.
Remove	Remove apps or folders from the profile if they are no longer needed in the mode. Select the app then select the **Remove** button. You can also drag apps outside of the canvas area and they will be added back to the Apps section.
App Attributes	Display the properties of the selected app. To edit the properties, see App Attributes for Workspace ONE Launcher.
Create Folder	Group apps together in a folder for further organization.

Table 2-3. Canvas Settings Descriptions (continued)

Setting	Description
Layout	Click to configure Launcher layout design elements such as icon grid and orientation preference. The available layout options can be found in Layout Settings.
Settings	Click to configure Launcher settings such as device settings and utilities to be allowed and the admin passcode to control exit from Launcher.

App Attributes for Workspace ONE Launcher

App Attributesallows you to view the properties of the selected app once it is added to the Preview window. You can view default values for public apps, internal apps, and bookmarks, and edit values for miscellaneous apps.

Table 2-4. App Attributes Settings Descriptions

Settings	Description
Application Name	Enter the name of the application displayed to the user. For a public or internal app, the application name is static and is pulled from the Application name present in Apps and Books. For Miscellaneous apps, the name is editable and the app on the device will show the name that is entered in this field.
Application ID	Enter the unique identifier for a given Android application. The format is com.<app details>.For example, for Workspace ONE Launcher: com.airwatch.lockdown.launcher. For a public or internal app, the application name is static and is pulled from the Application name present in Apps and Books. For Miscellaneous apps, the name is editable and changing the app ID directly affects whether the app would be whitelisted on the Launcher, meaning if it is wrong, the app will not show. For Miscellaneous apps, add a wildcard * character to create a rule for dynamic rule for automatic whitelisting. This will automatically add all the whitelisted apps for this App ID package without having to repush the Launcher profile everytime a new app is added. If there are multiple apps with the same Application ID (say through Miscellaneous apps), this will cause a conflict on the device side. Instead, if one of the apps with the given Application ID is added to the canvas screen, all the other apps carrying that same Application ID should be greyed out.
Launch App on Start Up	Enable to force an app to automatically start on Launcher start up or reboot. If your Launcher profile has more than one app, you can only set this field for one app.
Allow Certain Sub Packages	Allows you to whitelist certain apps that install alongside a main application. You cannot add sub packages within Hidden apps. By default, all sub packages should be whitelisted.
Sub Package Name	Create a whitelist that prevents the installation of all subpackages. For example, only whitelisting the **Sub Package Name** for AirWatch Calendar, this whitelist prevents the installation of AirWatch Contacts.

Hidden Apps

Hidden apps are apps that are not directly accessible to the user from the Workspace ONE Launcher home screen, but can be invoked by another application.

When a user selects a link inside a main app, if the app needed for that content has not been whitelisted they will see an error message. For example, if you have an app configured in the Workspace ONE Launcher profile that has a web link that will direct users to the browser, you have to whitelist the browser as a hidden app. The browser will not show up in the Workspace ONE Launcher profile on the device but will direct users specifically to the content needed. You can view App Attributes for Hidden Apps but the details cannot be edited.

Add Hidden Apps

Hidden apps are apps that have been whitelisted in the Workspace ONE UEM console to allow users to access resources outside a specified app. You will add Hidden apps after you have walked through the setup for either app mode.

Procedure

1. Select **Hidden App** tab.
2. Drag and drop apps to add them to the canvas. You can also select the desired app and select **Add To Launcher**.
3. Select the app and hit **Remove**to remove any apps you do not need.

Alerts

View **Alerts** to fix issues before pushing your configured Launcher mode to devices.

Alerts are viewed in the **Preview** section of the launcher window. The alerts icon displays the number of errors in red. You will not be alerted for warnings. Click the icon to view all alerts. You cannot save the mode until the errors are resolved.

Note Alerts will only display while configuring Template Mode.

Two types of alerts will display:

Table 2-5. Alert Descriptions

Alert Type	Description
Warnings	Alerts you if two elements are overlapping.
Errors	Alerts you if you are missing primary properties in the element. For example, missing text for the text element will result in an alert.

Template Mode Settings

Template Mode is the fully customizable mode of Workspace ONE Launcher. You can add apps, images, text, and other layout settings to customize a device locked down in kiosk mode with Template Mode. Common use cases are hospital waiting rooms, cabs, restaurants, and filing forms.

Table 2-6. Template Mode Settings - Basic Properties

Setting	Description
Size	Drag the borders of the widget to adjust size of the icon.
Position	Move the widget around the canvas to adjust the placement on the template.

Table 2-7. Template Mode Settings - App Selection

Setting	Description
Filter App List	Search for **Public**, **Internal**, or **Miscellaneous** apps to add to the Launcher profile. ■ For **Public** and **Internal** apps: Select the desired apps that appear in the filtered list. These apps are pulled from your managed apps list from **Apps & Books** menu in the Workspace ONE UEM console . The **Public** and **Internal** apps are not whitelisted through **Miscellaneous** apps. **Miscellaneous** apps are only used for native device apps. ■ To add **Miscellaneous** apps: Select **Add an App** and enter the **Application Name** and **Application ID** under the Miscellaneous option. Select the app to add it to the Launcher preview.

Table 2-8. Template Mode Settings - Text Properties

Setting	Description
Text	Enter the text display. The default text displays as Label View.
Text Color	Change the text color by selecting the color icons and selecting the desired color.
Background Color	Change the background color by selecting the color icon and selecting the desired color.
Text Position	Align the text in the desired area by selecting the circle from the box.
Font Weight	Select **Bold** or **Normal**.
Underline	Select **Yes** or **No** to underline the text.
Font Style	Select **Normal** or **Italic**.
Font Size	Move the bar to determine the size of the text.

Table 2-9. Template Mode Settings - Background Properties

Setting	Description
Background Image	Select **Upload** to load an image file from your desktop.
Background Image Size	Select **Fit To Wrapper**, **Keep Original**, or **Keep Aspect Ratio**.
Aspect Ratio Size	Move the bar to determine the aspect ratio. This option only applies if you have selected to **Keep Aspect Ratio** from the **Background Image Size** field.
Background Image Position	Align the app in the desired area by selecting the circle from the box.

Table 2-10. Template Mode Settings - App Icon Properties

Setting	Description
App Image Size	Select **Fit To Wrapper**, **Keep Original**, or **Keep Aspect Ratio**.
App Aspect Ratio	Move the bar to determine the aspect ratio. This option only applies if you have selected to **Keep Aspect Ratio** from the **App Icon Size** field.
App Icon Position	Align the app in the desired area by selecting the circle from the box.

Settings for Workspace ONE Launcher

The available settings for the Workspace ONE Launcher profile varies depending on if you are opted into Android using EMM Registration or using Android (Legacy).

For deploying Workspace ONE Launcheras a Work Managed device, see Device Settings Matrix for Android Deployment Launcher Device Settings Matrix for Android Deployment. To useWorkspace ONE Launcher for Android (Legacy) deployment, see Launcher Device Settings Matrix for Android (Legacy) Deployment.

Table 2-11. Workspace ONE Launcher Profile Settings - Administrative Passcode

Setting	Description
Administrative Passcode	Set a passcode to allow authorized users to perform admin tasks on the device. This passcode is provided only to authorized users. The profile cannot be saved unless an administrative passcode is entered. If someone is trying to exit the launcher and enters the Administrative Passcode incorrectly, the option disappears after 10 unsuccessful attempts, you can restart the device and the option reappears.
Persist Admin Passcode If Launcher Profile Is Removed From Device	Require the passcode to be entered if the Launcher profile has been removed from the device.

Table 2-12. Workspace ONE Launcher Profile Settings - Icon Settings

Setting	Description
Prevent Icon Rearranging	Enable to disable users from moving icons around on the Launcher screen from the device.
Icon Size	Select as Small, Medium, or Large to determine how an icon appears on the display.

Table 2-13. Workspace ONE Launcher Profile Settings - Device Preferences

Setting	Description
App Icons	Allow app icons on the device home screen.
Settings	Allow device network and other granular settings to be enabled.
Utilities	Allow devices management settings to be enabled.
Hardware Keys	Enable or disable hardware keys on the device.
Quick Launch Icons	Allow shortcut icons on the device home screen.

Administrative Passcode

The administrative passcode allows users to access the device menu to add applications or to exit from the Workspace ONE Launcher mode. The passcode is required to perform all actions in **Admin Mode** from the device.

The **Preference** tab from each app mode allows you to establish the passcode. The **Persist Admin Passcode If Kiosk Profile is Removed From Device** check box prompts the user for the admin passcode if they are attempting to remove the Launcher profile from their device.

If someone tries to use the Exit Launcher setting from the device and enters the Administrative Passcode incorrectly, the option disappears after 10 unsuccessful attempts, you can restart the device and the option reappears.

There are two use cases for this option:

- **Remove Profile** – Removes the Workspace ONE Launcher profile from the device. This option restricts users from using any launcher apps and the device will be locked down and display a standard screen saver
- **Check In/Check Out** – Displays the **Check Out** credentials page when a user checks in a device after use. The user can access device side functions but not Launcher apps or settings.

Launcher Device Settings Matrix for Android Deployment

The **Settings** section of each VMWare Launcher allows you to set an administrative passcode, establish icon settings, and enable/disable various functions of the Launcher profile for Android

device owner deployment. Available preferences vary based on the selected mode you are configuring.

The following matrix compares the Launcher device capabilities across the different app modes. Some settings are dependent on additional factors such as permissions and COSU mode limitations and are denoted as such.

Key:

- Usage Access: Requires Usage Access permission.
- COSU mode: COSU setup removes certain features for security to prevent users escaping out of Lock mode.

Note Usage Access permission is only required on non-Samsung devices. Usage Access permission for Samsung devices is a native feature requiring no prompt on the following devices:

- Samsung SAFE MDM 5.4
- For Android (Legacy) Work Profile - Launcher 3.0 and Workspace ONE Intelligent Hub 7.1 is required.
- For Android Work Managed devices - Launcher 3.0 and Workspace ONE Intelligent Hub 9.0.1 is required.

Table 2-14. Supported Device Settings for Android

Category	Preference	Single App	Multi App	Template Mode
App Icons	Allow Hub Icon on Home Screen		✓	
App Icons	Allow Phone Icon		✓	
App Icons	Allow Contacts Icon		✓	
Settings	Display Setting	✓	✓	✓
Settings	Sound Setting	✓	✓	✓
Settings	Screen Lock (Usage Access)	✓	✓	✓
Settings	Language Setting (Usage Access)	✓	✓	✓
Settings	Bluetooth Setting (Usage Access)	✓	✓	✓
Settings	Wi-Fi Settings (Usage Access)	✓	✓	✓
Settings	Security settings (Usage Access)	✓	✓	✓
Settings	Application Setting	✓	✓	✓
Settings	Allow Tethering Setting (Usage Access)	✓	✓	✓
Settings	Allow GPS Setting (Usage Access)	✓	✓	✓
Utilities	Allow Widgets		✓	

Table 2-14. Supported Device Settings for Android (continued)

Category	Preference	Single App	Multi App	Template Mode
Utilities	Allow Keyguard (Android 9.0+)	✓	✓	✓
Utilities	Allow Home Button (Android 9.0+)	✓		
Utilities	Allow App Manager (Android 6.0 and Android 6.0.1)	✓	✓	✓
Utilities	Allow Task List (COSU)	✓	✓	✓
Utilities	Allow Bar (COSU)	✓	✓	✓
Utilities	Allow Airplane Mode	✓	✓	✓
Utilities	Allow Stay Awake	✓	✓	✓
Quick Launch Icons	Bluetooth	✓	✓	✓
Quick Launch Icons	Wi-Fi	✓	✓	✓

Launcher Device Settings Matrix for Android (Legacy) Deployment

The **Settings** section of each Workspace ONE Launcher allows you to set an administrative passcode, establish icon settings, and enable/disable various functions of the Launcher profile. Available preferences vary based on the selected mode you are configuring.

The following matrix compares the Workspace ONE LauncherWorkspace ONE Launcher capabilities across the different app modes. To see available setting for Workspace ONE LauncherWorkspace ONE Launcher using COSU Mode, seeLauncher Device Settings Matrix for Android Deployment.

Table 2-15. Key

✓	Supported
✓*	Android 4.4 and below devices only

Table 2-16. Supported Device Settings for Android (Legacy)

Category	Preference	Single App	Multi App	Template Mode
App Icons	Allow Hub Icon on Home Screen		✓	
App Icons	Allow Phone Icon		✓	
App Icons	Allow Contacts Icon		✓	
Settings	Display Setting	✓	✓	✓
Settings	Sound Setting	✓	✓	✓
Settings	Screen Lock	✓*	✓	✓

Table 2-16. Supported Device Settings for Android (Legacy) (continued)

Category	Preference	Single App	Multi App	Template Mode
Settings	Language Setting	✓*	✓	✓
Settings	Bluetooth Setting	✓*	✓	✓
Settings	Wi-Fi Settings	✓	✓	✓
Settings	Security settings	✓*	✓	✓
Settings	Application Setting	✓	✓	✓
Settings	Allow Cellular Data Setting (Android 4.4 and Below)	✓*	✓	✓
Settings	Allow Tethering Setting	✓*	✓	✓
Settings	Allow GPS Setting	✓	✓	✓
Utilities	Allow Widgets		✓	
Utilities	Allow App Manager	✓	✓	✓
Utilities	Allow Recent Task List	✓*	✓	✓
Utilities	Allow Status Bar (Safe v3.0+)	✓	✓	✓
Utilities	Allow Notification Bar	✓	✓	✓
Utilities	Allow Navigation Bar (Safe v3.0+)	✓		✓
Utilities	Allow Mini Launcher Bar (Safe v3.0+)	✓	✓	✓
Utilities	Allow Airplane Mode (Android 4.1 and below Safe v5+)	✓	✓	✓
Utilities	Allow Stay Awake	✓	✓	✓
Hardware Keys	Allow Home Button (Safe v3.0+)	✓	✓	✓
Hardware Keys	Allow Back Button (Safe v3.0+)	✓	✓	✓
Hardware Keys	Allow Options Button (Safe v3.0+)	✓	✓	✓
Hardware Keys	Allow Volume Up Button (Safe v3.0+)	✓	✓	✓
Hardware Keys	Allow Volume Down Button (Safe v3.0+)	✓	✓	✓
Quick Launch Icons	Allow GPS (Safe v3.0+)	✓	✓	✓
Quick Launch Icons	Bluetooth	✓	✓	✓
Quick Launch Icons	Wi-Fi	✓	✓	✓
Quick Launch Icons	Cellular Data (Android 4.4 and below)	✓*	✓	✓

Shared Devices

3

Shared Device/Multi-User Device functionality in Workspace ONE UEM powered by AirWatch ensures that security and authentication are in place for every unique end user. Shared devices can also allow only specific end users to access sensitive information.

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE UEM powered by AirWatch lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users.

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, Workspace ONE UEM uses a simple login or log-out process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end-user role determines their level of access to corporate resources such as content, features, and applications. This role ensures the automatic configuration of features and resources that are available after the user logs in.

The login or log-out functions are self-contained within the Workspace ONE Intelligent Hub. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

Shared Device capabilities are also possible natively on Apple iPads integrated with Apple Business Manager. This functionality called Shared iPads for Business leverages the user's Managed Apple ID for login and does not take place in the Workspace ONE Intelligent Hub for login and logout. To know more about configuring Shared iPads for Business with Apple Business Manager and steps to achieve this functionality, see **Shared iPads for Business** in *Introduction to Apple Business Manager Guide* available on docs.vmware.com.

Shared Devices Capabilities

There are basic capabilities surrounding the functionality and security of devices that are shared across multiple users. These capabilities offer compelling reasons to consider shared devices as a cost-effective solution to making the most of enterprise mobility.

Functionality

- Personalize each end-user experience without losing corporate settings.

- Logging in a device configures it with corporate access and specific settings, applications, and content based on the end-user role and organization group (OG).
- Allow for a log in/log out process that is self-contained in the Workspace ONE Intelligent Hub or Workspace ONE Access.
- After the end user logs out of the device, the configuration settings of that session are wiped. The device is then ready for login by another end user.

Security

- Provision devices with the shared device settings before providing devices to end users.
- Log in and log out devices without affecting an enrollment in Workspace ONE UEM.
- Authenticate end users during a login with directory services or dedicated Workspace ONE UEM credentials.
- Authenticate end users using Workspace ONE Access.
- Manage devices even when a device is not logged in.

Platforms That Support Shared Devices

The following devices support shared device/multi-user device functionality.

- Android 4.3 or later
- iOS devices with Workspace ONE Intelligent Hub 4.2 or later.
  - For details about logging in and out of shared iOS devices, see the topic *Log In and Log Out of Shared iOS Devices* in the **iOS Platform Guide**, available on docs.vmware.com.
- MacOS devices with Workspace ONE Intelligent Hub 2.1 or later.

This chapter includes the following topics:

Define the Shared Device Hierarchy

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

Procedure

1 Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**.

Here, you can see an OG representing your company.

2 Ensure the **Organization Group Details** displayed are accurate, and then use the available settings to make modifications, if necessary. If you make changes, select **Save**.

3 Select **Add Child Organization Group**.

4 Enter the following information for the first OG underneath the top-level OG.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG. Ensure that users sharing devices receive the **Group ID** as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when **Type** is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

5 Select **Save**.

Configure Shared Devices

Similar to single-user device staging, multi-user staging (a "shared device") allows an IT administrator to provision devices to be used by more than one user.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Shared Device**.

2 Select **Override** and complete the **Grouping** section.

Setting	Description
Group Assignment Mode	Configure devices in one of three ways: ■ Select **Prompt User for Organization Group** to have the end user enter a Group ID for an organization group upon login. With this method, you have the flexibility to provide access to the settings, applications, and content of the organization group entered. Using this approach, an end user is not restricted to accessing only the settings, applications, and content for the organization group to which they are enrolled. ■ Select **Fixed Organization Group** to limit your managed devices to settings and content applicable to a single organization group. Each end user who logs in to a device has access to the same settings, applications, and content. This method can be beneficial in a retail use case where employees use shared devices for similar purposes such as checking inventory. ■ Select **User Group Organization Group** to enable features based on both user groups and organization groups across your hierarchy. When an end user logs in to a device, they have access to specific settings, applications, and content based on their assigned role within the hierarchy. For example, an end user is a member of the 'Sales' user group, and that user group is mapped to the 'Standard Access' organization group. When that end user logs in to the device, the device is configured with the settings, applications, and content available to the 'Standard Access' organization group. You can map user groups to organization groups on the UEM console. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**. Select the **Grouping** tab and fill in the required details.
Always Prompt for Terms of Use	Prompts the end users to accept your **Terms of Use** agreement before they log in to a device.

3 Complete the **Security** section, as applicable.

Setting	Description
Require Shared Device Passcode	**(For iOS devices only)**Require users to create a Shared Device passcode in the Self-Service Portal to check out devices. This passcode is different from a Single Sign On passcode or a device-level passcode.
Require Special Characters	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.

Setting	Description
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.
Auto Logout	Configure an automatic log out after a specific time period.
Auto Logout After	Set the length of time that must elapse before the **Auto Log out** function activates in **Minutes**, **Hours**, or **Days**.
iOS Single App Mode	Select this check box to configure Single App Mode, which locks the device into a single application when an end user logs in to the device. To check out an iOS device in Single App Mode, end users log in using their credentials. When the device is checked in again, it returns to Single App Mode. Enabling Single App Mode also disables the Home button on the device. **Note** Single App Mode applies only to Supervised iOS devices.

4 Configure the **Logout Settings**, as applicable.

Setting	Description
Clear Android App Data	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Android Apps	Use the drop-down to select whether to Always reinstall app between users or never reinstall app between users. For Android (Legacy) deployments, you can opt to reinstall app if the Hub cannot clear app data between users.
Clear Android Device Passcode	This setting controls whether the current Android device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Allow PIN at Startup	Enable or disable Android Secure Startup, which requires an initial PIN entry to boot up the device. If disabled, users cannot enable Secure Startup during passcode setup. If Secure Startup is already disabled on the device, the device must be factory reset to enable it. This feature applies only to Android devices that do not have file-based encryption.
Clear iOS Device Passcode	This setting controls whether the current iOS device passcode is cleared when the user logs out (checks in) a multi-user shared device.

5 Select **Save**.

What to do next

For specific information about provisioning devices for single-user and multi-user device staging, see the topics Stage a Single-User Device and Stage a Multi-User Device.

Configure Android for Shared Device Use

To use shared device functionality on Android devices, enroll the device using the Workspace ONE Intelligent Hub, set the Workspace ONE Launcher application as the default home screen, and create and assign the Launcher profile. Workspace ONE Launcher is automatically downloaded during enrollment, but you will need to determine which version of the Launcher is pushed to devices.

Procedure

1 Navigate to **Devices > Device Settings > Android > Service Applications**.

2 Configure the applicable settings:

Setting	Description
Always use the Latest Version of Launcher	If this setting is enabled, the latest version of the app automatically pushes to devices when it becomes available.
Launcher Version	Manually choose the version you want to deploy from the drop-down menu.

3 Select **Save**.

4 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android > Launcher** and configure the Launcher profile at each child organization group. This profile should contain all of the necessary settings common to that organization group.

Important Make sure to enable the **Persist Admin Passcode If Launcher Profile Is Removed From Device setting**, as this will ensure that the staging user, as well as the shared device Users are not permitted to exit the Launcher without entering the Administrative Passcode.

Do not assign the Launcher profile to a staging user.

5 Enroll the device into the enrollment organization group using the staging user. The Launcher .apk installs and the login screen appears, by default.

Note The Launcher .apk needs to be installed before the Launcher profile is pushed as a part of the Shared Device settings.

6 Enter the shared device user Group ID, Name, and Password to log in, assigning the device to the Shared Device User and the proper child organization group. The Launcher profile will be applied to the device, and the console will reflect which user is logged in to the device.

Important Only enter the Group ID if you selected **Prompt for Organization Group** in the Group Organization Group assignment mode under the shared device settings.

7 Log out of the Launcher profile on the device. This reassigns the device back to the staging user, moves the device back to the original enrollment organization group, and removes the Launcher profile.

Log In and Log Out of Shared Android Devices

To use shared device functionality on Android devices, enroll the device using the Workspace ONE Intelligent Hub and set the VMware Workspace ONE Launcher as the default home screen. The Workspace ONE Launcher is automatically downloaded during enrollment.

Once the application is installed and set as the default home screen, the device is in a checked-in state. While in this state, the end user is unable to navigate away from this page and the device prompts the user to check out. To remove the profile and make the entire device accessible again, perform an Enterprise Wipe on the staging user device from the Workspace ONE UEM console.

Procedure

1. From the Workspace ONE Launcher log in page, users must enter their Group ID, user name, and password. If **Prompt User for Organization Group** is enabled on the console, end users are required to enter a **Group ID** to log in.
2. Select **Login** and accept the terms of use, if applicable.

   The device is configured. Once logged in, user profiles are pushed down based on the smart group and user group associations.

What to do next

To log out of an Android device, select **Launcher Settings** and select **Log Out** (door icon).

Using Workspace ONE Launcher 4

After successfully configuring and deploying Workspace ONE Launcher to your fleet of devices, the app is now ready to be used in your organization.

Depending on the device, OS being used, and the version of Workspace ONE Launcher, the profile may require the user to grant app permissions and set Workspace ONE UEM as the default launcher. Granting app permissions allows Workspace ONE UEM console to push launcher settings to control the device, and setting Workspace ONE Launcheras the default overrides the native launcher on the device.

Once users have prepared their devices, they can further customize the layout by adding folders and widgets, and other elements. Admin mode allows users to access higher privileges such as creating shortcuts and other settings in preferences.

Admins set preferences that determine the available customization settings on Launcher devices during Workspace ONE Launcher setup. Settings such as: adding a folder, moving an icon, and swapping the position of an icon, folder or widget can be changed by the end user. View the available preferences in Launcher Device Settings Matrix for Android Deployment and Launcher Device Settings Matrix for Android (Legacy) Deployment.

By default, any changes the user makes to the Workspace ONE Launcher set up, as allowed by the admin in the device preferences, remains on the device in the event the Workspace ONE Launcher is reloaded, admin pushes the profile again, or user exits Launcher. If the admin has to re-push the Workspace ONE Launcher profile that includes changes to the preferences, the new profile overrides any changes the user has made only in the case where the configurations conflict. For example, if the user rearranges the icon on the screen and then the admin has disables that feature in the latest version of the profile, the icons revert to the original position. Another example is if the user has moved around the icons as allowed by the admin and then the admin updates the profile so that there is a different icon in one of the positions, the admins icon will be retained at that position.

Device Requirements

The following tables break down the requirements by Workspace ONE Launcher version and Android OS and also breaks down the requirements by Android setup.

Table 4-1. Android Requirements

Launcher Version	Android 5.0 and Below Required Additional End User Steps	Android 6.0 Required Additional End User Steps
Workspace ONE Launcher 2.1+ (SAFE)	No setup required	Grant permission required
Workspace ONE Launcher 2.1+ (Non-SAFE)	Users have to clear the device's native launcher and set AirWatch as default launcher.	Grant permission required Users have to clear s native launcher on the device and set AirWatch as the default launcher.
Launcher 2.0.1 & Below-SAFE	No setup required	Not supported
Launcher 2.0.1 & Below- Non-SAFE	No setup required	Not supported

Table 4-2. Android versus Android (Legacy) Setup

Launcher Version	Android Required Additional End User Steps	Android (Legacy) Required Additional End User Steps
COSU Mode	Required	Not applied
Default Launcher	Automatic	User acceptance required
Notification Access Permission	Configurable	Configurable
Shared Device	Supported	Supported
Usage Access Permission	Configurable	Configurable

Prepare Launcher Devices for Deployment

Once the Workspace ONE Launcher profile is pushed to user devices, users have to grant app permissions which allow the profile to access features on the device and set Workspace ONE Launcher as the default launcher.

1 Wait for the Workspace ONE LauncherWorkspace ONE Launcher profile to be pushed to device and open the Launcher once installed.

2 Tap **Grant** on the "Launcher requires permission" screen.

3 Toggle **Permit Usage access** on. Usage access grants the Workspace ONE LauncherWorkspace ONE Launcher app permission to track what other apps are being used, how often, operator, language settings, and additional details.

4 Navigate to **Settings > Launcher > App Info**.

5 Tap **Clear Defaults** under the "Launch by Default" section.

6 Tap **Workspace ONE Launcher** on the Select a Home app prompt.

Using Launcher in Offline Mode

Offline mode is used when devices are being used in check-in check-out mode and allows users to continue their work even when they are unable to log in as themselves or are in areas where network connectivity is unstable.

This setting is applied to both end-users, the staging user, or an organization group that includes both. Assigning to all users ensures the offline mode profile is present when moving between users.

Use the Configure Workspace ONE Launcher Profile configuration in the Workspace ONE UEM console to enable offline mode. Once a user attempts to log in and server connection is not detected, they will select **Use Offline Mode** to continue using Launcher in offline mode. Any changes made while using offline mode are not saved.

This chapter includes the following topics:

Add Folders

Users can add folders to the Workspace ONE Launcher home screen to organize and structure the app further on their device. Users can use folders to group apps with multiple packages. For example, users can group all social media applications together in one folder.

Procedure

1. Tap the plus sign from the **Options** menu or long press the home button.
2. Tap **Folder**.
3. Enter a **Folder name** and select **OK**. The folder displays on the home screen.
4. Drag desired apps into the folder.

Add Widgets

Users can insert widgets for whitelisted apps on the device inside the Workspace ONE Launcher profile. If the profile is only configured for a set number of pages, users can add more widgets only if there is space available.

Procedure

1. Tap the plus sign from the **Options** menu.
2. Tap **Widget**.
3. Select desired widget from the list.
4. Tap **Create**.

   The selected widget gets added to the home screen.

Results

For non-whitelisted apps, a message displays on the screen notifying the users they cannot add widgets to their home screen.

View Workspace ONE LauncherDetails

The device native status bar is hidden when the Workspace ONE Launcher profile is active on a device hiding details such as battery, time, and Wi-Fi. Users can insert a **Launcher Device Details** widget to the home screen.

In addition to these steps, users can also access the device details on their device through **Settings > Device Details**.

Procedure

1. Tap the plus sign from the **Options** menu or long press the home button.
2. Tap **Add Widget** and select **Device Details** from the list. You can position the widget anywhere on the screen.
3. Tap the **Devices Details** widget to add it to your home screen. The widget shows the battery life, time, Wi-Fi or network connection, and signal strength.
4. Tap the widget to open the full device details page.

View Status Bar

Users cannot view the status bar or Workspace ONE Launcher action bar on their device when devices are locked into Template mode. Users can swipe down the screen to display the status bar.

Procedure

1 Navigate to **Devices > Profiles > List view > Add > Add Profile > Android > Device > Launcher > Configure > Template Mode**.

2 Select **Preferences** and enable **Allow Status Bar** and **Allow Mini Launcher Bar**.

View Notifications

Notifications for different applications display inside Workspace ONE Launcher.

Available notifications display as an alert on the Options menu.

Procedure

1 Tap the alert.

2 View notifications from the Options menu.

3 Open the specified app by tapping the notification.

Ghost Icons

Ghost Icons are placeholder icons for apps that are whitelisted for user but are not installed on the device.

In the Workspace ONE UEM console you may have whitelisted ten applications but only five are installed on the device. Users can see icon placeholders for the apps that are not installed. Depending on the app mode that has been configured, the behavior of the ghost icons vary:

Table 4-3. Ghost Icons Behavior

App Mode	Behavior
Single App Mode	For public applications, users tap the icon and are redirected to the Google Play Store to download the app. For internal application, users tap the icon and are redirected to the AirWatch Catalog too download the app.
Multi App Mode	For public applications, users tap the icon and are directed to the Google Play store to download the app.
On Demand	Ghost icon displays on device until user taps itto start download.
Auto Push	Ghost icon will display on device and app is automatically installed as the Launcher profile is deployed to devices.

Even if the Play Store has not been whitelisted in the Workspace ONE UEM console , it is temporarily whitelisted to allow the users to download the app. Once downloaded, the app appears and is ready for use.

Device Settings

Users can access native device settings from the **Options** menu and adjust them according to their business needs.

Table 4-4. Native Device Settings Descriptions

Setting	Description
Sound	Adjust the volume levels.
Display	Adjust brightness and set sleep timer.
Applications	Uninstall applications.
Wi-Fi	Connect the device to a Wi-Fi network.
Cellular Data*	Enable the use of network data over Wi-Fi.
Bluetooth*	Pair a Bluetooth device.
Location*	Enable GPS services.
Security*	Set device administrator settings.
Language*	Determine the language and input options.
Tethering*	Connect the device as a mobile hotspot.
Screen Lock*	Configure screen lock settings such as a PIN or password.
App Manager	View running applications and use the **Kill app** option to force stop.
Denied Apps	Displays a list of apps the user attempted to open from within an allowed app so admins can choose to allow those apps as needed.
User Information	Displays user information.
About	Shows version information, privacy policy, and legal agreement.
Help	Opens the tutorial for onboarding.
*	These settings are not available while running Workspace ONE Launcheron Android 5.0 devices.

Admin Mode

Admin mode grants privileges that allow users to perform admin tasks from the Workspace ONE Launcher profile on the device without having to exit the launcher. You can also use Admin Mode to enable a feature, troubleshoot a problem, or exit AirWatch app.

This mode is passcode protected, which you can configure in the Preferences section of the app mode. Admin mode is only available for Multi App and Template modes.