

UEM System Administration for Application Developers

Workspace ONE for Android

Android applications can be integrated with the VMware Workspace ONE® platform. Integration work will require access to a Workspace ONE Unified Endpoint Manager console, and the completion of administrative tasks there. Follow the instructions below to set up and administer a Workspace ONE console that supports application development.

This guide only covers tasks necessary to support application development. It doesn't replace the system administrator user guides for the Workspace ONE product.

This document is part of the Workspace ONE Integration Guide for Android set.

Table of Contents

Introduction.....	3
VMware TestDrive service.....	3
Abbreviations and Terms.....	4
Task: Set up a management console.....	5
App Development Support System Administrator Permissions.....	5
How to set up a management console in VMware TestDrive.....	6
Task: Register for Android Enterprise Mobility Management.....	8
Task: Configure management console enrollment.....	13
Introduction to Organization Groups.....	13
Recommended Organization Group Structure.....	14
How to set up the recommended Organization Group structure.....	16
How to log in and select an Organization Group.....	28
Task: Set up the mobile application catalog.....	31
Task: Configure end users.....	33
Recommended End User Configuration.....	34
How to create an end user account.....	35
How to delete an end user account.....	37
Task: Enroll a developer device.....	38
How to find out the enrollment server address.....	39
How to enroll an Android device in Device Owner managed mode.....	40

How to enroll an Android device in Profile Owner managed mode.....	44
How to enroll an Android device in Registered mode.....	46
Task: Configure security settings.....	49
How to configure data loss prevention at the Organization Group level.....	50
How to override data loss prevention configuration for a specific app.....	52
Next Steps.....	56
Troubleshooting.....	57
Security Code.....	57
Apps missing from list view.....	57
Appendix: How to enroll an app in standalone mode.....	58
Document Information.....	62

Introduction

Development of an Android application that is integrated with Workspace ONE will require access to a Workspace ONE Unified Endpoint Manager console. The console will be used to

- manage enrollment of mobile devices and applications in various modes.
- manage the availability and installation of mobile applications, including applications under development.
- manage the configuration of applications.
- manage end users.

This guide covers the following enrollment modes.

- Managed Android in Device Owner (DO) mode, sometimes referred to as Work Managed mode.
- Managed Android in Profile Owner (PO) mode, sometimes referred to as Work Profile mode.
- Unmanaged Android, known as registered mode.

All enrollment modes can be supported by a single console. The Workspace ONE platform supports other enrollment modes for Android, such as Corporate Owned Personally Enabled (COPE), but these aren't in scope of this guide.

Best practice is to have a separate console instance, tenant, or organisation group, set aside for software development.

VMware TestDrive service

VMware operates a service, VMware TestDrive, that can be used to host a management console instance for application development support. The service is free, doesn't need system administrator expertise to utilize, and doesn't require the installation of any client nor server software.

This guide starts with instructions for setting up a TestDrive UEM. In case you don't use TestDrive, the remaining instructions will still be applicable to your UEM deployment.

Abbreviations and Terms

The following abbreviations and terms are used with the following meanings in this guide.

- EMM is an abbreviation for Enterprise Mobility Management.
- UEM is an abbreviation for Unified Endpoint Manager and is used here to mean the Workspace ONE management console.
- Enrollment means the establishment of a trusted connection between a management console and a mobile device or application.

Task: Set up a management console

Setting up a management console is a system administrator task for application developers. You can skip this task if you already have an administrator account on a UEM console with the required permissions.

App Development Support System Administrator Permissions

To support app development, you will need the following system administrator permissions on your UEM.

- Android EMM access, which requires registration from the UEM with Google.
- Upload an application package (APK) file.
- Either create an organisation group for an end user, or get the name of an existing group.
- Either create a new end user with a suitable profile for development purposes, or get the name of an existing suitable user.
- Either create enrolment credentials for an end user, or get existing credentials.

If you have UEM access and all these permissions then you can skip this task.

Otherwise, you can utilize the VMware TestDrive service.

How to set up a management console in VMware TestDrive

VMware operates a service, VMware TestDrive, that can be used to host a Workspace ONE UEM management console to support application development efforts.

To set up a TestDrive UEM, proceed as follows.

1. Register at <https://testdrive.vmware.com>

When you open the above link, your browser will be redirected to the service home page. The home page will have a link or some other way to initiate the sign-up process.

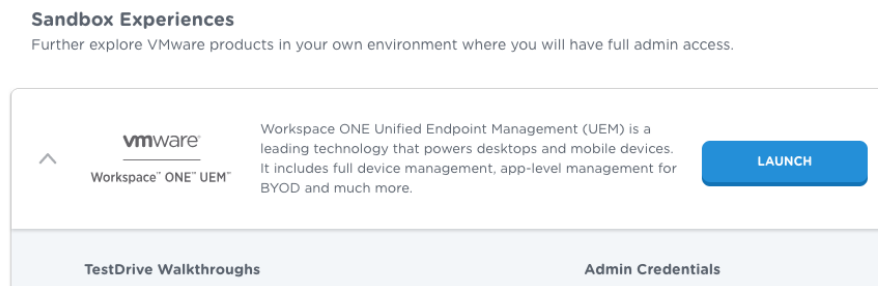
Sign up and set a passcode with one of the following email addresses.

- Your vmware.com email address if you are a member of staff at VMware, or a contractor, or otherwise have a vmware.com email address.
- An email address from an account or domain registered in the VMware Partner Connect portal if you are a member of the VMware Technology Alliance Program (TAP).
- An email address from an account or domain registered in the VMware Customer Connect portal if you are a customer of VMware.

2. Launch the Sandbox Experience: Workspace ONE UEM.

Navigate to My Products, Digital Workspace, Sandbox Experiences, VMware Workspace ONE UEM, and click Launch.

Ignore the Ready to Use Experiences, which aren't suitable for support of app development.



Screen Capture: VMware TestDrive UEM Launch

The UEM login page will open, in a new browser tab or window.

3. Log in to the UEM.

The credentials you will need can be found in the TestDrive user interface, as follows.

- In list mode, click the expand control.
- In grid mode, click the i in a circle.

You will need the Admin Credentials username and password.

This completes setting up a management console. You are now ready to continue with the next [Task: Register for Android Enterprise Mobility Management](#).

Task: Register for Android Enterprise Mobility Management

Registering for Android EMM is a system administrator task for application developers. You can skip this task if your UEM console is already registered. If you don't have access to a UEM, see the preceding [Task: Set up a management console](#).

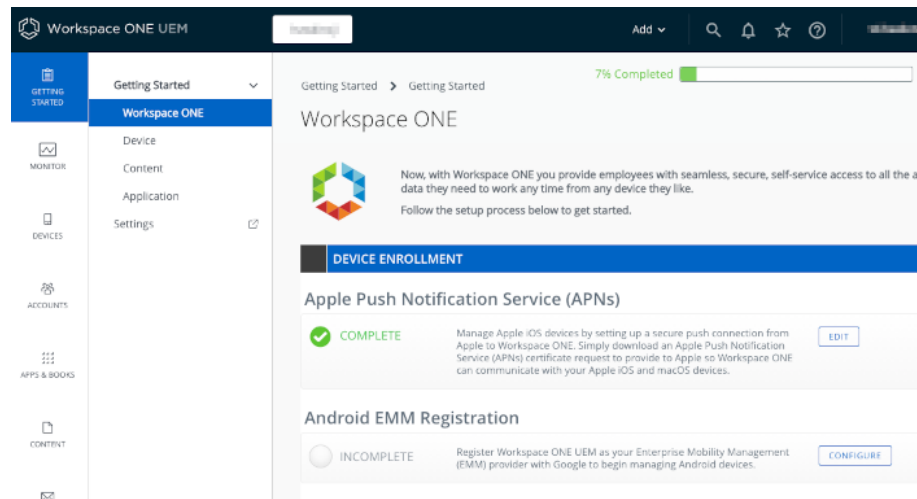
Note that the UEM must be registered for EMM with Google, even if you aren't using any form of device management.

You will need a gmail.com email address or other Google account. You might want to create one for the purpose, in case you have a personal gmail.com address already and don't want to use it for EMM registration.

1. Open the UEM Getting Started page.

Launch and log in to your TestDrive sandbox UEM. Navigate to Getting Started, Workspace ONE, if it isn't open by default.

The following screen capture shows you the location in the UEM user interface.



Screen Capture: UEM Getting Started Android EMM Registration

2. Select to configure Android EMM Registration.

This opens a screen that describes the necessary interactions, which will take place in the Google Play website. The following screen capture shows the page.

Android EMM Registration



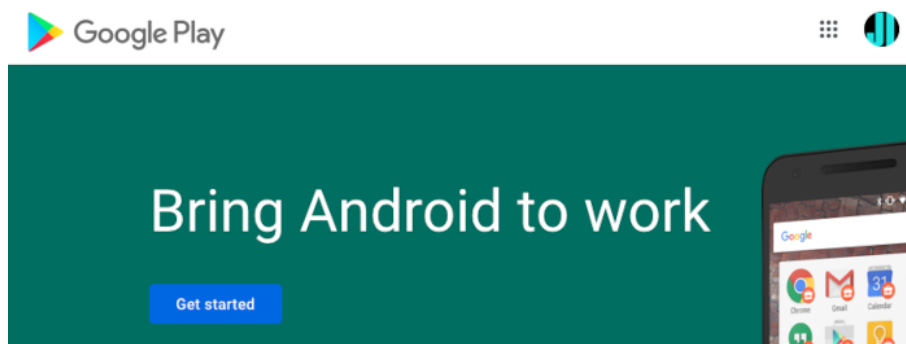
To start managing Android dev register Workspace ONE UEM : Mobility Management (EMM) p
You will automatically be redir register. Simply sign in with an which will serve as your admin Android configuration. After re automatically be redirected ba UEM.

REGISTER WITH GOOGLE

Screen Capture: UEM Android EMM Registration

3. Select to Register With Google.

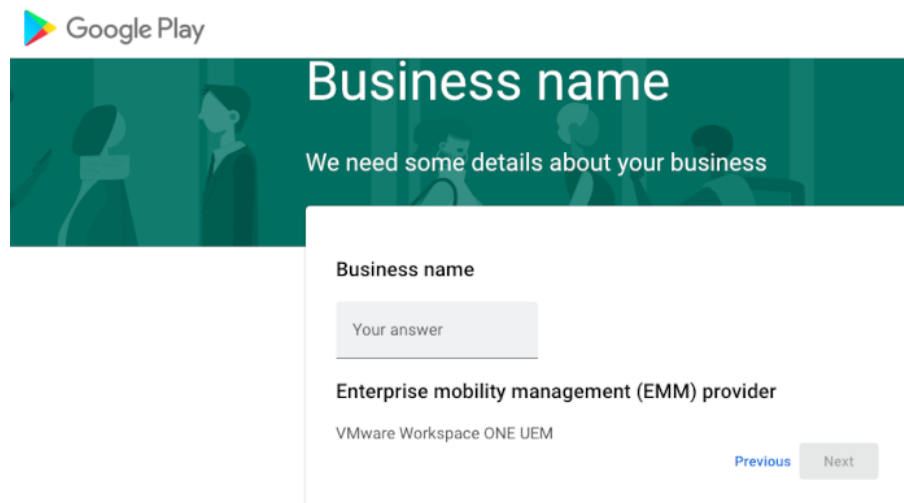
This will open a first page in the Google Play website. In the top right corner, check that the Google account is as expected. If it isn't, then log out and log in with the required account. The following screen capture shows the page.



Screen Capture: Google Play bring Android to work

4. Click the button: Get started.

This will open a page on which you register a business name and EMM provider. The following screen capture shows the page.



Google Play

Business name

We need some details about your business

Business name

Enterprise mobility management (EMM) provider

VMware Workspace ONE UEM

[Previous](#) [Next](#)

Screen Capture: Google Play Business Name Registration

You can use your own name as the business name. You'll only be managing your own devices. The EMM provider should be pre-populated.

5. Enter your own name as the business name and click next.

This will open a page on which you must confirm that you accept the relevant agreement. On this page you can also enter contact details, or you can leave them blank. The following screen capture shows the page.

Google Play

Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available at the moment.

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

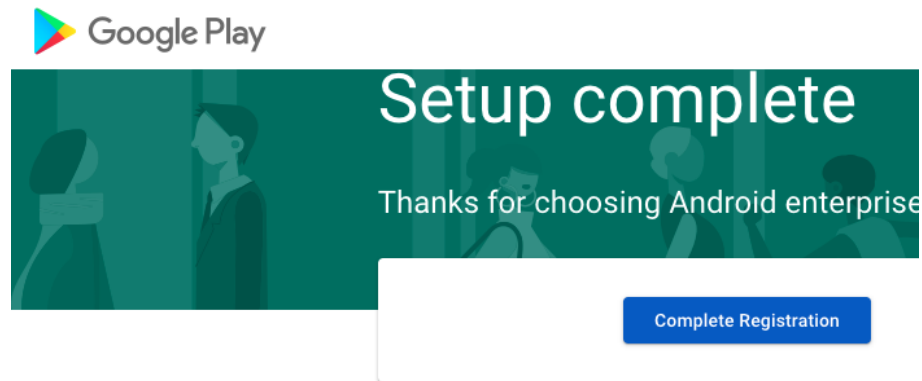
I have read and agree to the [Managed Google Play agreement](#).

[Previous](#) [Confirm](#)

Screen Capture: Google Play Confirmation

6. **Accept the relevant agreement and click Confirm.**

This will open a final page on which you complete registration. In the top right corner, check that the Google account is as expected. If it isn't, close the page and start again after logging in with your correct Google account. The following screen capture shows the page.



Screen Capture: Google Play Complete Registration

This completes registration for Android Enterprise Mobility Management. You are now ready to continue with the next [Task: Configure management console enrollment](#).

Task: Configure management console enrollment

Configuring the management console for enrollment is a system administrator task for application developers. The enrollment configuration task is dependent on the [Task: Register for Android Enterprise Mobility Management](#). The following instructions assume that the dependent task is complete already.

Workspace ONE supports the following types of enrollment for Android.

- Managed Android in Device Owner (DO) mode, sometimes referred to as Work Managed mode.
- Managed Android in Profile Owner (PO) mode, sometimes referred to as Work Profile mode.
- Unmanaged Android, known as registered mode.

The types of enrollment that will be available for a mobile device or app are specified in the UEM configuration, in the *Organization Group* structure.

Introduction to Organization Groups

The organization group (OG) is a fundamental concept of Workspace ONE UEM administration. This introduction gives an overview for application developers.

A UEM can have multiple OGs, organized in a hierarchical tree structure. Features for enrollment, policies, and settings, are all configured in the OG structure. When an end user device or app enrolls, it will be assigned to one OG. The policies and settings of that OG then apply to that device or app.

An OG at a lower level of the structure, referred to as a *child* OG, inherits the configuration of its parent OG. The configuration of the parent OG will specify which parts of the configuration can be overridden in a child OG. Each OG has up to one parent.

Each OG has an identifier, referred to as its *Group ID*, and a *name*. The Group ID sometimes has to be entered in the mobile user interface. The name will be used for display purposes in the console and mobile user interfaces.

When the TestDrive hosting service instantiates a sandbox UEM server, it configures one OG, referred to here as the *root* OG.

- You cannot remove the root OG.
- The root OG doesn't have a parent OG.
- You cannot create siblings to the root OG.
- You can rename the root OG.
- You can create child OGs under the root OG.

This guide recommends adding a layer of child OGs to the structure so that the configuration can support all types of UEM enrollment without being changed. See the [Recommended Organization Group Structure](#) for details and a diagram.

Recommended Organization Group Structure

This guide recommends creating an OG structure that includes all types of UEM enrollment. This will enable the application development effort to proceed and support all types of enrollment without the need to reconfigure the UEM.

The following recommendations are also made.

- Configure selection of enrollment type by the end user.
- Use two- or three-letter values for OG Group ID values, to facilitate manual entry in the mobile user interface.
- Use longer, descriptive texts for OG names.
- Add a separate child OG for standalone enrollment. Standalone enrollment is supported by the Workspace ONE Boxer email app, the Workspace ONE Web browser, Workspace ONE PIV-D Manager, and other apps in the VMware productivity suite.

This diagram represents a recommended OG structure, as a UML Object Diagram.

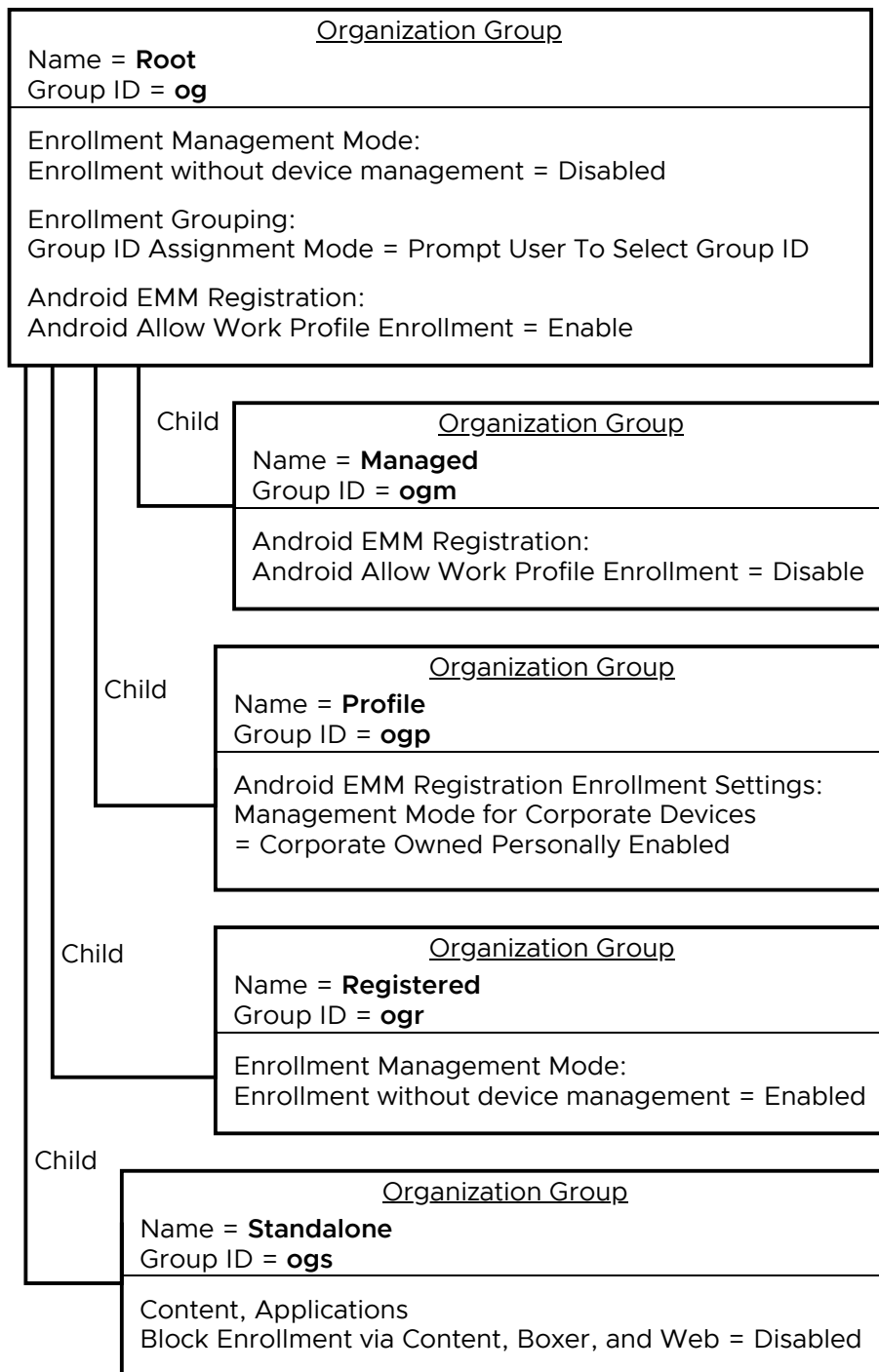


Diagram 1: Organization Group Structure

Follow the [How to set up the recommended Organization Group structure](#) instructions to set up the above OG structure.

How to set up the recommended Organization Group structure

To set up the [Recommended Organization Group Structure](#), proceed as follows.

1. Log in to the UEM and navigate to: Groups & Settings, Groups, Organization Groups, Details.

This opens the root OG in the Details view.

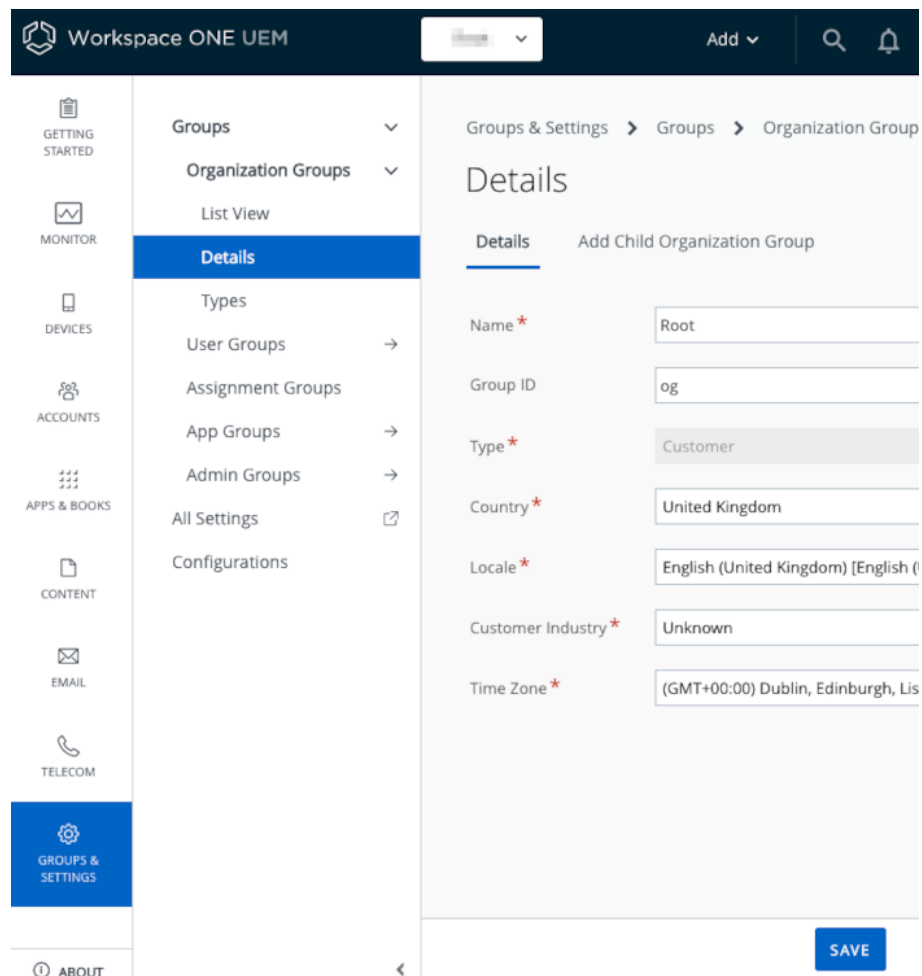
2. Set the name and Group ID of the root OG.

In the Details view, enter the following field values.

- Name: Root
- Group ID: og

There is no need to set any other field values.

The following screen capture shows how the screen could look when the values have been entered.

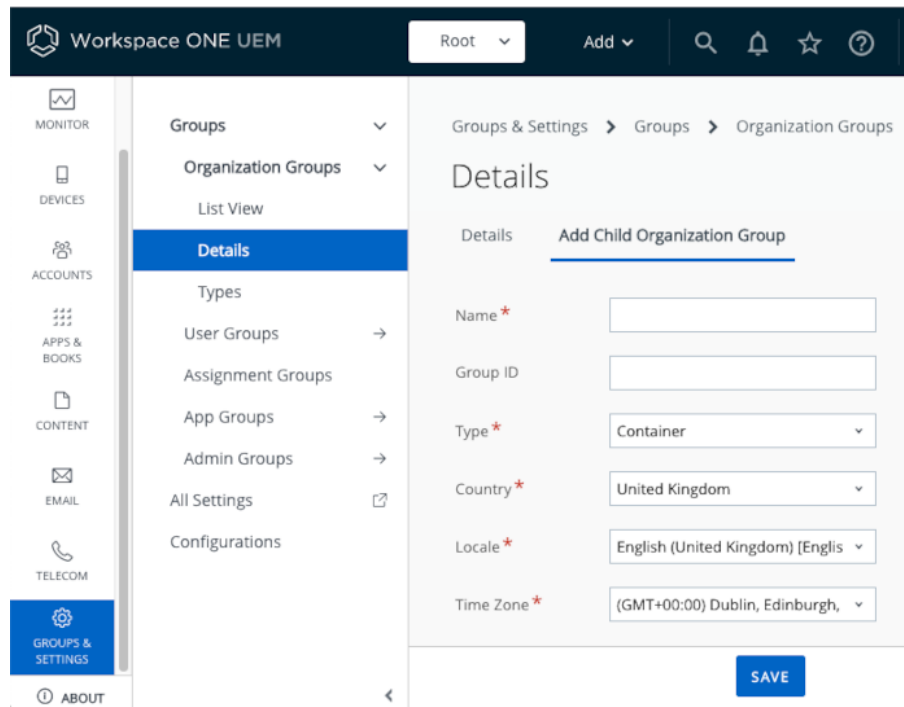


Screen Capture: UEM OG Details

Click the Save button at the bottom of the screen to save the changes. A message will be displayed to confirm that the change has been made.

3. Add a first child OG.

Still in the Details view of the root OG, select the option to Add Child Organization Group. This option appears as a tab. The following screen capture shows the location and appearance after selection.



Screen Capture: UEM Add Child OG

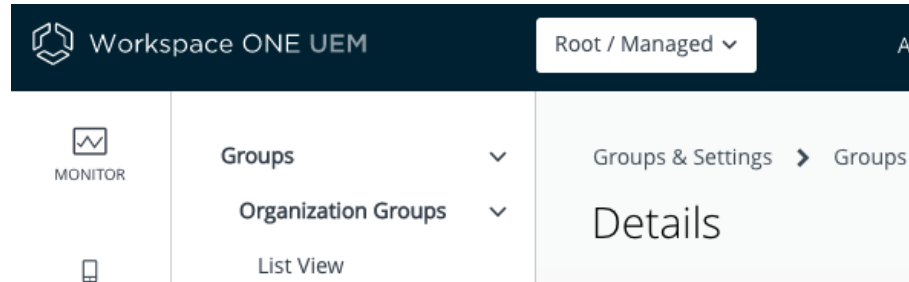
Enter the following field values for the first child OG.

- Name: Managed
- Group ID: ogm

Click the Save button at the bottom of the screen to save the changes. This will create the child OG and select it.

4. Select the root OG.

At the top of the page, locate the OG selection control. It will be displaying the name of the root OG and child OG separated by an oblique, as shown in the following screen capture.



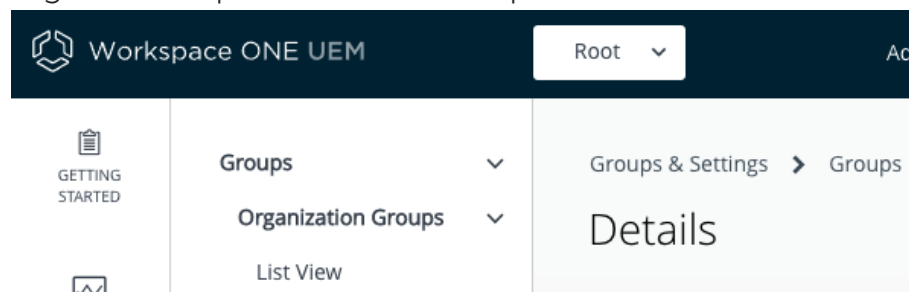
Screen Capture: UEM Selected OG

The name of the root OG mightn't have updated to reflect the recent name change. In that case, refresh the browser view.

Click to expand the control and then click to select the root OG.

The control will change to show the name of the root OG only. If it doesn't, try again.

The following screen capture shows the required OG selection.



Screen Capture: UEM Root OG Selected

Note: Check the current OG selection whenever you make configuration changes in the UEM. Almost all configuration will be applied at the OG level.

5. Add the other child OGs.

Repeat the preceding steps to add the second child OG, with the following values.

- Parent: root OG.
- Child Name: `Profile`
- Child Group ID: `ogp`

Save, reselect the root OG and then repeat the process again with the following values.

- Parent: root OG.
- Child Name: `Registered`
- Child Group ID: `ogr`

Save, reselect the root OG and then repeat the process again with the following values.

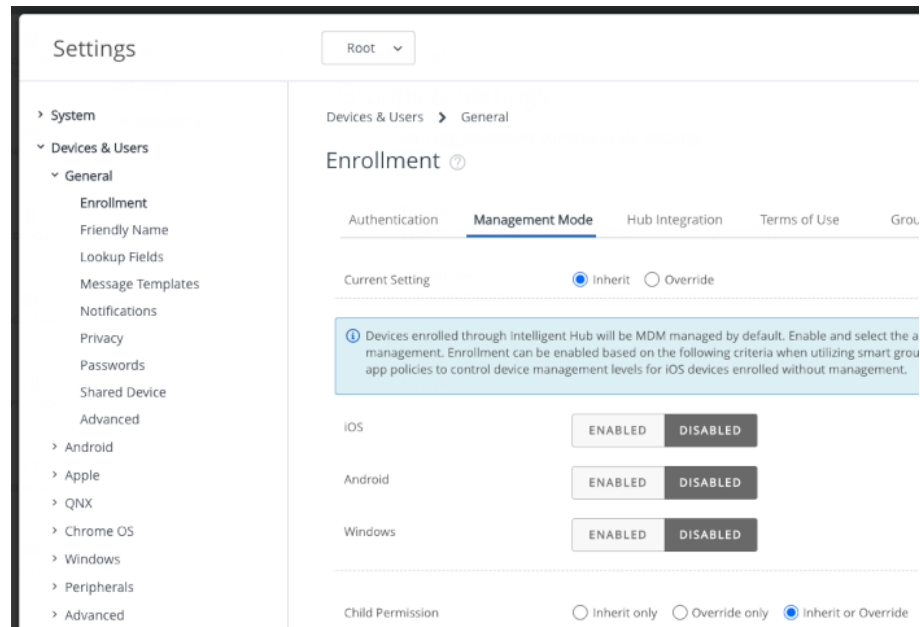
- Parent: root OG.
- Child Name: `Standalone`
- Child Group ID: `ogs`

Save and then continue to the next instruction.

6. Configure registered mode enrollment.

First, check that registered mode isn't the default in the root OG. Select the root OG, see above, and navigate to: Groups & Settings, All Settings, Devices & Users, General, Enrollment, Management Mode. By default, the option to enrol without device management should be disabled.

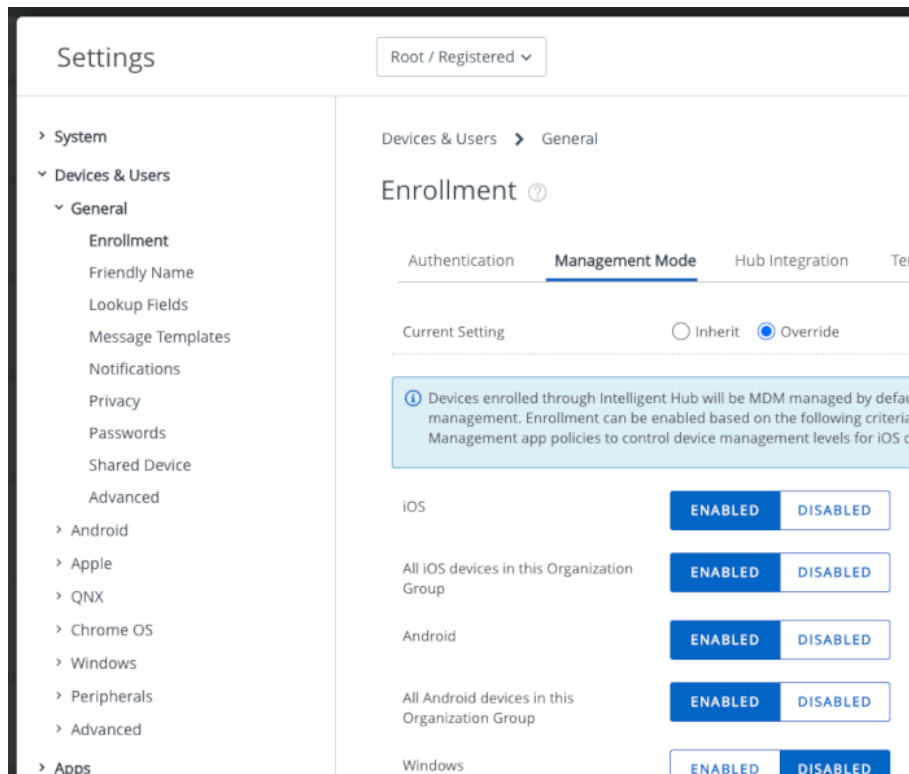
The following screen capture shows the location and setting.



Screen Capture: UEM Root OG Management Mode Settings

The managed OG and profile OG should inherit the same Management Mode settings. Check this by selecting each one and navigating as necessary.

Next, select the registered OG, navigate to Management Mode and set the option to enrol without device management to enabled and in all devices in the OG. If necessary, select Current Setting: Override at the top of the settings. The following screen capture shows the location and setting.

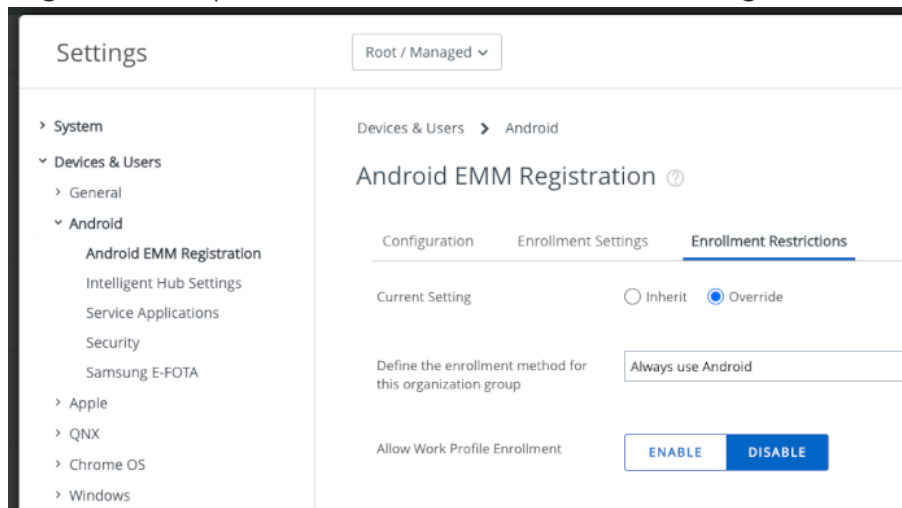


Screen Capture: UEM Registered OG Management Mode Settings
Save and then continue to the next instruction.

7. Configure managed mode enrollment.

Select the managed OG, see above, and navigate to: Groups & Settings, All Settings, Devices & Users, Android, Android EMM Registration, Enrollment Restrictions. Select Allow Work Profile Enrollment: disable. If necessary, select Current Setting: Override at the top of the settings.

The following screen capture shows the location and setting.



Screen Capture: UEM Managed OG Enrollment Restrictions

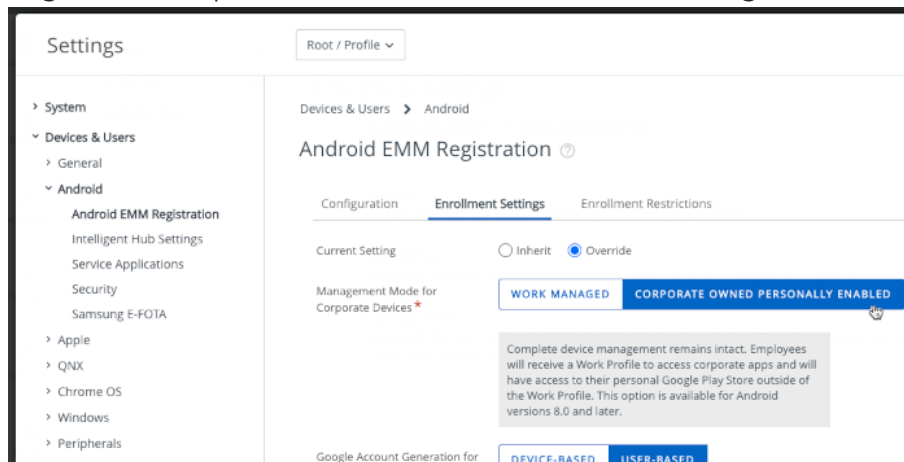
Save your changes.

Check that the root OG has the default setting, Allow Work Profile Enrollment: enable. Also check that the profile OG inherits that setting.

8. **Configure profile mode enrollment.**

Select the profile OG, see above, and navigate to: Groups & Settings, All Settings, Devices & Users, Android, Android EMM Registration, Enrollment Settings. Set the option Management Mode for Corporate Devices: Corporate Owned Personally Enabled. If necessary, select Current Setting: Override at the top of the settings.

The following screen capture shows the location and setting.

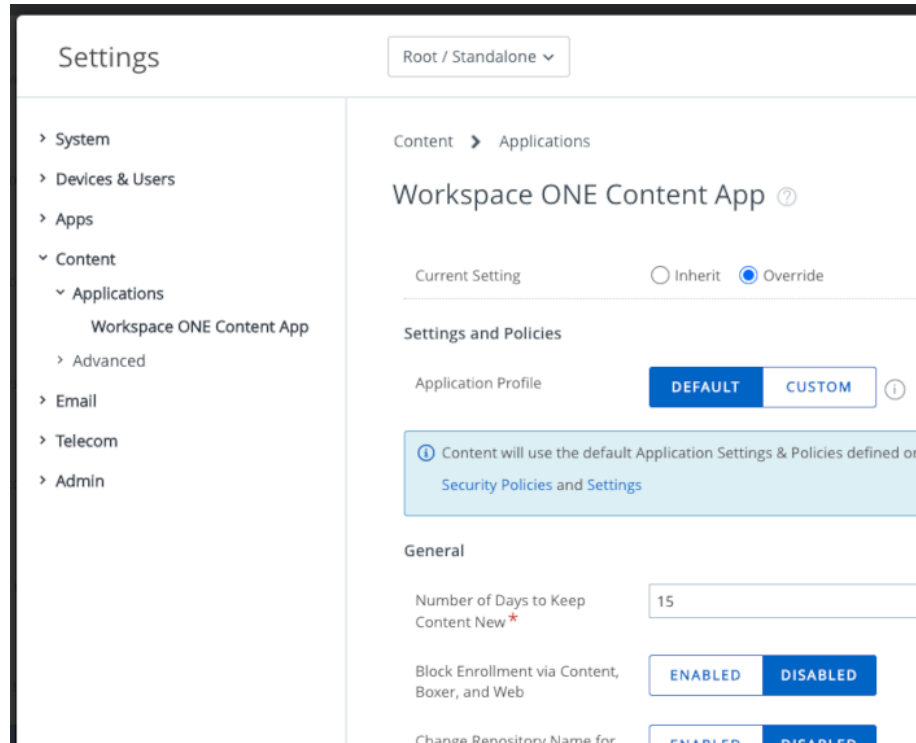


Screen Capture: UEM Profile OG Enrollment Settings

Save and then continue to the next instruction.

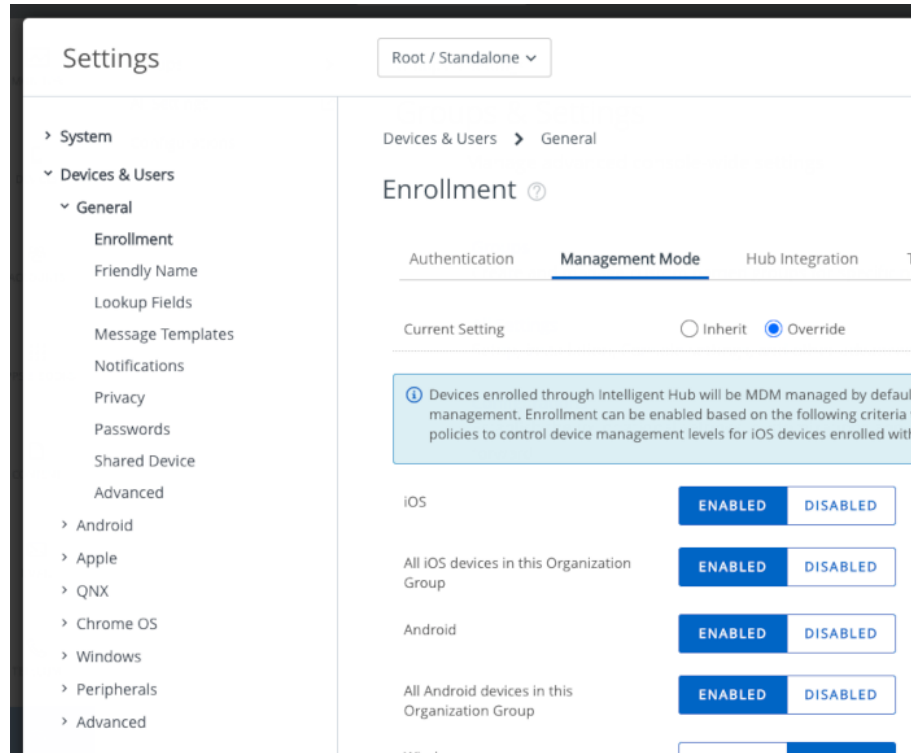
9. Configure standalone enrollment.

First, select the standalone OG, see above, and navigate to: Groups & Settings, All Settings, Content, Applications, Workspace ONE Content App. Set the option Block Enrollment via Content, Boxer, and Web: Disabled. If necessary, select Current Setting: Override at the top of the settings. The following screen capture shows the location and setting.



Screen Capture: UEM Standalone OG Unblock Enrollment

Next, with the standalone OG still selected, navigate to Groups & Settings, All Settings, Devices & Users, General, Enrollment, Management Mode and set the option to enrol without device management to enabled and in all devices in the OG. (This configuration is also required for the registered OG, above.) If necessary, select Current Setting: Override at the top of the settings. The following screen capture shows the location and setting.



Screen Capture: UEM Standalone OG Management Mode Settings
 Save and then continue to the next instruction.

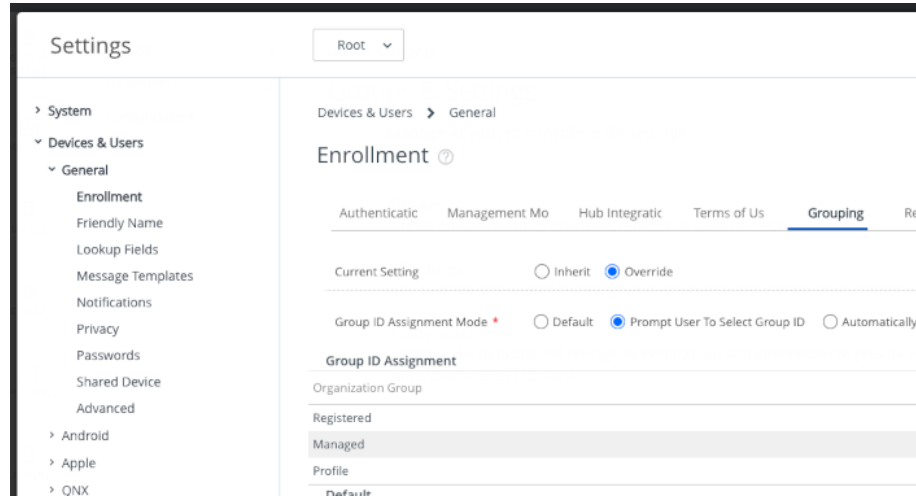
10. Configure OG selection at enrollment time.

Select the root OG, see above, and navigate to: Groups & Settings, All Settings, Devices & Users, General, Enrollment, Grouping.

Select Group ID Assignment Mode: Prompt User To Select Group ID.

If necessary, select Current Setting: Override at the top of the settings.

The following screen capture shows the location and setting.



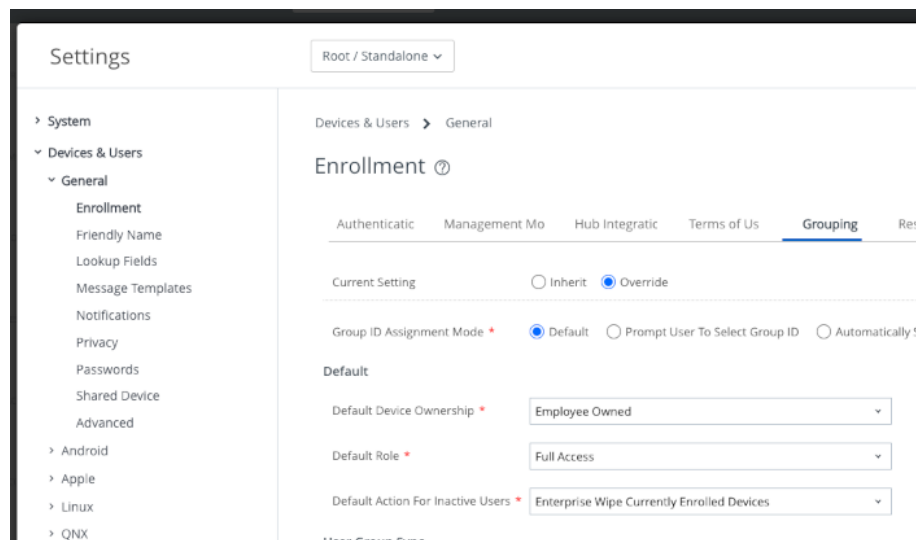
Screen Capture: UEM Root OG Enrollment Grouping

Next, select the standalone OG, see above, and navigate to the same screen: Groups & Settings, All Settings, Devices & Users, General, Enrollment, Grouping.

For this OG, select Group ID Assignment Mode: Default.

If necessary, select Current Setting: Override at the top of the settings.

The following screen capture shows the location and setting.



Screen Capture: UEM Standalone OG Enrollment Grouping

This completes enrollment mode configuration. Check that the OG structure and settings are the same as shown in the [Recommended Organization Group Structure](#) diagram.

Now is a good time to review [How to log in and select an Organization Group](#).

How to log in and select an Organization Group

Whenever you log in to the UEM, you should check the OG selection. You should also check the OG selection before changing a configuration setting, creating an end user, adding an application, or taking any other system administration action. Almost all system administration is applied at the OG level.

Proceed as follows.

1. Get the administrator login credentials.

If you are using a VMware TestDrive UEM, you can get the default credentials from the service home page. Note that if you change your login credentials, the TestDrive home page won't be updated and will still show the default credentials.

Navigate to this address in a web browser: <https://testdrive.vmware.com>

When you open the above link, your browser will be redirected to the service home page. Log in to TestDrive using the credentials with which you registered.

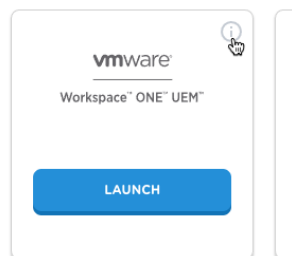
(If you haven't registered and don't have access to another UEM, see the [Task: Set up a management console](#) for instructions.)

Navigate to My Products, Digital Workspace, Sandbox Experiences, VMware Workspace ONE UEM. The credentials you will need can be found as follows.

- In list mode, click the expand control.
- In grid mode, click the i in a circle.

The following screen captures show where to click in the TestDrive user interface.

Sandbox Experiences
Further explore VMware products in y



Screen Capture: TestDrive View Credentials in Grid Mode

Sandbox Experiences

Further explore VMware products in yc



Screen Capture: TestDrive View Credentials in List Mode

You will need the Admin Credentials username and password.

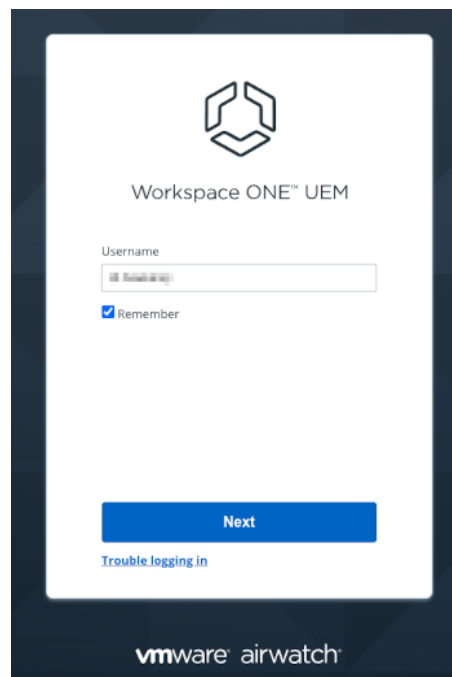
2. Open the UEM console login page.

If you are using TestDrive, navigate to My Products, Digital Workspace, Sandbox Experiences, VMware Workspace ONE UEM, and click Launch.

The UEM login page will open, in a new browser tab or window.

3. Log in to the UEM.

The initial appearance of the login screen is shown in the following screen capture.



Screen Capture: UEM Login First Screen

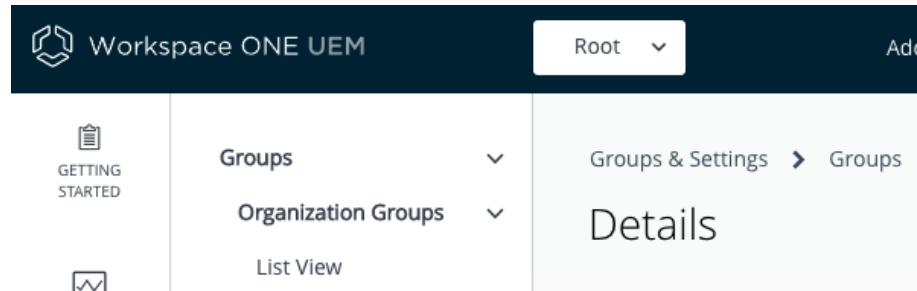
Enter the admin username if it isn't pre-populated and click Next, then enter the admin password and click Log In.

You are now logged in to the UEM.

4. Select the required OG.

At the top of the page, locate the OG selection control. It might already display the required OG.

The following screen capture shows the OG selection control.



Screen Capture: UEM Root OG Selected

In the above screen capture, the selected OG is: Root.

If the required OG isn't already displayed then click to expand the control and then click again to select the required OG. The control will change to show the name of the required OG, and its hierarchy if it is a child OG. If it doesn't, try again.

This completes logging in to the console and selecting an OG.

If you haven't already done so, you are now ready to continue to the next [Task: Set up the mobile application catalog](#).

Task: Set up the mobile application catalog

Setting up the mobile application catalog is a system administrator task for application developers. This task is dependent on the [Task: Configure management console enrollment](#). The following instructions assume that the dependent task is complete already.

The mobile application catalog will be used to make your app in development available to install onto your developer device. Installation could be via selection in Hub, or by pushing from the UEM.

Setting up the catalog is a common task for UEM administrators and the relevant online documentation will be used here.

Set up the Workspace ONE mobile application catalog as follows.

1. **Log in to the UEM and select the root OG.**

For instructions, see [How to log in and select an Organization Group](#).

2. **Activate Hub Services.**

Follow the instructions here: [Activate Hub Services for Existing UEM Customers](#)

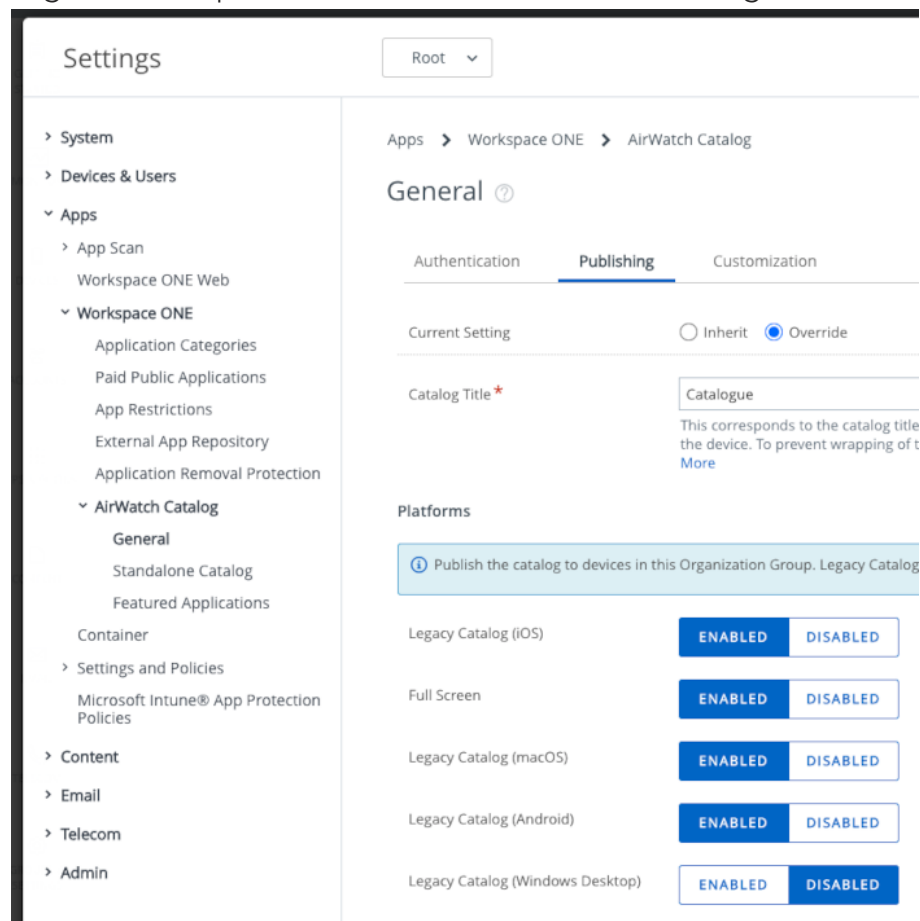
3. **Create your catalog.**

Follow the instructions here: [Customize the App Catalog in Hub Services](#)

4. **Activate the AirWatch Catalog.**

In some cases, it has seemed necessary to activate the legacy AirWatch catalog feature. To do so, navigate to: Groups & Settings, Apps, Workspace ONE, AirWatch Catalog, General, Publishing. Select Legacy Catalog (Android): enabled.

The following screen capture shows the location and setting.



Screen Capture: UEM Legacy Catalog Settings

This completes setting up the mobile application catalog. You are now ready to continue to the next [Task: Configure end users](#).

Task: Configure end users

Configuring end users in the UEM management console is a system administrator task for application developers. The following instructions refer to some concepts introduced in the [Task: Configure management console enrollment](#).

The end user configuration described in this guide is intended only to support application development, not for production Workspace ONE deployments.

This guide doesn't cover end user configuration in depth. The recommendations here are intended to support application development only and aren't suitable for production Workspace ONE deployments. See the system administrator user guides for the Workspace ONE product for authoritative and complete information.

See the [Recommended End User Configuration](#) for details.

Recommended End User Configuration

This guide recommends configuring UEM *Basic* end users to support application development. Basic end users enroll by entering a user name and password at the device.

Basic user accounts exist only in the UEM management console and aren't linked to, for example, users in a Lightweight Directory Access Protocol (LDAP) directory. For that reason they could be the easiest type of account to set up and manage for development purposes.

Every UEM supports Basic users by default. In some deployments, Basic users will be the only option.

The following recommendations are also made.

- Set users as managed by, and enrolling into, the root OG. See the [Task: Configure management console enrollment](#) for details of what is meant by root OG.
- Create no more users than are needed. One might be enough.
- Set each user's password to be the same as its username. This would be bad practice in production, but is OK during development.
- Use short values for username and password. During development you might enroll and unenroll frequently. Single-letter values, such as "a", are supported.

Your TestDrive UEM will come with a single automatic end user account. You mightn't be allowed to change the automatic account's username to comply with the above recommendations. In that case, add a new user that does comply.

Follow the [How to create an end user account](#) instructions to create an end user with the above configuration.

How to create an end user account

To create an end user account in line with the above recommended configuration, proceed as follows.

1. **Log in to the UEM and select the root OG.**

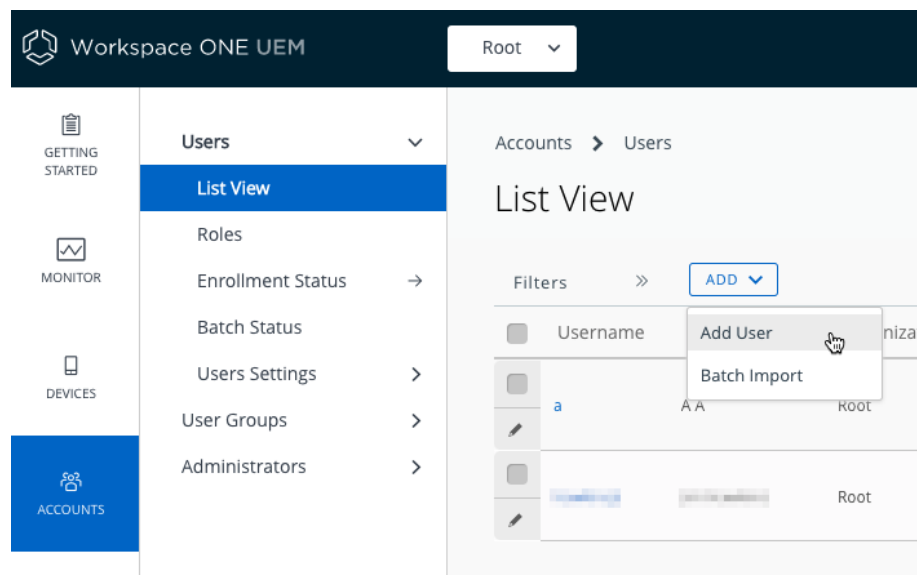
For instructions, see [How to log in and select an Organization Group](#).

2. **Navigate to Accounts, Users, List View.**

Clicking on Accounts might do the whole navigation.

3. **Select to add an end user.**

The following screen capture shows the location of the control in the user interface. The Root OG has been selected.



Screen Capture: UEM Add End User in Root OG

The Add/Edit User screen will open.

4. Fill in the details for the new end user, for example as follows.

- Security Type: Basic.
- Username: Enter a short value, for example “a”.
- Password: Enter the Username value.
- Confirm Password: Enter the Username value again.
- Full Name: Enter a short value, for example “A” in the First Name and Last Name fields.
- Email address: Enter your email address.
- Enrollment Organization Group: Root, the default.
- Allow user to enroll into additional Organization Groups: Disabled, the default.
- User Role: Full Access, the default.
- Notification Message Type: None.

The following screen capture shows sample filled-in values.

Screen Capture: UEM Add/Edit End User Sample Values, upper

Screen Capture: UEM Add/Edit End User Sample Values, lower

5. Click Save to add the user account.

This completes end user account creation. The end user can be used for the [Task: Enroll a developer device](#).

How to delete an end user account

In case you want to delete an end user account, proceed as follows.

Your TestDrive UEM will come with a single automatic end user account. You mightn't be allowed to delete the automatic account.

1. Log in to the UEM and select the root OG.

For instructions, see [How to log in and select an Organization Group](#).

2. Navigate to Accounts, Users, List View.

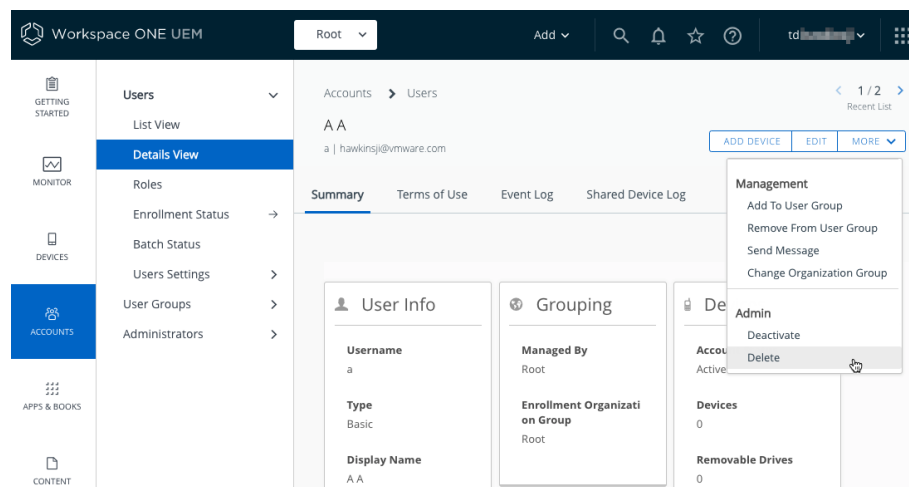
Clicking on Accounts might do the whole navigation.

3. Click anywhere blank in the row for the end user you wish to delete.

This opens a detailed view of the end user account.

4. In the actions at the top right, click More to expand the actions then, under Admin click Delete.

The following screen capture shows the expanded actions in the user interface.



Screen Capture: UEM Delete End User

If the Delete action doesn't appear then the user cannot be deleted.

5. A confirmation message will be displayed. Click OK to dismiss it.

The end user account has now been deleted.

Task: Enroll a developer device

Enrolling a developer device is a common task for application developers. The following instructions refer to some concepts introduced in the [Task: Configure management console enrollment](#).

This guide gives instructions for enrolling in any of the following modes.

- Managed Android in Device Owner (DO) mode, sometimes referred to as Work Managed mode.
- Managed Android in Profile Owner (PO) mode, sometimes referred to as Work Profile mode.
- Unmanaged Android, known as registered mode.

You should test your application in all modes that your end users will use in production. In case you don't have known end users yet, consider the following general recommendations.

- Android DO managed mode can be used on a developer device that you don't mind resetting to its factory default state. Enrollment will delete all data on the device.
- Android PO managed mode can be used on a developer device that doesn't already have a work profile. However, PO mode isn't recommended for application development for the following reasons.
 - You will have to upload your app to an enterprise Play Store instance. The store doesn't allow some package name prefixes, and doesn't appear to support removal, nor replacement without upgrade.
 - You will have to follow a different procedure to side load your app in development from Android Studio or the Android Debug Bridge (adb) tool. In PO mode, the device has an additional user account. The default Gradle files mightn't facilitate automated testing of your app in PO mode.
- Registered mode can be used on any device that isn't already enrolled against a Workspace ONE UEM console, and doesn't have any standalone enrolled apps. (The Workspace ONE Boxer email app, the Workspace ONE Web browser, and other apps in the VMware productivity suite support standalone enrollment.) No device data will be lost.

The enrollment instructions for different modes are substantially but not completely the same. Common instructions are duplicated to so that each subsection can be followed independently.

In any mode, you will first need to know [How to find out the enrollment server address](#).

How to find out the enrollment server address

To find out the enrollment server address for a UEM proceed as follows.

1. Log in to the UEM and select the root OG.

For instructions, see [How to log in and select an Organization Group](#).

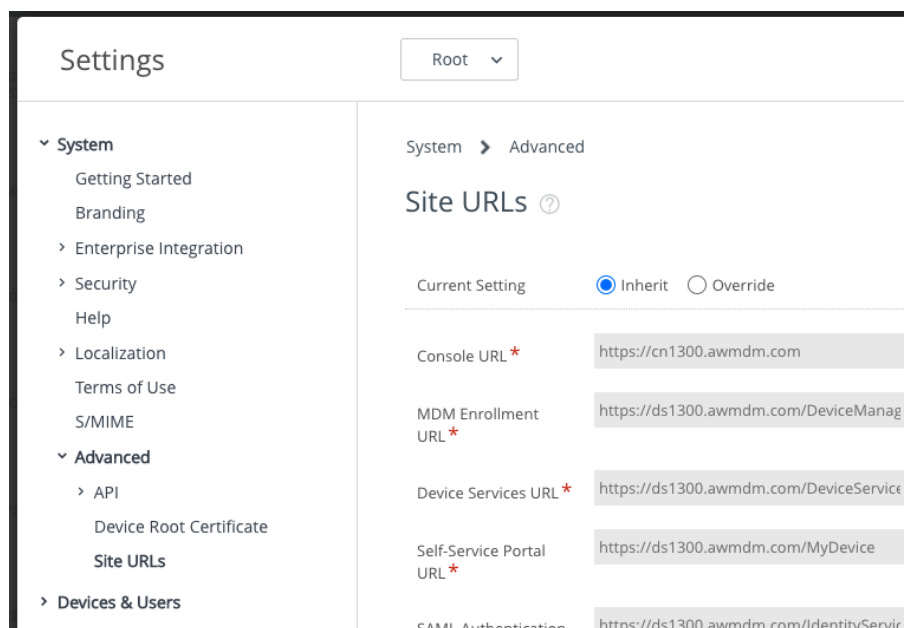
2. Navigate to: Groups & Settings, All Settings, System, Advanced, Site URLs.

This opens a page with a list of site uniform resource locator (URL) values.

3. Locate the Device Services URL in the list.

The enrollment server address is the host portion of the Device Services URL.

The following screen capture shows the location of the required address in the user interface.



Screen Capture: UEM Device Services URL

In the above screen capture, the enrollment server address is:

`ds1300.awmdm.com`

Make a note of the address and then proceed to one of these sets of instructions, depending on which type of enrollment you are using.

- [How to enroll an Android device in Device Owner managed mode](#)
- [How to enroll an Android device in Profile Owner managed mode](#)
- [How to enroll an Android device in Registered mode](#)

How to enroll an Android device in Device Owner managed mode

In general, only new or factory reset devices can be enrolled in Android Device Owner (DO) managed mode. In order to use an ordinary Android smartphone or tablet as your developer device in DO mode, you must first reset it to factory defaults and erase all data.

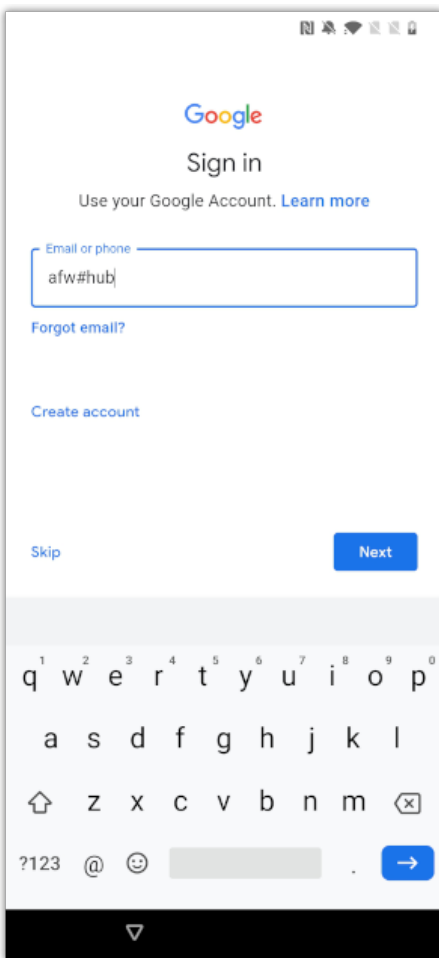
These instructions assume that the [Recommended Organization Group Structure](#) has been configured in the UEM. Some steps will be different if that isn't the case.

1. **Switch on your developer device if it is new, or reset it to factory defaults and erase all data.**
2. **Follow the out-of-box activation instructions until you reach the Google sign-in screen.**
 - You can skip any instructions that don't apply to developer devices such as restoring preferences, apps, and data from an earlier device.
 - You will require an internet connection, either mobile data or Wi-Fi.

3. On the sign-in screen, enter the Workspace ONE Intelligent Hub special identifier instead of an email address or phone number.

The identifier is: `afw#hub`

The following screen capture shows how this might appear as entered on the sign-in screen.

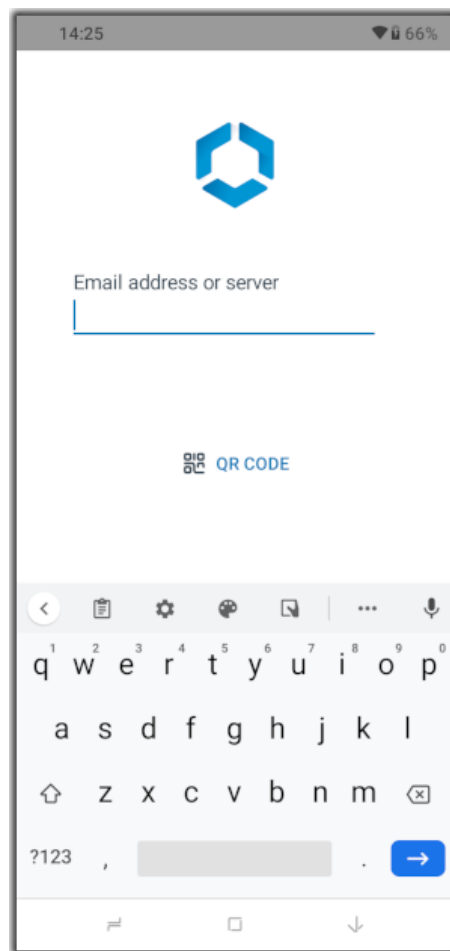


Screen Capture: Sign-in Screen with Workspace ONE Intelligent Hub special identifier

4. Tap **Next** and then follow the ensuing instructions until you reach a screen with the **Workspace ONE Intelligent Hub** logo and a prompt for email address or server.

The instructions will include installing Workspace ONE Intelligent Hub and setting up as a work device, as well as setting some user preferences. You will be warned that the device isn't private. There is no need to switch on any optional Google Services.

The following screen capture shows the screen with logo and prompt.



Screen Capture: Workspace ONE Intelligent Hub logo and prompt

5. Enter the enrollment server address and tap **Next**.

See the instructions [How to find out the enrollment server address](#) if necessary.

There will be some processing and then the prompt will reappear with an additional field requiring entry: Group ID.

6. Enter the Group ID of your root OG.

In the [Recommended Organization Group Structure](#) the Group ID is: og

There will be some more processing and then you will be prompted to select a group for your device.

7. Select the group Managed and tap to continue.

You will be prompted for a Username and Password.

8. Enter the username and password of an end user account and tap Next.

If the [Recommended End User Configuration](#) has been set up then the username and password could both be: a

There will be some more processing. You might be prompted to save the password just entered but this can be ignored.

When enrollment processing has finished, you will be prompted to accept a privacy agreement.

9. Accept the privacy agreement by tapping: I Understand.

You will be prompted to opt in to additional data sharing.

10. Select “Not Now” and confirm by tapping “Don’t Send” when prompted.

There will be some more processing and device set-up will finalize.

11. Set a passcode for the device if prompted to do so. Acknowledge any other warnings.

This completes Android Device Owner managed mode enrollment. The device is now ready for developer use.

For instructions with screen captures of every stage, see this tutorial on the VMware Tech Zone website:

https://techzone.vmware.com/managing-android-devices-workspace-one-operational-tutorial#_1211546

How to enroll an Android device in Profile Owner managed mode

A device that doesn't already have a work profile have can be enrolled in Android Profile Owner (PO) managed mode. PO mode isn't recommended for general application development for the reasons given in the introduction to this [Task: Enroll a developer device](#) but might be required as a test case.

Warnings

- The Workspace ONE Intelligent Hub application cannot be enrolled with more than one management console at a time. If Hub is already installed and enrolled on your developer device, then it must now be removed and re-installed, or must be reset, i.e. have its storage cleared. Removing or resetting the Hub may cause removal of any associated applications from the device.
- Any VMware productivity apps already installed on an unmanaged developer device might stop working when it is enrolled in PO mode. This applies whether the apps were enrolled standalone or through Hub running in registered mode. The VMware productivity apps include the Workspace ONE Boxer email app, and the Workspace ONE Web browser, for example.

Tip: Set a device passcode before you begin enrolment. Typical UEM configurations will require a passcode, as a security policy. If a device passcode isn't set at the start of the enrolment interaction, you will be forced to set it as an enrolment step, which sometimes doesn't go smoothly.

These instructions assume that the [Recommended Organization Group Structure](#) has been configured in the UEM. Some steps will be different if that isn't the case.

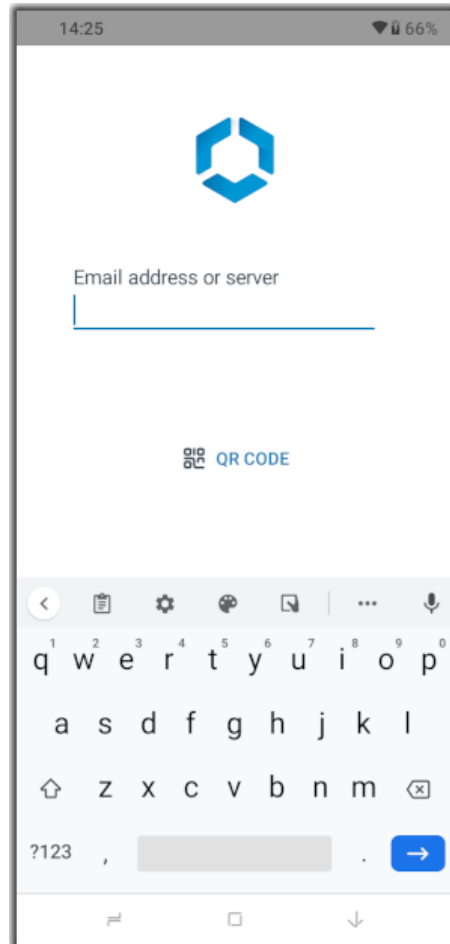
Proceed as follows.

1. Install the Workspace ONE Intelligent Hub mobile application.

The Hub can be installed from the Google Play Store. Search for “workspace one intelligent hub”, for example.

2. Open the Hub app.

The screen will show the Workspace ONE Intelligent Hub logo and a prompt for email address or server, as in the following screen capture.



Screen Capture: Workspace ONE Intelligent Hub logo and prompt

3. Enter the enrollment server address and tap Next.

See the instructions [How to find out the enrollment server address](#) if necessary.

There will be some processing and then the prompt will reappear with an additional field requiring entry: Group ID.

4. Enter the Group ID of your root OG.

In the [Recommended Organization Group Structure](#) the Group ID is: og

There will be some more processing and then you will be prompted to select a group for your device.

5. **Select the group Profile and tap to continue.**

You will be prompted for a Username and Password.

6. **Enter the username and password of an end user account and tap Next.**

If the [Recommended End User Configuration](#) has been set up then the username and password could both be: a

There will be some more processing. You might be prompted to save the password just entered. Ignore or decline the option.

When enrollment processing has finished, you will be prompted to accept a privacy agreement.

7. **Accept the privacy agreement by tapping: I Understand.**

You will be prompted to opt in to additional data sharing.

8. **Select “Not Now” and confirm by tapping “Don’t Send” when prompted.**

There will be some more processing then you will be prompted to change the way that you work.

9. **Tap Accept & Continue.**

There will be some more processing and notification that Hub configuration is in process.

This completes Android Profile Owner mode enrollment. The device is now ready for developer use.

How to enroll an Android device in Registered mode

A device that isn't already enrolled with Workspace ONE, and doesn't have any standalone enrolled apps installed, can be enrolled in registered mode.

The Workspace ONE Boxer email app, the Workspace ONE Web browser, and other apps in the VMware productivity suite support standalone enrollment. Any of those apps that are on the device might stop working when the device is enrolled in registered mode.

These instructions assume that the [Recommended Organization Group Structure](#) has been configured in the UEM. Some steps will be different if that isn't the case.

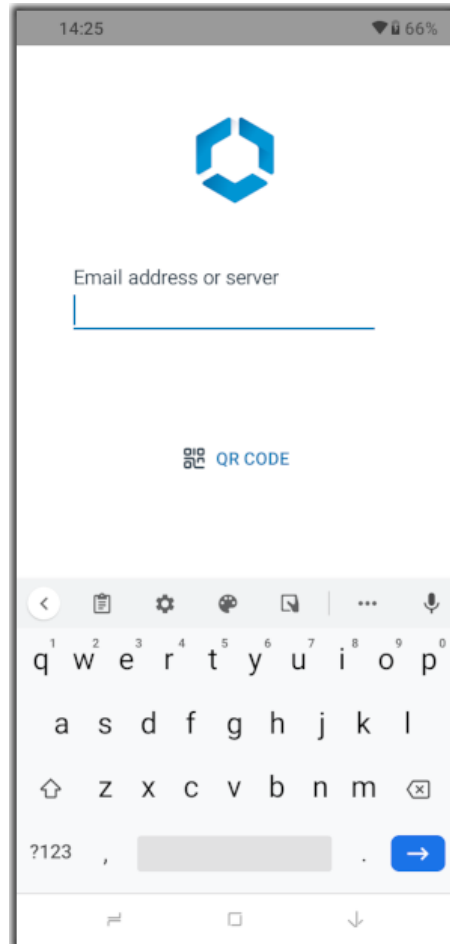
Proceed as follows.

1. **Install the Workspace ONE Intelligent Hub mobile application.**

The Hub can be installed from the Google Play Store. Search for “workspace one intelligent hub”, for example.

2. Open the Hub app.

The screen will show the Workspace ONE Intelligent Hub logo and a prompt for email address or server, as in the following screen capture.



Screen Capture: Workspace ONE Intelligent Hub logo and prompt

3. Enter the enrollment server address and tap Next.

See the instructions [How to find out the enrollment server address](#) if necessary.

There will be some processing and then the prompt will reappear with an additional field requiring entry: Group ID.

4. Enter the Group ID of your root OG.

In the [Recommended Organization Group Structure](#) the Group ID is: og

There will be some more processing and then you will be prompted to select a group for your device.

5. **Select the group Registered and tap to continue.**

You will be prompted for a Username and Password.

6. **Enter the username and password of an end user account and tap Next.**

If the [Recommended End User Configuration](#) has been set up then the username and password could both be: a

There will be some more processing. You might be prompted to save the password just entered. Ignore or decline the option.

When enrollment processing has finished, you will be prompted to accept a privacy agreement.

7. **Accept the privacy agreement by tapping: I Understand.**

You will be prompted to opt in to additional data sharing.

8. **Select “Not Now” and confirm by tapping “Don’t Send” when prompted.**

There will be some more processing.

This completes Registered mode enrollment. The device is now ready for developer use.

Task: Configure security settings

Configuring security settings is a system administrator task for application developers. This is an optional task that you may do in order to demonstrate or test the features of the Workspace ONE software development kit (SDK).

This guide doesn't cover security settings configuration in depth. See the system administrator user guides for the Workspace ONE product for authoritative and complete information.

Default security settings are set at the organization group (OG) level. For an introduction to the OG concept, see the [Task: Configure management console enrollment](#). Security settings from the OG can be overridden for specific apps, by using a custom SDK profile.

Security settings includes data loss prevention (DLP) settings. Those will be used as an example here.

How to configure data loss prevention at the Organization Group level

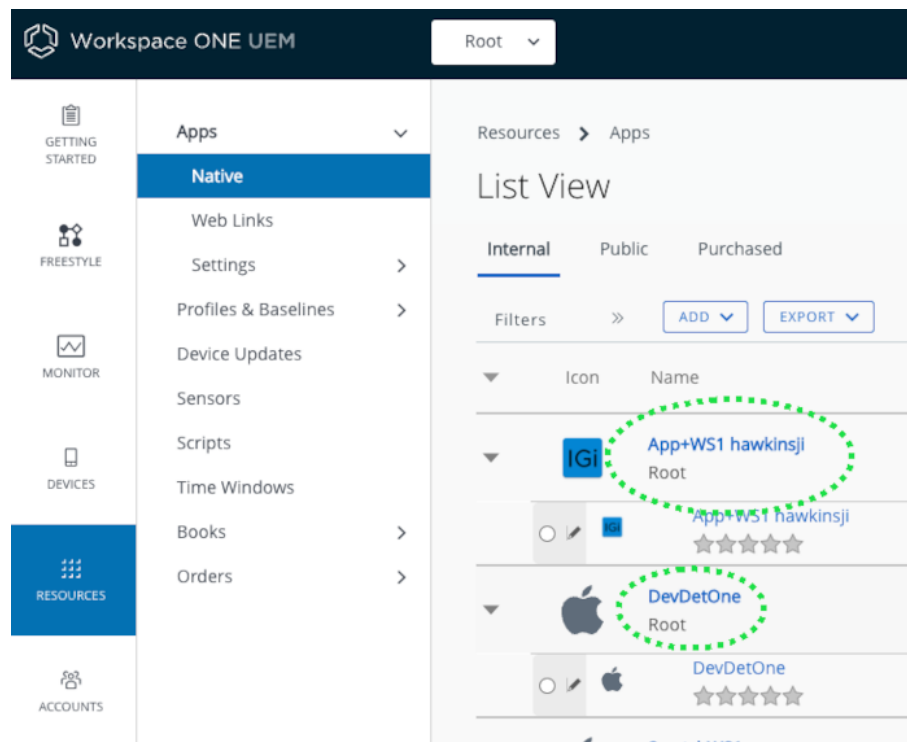
To configure DLP settings at the OG level proceed as follows.

1. Log in to the UEM and select an OG.

See the instructions [How to log in and select an Organization Group](#) if necessary.

If you are unsure which OG to select, use the one that is managing your app. You can find out the OG name by navigating to Resources (or it may be labelled Apps or Apps & Books), Apps, Native. Then select the tab on which your app appears. This will be Internal if your app APK was uploaded directly to the UEM, or Public if the APK was uploaded to your enterprise app store.

This screen capture shows how the list view might appear in the console user interface.



Screen Capture: UEM Apps list view showing managing organization groups

In this screen capture there are two apps: App+WS1 hawkinsji and DevDetOne. Both are managed by the OG: Root.

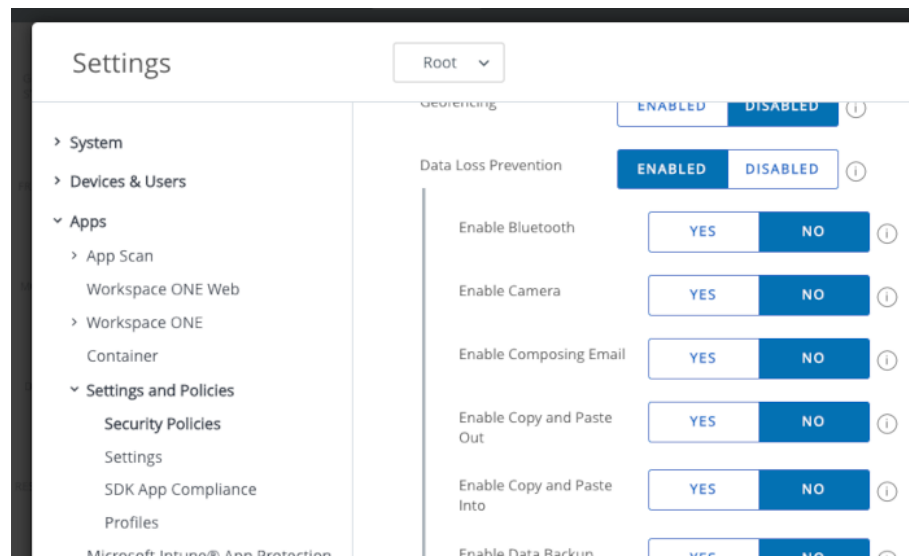
2. **Navigate to: Groups & Settings, All Settings, Apps, Settings and Policies, Security Policies.**

This opens the Security Policies configuration screen, on which a number of settings can be switched on and off, and configured.

3. **For the Data Loss Prevention setting, select Enabled.**

When Enabled is selected, further controls will be displayed.

This screen capture shows the location of the setting in the console user interface.



Screen Capture: UEM Data Loss Prevention configuration at the organization group level

4. **For actions that end users aren't allowed to do, select No.**

If you find the console user interface difficult to interpret, here's are some tips.

- To check which setting is in effect, check if the Yes or No next to the action has the same color scheme as the Enabled next to Data Loss Prevention. For example, if the Yes next to Enable Copy and Paste Out has the same color scheme as the Enabled next to Data Loss Prevention, then copy and paste out is allowed.
- Most of the individual action selectors have the opposite sense to the Data Loss Prevention (DLP) selector. DLP Enabled means that restrictions are in effect; Enable Printing Yes means that printing isn't restricted.

5. **To superimpose a watermark on the app user interface (UI), select Enable Watermark: Yes.**

UI Watermark is only supported by the SDK for Android at time of writing.

6. Select Save to commit your changes to the configuration.

This concludes DLP configuration at the OG level.

How to override data loss prevention configuration for a specific app

You can override the DLP configuration for a specific app by setting up a custom SDK profile and assigning it to the app. Proceed as follows.

1. Log in to the UEM and select an OG.

See the notes on the same step in the preceding instructions [How to configure data loss prevention at the Organization Group level](#).

2. Navigate to: Groups & Settings, All Settings, Apps, Settings and Policies, Profiles.

This opens a page that lists any SDK custom profiles that have already been created.

This screen capture shows the appearance of the Profiles page and its location in the UEM console user interface.

The screenshot displays the 'Settings' page in the UEM console. The left-hand navigation pane is expanded to 'Settings and Policies', where 'Profiles' is selected. The main content area shows the 'Profiles' page, which includes an 'ADD PROFILE' button and a table of existing profiles.

	Status	Profile Name
<input type="radio"/>	Active	Boxer-Passcode
<input type="radio"/>	Active	Boxer-Passcode
<input type="radio"/>	Active	CTK Consumer
<input type="radio"/>	Inactive	For cert installati
<input type="radio"/>	Active	IDPV certs
<input type="radio"/>	Inactive	PIV-D Certificate
<input type="radio"/>	Active	PIV-D Certificate

Screen Capture: UEM Custom SDK Profiles

3. Either select an existing profile, or select to add a profile.

If you selected to add a profile, a Select Configuration Type dialog will open.
Select: SDK Profile.

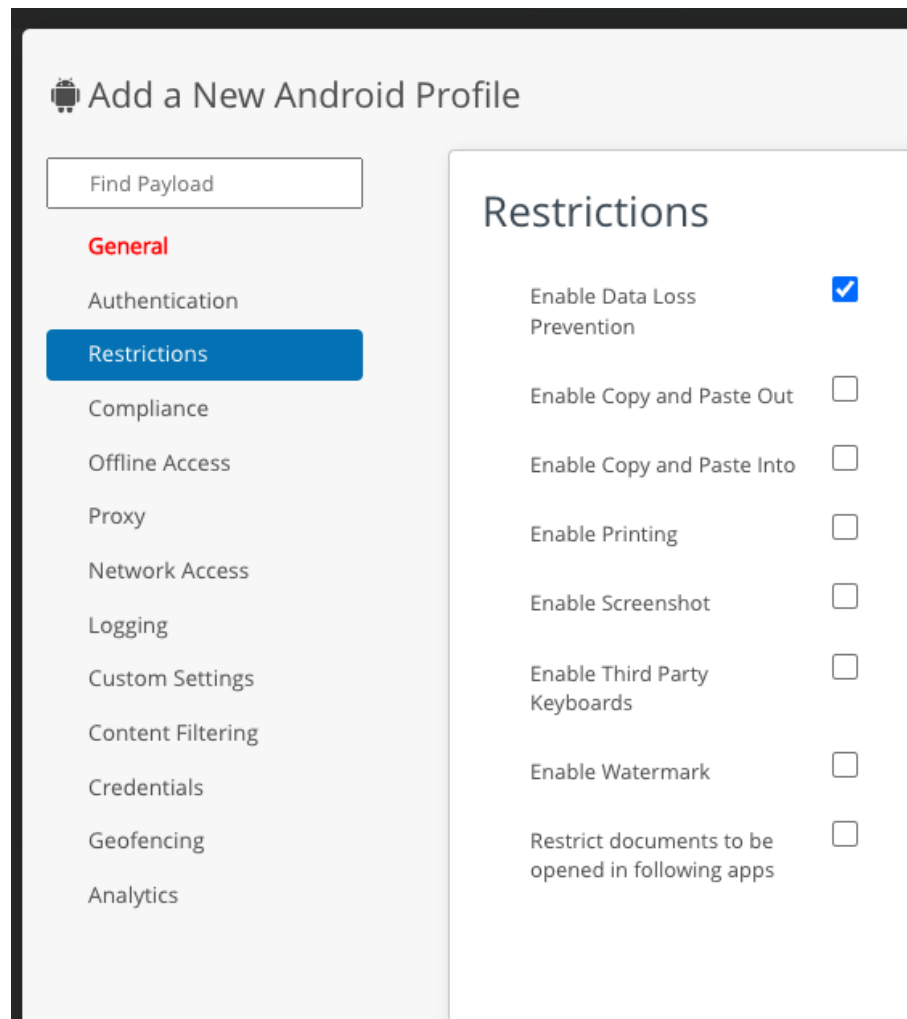
A second dialog will then open on which you have a choice of mobile operating systems, Android or Apple iOS. Select whichever your app runs on.

A page on which you can create or edit the profile will open.

4. Select the Restrictions item in the navigation panel.

If you selected to edit a profile, and the profile already had a DLP configuration, the configuration will be shown.

If you created a new profile, or if the profile you selected didn't have a DLP configuration, no configuration will be shown. Instead, there will be a Configure button. Click the button and a default configuration will be shown.



Screen Capture: UEM Custom SDK Profile Restrictions

5. Configure the allowed and disallowed end user actions.
6. Click Save to create the new profile, or to save your changes to the existing profile.

If you selected to create a new profile, you will have to give it a name before you can save.

Make a note of the name of the profile that you created or edited.

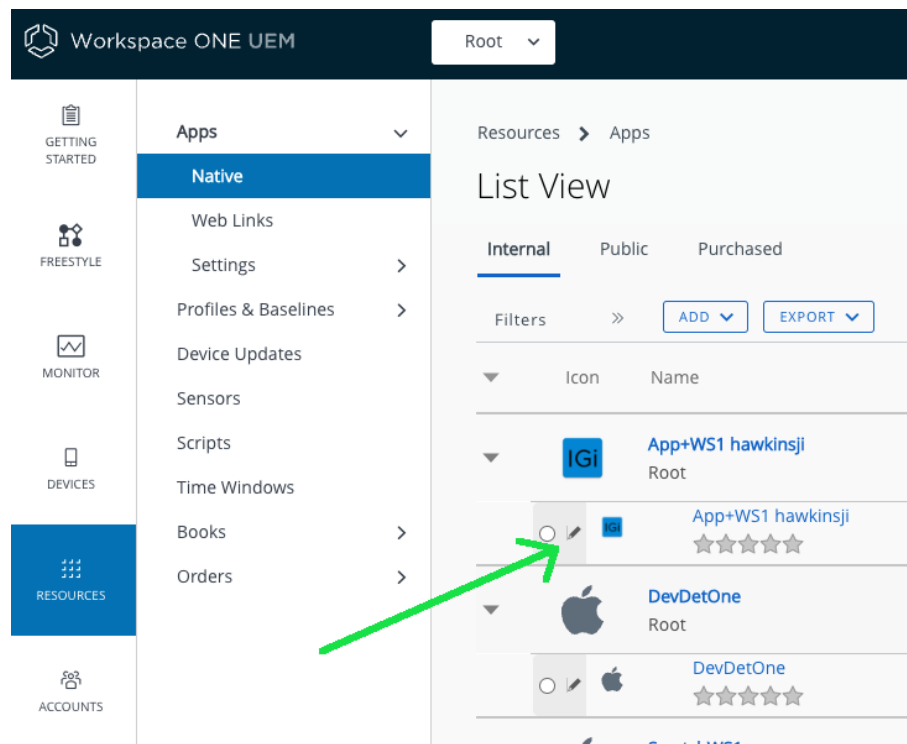
7. Close the Profiles page by clicking the X in the top left corner.
8. Open the app list.

Navigate to Resources (or it may be labelled Apps or Apps & Books), Apps, Native. Then select the tab on which your app appears. This will be Internal if your app APK was uploaded directly to the UEM, or Public if the APK was uploaded to your enterprise app store.

This opens a table view in which each row is either an app or an app version.

9. Open the details of your app's configuration.

Click on the pencil icon next to the version of your app. This screen capture shows the location in the UEM console user interface.

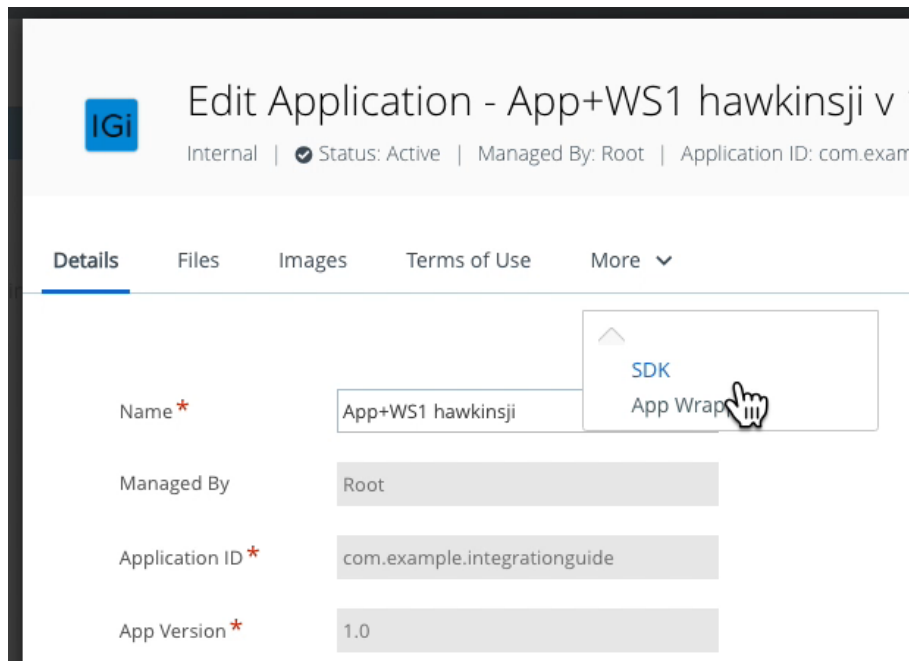


Screen Capture: UEM Edit App Configuration

This opens an Edit Application dialog.

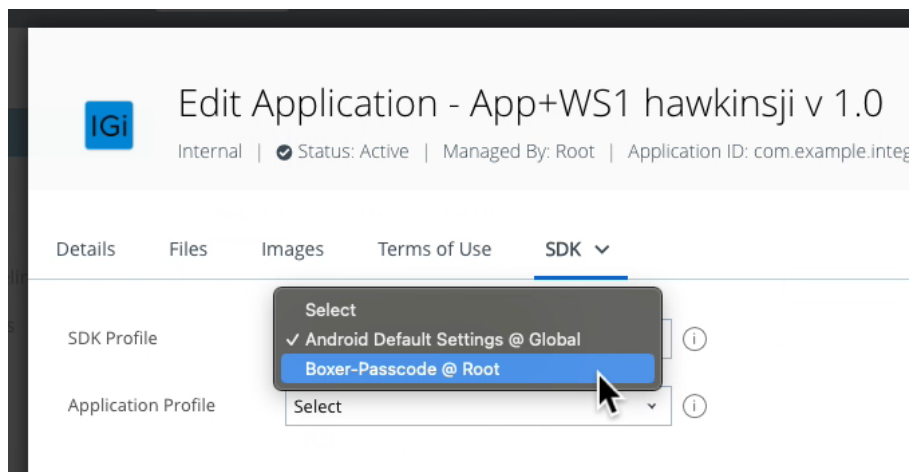
10. Set the app to use the custom SDK profile.

Select the More drop-down in the Edit Application dialog, and then the SDK menu item, as shown in this screen capture.



Screen Capture: UEM Configure App select SDK tab

In the SDK Profile drop-down that appears, select the custom SDK profile that you created or edited earlier.



Screen Capture: UEM Configure App set SDK custom profile

In that screen capture the custom SDK profile being selected is: Boxer-Passcode.

11. Finalise the SDK profile setting.

Click Save & Assign on the Edit Application dialog, then click Save on the assignment dialog, then click Publish on the preview dialog.

The app version screen will open, on the Assignment tab.

This concludes overriding data loss prevention configuration for a specific app.

Next Steps

Test the DLP settings in your app, or in one of the sample apps from the Open Source repository.

Troubleshooting

In case of difficulties, check these troubleshooting tips.

Security Code

You might be prompted to enter a security code to complete a destructive action, such as deleting an uploaded app. The default security code for a UEM hosted by the TestDrive service is 1234.

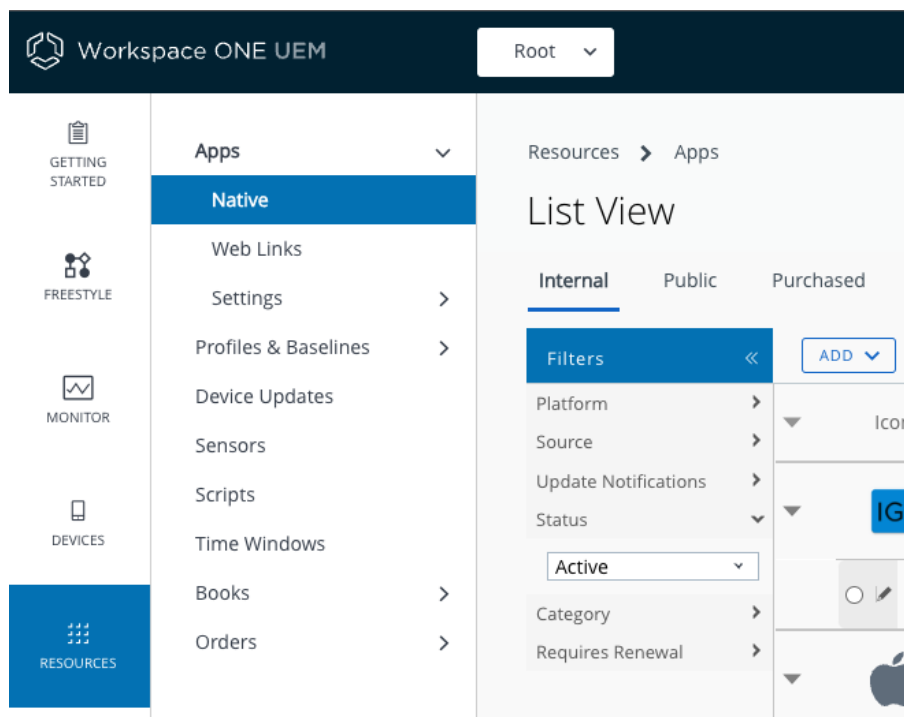
Apps missing from list view

You might find that an app you expect to see in a list view in the UEM doesn't appear. This could be due to an implicit filter.

You can check what filters have been applied to the current list view, as follows.

1. Look for the word **Filters** in the row of controls just above the column headings. Next to **Filters** will be a double chevron, **>>**, indicating expandability. Click to expand the **Filters**.
2. Check the filters in the expanded list. A common cause of missing items is the **Status** filter. Expand it and check if only active apps are included, for example.

This screen capture shows the expanded controls.



Screen Capture: UEM Filters expanded

If you, for example, set the Status filter to All then the expected app might appear.

Appendix: How to enroll an app in standalone mode

Enrolling an app in standalone mode isn't a common task for application developers but is convenient to include here. The instructions in this guide could also be used to set up a demonstration or laboratory environment in which standalone enrollment could play a part.

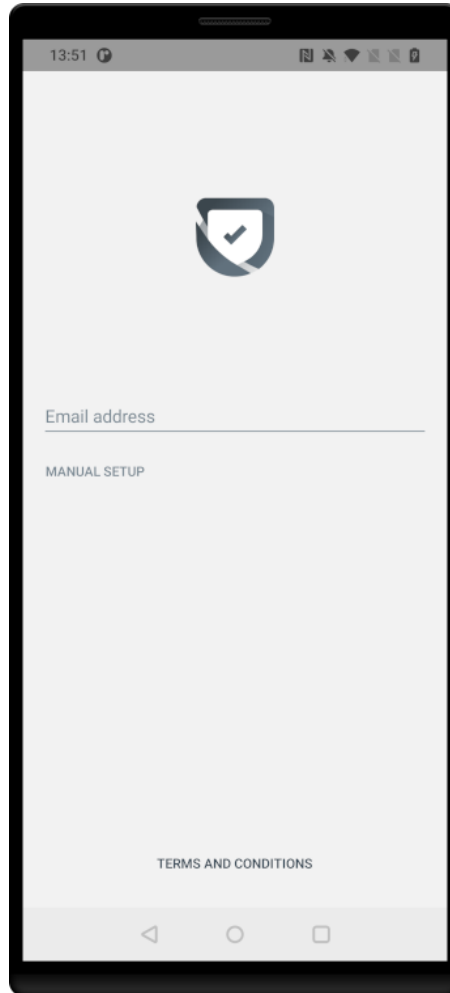
Standalone enrollment is supported by the Workspace ONE Boxer email app, the Workspace ONE Web browser, Workspace ONE PIV-D Manager, and other apps in the VMware productivity suite. However, these apps won't enroll standalone if Workspace ONE Intelligent Hub is already installed on the device.

These instructions refer to some concepts introduced in the [Task: Configure management console enrollment](#), and assume that the [Recommended Organization Group Structure](#) has been configured in the UEM. Some steps will be different if that isn't the case.

Proceed as follows.

1. Install the mobile app, for example from the Google Play Store, and launch it.

The screen will show the app logo and a prompt for email address, as in the following screen capture.



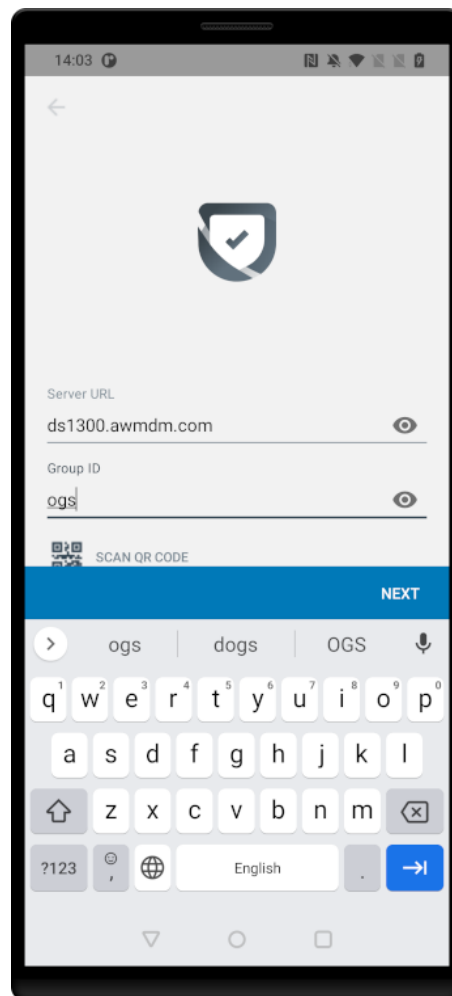
Screen Capture: App logo and prompt

2. Select the Manual Setup option. You will now be prompted for the Server URL and Organization Group ID. Enter the enrollment server address and the Group ID of the standalone OG.

See the instructions [How to find out the enrollment server address](#) if necessary.

In the [Recommended Organization Group Structure](#) the Group ID is: ogs

This screen capture shows the user interface with filled-in values.



Screen Capture: Server and OG prompt

3. Tap Next.

There will be some processing and you will be prompted for a Username and Password.

4. **Enter the username and password of an end user account and tap Next.**

If the [Recommended End User Configuration](#) has been set up then the username and password could both be: a

There will be some more processing.

When enrollment processing has finished, you will be prompted to accept a privacy agreement.

5. **Accept the privacy agreement by tapping: I Understand.**

You will be prompted to opt in to additional data sharing.

6. **Select “Not Now” and confirm by tapping “Don’t Send” when prompted.**

There will be some more processing.

The app has now been enrolled in standalone mode and is ready for use.

Document Information

Published Locations

This document is available

- in Markdown format, in the repository that also holds the sample code:
<https://github.com/vmware-samples/...UEMSysAdminForAppDevs/>
- in Portable Document Format (PDF), on the VMware website:
<https://developer.vmware.com/...UEMSysAdminForAppDevs.pdf>

Revision History

09nov2022 First publication.

Legal

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2022 VMware, Inc. All rights reserved.
This content is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <https://www.vmware.com/go/patents>.
VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.
The Workspace ONE Software Development Kit integration samples are licensed under a two-clause BSD license.
SPDX-License-Identifier: BSD-2-Clause