

# Citrix Endpoint Management Knox Platform for Enterprise

October 2020  
Samsung R&D Centre UK  
(SRUK)

1. Pre-requisites for Knox Platform for Enterprise
2. Managed Google Play [MGP] Configuration
3. Android Enterprise Deployment Modes
  - Work Profile
  - Fully Managed Device
  - Dedicated Device
  - Fully Managed Device with a Work Profile
4. Android Enterprise configuration
5. Work Profile enrollment flow
6. Fully Managed enrollment flow
7. Fully Managed Device with a Work Profile enrollment flow
8. Dedicated Device configuration
9. Configure Knox Service Plugin [KSP] Standard and Premium

## Contacts:

[sruk.rtam@samsung.com](mailto:sruk.rtam@samsung.com)

## Knowledge Base:

<https://www.citrix.com/support/>

1. Obtain access to Endpoint Management console
2. A Gmail account to map to Endpoint Management for Managed Google Play
3. Consider what enrollment method to use:
  - Knox Mobile Enrollment (KME)
  - QR Code enrollment
  - Email enrollment
  - Server details enrollment

# Configure Android Enterprise

- Within the Endpoint Management console, select the cog icon in the top right corner
- Select Android Enterprise
- Select Connect

The screenshot displays the Citrix Endpoint Management console interface. At the top, a green navigation bar contains the tabs 'Analyze', 'Manage', 'Configure', and 'Monitor'. On the right side of this bar, there are three icons: a cloud, a gear (highlighted with a red box), and a key. The main content area is divided into three columns. The left column, titled 'Settings', includes sections for 'Authentication' (with 'Derived Credentials for iOS' and 'Identity Provider (IDP)'), 'Certificate Management' (with 'Certificates', 'Credential Providers', and 'PKI Entities'), and 'Client' (with 'Client Branding', 'Client Properties', and 'Client Support'). The middle column, titled 'Platforms', lists 'Alexa for Business', 'Android Enterprise' (highlighted with a red box), 'Android SafetyNet', 'Apple Configuration', 'Apple Deployment', and 'Google Chrome'. The right column, titled 'Frequently Accessed Items', lists 'Android Enterprise', 'Enrollment', 'Certificates', 'Identity Provider (IDP)', and 'Release Management'. Below the 'Platforms' section, a modal window titled 'Android Enterprise' is open. It contains the text: 'To set up Android Enterprise for your company, bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.' Below this is an information icon and a note: 'If you're a G Suite customer, it's recommended to use legacy Android Enterprise settings to manage Android. Click on ▼ to switch back.' At the bottom of the modal, there is a section titled 'We are taking you out to Google Play to register Citrix as your EMM provider' with the subtext: 'When you click Connect, a window opens. If a window doesn't open, check your pop-up settings. Sign in to Google Play with your corporate Google ID. Enter your organization name and confirm that Citrix is your EMM provider.' A green 'Connect' button (highlighted with a red box) is located at the bottom right of the modal.

Settings

Authentication

Derived Credentials for iOS

Identity Provider (IDP)

Certificate Management

Certificates

Credential Providers

PKI Entities

Client

Client Branding

Client Properties

Client Support

Notifications

Carrier SMS Gateway

Notification Server

Notification Templates

Platforms

Alexa for Business

Android Enterprise

Android SafetyNet

Apple Configuration

Apple Deployment

Google Chrome

Server

ActiveSync Gateway

Citrix Gateway

Cloud Connector Allow List

Endpoint Management Tools

Enrollment

Firebase Cloud Messaging

LDAP

Frequently Accessed Items

Android Enterprise

Enrollment

Certificates

Identity Provider (IDP)

Release Management

**Android Enterprise** ▼

To set up Android Enterprise for your company, bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

*If you're a G Suite customer, it's recommended to use legacy Android Enterprise settings to manage Android. Click on ▼ to switch back.*

**We are taking you out to Google Play to register Citrix as your EMM provider**

When you click Connect, a window opens. If a window doesn't open, check your pop-up settings.

Sign in to Google Play with your corporate Google ID. Enter your organization name and confirm that Citrix is your EMM provider.

**Connect**

# Configure Android Enterprise

- Sign in with your Google Account and select **Get started**
- Enter a Business name, select **Next**
- Data Protection Officer and EU Representative are optional, select **Confirm**
- Select **Complete Registration**

The image displays a sequence of four screenshots from the Android Enterprise configuration process, with key buttons highlighted by red boxes:

- Screen 1: Bring Android to Work**  
The 'Get started' button is highlighted.
- Screen 2: Business name**  
The 'Next' button is highlighted.
- Screen 3: Data Protection Officer and EU Representative**  
The 'Confirm' button is highlighted.
- Screen 4: Set up complete**  
The 'Complete Registration' button is highlighted.

# Android Enterprise Deployment Modes

## Deployment Modes

Android Enterprise can be deployed in the following 4 deployment modes

1. Work Profile [*formerly known as Profile Owner*]
2. Fully Managed Device [*formerly known as Device Owner*]
3. Fully Managed Device with a Work Profile [*formerly known as COMP*]
4. Dedicated device [*formerly known as COSU*]

Citrix Endpoint Management can support all of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in Citrix Endpoint Management for your device fleet.



# Work Profile Configuration

In order to enroll with Work Profile, you should create an enrollment profile.

- Within Endpoint Management navigate to: Configure, Enrollment Profiles, select Add
- Enter a Enrollment profile name of your choice, select Next
- For Management, select Android Enterprise
- For Device owner mode, select None - BYOD work profile will automatically turn on
- Select Next

The image displays three sequential screenshots of the Citrix Cloud Endpoint Management interface, illustrating the steps to create an enrollment profile.

**Screenshot 1: Enrollment Profiles**  
The interface shows the 'Configure' tab selected. Under 'Enrollment Profiles', the 'Add' button (represented by a plus icon) is highlighted with a red box.

**Screenshot 2: Enrollment Info**  
The 'Enrollment Profile' section is active. The 'Enrollment profile name' field is highlighted with a red box. The 'Total number of devices a user can enroll' is set to 'unlimited'. A 'Next >' button is highlighted with a red box.

**Screenshot 3: Enrollment Configuration**  
The 'Enrollment Configuration' screen is shown. Under 'Device management', 'Management' is set to 'Android Enterprise' (highlighted with a red box). Under 'Device owner mode', 'None' is selected (highlighted with a red box). The 'BYOD work profile' toggle is turned 'On'. Under 'Application management', 'Citrix MAM' is turned 'On'. Under 'User consent', 'Allow users to decline device management' is turned 'On'. A 'Next >' button is highlighted with a red box.



# Work Profile Configuration

- For iOS, Application management and User consent are optional, select Next
- For Windows, Device Management, User consent and Workspace integration are optional, select Next
- Select a Delivery Group and select Save

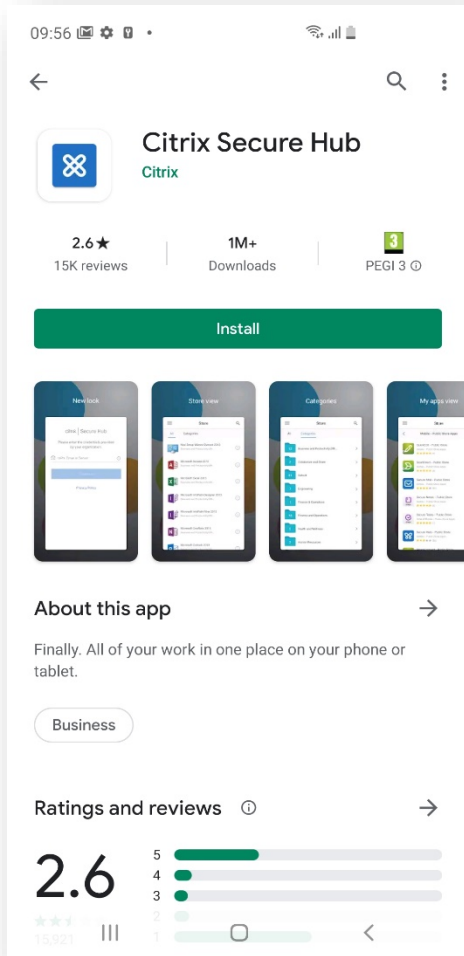
The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the steps to configure a Work Profile.

**Screenshot 1 (Top Left):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Enrollment Profile' list on the left has 'iOS' selected. The 'Enrollment Configuration' section shows 'Device management' with 'Apple Device enrollment' selected, 'Application management' with 'Citrix MAM' selected, and 'User consent' with 'Allow users to decline device management' selected. The 'Next >' button is highlighted with a red box.

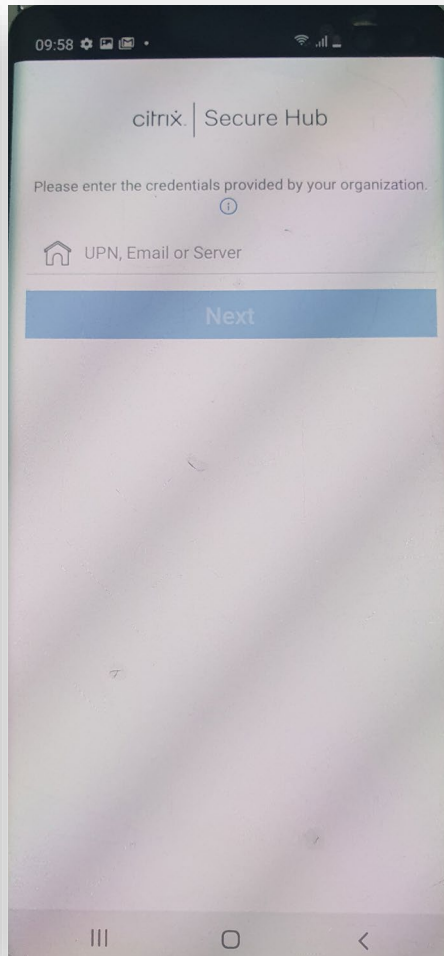
**Screenshot 2 (Top Right):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Enrollment Profile' list on the left has 'Windows' selected. The 'Enrollment Configuration' section shows 'Device management' with 'Fully managed' selected, 'User consent' with 'Allow users to decline device management' selected, and 'Workspace integration' with 'Enrollment through Workspace app' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 3 (Bottom):** Shows the 'Delivery Group Assignment' page. The 'Enrollment Profile' list on the left has '3 Assignment (optional)' selected. The 'Delivery Group Assignment' section shows 'Choose delivery groups' with a search bar and a list of delivery groups. 'TestUser' is selected, and the 'Save' button is highlighted with a red box.

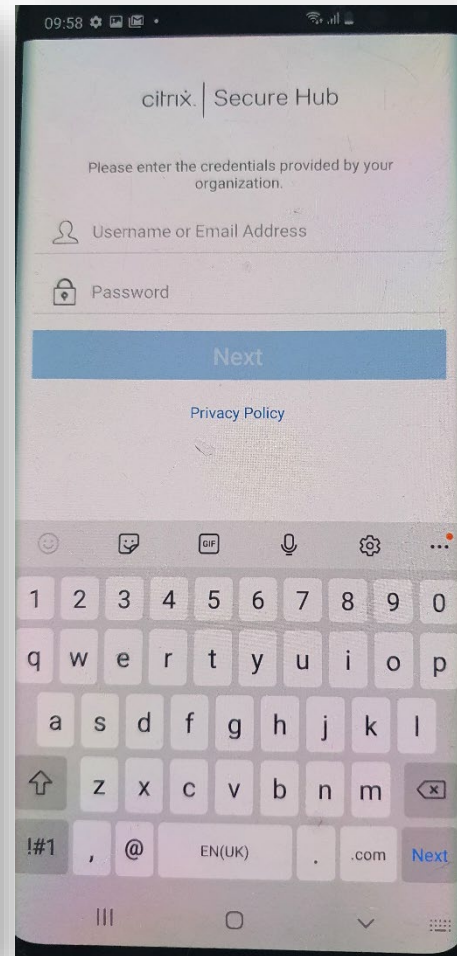
# Android Enterprise: Work Profile Enrollment



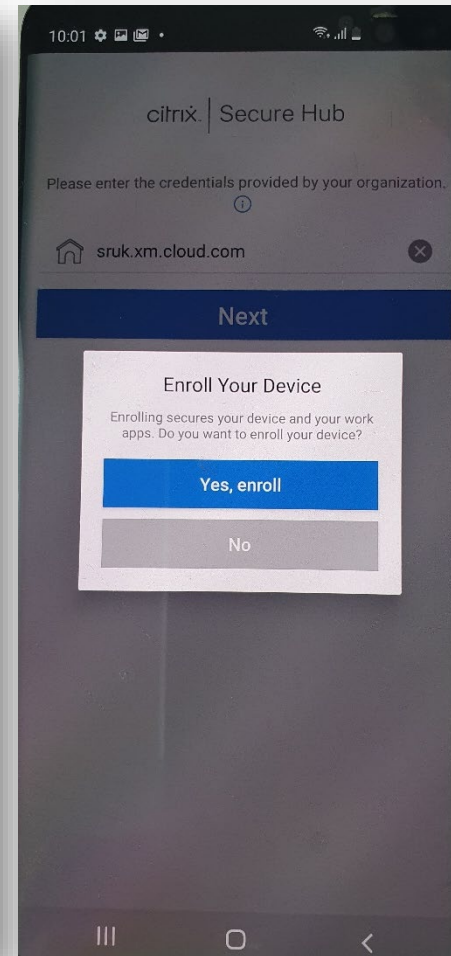
Install Citrix Secure Hub  
From the Google Play Store



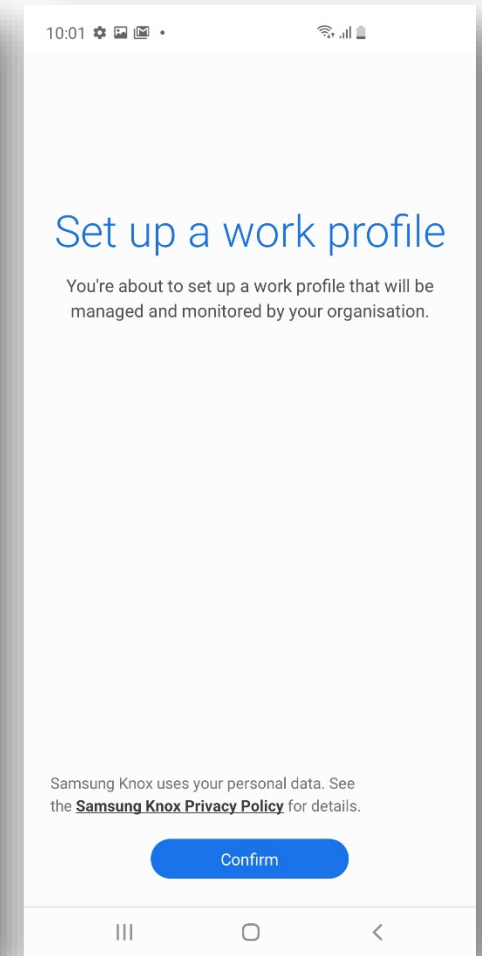
Open Secure Hub and enter  
Your Citrix Endpoint Management  
Server URL



Enter your Citrix credentials  
and select Next



Yes, enroll

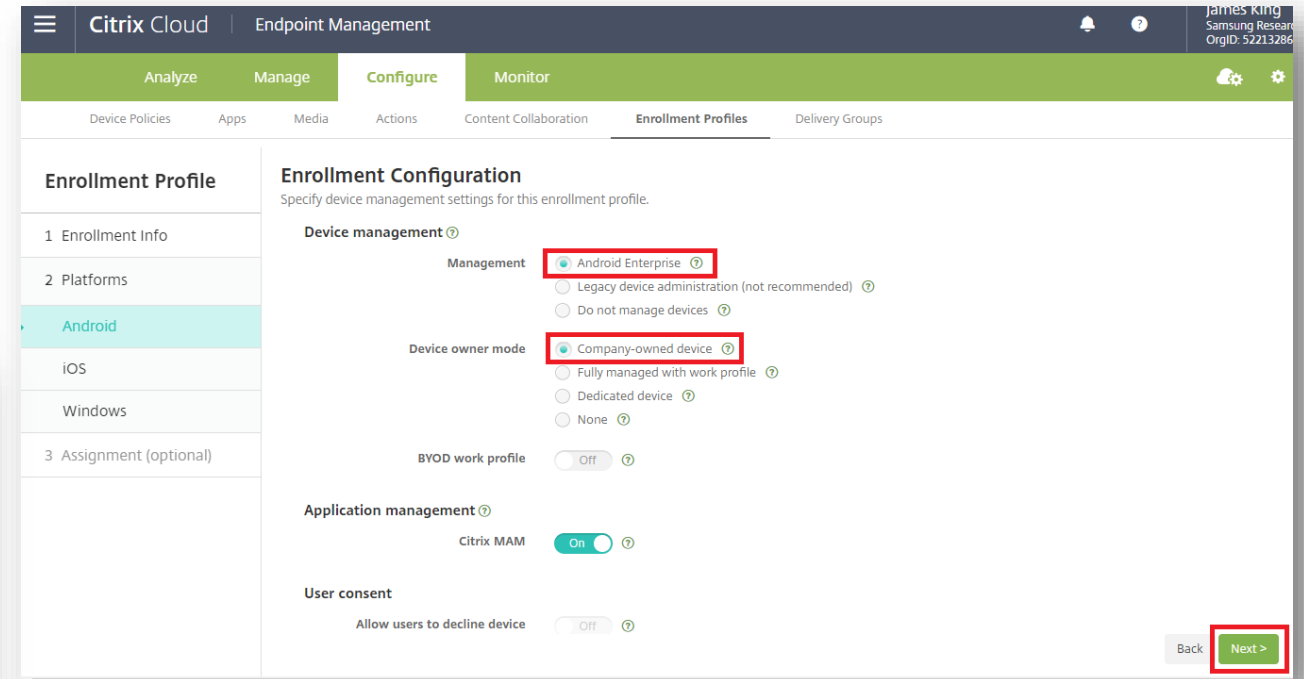
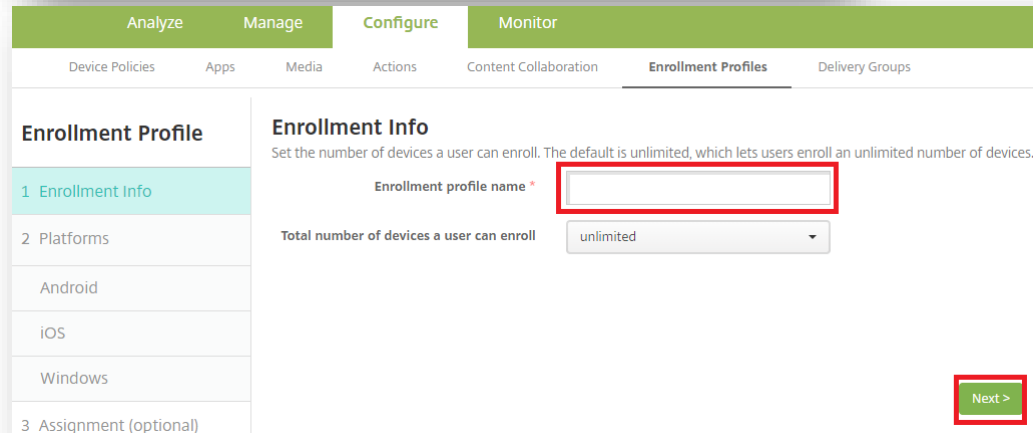
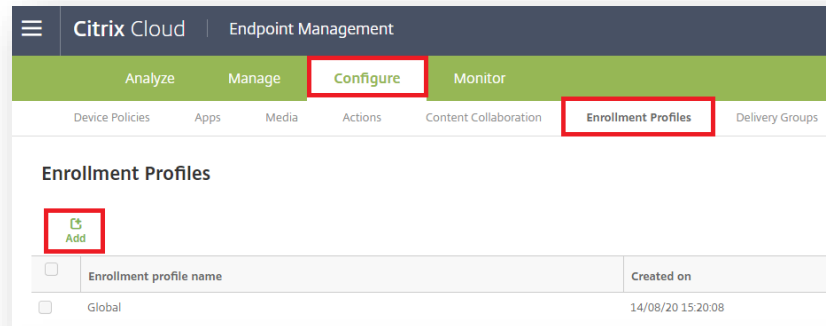


Confirm

# Fully Managed Device Configuration

**In order to enroll a Fully Managed device, you should create an enrollment profile.**

- Within Endpoint Management navigate to: Configure, Enrollment Profiles, select Add
- Enter a Enrollment profile name of your choice, select Next
- For Management, select Android Enterprise
- For Device owner mode, select Company-owned device
- Select Next



# Fully Managed Device Configuration

- For iOS, Application management and User consent are optional, select Next
- For Windows, Device Management, User consent and Workspace integration are optional, select Next
- Select a Delivery Group and select Save

The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the steps to configure a Fully Managed Device.

**Screenshot 1 (Top Left):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Device management' section has 'Apple Device enrollment' selected. The 'Application management' section has 'Citrix MAM' selected. The 'User consent' section has 'Allow users to decline device management' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 2 (Top Right):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Device management' section has 'Fully managed' selected. The 'User consent' section has 'Allow users to decline device management' selected. The 'Workspace integration' section has 'Enrollment through Workspace app' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 3 (Bottom):** Shows the 'Delivery Group Assignment' page. The 'Choose delivery groups' section has 'TestUser' selected. The 'Delivery groups to receive app assignment' section shows 'TestUser'. The 'Save' button is highlighted with a red box.

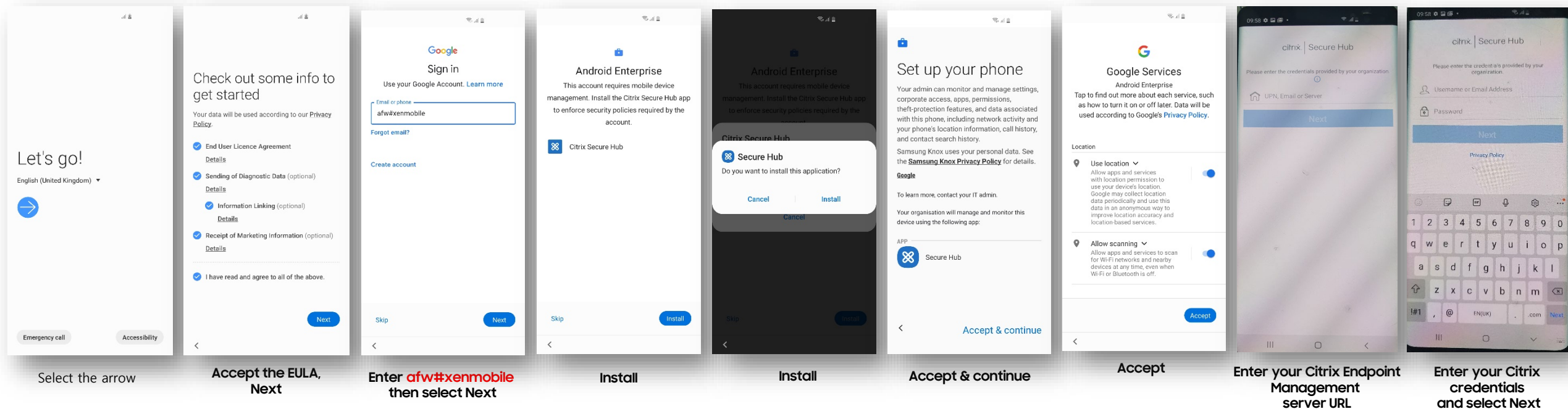
# Android Enterprise: Fully Managed Enrollment

## Android Enterprise Company-owned Device Deployment

To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Company-owned device.

1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

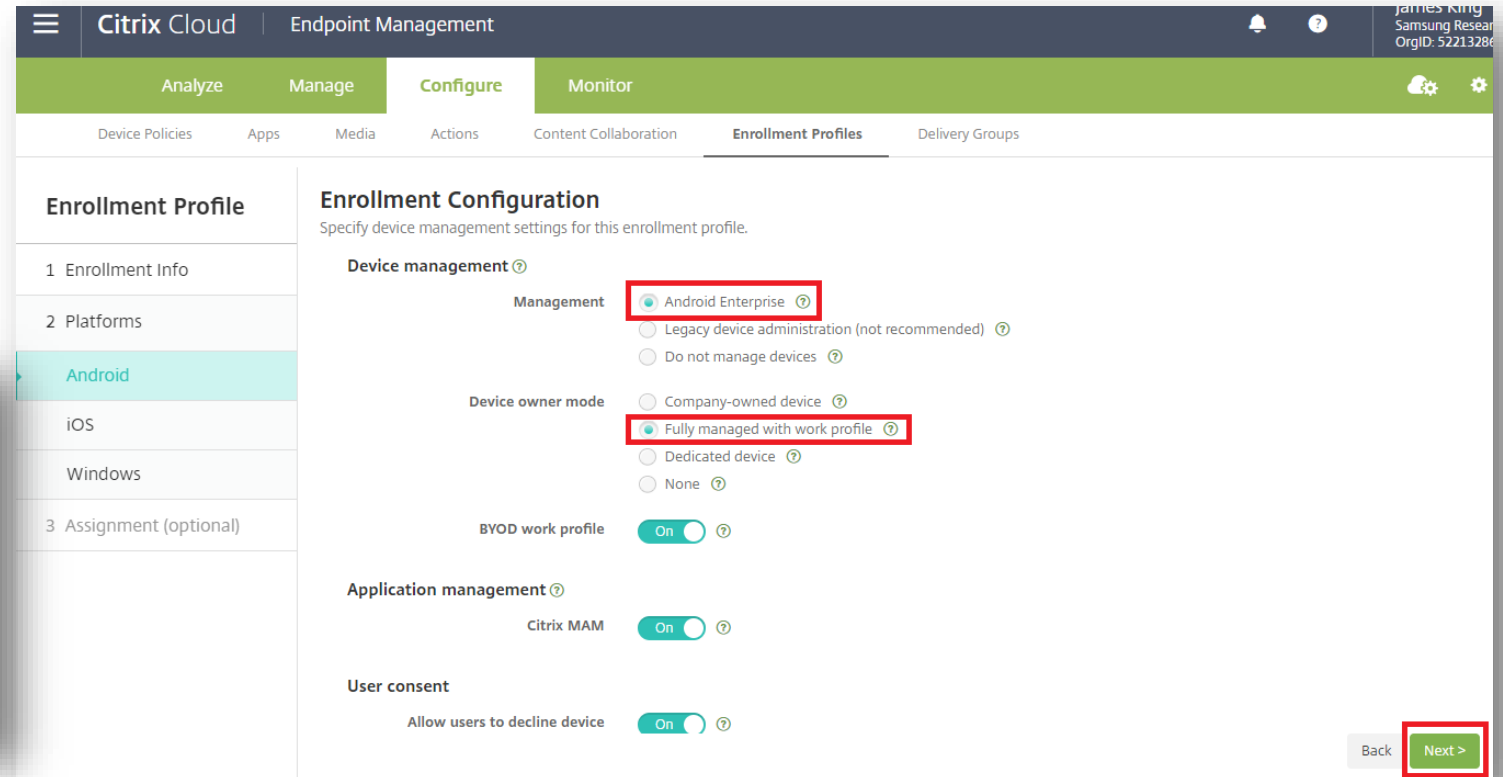
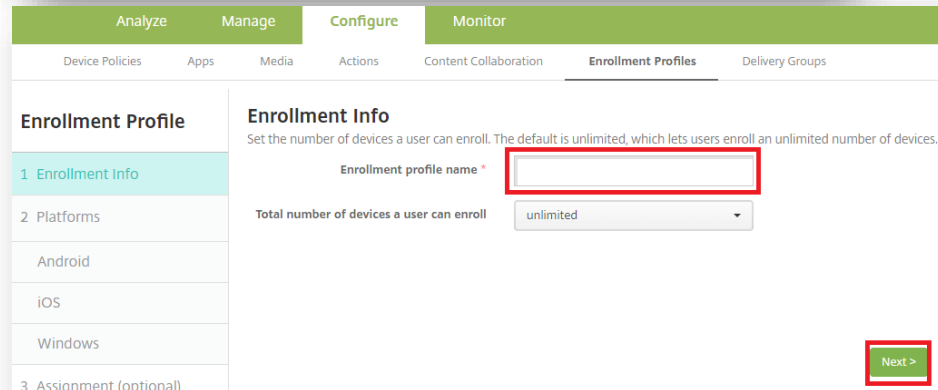
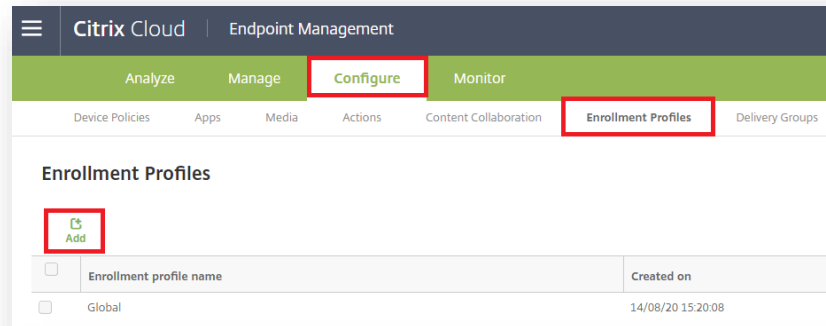
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



# Fully Managed with a Work Profile Configuration

In order to enroll Fully Managed with a Work Profile, you should create an enrollment profile.

- Within Endpoint Management navigate to: Configure, Enrollment Profiles, select Add
- Enter a Enrollment profile name of your choice, select Next
- For Management, select Android Enterprise
- For Device owner mode, select Fully Managed with Work Profile
- Select Next



# Fully Managed with a Work Profile Configuration

- For iOS, Application management and User consent are optional, select Next
- For Windows, Device Management, User consent and Workspace integration are optional, select Next
- Select a Delivery Group and select Save

The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the steps to configure a Work Profile.

**Screenshot 1: Enrollment Configuration (iOS)**

The console shows the 'Enrollment Configuration' page for an iOS profile. The 'Device management' section has 'Apple Device enrollment' selected. The 'Application management' section has 'Citrix MAM' selected. The 'User consent' section has 'Allow users to decline device management' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 2: Enrollment Configuration (Windows)**

The console shows the 'Enrollment Configuration' page for a Windows profile. The 'Device management' section has 'Fully managed' selected. The 'User consent' section has 'Allow users to decline device management' selected. The 'Workspace integration' section has 'Enrollment through Workspace app' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 3: Delivery Group Assignment**

The console shows the 'Delivery Group Assignment' page. The 'Choose delivery groups' section has 'TestUser' selected. The 'Delivery groups to receive app assignment' section shows 'TestUser'. The 'Save' button is highlighted with a red box.

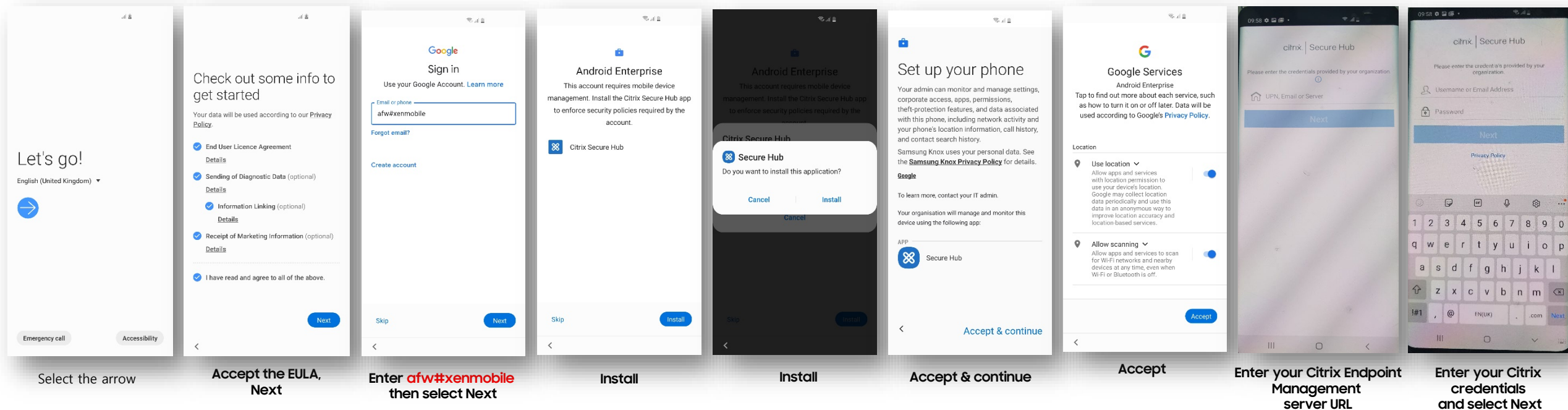


# Android Enterprise: Fully Managed with a Work Profile Enrollment

To enroll your device as an Android Enterprise Fully Managed with a Work Profile, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Fully Managed with a Work Profile.

1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.

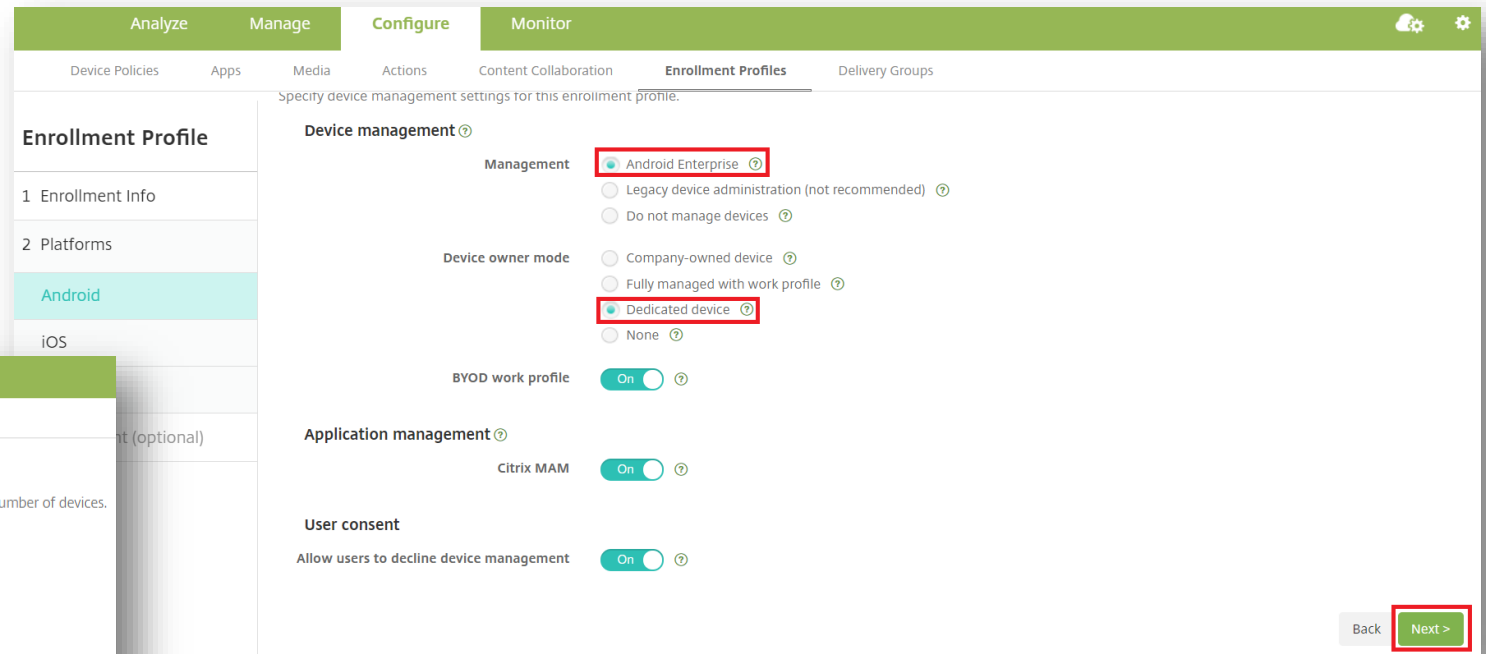
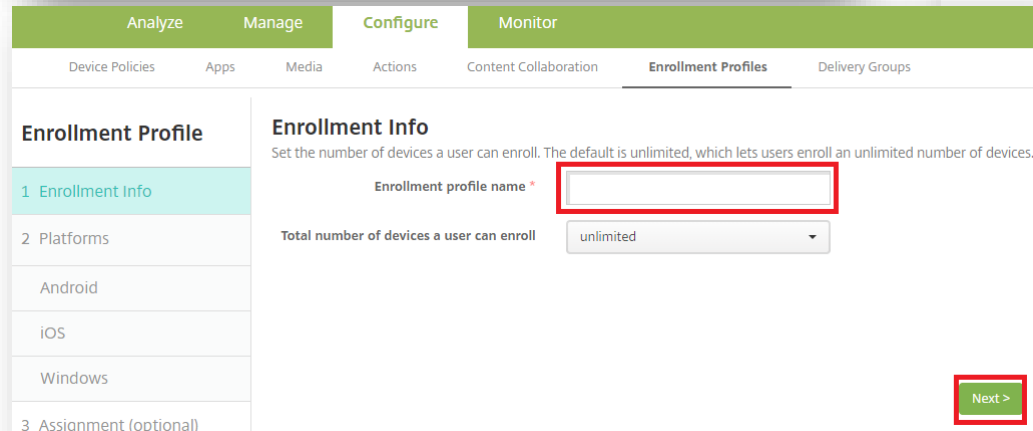
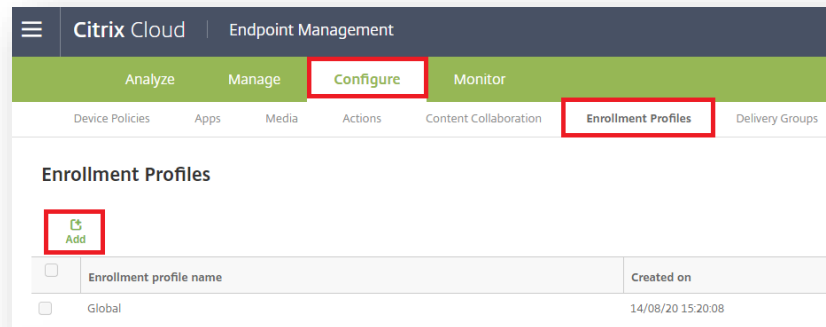




# Dedicated Device Configuration

In order to enroll a Dedicated device, you should create an enrollment profile.

- **Within Endpoint Management navigate to: Configure, Enrollment Profiles, select Add**
- **Enter a Enrollment profile name of your choice, select Next**
- **For Management, select Android Enterprise**
- **For Device owner mode, select Dedicated device**
- **Select Next**



# Dedicated Device Configuration

- For iOS, Application management and User consent are optional, select Next
- For Windows, Device Management, User consent and Workspace integration are optional, select Next
- Select a Delivery Group and select Save

The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the steps to configure an enrollment profile.

**Screenshot 1 (Top Left):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Enrollment Profile' sidebar on the left has 'iOS' selected under '2 Platforms'. The 'Enrollment Configuration' section shows 'Device management' with 'Apple Device enrollment' selected, 'Application management' with 'Citrix MAM' selected, and 'User consent' with 'Allow users to decline device management' selected. The 'Next >' button is highlighted with a red box.

**Screenshot 2 (Top Right):** Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Enrollment Profile' sidebar on the left has 'Windows' selected under '2 Platforms'. The 'Enrollment Configuration' section shows 'Device management' with 'Fully managed' selected, 'User consent' with 'Allow users to decline device management' selected, and 'Workspace integration' with 'Enrollment through Workspace app' selected. The 'Next >' button is highlighted with a red box.

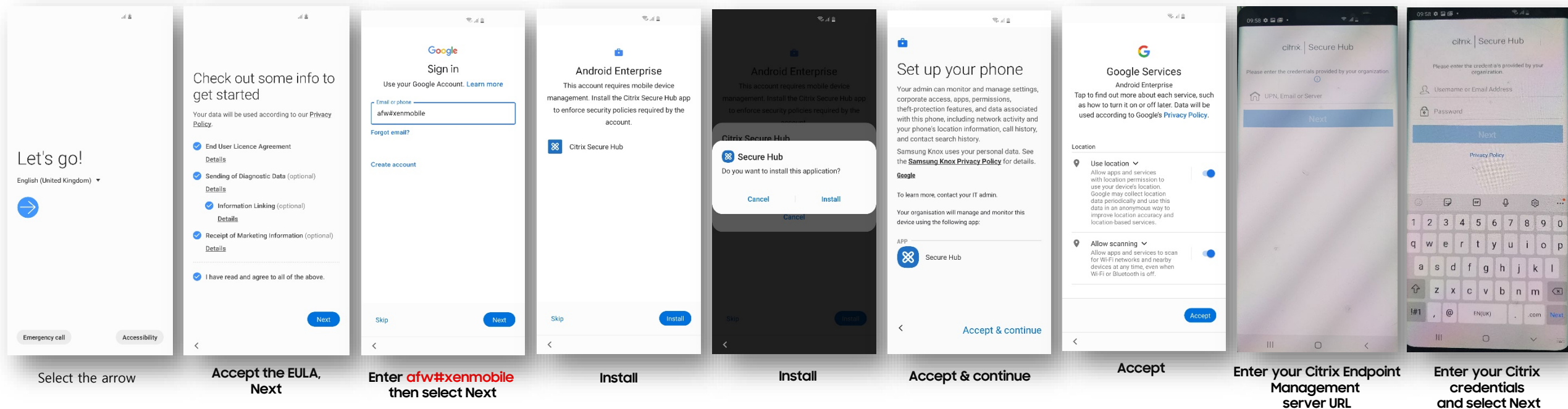
**Screenshot 3 (Bottom):** Shows the 'Delivery Group Assignment' page. The 'Enrollment Profile' sidebar on the left has '3 Assignment (optional)' selected. The 'Delivery Group Assignment' section shows 'Choose delivery groups' with a search bar and a list of delivery groups. 'TestUser' is selected with a red box. The 'Save' button is highlighted with a red box.

# Android Enterprise: Dedicated Device Enrollment

To enroll your device as an Android Enterprise Dedicated device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Dedicated device.

1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



The Knox Platform for Enterprise solution provides a robust set of features on top of the core Android Enterprise platform, to fill security and management gaps and meet the strict requirements of highly regulated industries.

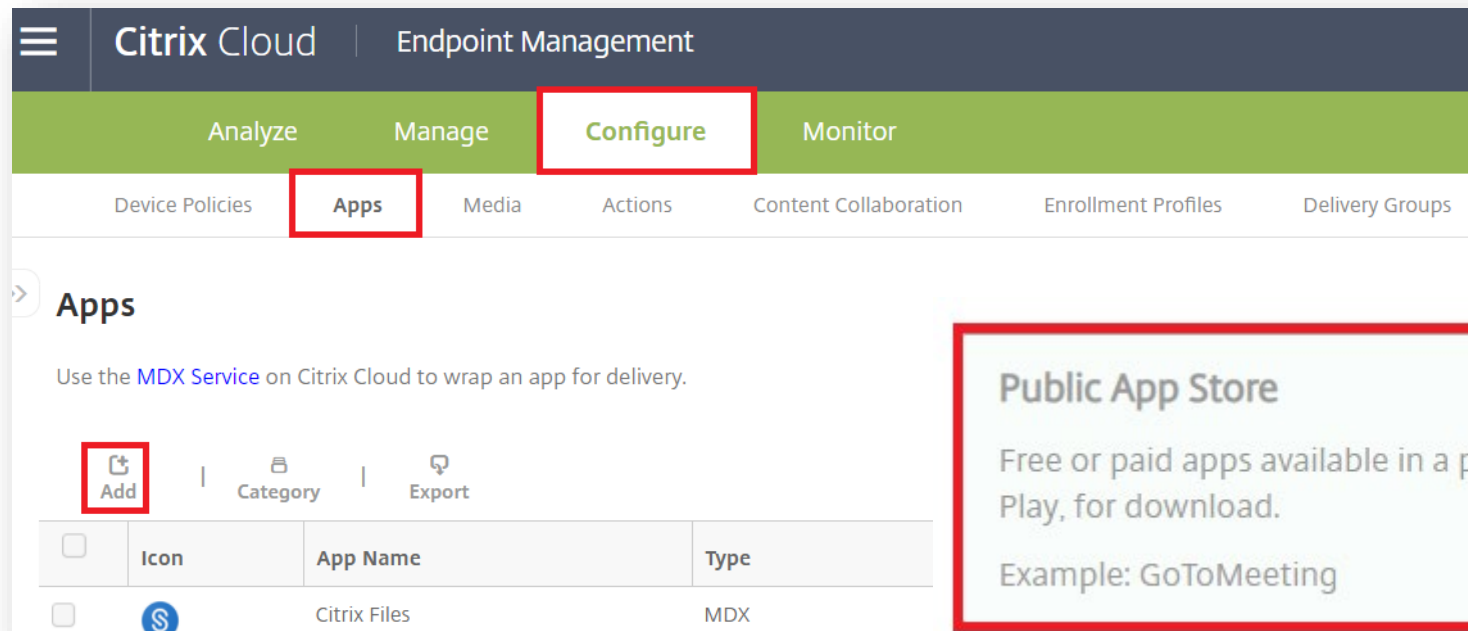
The Knox Platform for Enterprise solution comes in a two tiered offering:

- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [\$]

Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise on Android 8.0 or above.



- Within Endpoint Management Console, navigate to: Configure, Apps
- Select Add, then select Public App Store



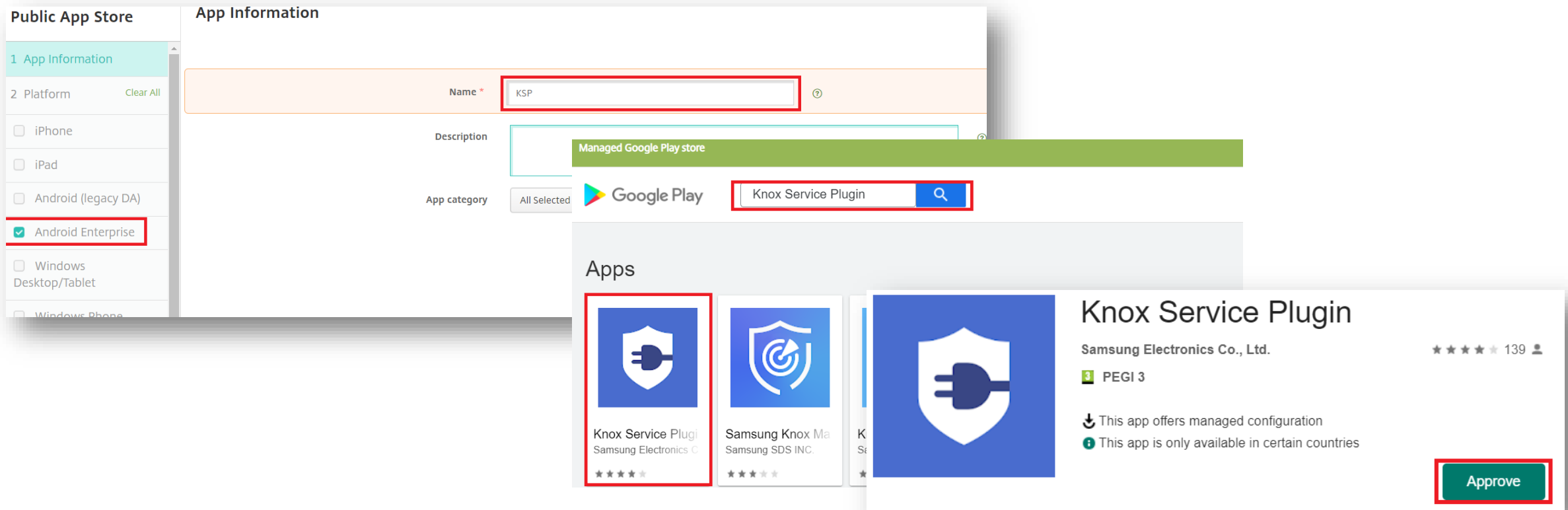
## Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

# Configure Knox Platform for Enterprise using Knox Service Plugin

- Enter a Name of your choice
- Tick only Android Enterprise on the left column
- Select Next
- Search for and Approve the Knox Service Plugin



**Public App Store**

1 App Information

2 Platform [Clear All](#)

☐ iPhone

☐ iPad

☐ Android (legacy DA)

☒ Android Enterprise

☐ Windows Desktop/Tablet

☐ Windows Phone

**App Information**

Name \*

Description

App category

**Apps**

**Knox Service Plugin**

Samsung Electronics Co., Ltd. ★★★★★ 139

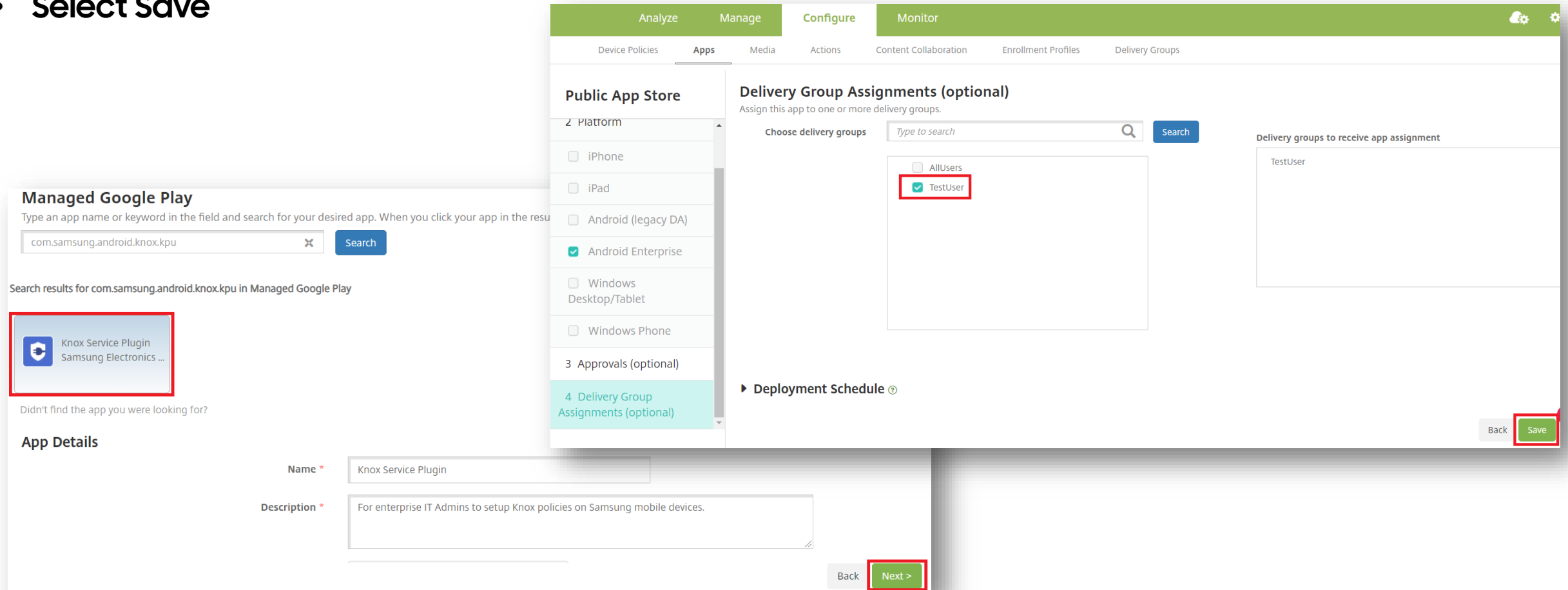
1 PEGI 3

↓ This app offers managed configuration

ⓘ This app is only available in certain countries

# Configure Knox Platform for Enterprise using Knox Service Plugin

- Select Knox Service Plugin
- Select Next
- Select a Delivery Group of your Choice
- Select Save



The screenshot displays the Knox Platform configuration interface, specifically the 'Managed Google Play' section. The interface is divided into several panels:

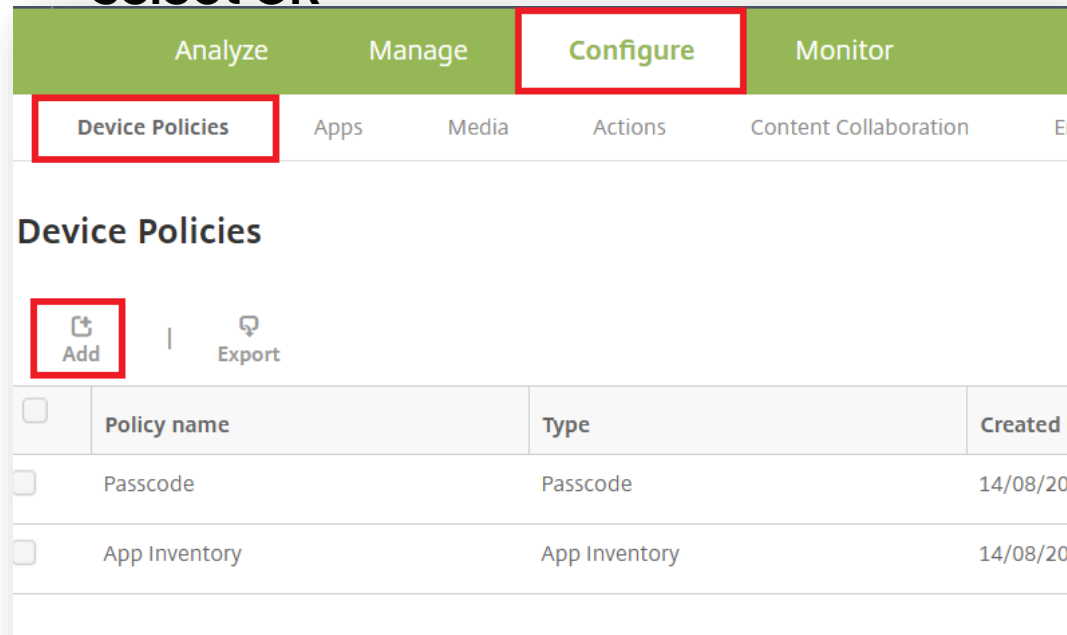
- Managed Google Play:** A search bar contains the text 'com.samsung.android.knox.kpu'. Below the search bar, the search results for 'com.samsung.android.knox.kpu' in Managed Google Play are shown. The first result, 'Knox Service Plugin' by Samsung Electronics, is highlighted with a red box.
- App Details:** A form for entering app details. The 'Name' field is filled with 'Knox Service Plugin'. The 'Description' field contains the text 'For enterprise IT Admins to setup Knox policies on Samsung mobile devices.'.
- Delivery Group Assignments (optional):** A section for assigning the app to one or more delivery groups. The 'Choose delivery groups' section shows a list of delivery groups: 'AllUsers' and 'TestUser'. The 'TestUser' group is selected, indicated by a green checkmark and a red box.
- Deployment Schedule:** A section for setting the deployment schedule, currently showing a dropdown menu.

At the bottom of the interface, there are two buttons: 'Back' and 'Next >'. The 'Next >' button is highlighted with a red box.

# Configure Knox Platform for Enterprise using Knox Service Plugin

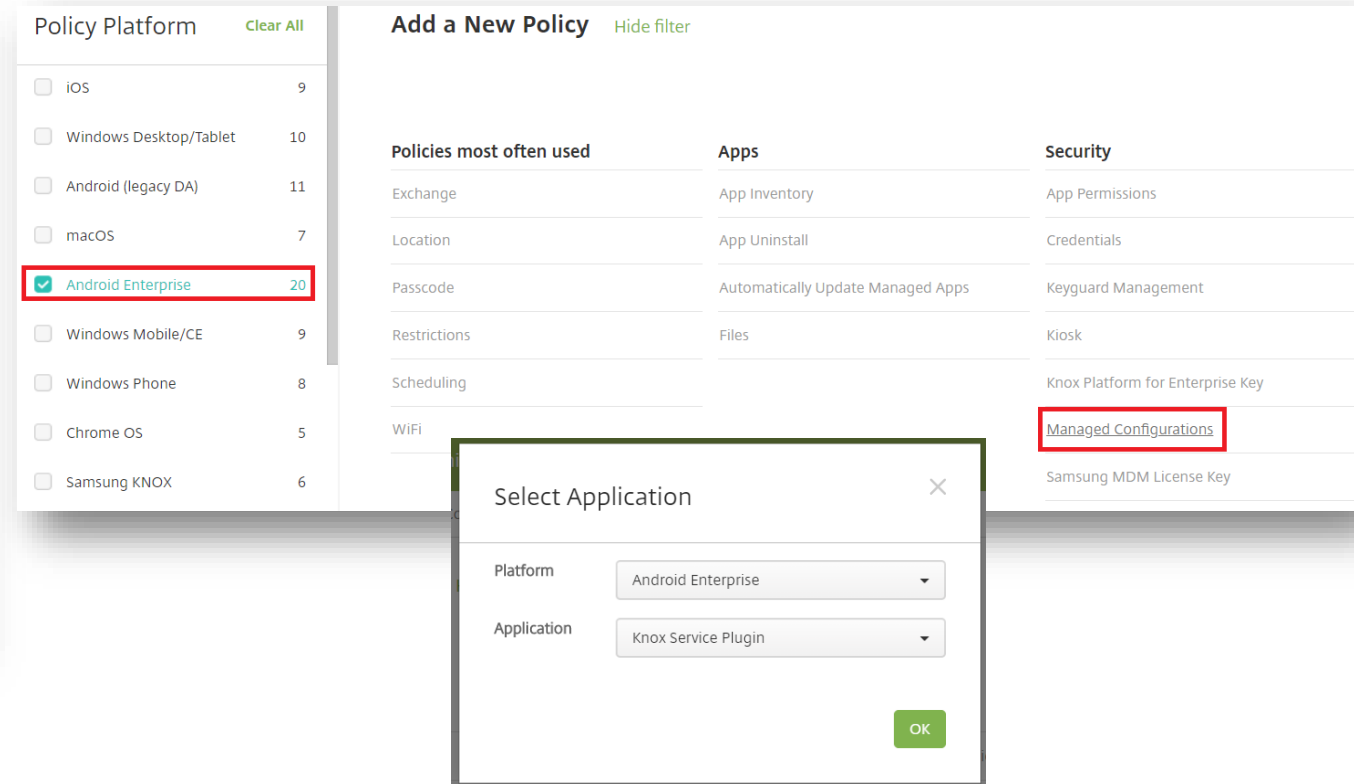
To make use of the KSP features you need to create a Device Policy. Follow the instructions below:

- Within the console, navigate to: **Configure > Device Policies > Add**
- Tick **Android Enterprise** under Policy Platform and then select **Managed Configurations**
- Set the Platform to **Android Enterprise** and set Application to **Knox Service Plugin**
- **Select OK**



The screenshot shows the Knox console interface. The top navigation bar has four tabs: **Analyze**, **Manage**, **Configure** (highlighted with a red box), and **Monitor**. Below the navigation bar, there are sub-tabs: **Device Policies** (highlighted with a red box), **Apps**, **Media**, **Actions**, and **Content Collaboration**. The main content area is titled **Device Policies** and contains an **Add** button (highlighted with a red box) and an **Export** button. Below these buttons is a table with the following columns: **Policy name**, **Type**, and **Created**.

Policy name	Type	Created
Passcode	Passcode	14/08/20
App Inventory	App Inventory	14/08/20



The screenshot shows the **Add a New Policy** dialog box. On the left, the **Policy Platform** list includes: **iOS** (9), **Windows Desktop/Tablet** (10), **Android (legacy DA)** (11), **macOS** (7), **Android Enterprise** (20) (highlighted with a red box and checked), **Windows Mobile/CE** (9), **Windows Phone** (8), **Chrome OS** (5), and **Samsung KNOX** (6). On the right, the **Add a New Policy** section has three columns: **Policies most often used**, **Apps**, and **Security**. The **Security** column includes **Managed Configurations** (highlighted with a red box). A **Select Application** modal is open, showing **Android Enterprise** as the selected platform and **Knox Service Plugin** as the selected application. The **OK** button is highlighted with a green box.



# Configure Knox Platform for Enterprise using Knox Service Plugin

- Enter a Policy name of your choice, select Next
- If you're using KPE Premium features, enter your Knox Suite License Key
- Scroll down to see all the available features, select Add against the features you would like to use.
- Once you're finished select Next

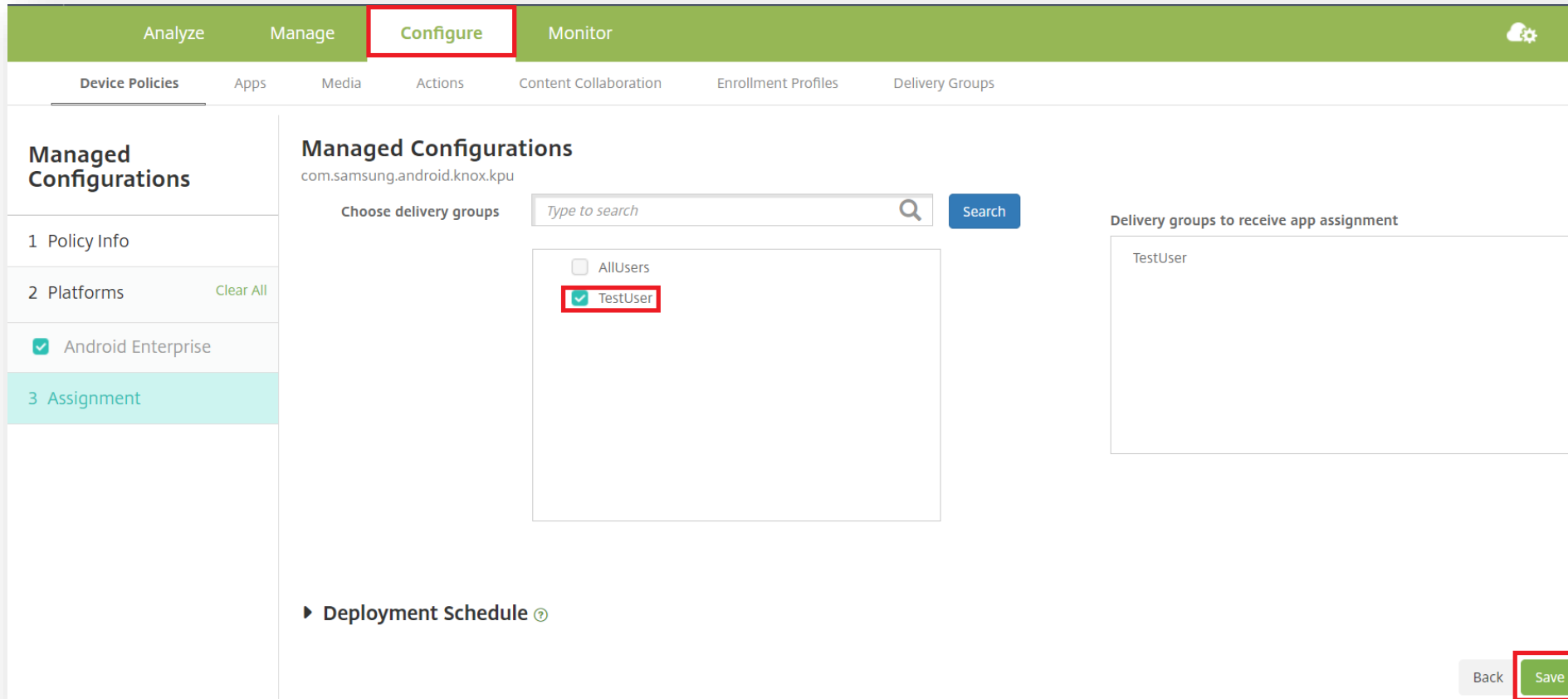
The image displays two screenshots of the Knox configuration interface. The top screenshot shows the 'Policy Information' section with the following details:

- Managed Configurations:** 1 Policy Info, 2 Platforms (Clear All), 3 Assignment.
- Policy Information:** com.samsung.android.knox.kpu
- Policy Name:** KSP (highlighted with a red box)
- Description:** (empty text area)
- Next >** button (highlighted with a red box)

The bottom screenshot shows the 'App Separation policies' section with the following details:

- Profile name:** Knox profile
- KPE Premium or Knox Suite License key:** XXXX-XXXX-XXXX-XXXX-XXX (highlighted with a red box)
- Debug Mode:** OFF
- App Separation policies:** Add (highlighted with a red box), Delete
- Configuration:** (empty table with a note: Click 'Add' to add new Configuration)
- Back** and **Next >** buttons (highlighted with a red box)

- Choose a delivery group
- Select Save



The screenshot displays the Knox configuration interface. At the top, a green navigation bar contains the tabs 'Analyze', 'Manage', 'Configure' (highlighted with a red border), and 'Monitor'. Below this, a secondary navigation bar lists various categories: 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Managed Configurations' and shows the configuration for 'com.samsung.android.knox.kpu'. On the left, a sidebar lists steps: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment' (highlighted in teal), and '4 Deployment Schedule'. The 'Assignment' step is active, showing a 'Choose delivery groups' section with a search bar and a list of groups: 'AllUsers' (unchecked) and 'TestUser' (checked, highlighted with a red box). To the right, a section titled 'Delivery groups to receive app assignment' lists 'TestUser'. At the bottom right, there are 'Back' and 'Save' buttons, with the 'Save' button highlighted by a red box.

**This is version 2.0 of this document.**

**Thank you!**

