

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

Knowledge Base:

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

Pre-Requisites for Knox Platform for Enterprise

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 (settings), and a key. The gear icon is highlighted with a red square. Below the navigation bar, the main content area is divided into several sections. On the left, there is a 'Settings' sidebar with categories: 'Authentication' (Derived Credentials for iOS, Identity Provider (IDP)), 'Certificate Management' (Certificates, Credential Providers, PKI Entities), and 'Client' (Client Branding, Client Properties, Client Support). The main content area is divided into three columns: 'Notifications' (Carrier SMS Gateway, Notification Server, Notification Templates), 'Platforms' (Alexa for Business, **Android Enterprise** (highlighted with a red square), Android SafetyNet, Apple Configuration, Apple Deployment, Google Chrome), and 'Server' (ActiveSync Gateway, Citrix Gateway, Cloud Connector Allow List, Endpoint Management Tools, Enrollment, Firebase Cloud Messaging, LDAP). On the right side of the main content area, there is a 'Frequently Accessed Items' section listing: Android Enterprise, Enrollment, Certificates, Identity Provider (IDP), and Release Management. A modal window titled 'Android Enterprise' is open in the foreground. 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, there 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 text: '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 is highlighted with a red square 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.

i 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 setup 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.

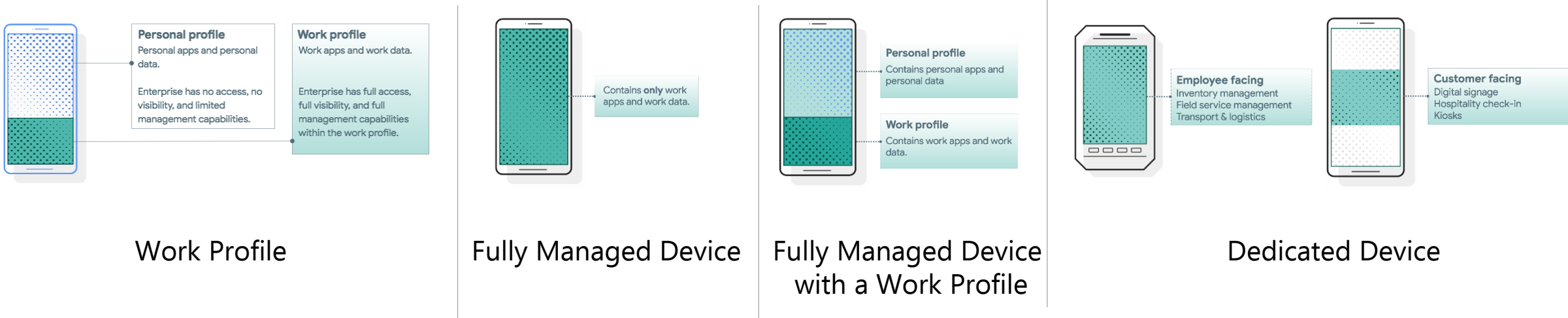
Android Enterprise Deployment Modes

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 List
The interface shows the 'Enrollment Profiles' section under the 'Configure' tab. An 'Add' button (represented by a plus icon) is highlighted with a red box.

Screenshot 2: Enrollment Info Form
The 'Enrollment Info' form is shown. 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 Form
The 'Enrollment Configuration' form is shown. The 'Management' section has 'Android Enterprise' selected (highlighted with a red box). The 'Device owner mode' section has 'None' selected (highlighted with a red box). The 'BYOD work profile' toggle is turned 'On'. The 'Application management' section has 'Citrix MAM' turned 'On'. The 'User consent' section has 'Allow users to decline device management' 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

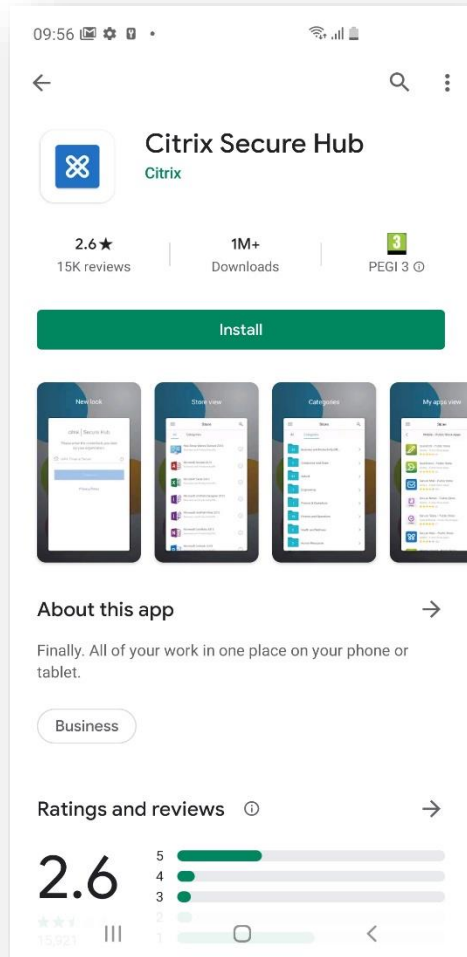
The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the steps for configuring a Work Profile.

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

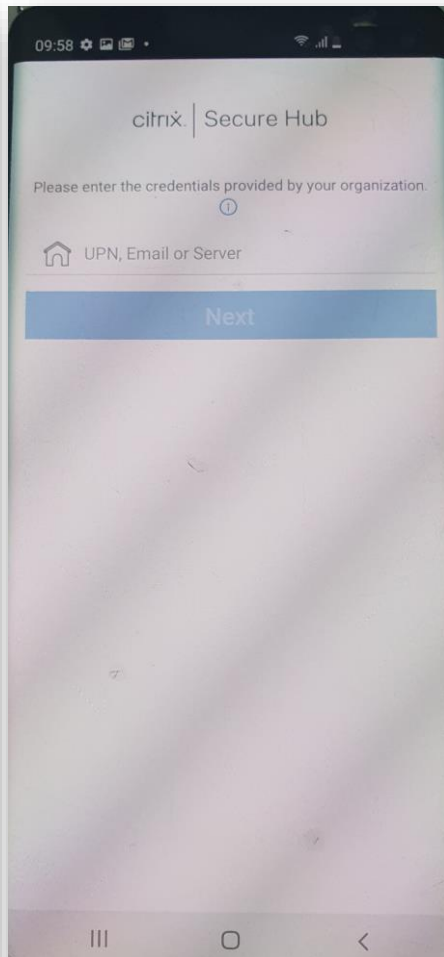
Screenshot 2 (Top Right): Shows the 'Enrollment Profile' configuration page for Windows. The 'Enrollment Configuration' section includes 'Device management' (Fully managed), 'User consent' (Allow users to decline device management), and 'Workspace integration' (Enrollment through Workspace app). The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

Screenshot 3 (Bottom): Shows the 'Delivery Group Assignment' page. The 'Choose delivery groups' section lists 'AllUsers' and 'TestUser', with 'TestUser' selected and highlighted by a red box. The 'Save' button is highlighted with a red box.

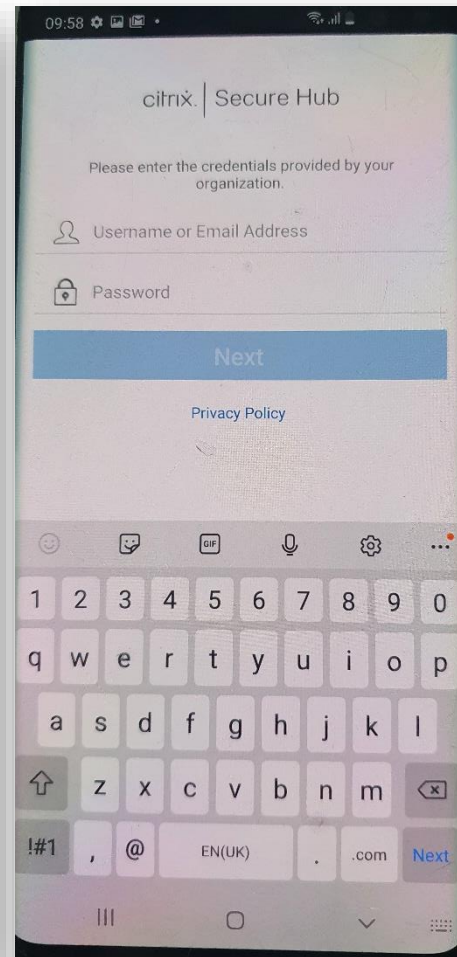
Android Enterprise: Work Profile Enrollment



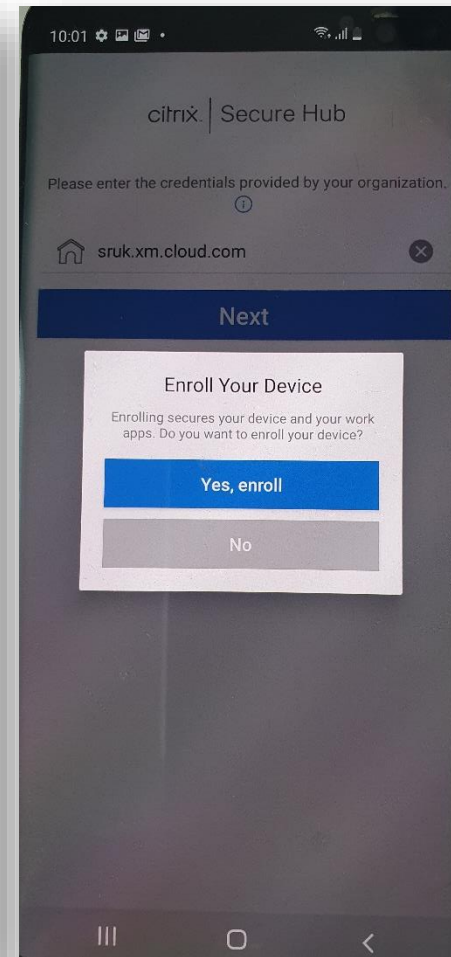
Install Citrix Secure Hub
From the Google Play Store



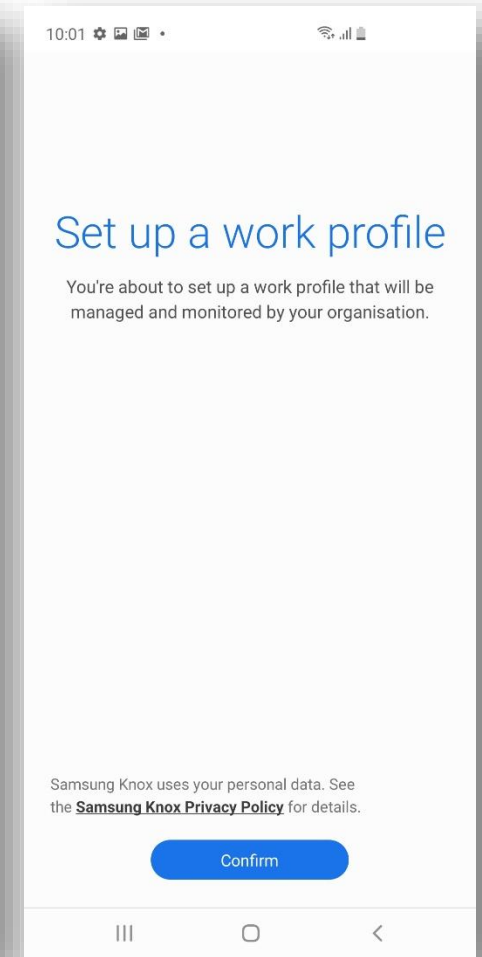
Open Secure Hub and enter
Your Citrix Endpoint Management
Server URL



Enter your Citrix credentials
and select Next



Yes, enroll

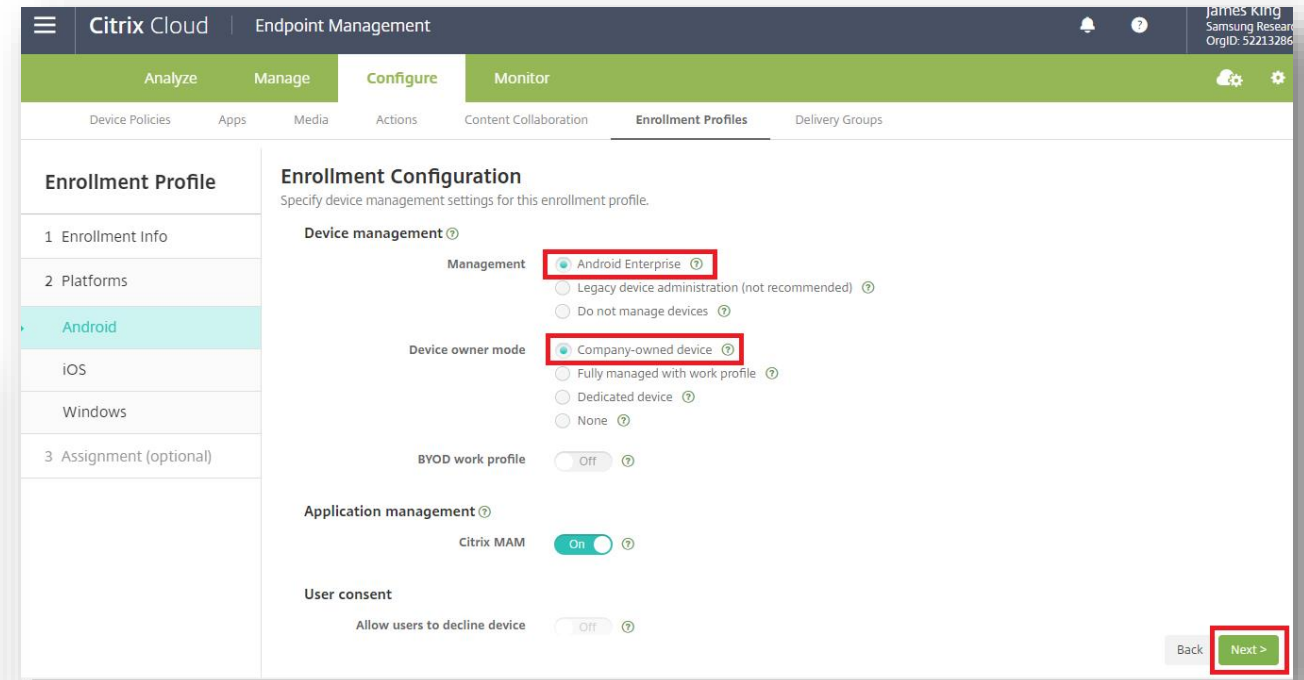
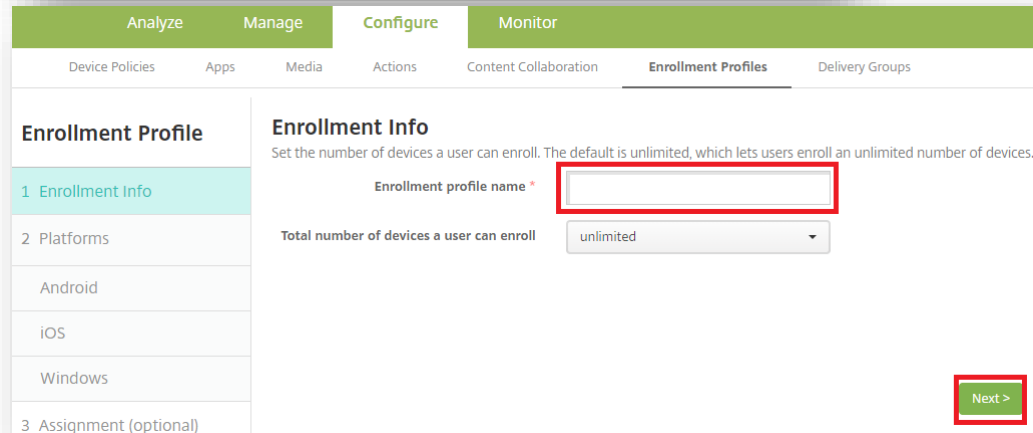
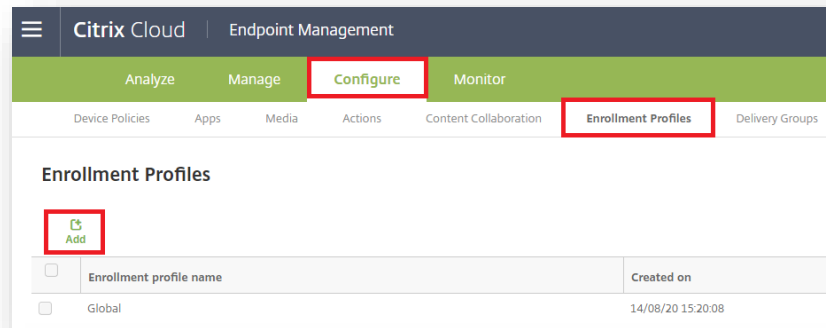


Confirm

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: Enrollment Configuration for iOS

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

Screenshot 2: Enrollment Configuration for Windows

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

Screenshot 3: Delivery Group Assignment

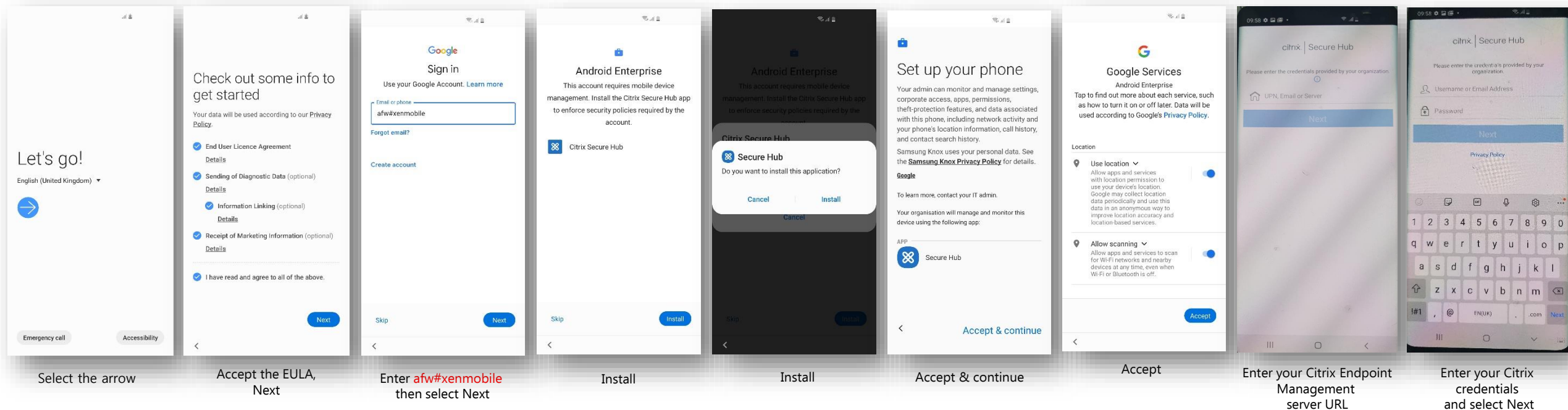
The console shows the 'Delivery Group Assignment' page. The 'Choose delivery groups' section has a search bar and a list of delivery groups. 'TestUser' is selected, and the 'Save' button is highlighted with a red box.

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.

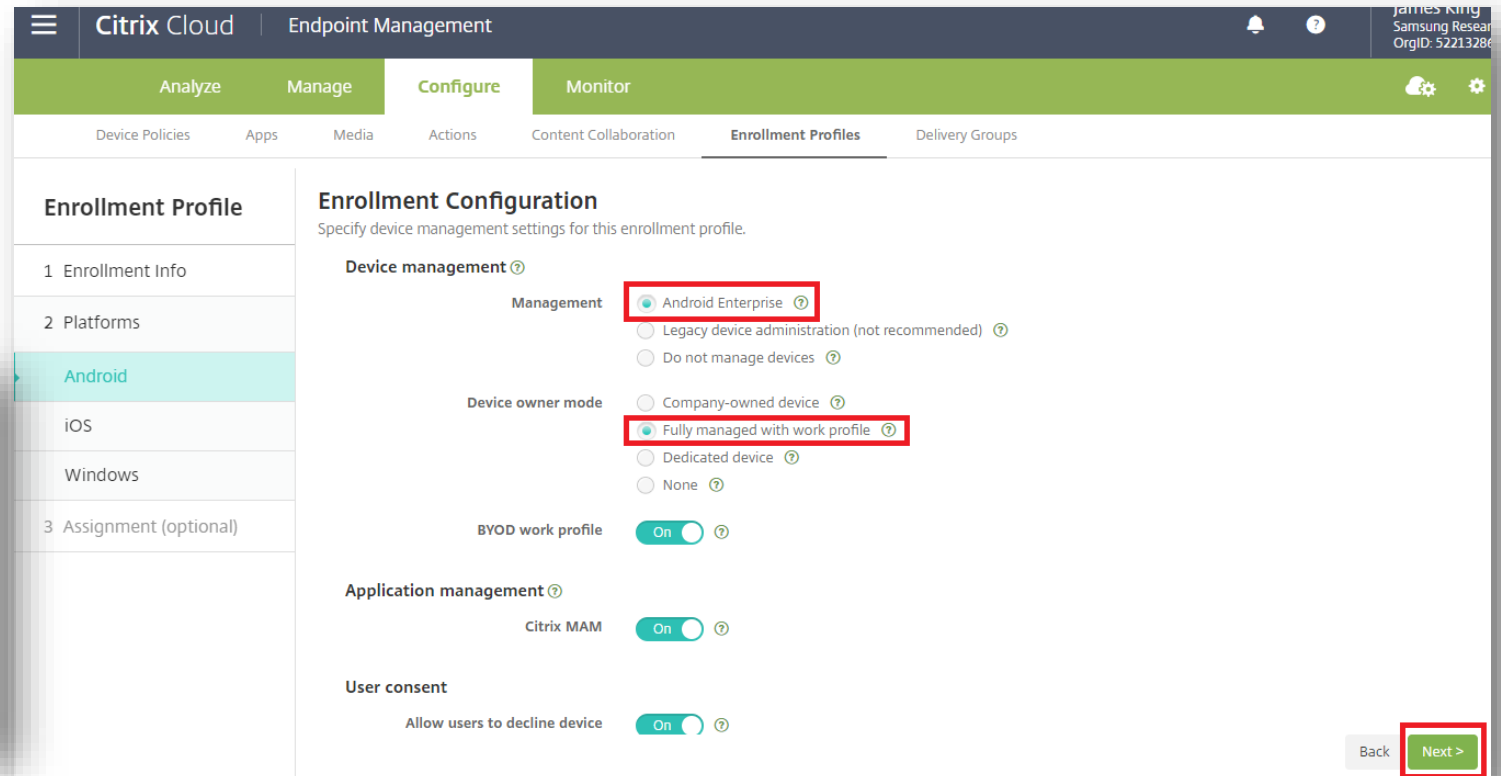
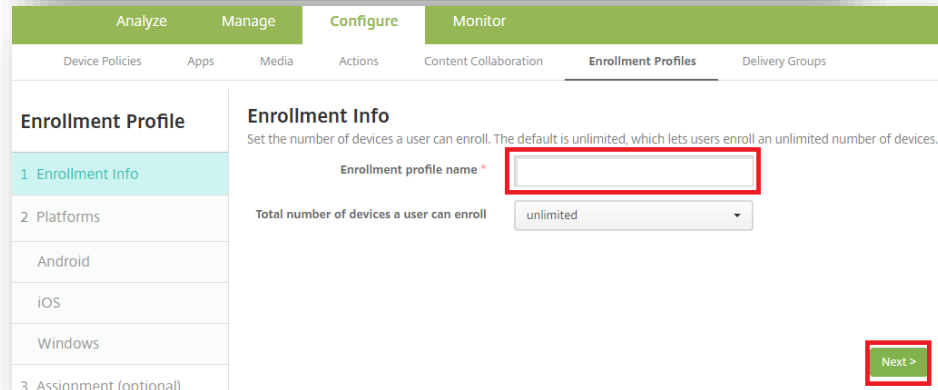
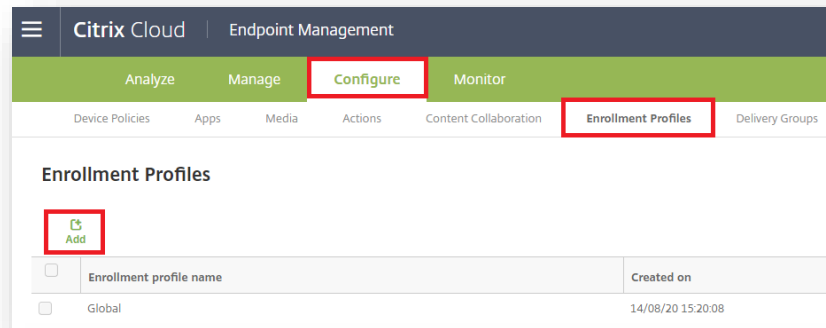
1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
 2. QR Code Enrollment / NFC Enrollment
 3. Knox Mobile Enrollment
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



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 for iOS

- Enrollment Profile:** 1 Enrollment Info, 2 Platforms (Android, iOS, Windows), 3 Assignment (optional).
- Enrollment Configuration:** Specify device management settings for this enrollment profile.
 - Device management:** Management: ☒ Apple Device enrollment, ☐ Do not manage devices.
 - Application management:** Citrix MAM: ☒ On.
 - User consent:** Allow users to decline device management: ☒ On.
- Next >** button is highlighted.

Screenshot 2: Enrollment Configuration for Windows

- Enrollment Profile:** 1 Enrollment Info, 2 Platforms (Android, iOS, Windows), 3 Assignment (optional).
- Enrollment Configuration:** Specify device management settings for this enrollment profile.
 - Device management:** Management: ☒ Fully managed, ☐ Do not manage devices.
 - User consent:** Allow users to decline device management: ☒ On.
 - Workspace integration:** Enrollment through Workspace app: ☐ Off.
- Next >** button is highlighted.

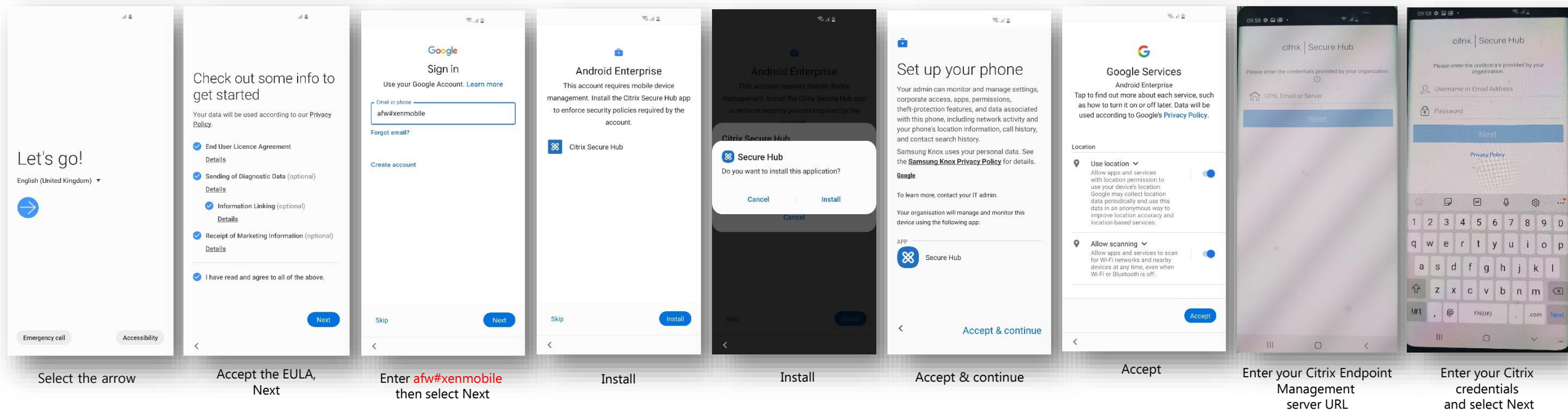
Screenshot 3: Delivery Group Assignment

- Enrollment Profile:** 1 Enrollment Info, 2 Platforms (Android, iOS, Windows), 3 Assignment (optional).
- Delivery Group Assignment:** Attach this enrollment profile to one or more delivery groups.
 - Choose delivery groups:** Type to search, Search button.
 - Delivery groups to receive app assignment:** TestUser.
 - TestUser** is selected in the list.
- Save** button is highlighted.

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.

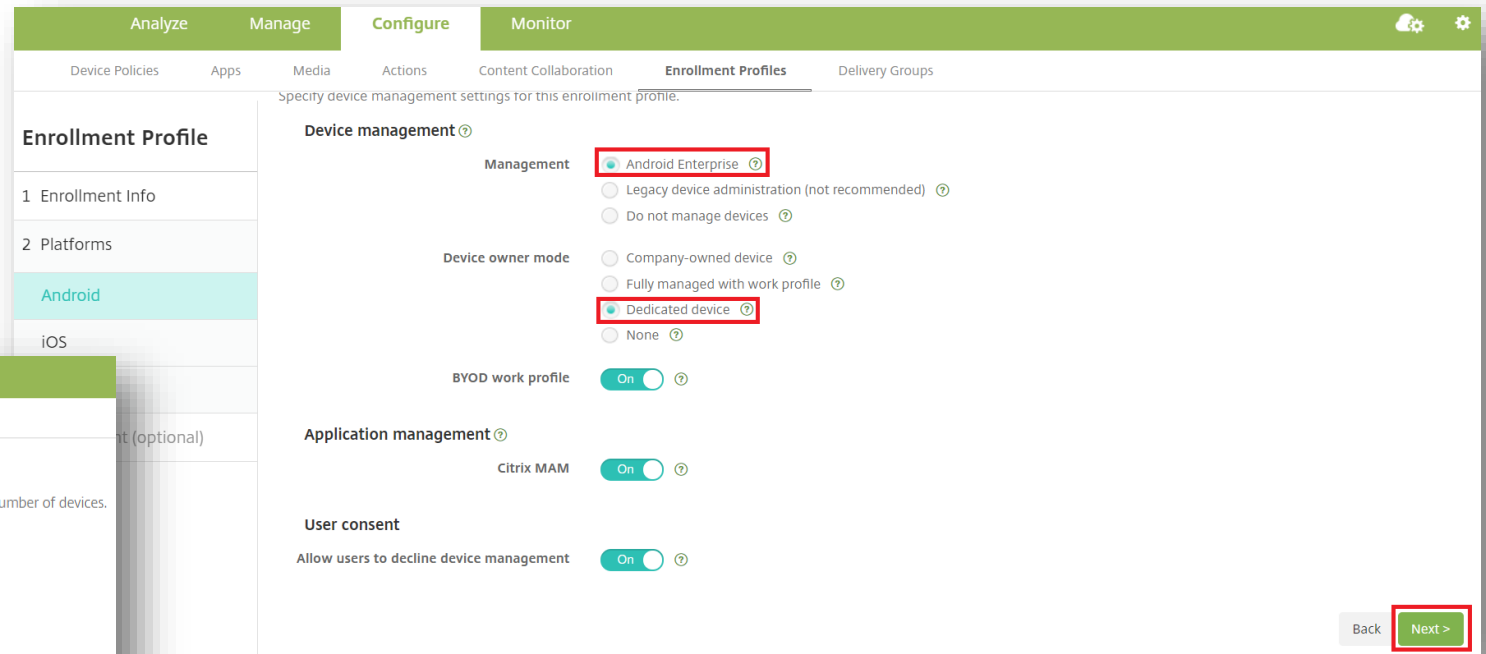
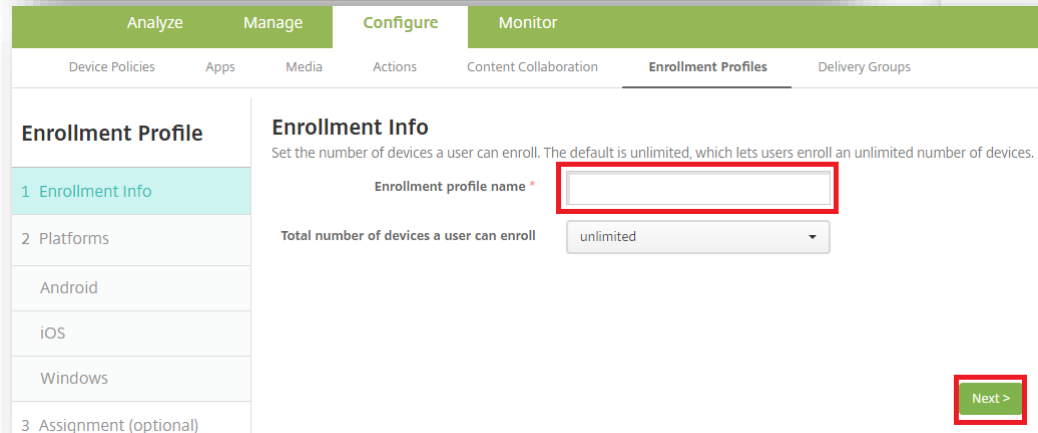
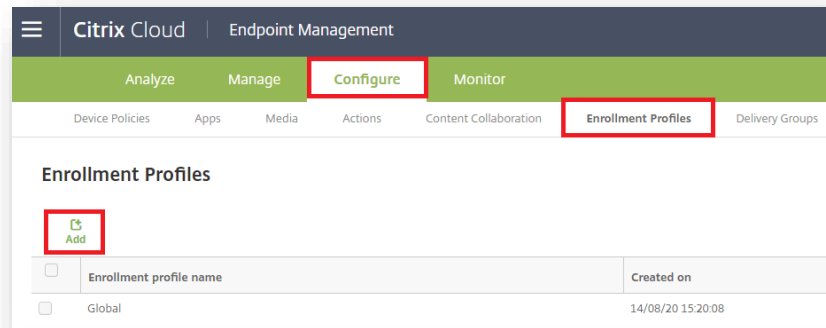
1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
 2. QR Code Enrollment / NFC Enrollment
 3. Knox Mobile Enrollment
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



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 (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.

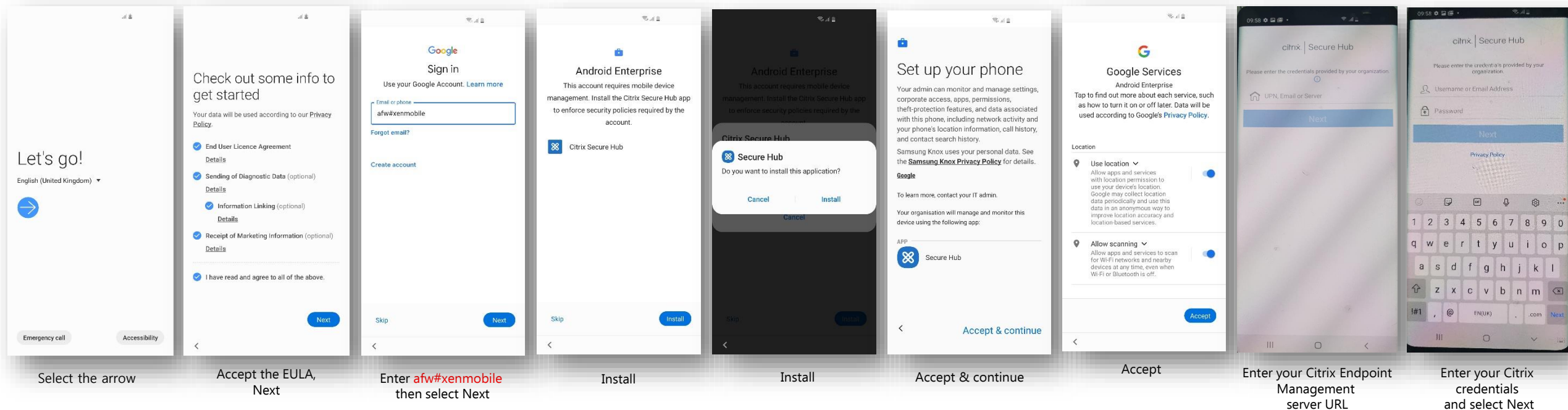
Screenshot 2 (Right): Shows the 'Enrollment Configuration' page for an 'Enrollment Profile'. The 'Enrollment Profile' list on the left has 'Windows' selected. The 'Enrollment Configuration' section shows 'Device management' with 'Fully managed' selected, 'User consent' with 'Allow users to decline device 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: 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:

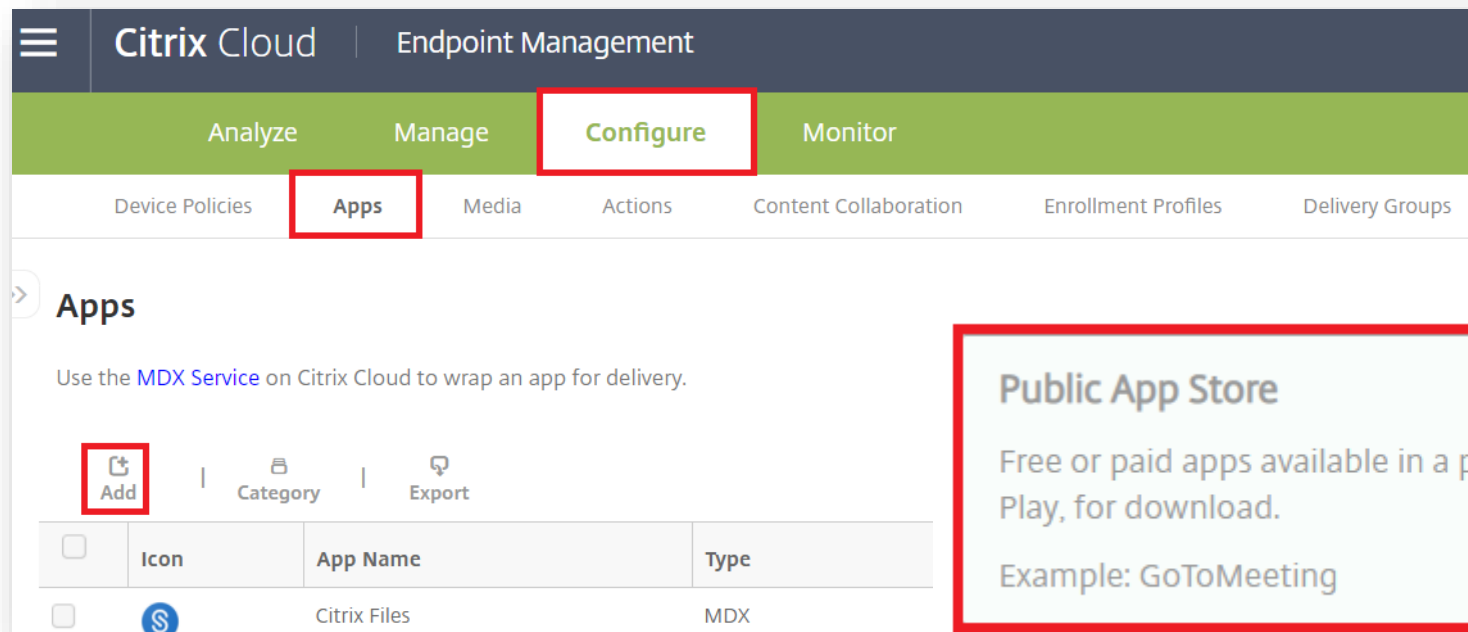
- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [\$]

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.



Configure Knox Platform for Enterprise using Knox Service Plugin

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



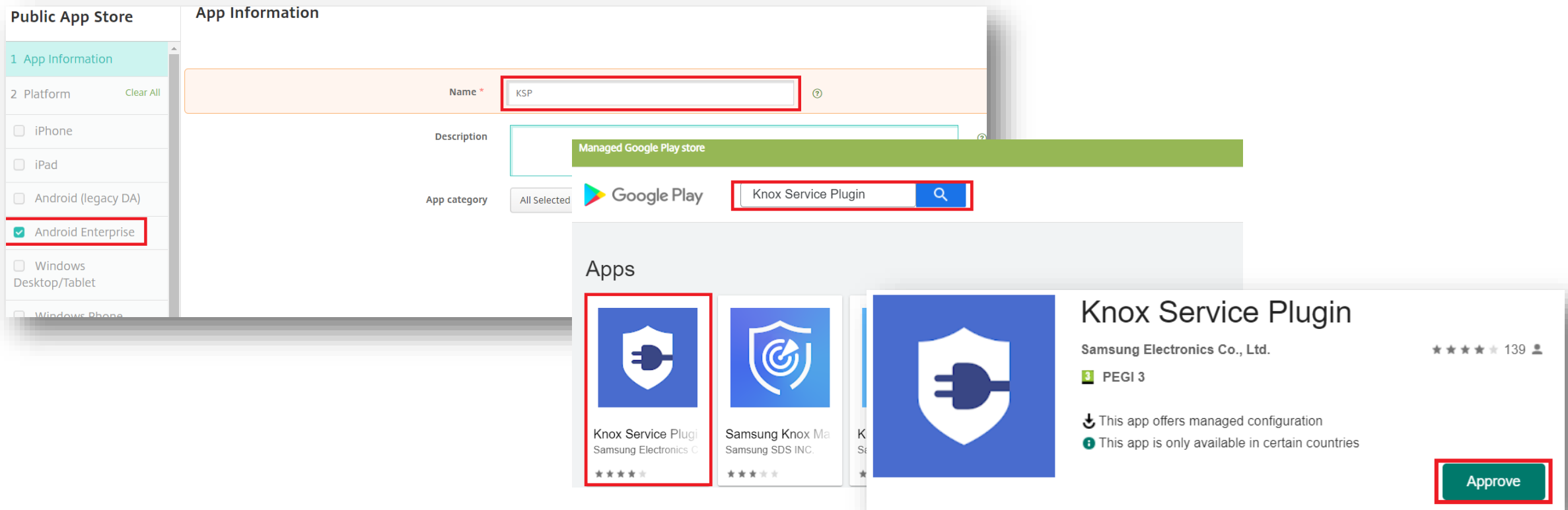
Public App Store

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

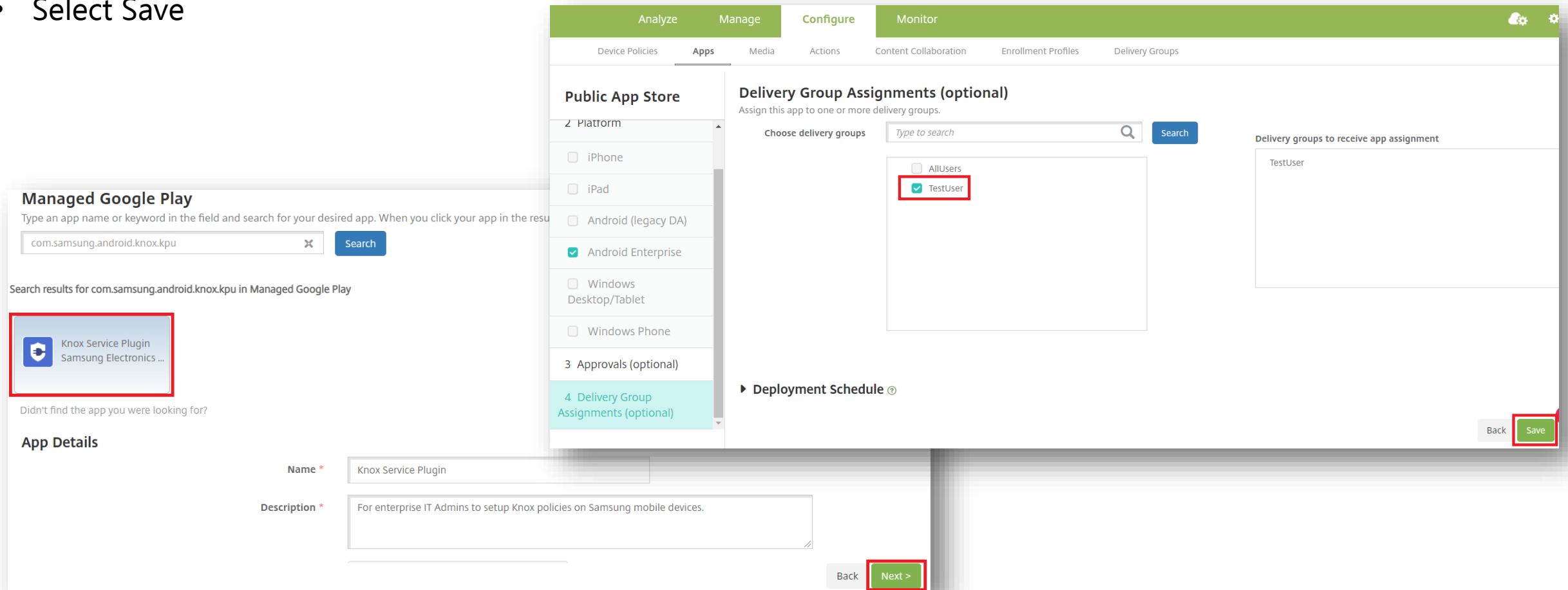
- Enter a Name of your choice
- Tick only Android Enterprise on the left column
- Select Next
- Search for and Approve the Knox Service Plugin



The screenshot displays the Knox configuration interface. On the left, the 'Public App Store' sidebar shows the 'Android Enterprise' checkbox selected. The main 'App Information' section has the 'Name' field set to 'KSP'. Below this, the 'App category' is set to 'Google Play'. A search bar shows 'Knox Service Plugin'. In the 'Apps' section, the 'Knox Service Plugin' app by Samsung Electronics Co., Ltd. is highlighted. The app details show a 5-star rating, PEGI 3 rating, and a note that it offers managed configuration. The 'Approve' button is highlighted in the bottom right corner.

Configure Knox Platform for Enterprise using Knox Service Plugin

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



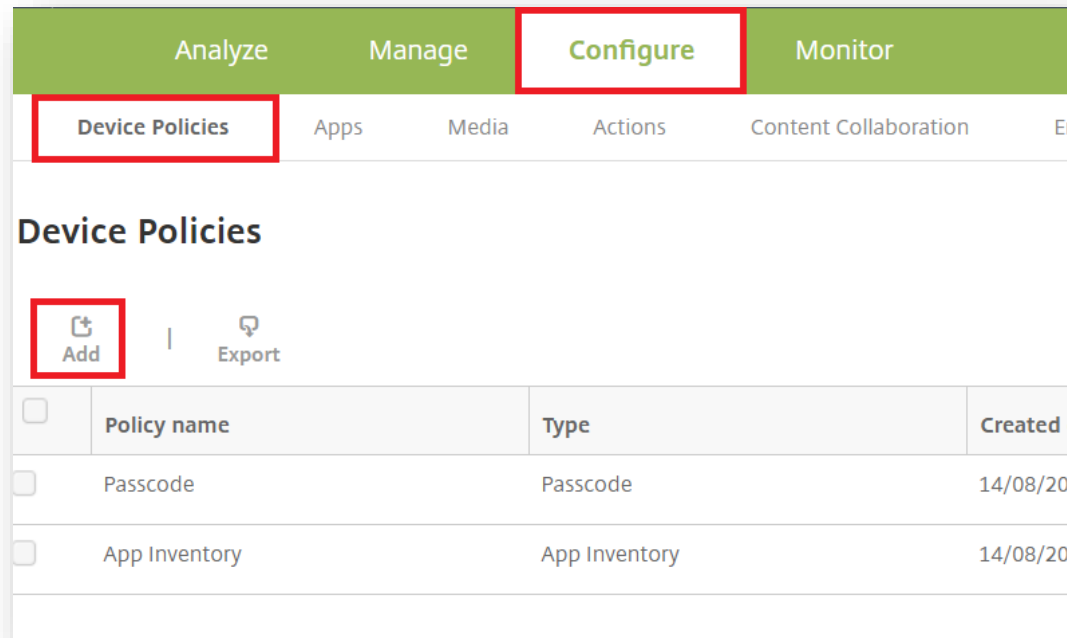
The screenshot displays the Knox Platform configuration interface, specifically the 'Managed Google Play' section. The interface is divided into several panels and sections:

- 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 is filled with 'For enterprise IT Admins to setup Knox policies on Samsung mobile devices.' The 'Next >' button is highlighted with a red box.
- 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' checkbox is checked and highlighted with a red box. The 'Delivery groups to receive app assignment' section shows 'TestUser' as the selected group. The 'Save' button is highlighted with a red box.

Configure Knox Platform for Enterprise using Knox Service Plugin

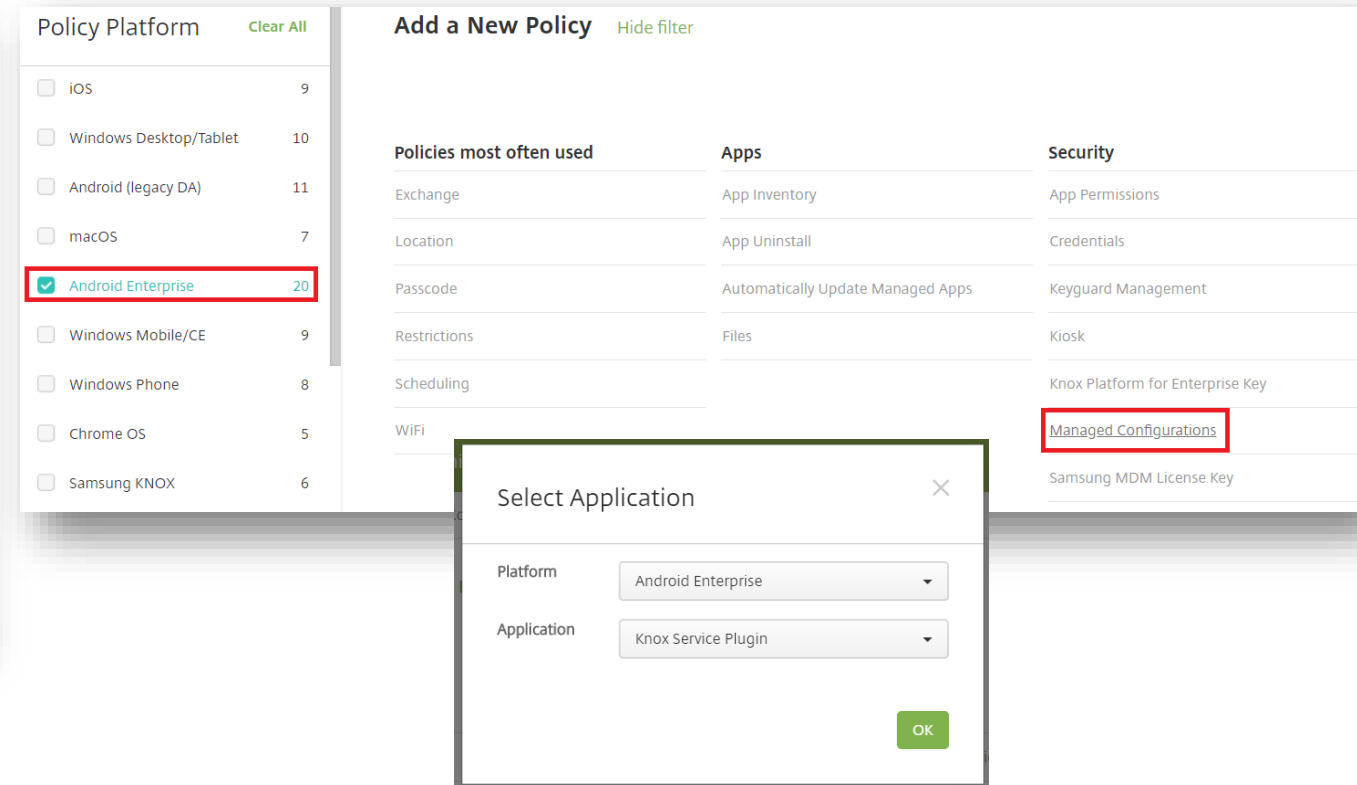
To make use of the KSP features you need to create a Device Policy. Follow the instructions below:

- 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 'Configure' tab in the Knox console. The 'Device Policies' sub-tab is selected. An 'Add' button is highlighted with a red box. Below it, a table lists existing policies:

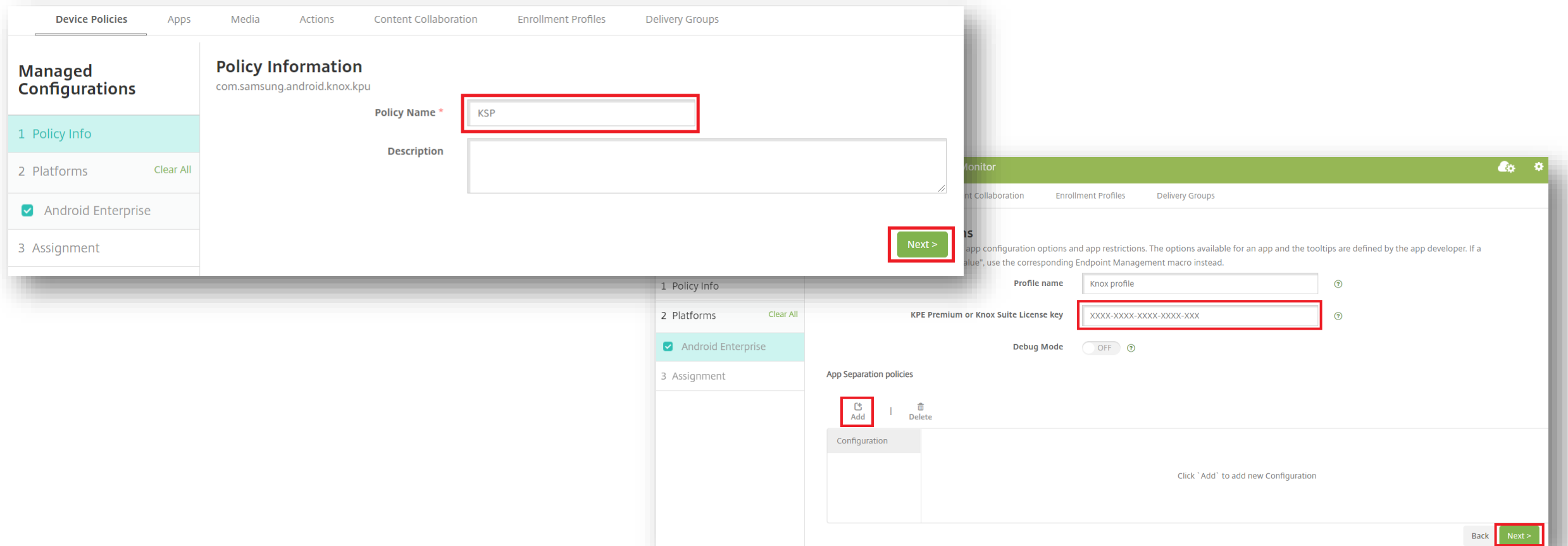
	Policy name	Type	Created
<input type="checkbox"/>	Passcode	Passcode	14/08/20
<input type="checkbox"/>	App Inventory	App Inventory	14/08/20



The screenshot shows the 'Add a New Policy' dialog. Under 'Policy Platform', 'Android Enterprise' is selected and highlighted with a red box. Under 'Security', 'Managed Configurations' is selected and highlighted with a red box. A 'Select Application' modal is also shown, with 'Android Enterprise' selected for Platform and 'Knox Service Plugin' selected for Application.

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, illustrating the steps to configure a policy.

Top Screenshot: Policy Information

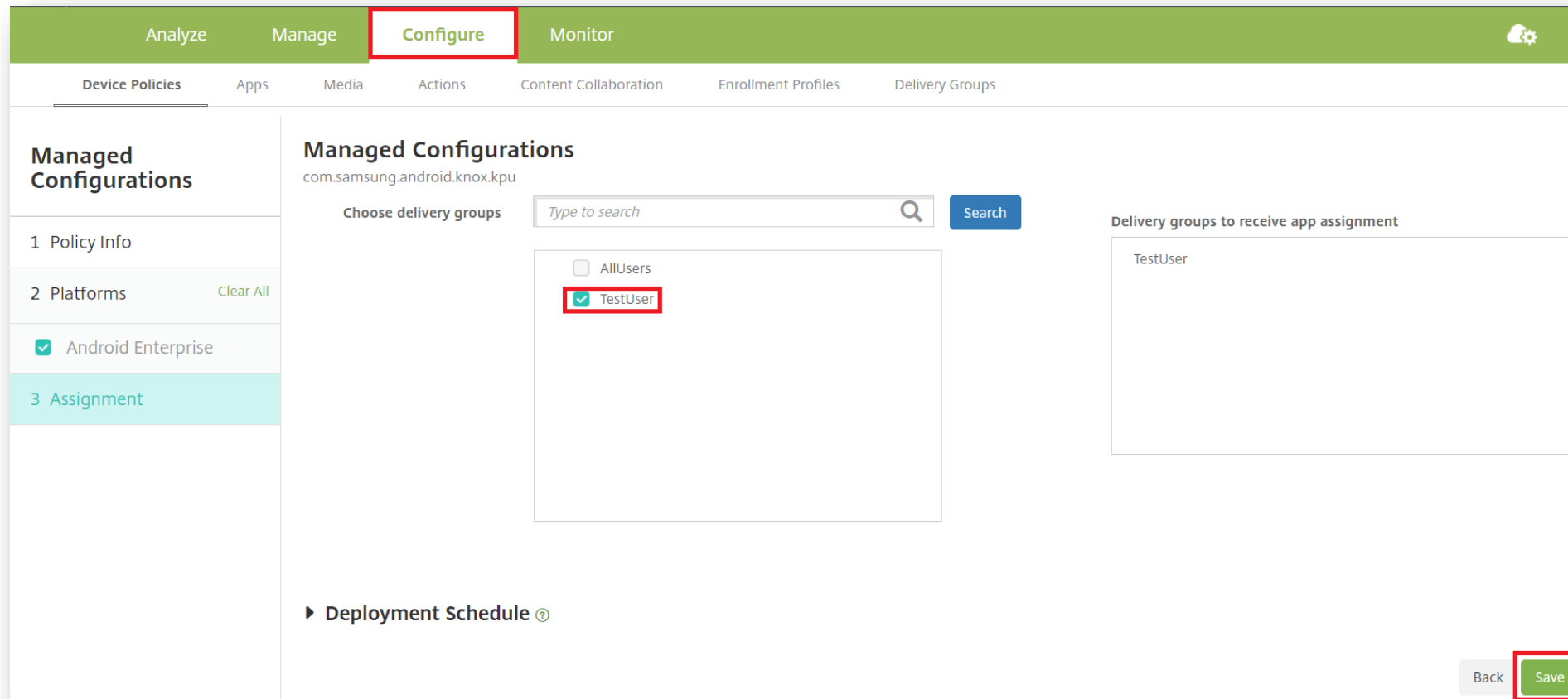
- Managed Configurations:**
 - 1 Policy Info
 - 2 Platforms [Clear All](#)
 - ☒ Android Enterprise
 - 3 Assignment
- Policy Information:**
 - com.samsung.android.knox.kpu
 - Policy Name ***: KSP
 - Description**: (Empty text area)
 - Next >** button

Bottom Screenshot: App Separation policies

- Managed Configurations:**
 - 1 Policy Info
 - 2 Platforms [Clear All](#)
 - ☒ Android Enterprise
 - 3 Assignment
- App Separation policies:**
 - Add** button (highlighted)
 - Delete** button
 - Configuration** section: Click 'Add' to add new Configuration
 - Profile name**: Knox profile
 - KPE Premium or Knox Suite License key**: XXXX-XXXX-XXXX-XXXX-XXX
 - Debug Mode**: OFF
 - Next >** button

Configure Knox Platform for Enterprise using Knox Service Plugin

- Choose a delivery group
- Select Save



This is version 2.0 of this document.

Thank you!

