

Citrix Endpoint Management Knox Platform for Enterprise

October 2021
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**
 - **Fully Managed Device with a Work Profile**
 - **Work Profile on a Company-Owned Device**
 - **Dedicated Device**
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/>

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. The top navigation bar includes 'Analyze', 'Manage', 'Configure', and 'Monitor'. A settings gear icon in the top right corner is highlighted with a red box. The main content area is divided into several sections: 'Settings' (with sub-sections like Authentication, Certificate Management, and Client), 'Notifications', 'Server', and 'Frequently Accessed Items'. The 'Platforms' section under 'Notifications' has 'Android Enterprise' highlighted with a red box. A modal window titled 'Android Enterprise' is open, providing instructions on how to set up Android Enterprise for a company by binding Citrix Endpoint Management as an EMM provider through Google Play. The modal includes a note for G Suite customers and a 'Connect' button, which is also highlighted with a red box.

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 Configurator
 - 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**

Google Play

Bring Android to Work

Get started

Business name

We need some details about your business

Business name

Your answer
Your Company

Enterprise mobility management (EMM) provider

Citrix

Previous Next

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

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

Previous Confirm

Set up complete

Thanks for choosing Android enterprise.

Complete Registration

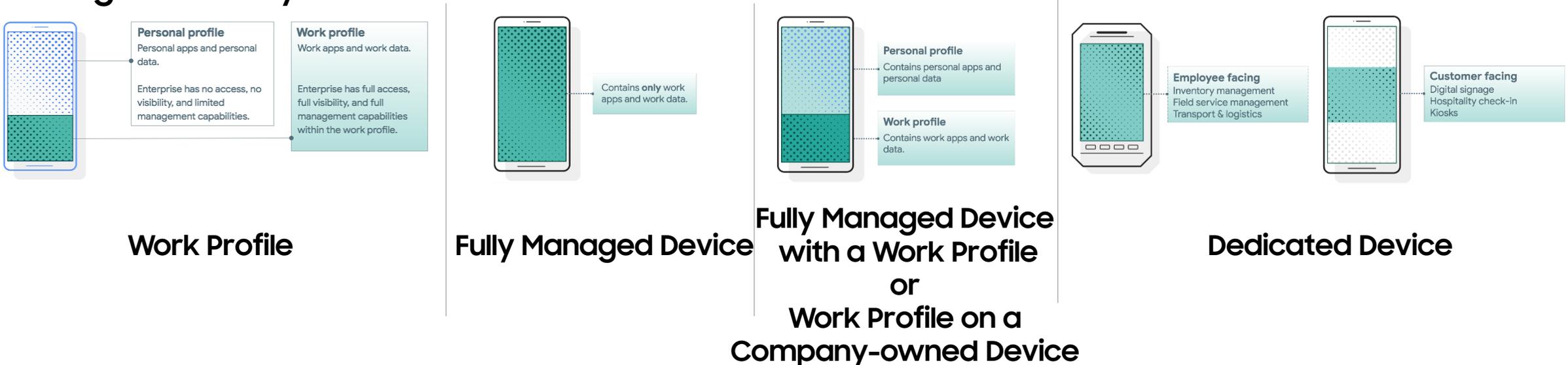
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 5 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, up to Android 10*]
4. Work Profile on Company-owned Device [WPC, on Android 11+]
5. 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 5 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 screenshot displays the Citrix Cloud Endpoint Management console. The 'Configure' tab is selected, and the 'Enrollment Profiles' section is active. The 'Add' button is highlighted. The 'Enrollment Profile' configuration page is shown, with the 'Enrollment Info' section selected. The 'Enrollment profile name' field is empty and highlighted. The 'Total number of devices a user can enroll' is set to 'unlimited'. The 'Next >' button is highlighted. The 'Enrollment Configuration' dialog is open, showing the 'Device management' section. The 'Management' radio button is set to 'Android Enterprise'. The 'Device owner mode' radio button is set to 'None'. 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. The 'Next >' button is highlighted.

Note: On the latest console, the second Device owner mode now reads:

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

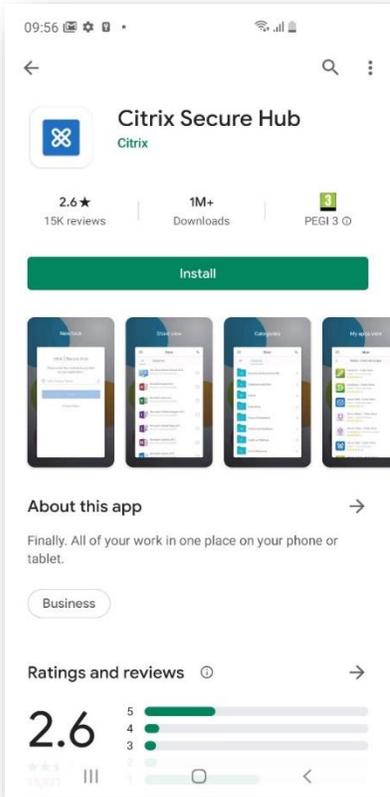
The image displays three screenshots of the Citrix Cloud Endpoint Management console, illustrating the configuration steps for a Work Profile.

Top Left Screenshot: Enrollment Configuration for iOS
The 'Enrollment Configuration' page for the 'iOS' platform. The 'Device management' section has 'Apple Device enrollment' selected. 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.

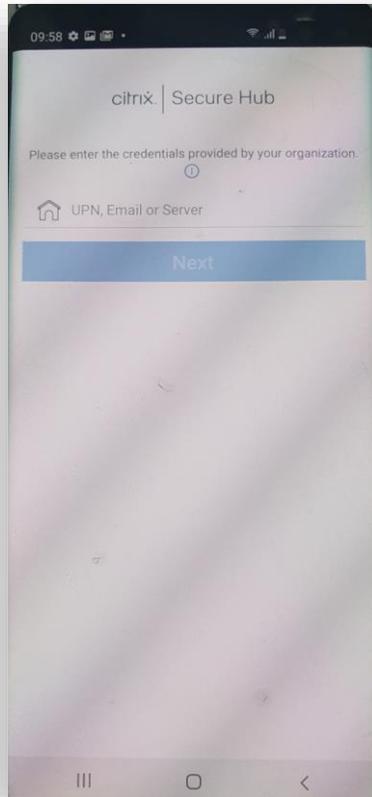
Top Right Screenshot: Enrollment Configuration for Windows
The 'Enrollment Configuration' page for the 'Windows' platform. The 'Device management' section has 'Fully managed' selected. The 'User consent' section has 'Allow users to decline device management' set to 'On'. The 'Workspace integration' section has 'Enrollment through Workspace app' set to 'Off'. The 'Next >' button is highlighted with a red box.

Bottom Screenshot: Delivery Group Assignment
The 'Delivery Group Assignment' dialog box. The 'Choose delivery groups' section has a search bar and a list of groups. 'TestUser' is selected with a red box. The 'Delivery groups to receive app assignment' section shows 'TestUser' in a list. The 'Save' button is highlighted with a red box.

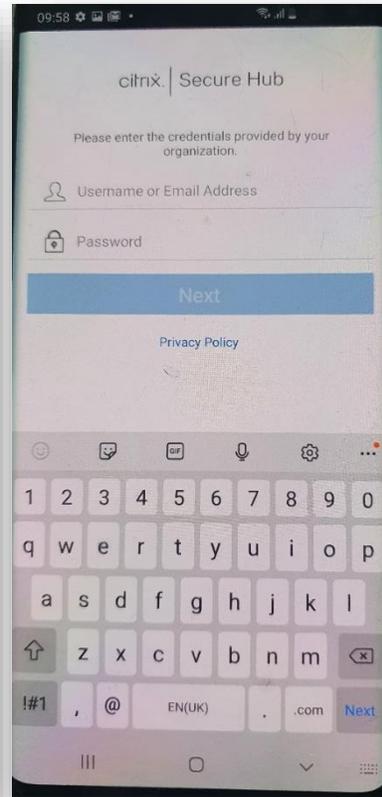
Android Enterprise: Work Profile Enrollment



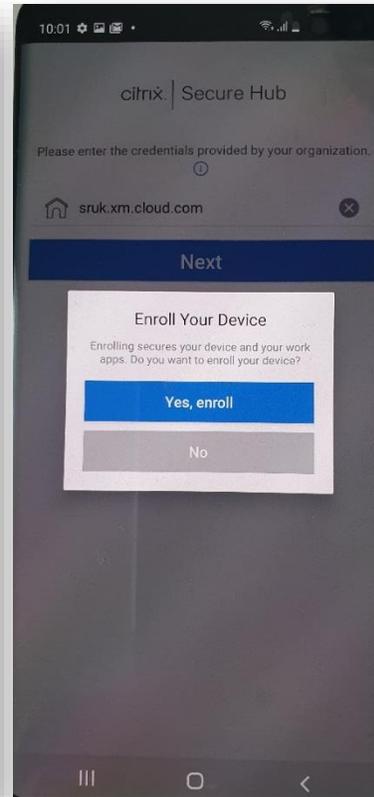
Install Citrix Secure Hub From the Google Play Store



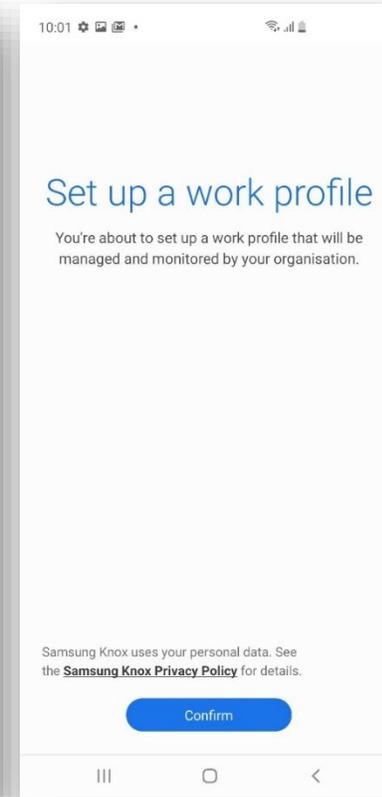
Open Secure Hub and enter your Citrix Endpoint Management Server URL



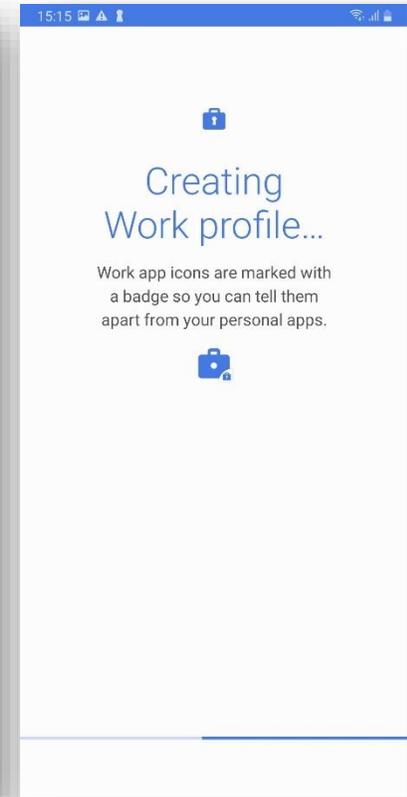
Enter your Citrix credentials and select Next



Yes, enroll



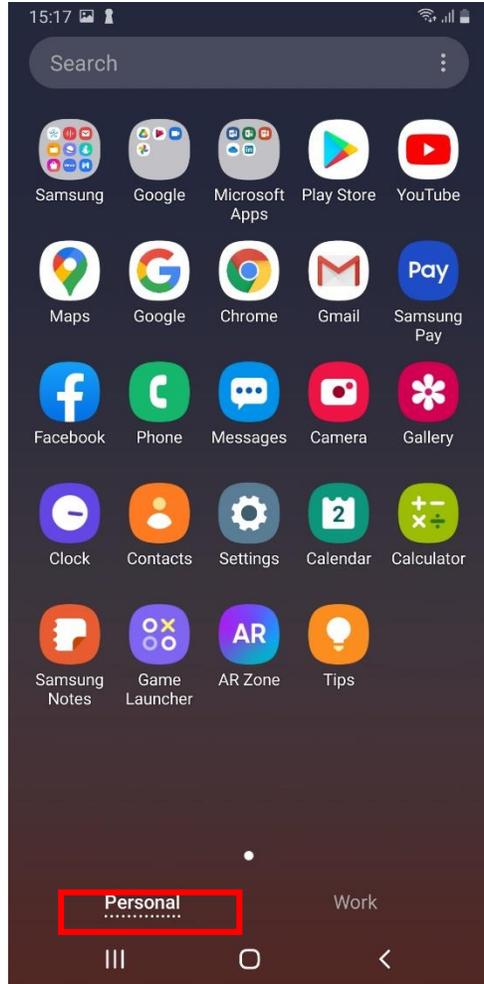
Confirm



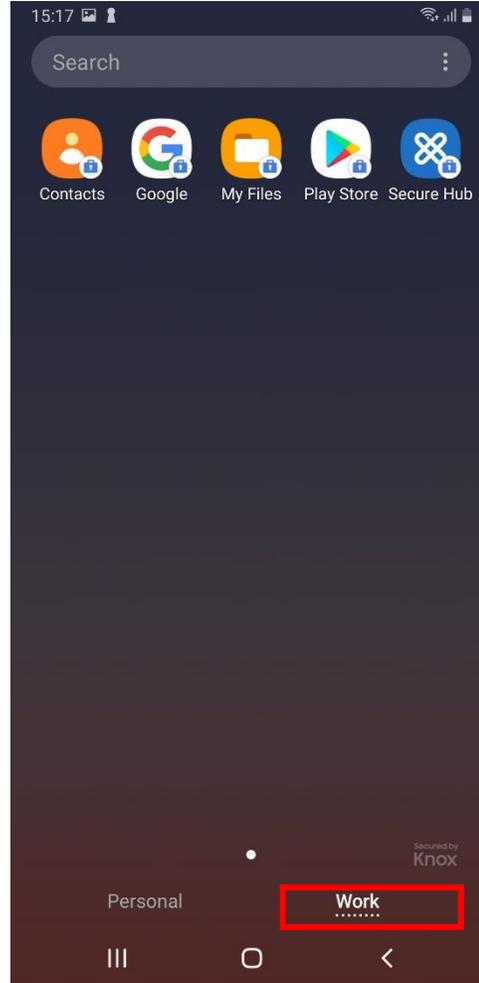
Creating Work profile...

Android Enterprise: Work Profile Enrollment

How to tell that Work Profile has been successfully set up:



Personal Tab



Work Tab

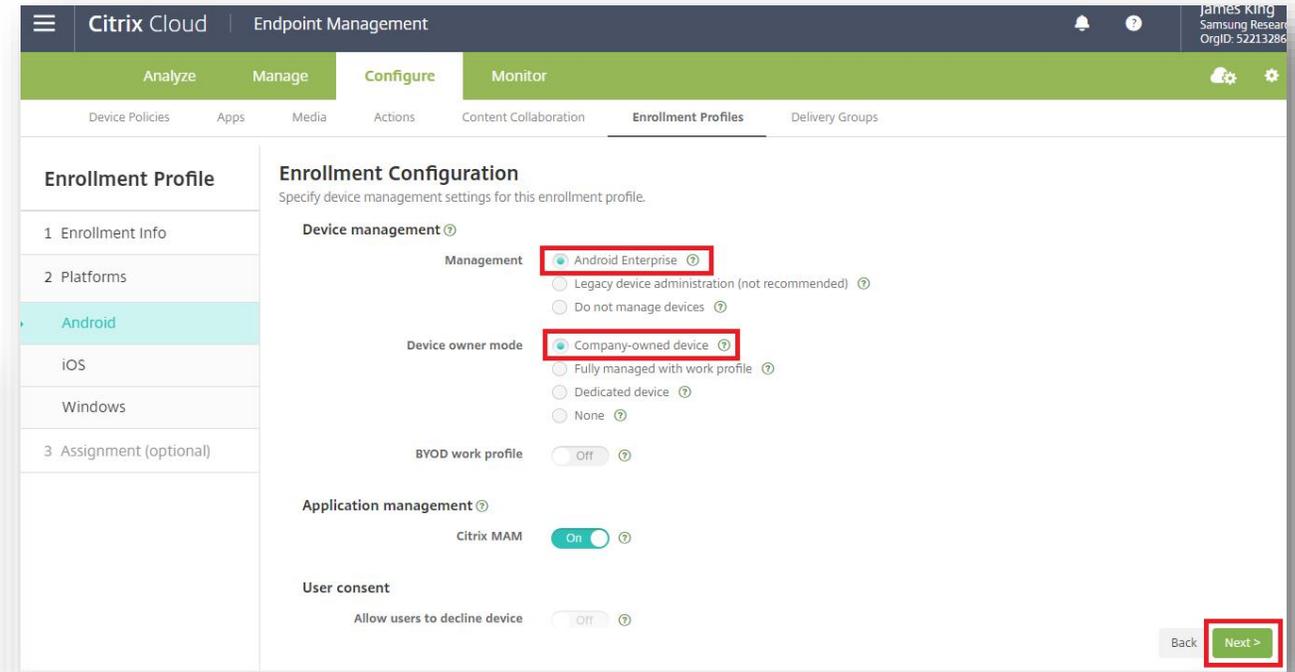
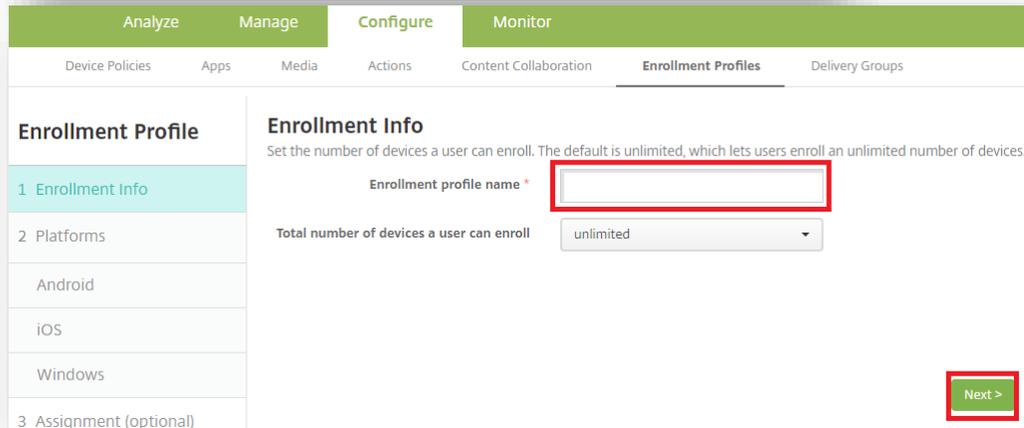
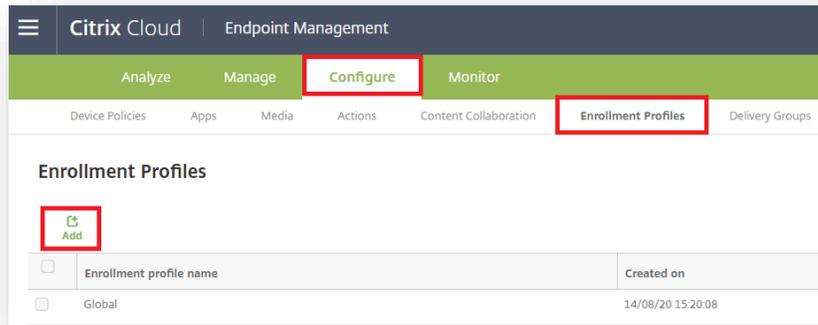


No mention of device belonging to your organization on lock screen

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



Note: On the latest console, the second Device owner mode now reads:

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 configuration process for a Fully Managed Device.

Top Left Screenshot: Shows the 'Enrollment Configuration' page for an 'iOS' device. The 'Device management' section has 'Apple Device enrollment' selected. The 'Application management' section has 'Citrix MAM' set to 'On'. The 'User consent' section has 'Allow users to decline device management' set to 'On'. A red box highlights the 'Next >' button.

Top Right Screenshot: Shows the 'Enrollment Configuration' page for a 'Windows' device. The 'Device management' section has 'Fully managed' selected. 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'. A red box highlights the 'Next >' button.

Bottom Screenshot: Shows the 'Delivery Group Assignment' dialog box. The 'Choose delivery groups' section has 'TestUser' selected. The 'Delivery groups to receive app assignment' section shows 'TestUser' listed. A red box highlights the 'Save' button.

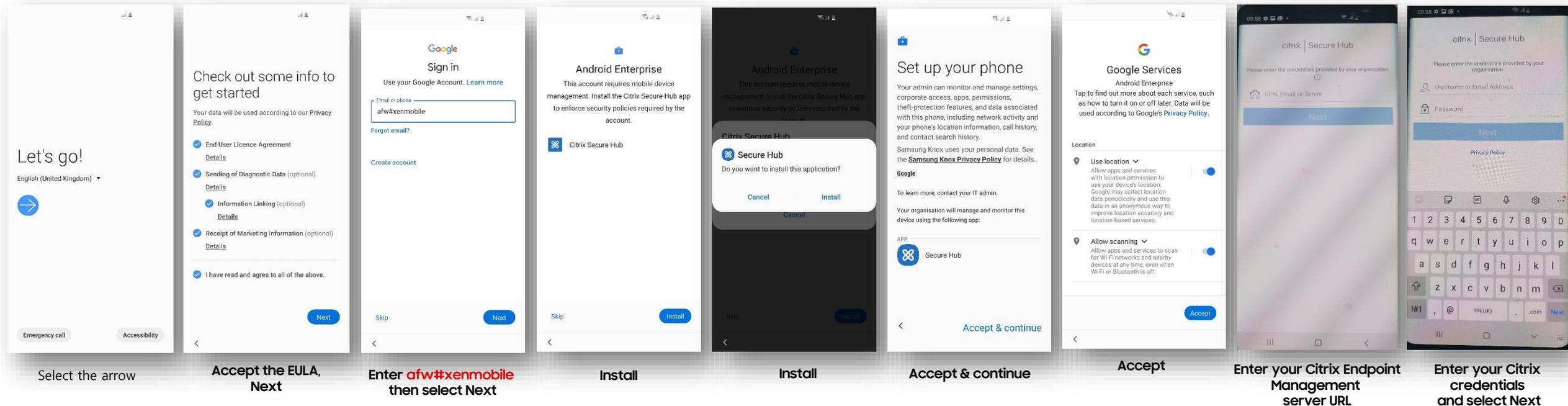
Android Enterprise: Fully Managed Device Enrollment

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.



Select the arrow

Accept the EULA, Next

Enter **afw#xenmobile** then select Next

Install

Install

Accept & continue

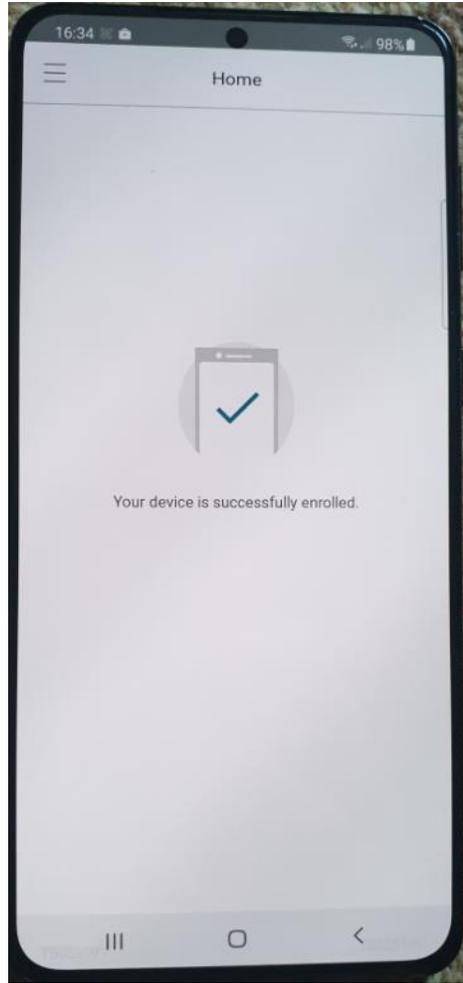
Accept

Enter your Citrix Endpoint Management server URL

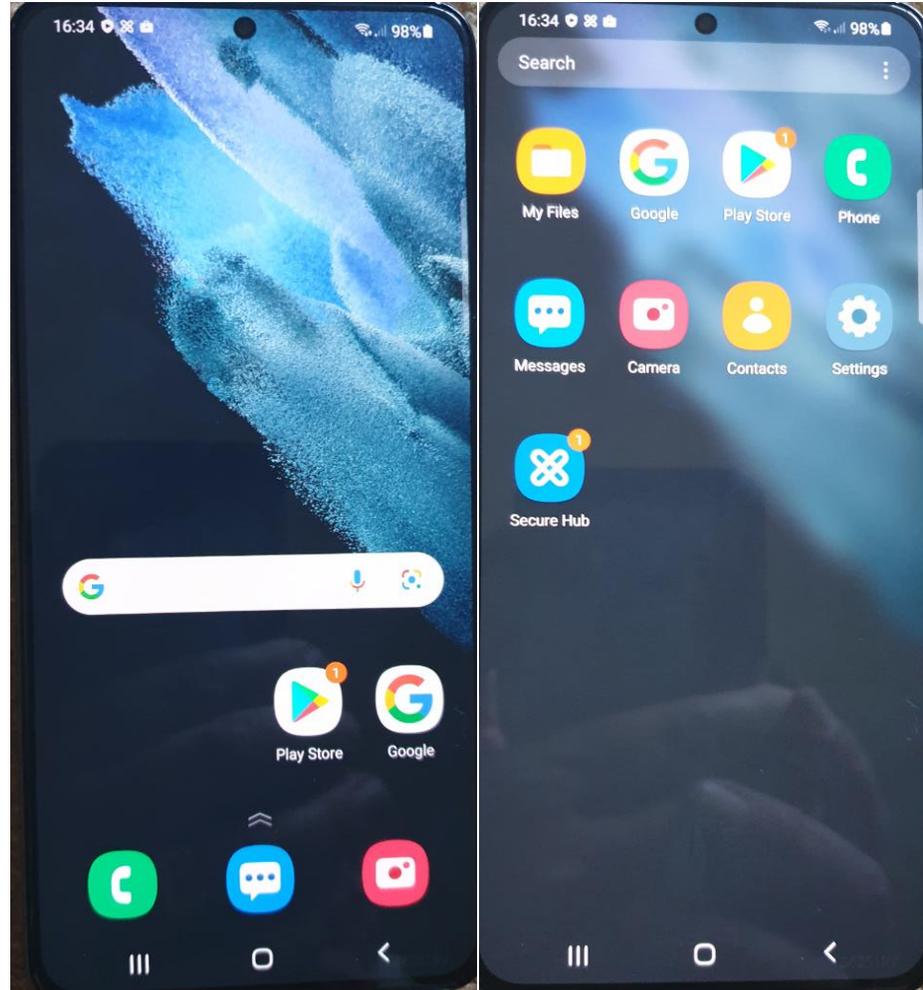
Enter your Citrix credentials and select Next

Android Enterprise: Fully Managed Device Enrollment

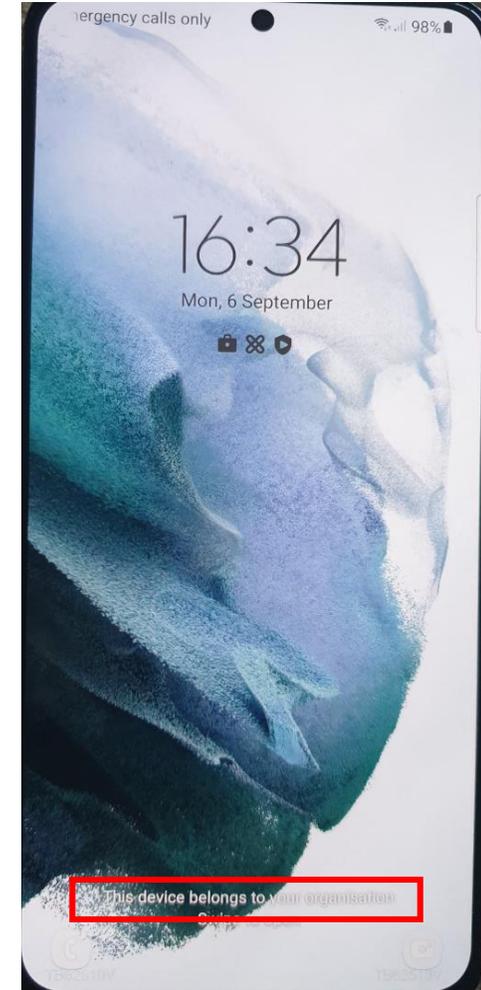
How to tell that a Fully Managed Device has been successfully set up:



Device is successfully enrolled



Sparse set of applications including Secure Hub

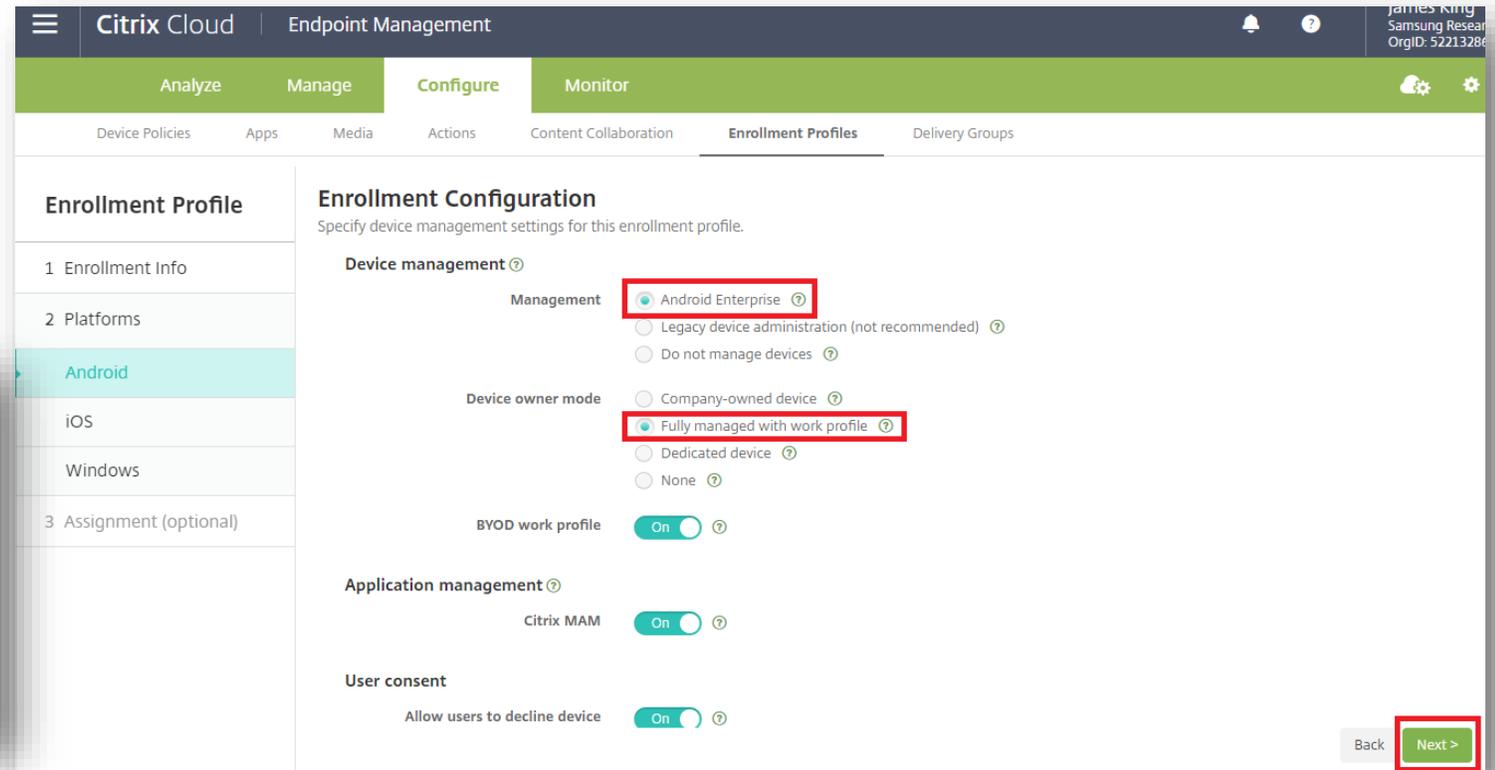
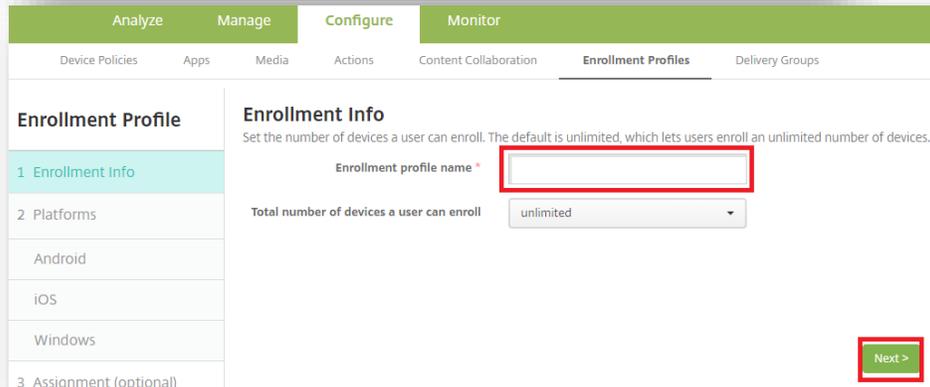
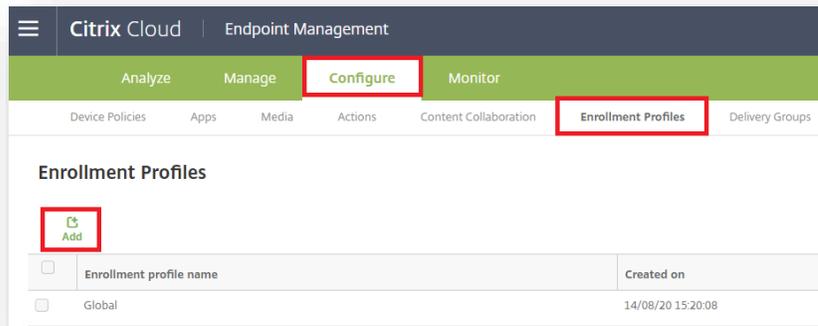


Device belongs to your organization on lock screen

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



Note: On the latest console, the second Device owner mode now reads:

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 configuration steps for a Work Profile.

Top Left Screenshot: Enrollment Configuration for iOS
The 'Enrollment Configuration' page for the 'iOS' platform. The 'Device management' section has 'Apple Device enrollment' selected. 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.

Top Right Screenshot: Enrollment Configuration for Windows
The 'Enrollment Configuration' page for the 'Windows' platform. The 'Device management' section has 'Fully managed' selected. 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.

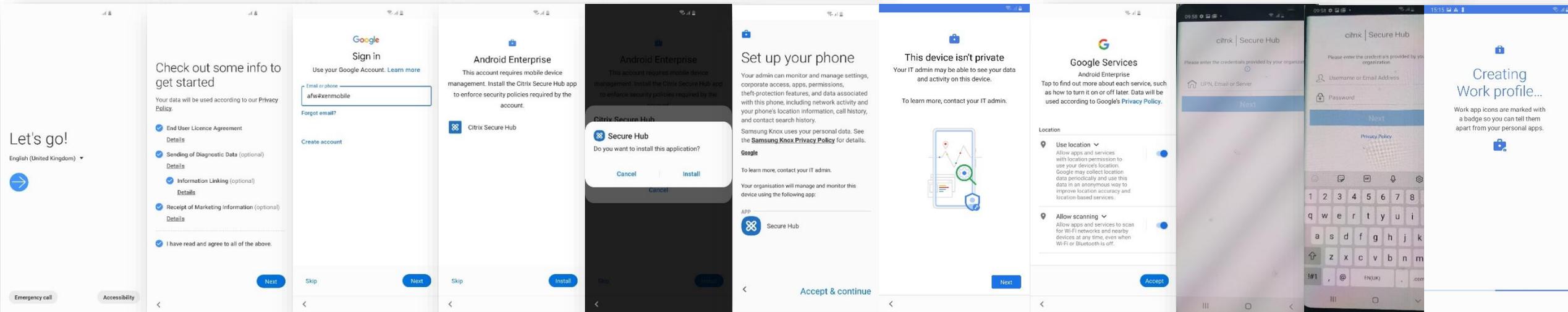
Bottom Screenshot: Delivery Group Assignment
The 'Delivery Group Assignment' dialog box. The 'Choose delivery groups' section has 'TestUser' selected with a red box around the checkbox. The 'Delivery groups to receive app assignment' section shows 'TestUser' listed. The 'Save' button is highlighted with 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.



Select the arrow Accept the EULA, Next Enter **afw#xenmobile** then select Next Install Install Accept & continue Next Accept Enter your Citrix Endpoint Management server URL and credentials and select Next Creating Work profile...

Android Enterprise: Fully Managed with a Work Profile Enrollment

How to tell that Fully Managed with a Work Profile has been successfully set up:



Personal Tab



Work Tab

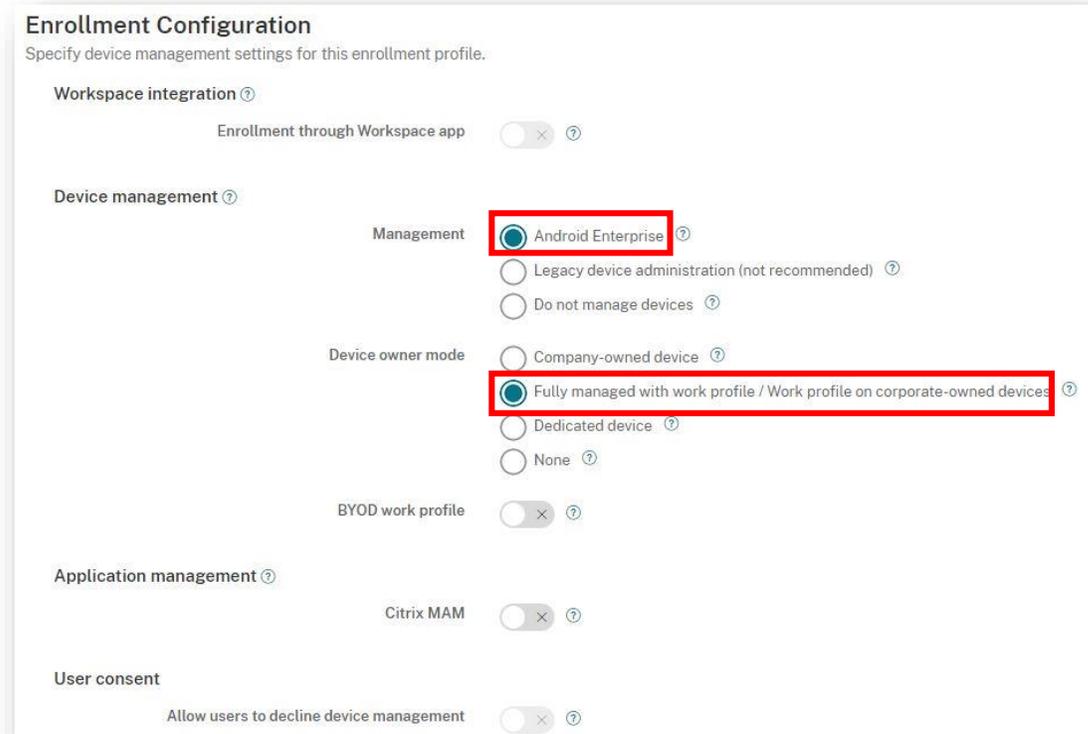
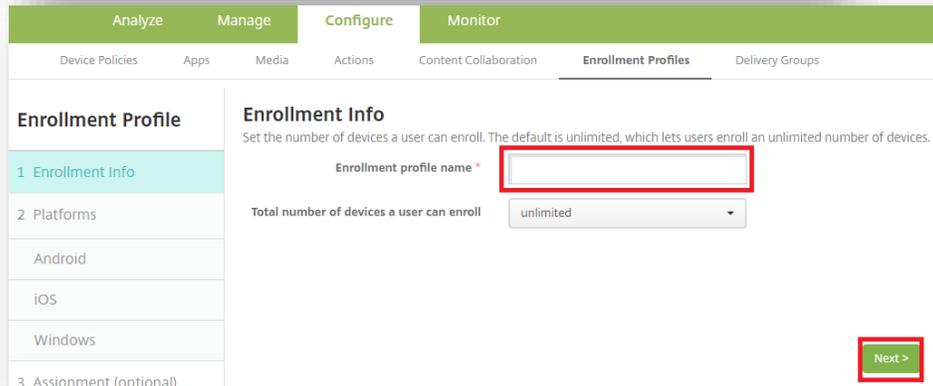
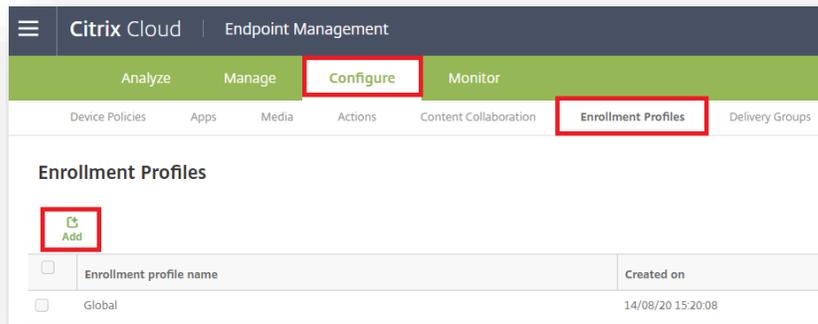


Device is managed by your organization on lock screen

Work Profile on a Company Owned Device Configuration

In order to enroll Work Profile on a Company Owned 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 Fully Managed with work profile/ Work profile on corporate-owned devices
- Select Next



Note: On the latest console, the second Device owner mode now reads:

20 Fully managed with work profile / Work profile on corporate-owned devices  **Secured by Knox**

Work Profile on a Company Owned 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 configuration steps for a Work Profile on a Company Owned Device.

Top Left Screenshot: Shows the "Enrollment Configuration" page for the "iOS" platform. The "Device management" section has "Apple Device enrollment" selected. The "Application management" section has "Citrix MAM" turned on. The "User consent" section has "Allow users to decline device management" turned on. The "Next >" button is highlighted with a red box.

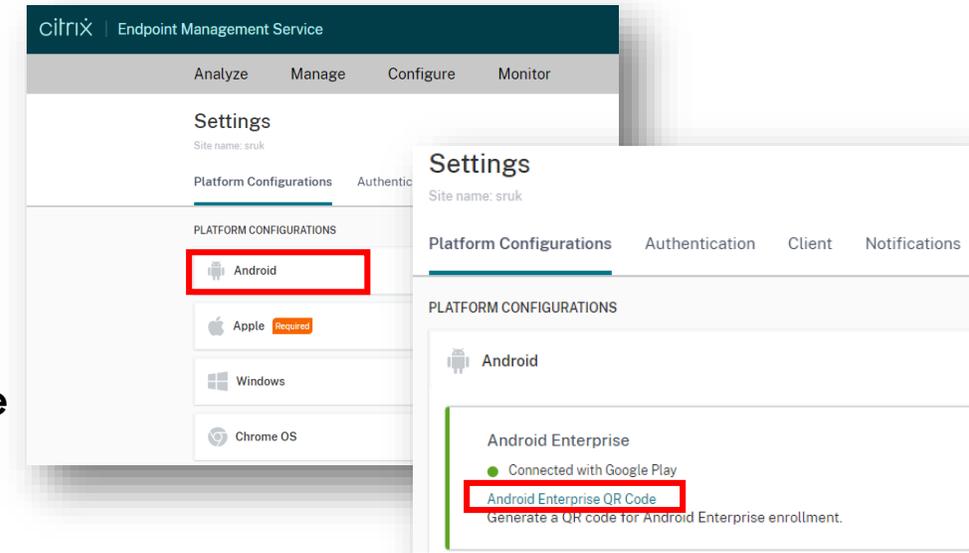
Top Right Screenshot: Shows the "Enrollment Configuration" page for the "Windows" platform. The "Device management" section has "Fully managed" selected. The "User consent" section has "Allow users to decline device management" turned on. The "Workspace integration" section has "Enrollment through Workspace app" turned off. The "Next >" button is highlighted with a red box.

Bottom Screenshot: Shows the "Delivery Group Assignment" dialog box. The "Choose delivery groups" section has "TestUser" selected with a red box. The "Delivery groups to receive app assignment" section shows "TestUser" listed. The "Save" button is highlighted with a red box.

At the time of writing, custom JSON code needs to be included in a QR Code or a KME Profile in order to enroll into WPC successfully.

To generate such a QR code, follow these steps:

- Within Endpoint Management navigate the Settings cog
- Select Android
- Select Android Enterprise QR Code
- Enter your server details, eg. domain.xm.cloud.com
- Enter your username and password to be used on the device
- Select Generate QR Code
- **IMPORTANT:**



To enroll devices in the work profile on corporate-owned devices mode, add **"desiredProvisioningMode": "managedProfile"**, to the custom JSON under **PROVISIONING_ADMIN_EXTRAS_BUNDLE**.

- Select Generate QR Code (again), resulting in:

Settings > Android Enterprise QR Code

Android Enterprise QR Code

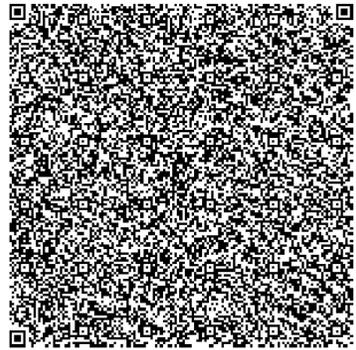
Generate a QR code for Android Enterprise enrollment. Specify the following information if needed or edit the JSON output directly.

Server FQDN

User name

Password

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBainzZRrrCQv6L006L10jcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
  "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
  "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
  "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
    "desiredProvisioningMode": "managedProfile",
    "serverURL": "domain.xm.cloud.com",
    "username": "username",
    "password": "password"
  }
}
```

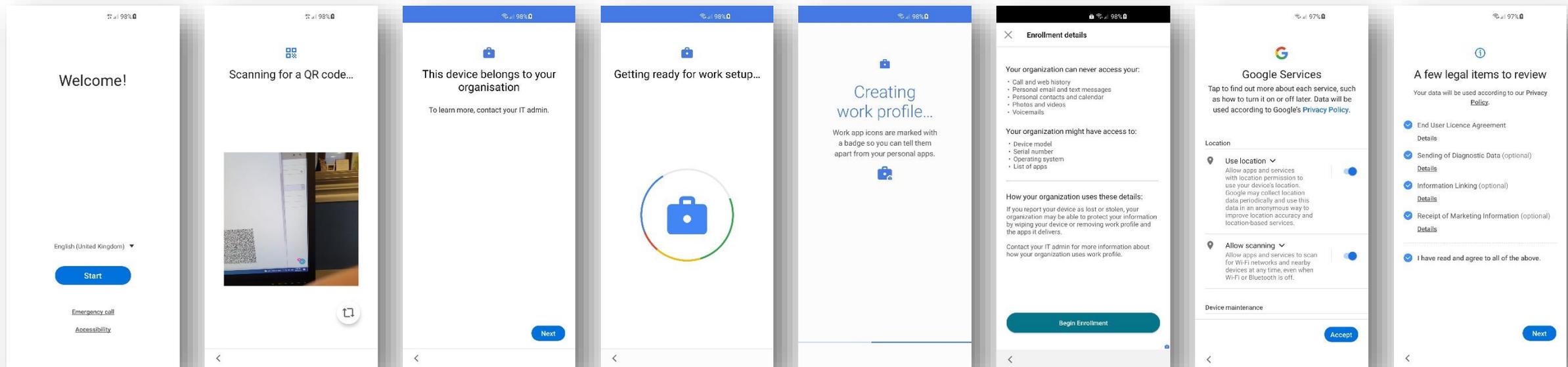


Android Enterprise: Work Profile on a Company Owned Device Enrollment

To enroll your device as an Android Enterprise Work Profile on a Company Owned Device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 2 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Work Profile on a Company Owned Device.

1. QR Code Enrollment / NFC Enrollment
2. Knox Mobile Enrollment

• Below is a screen-by-screen play to enroll your device using the QR Code method.



Select Start

Scan the QR code just generated & connect to WiFi

Select Next

Getting ready for work setup...

Creating work profile...

Begin Enrollment

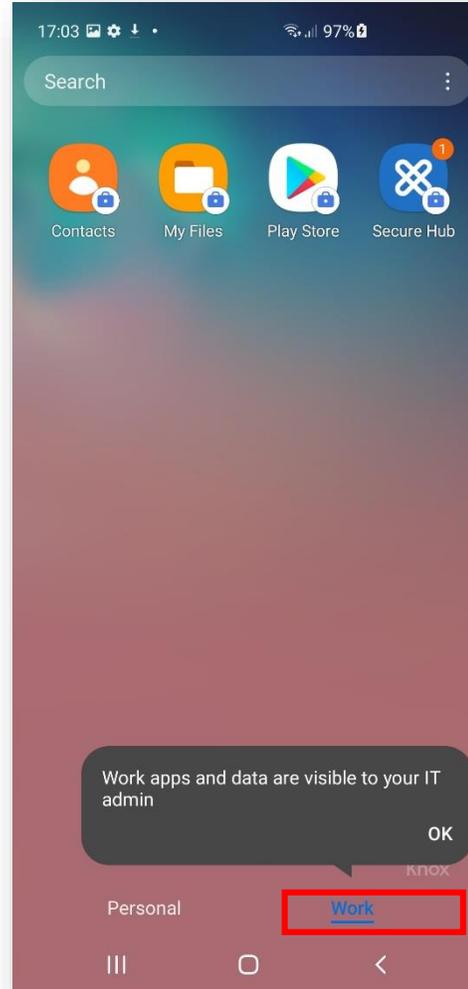
Accept Google Services

Accept the appropriate legal terms and select Next

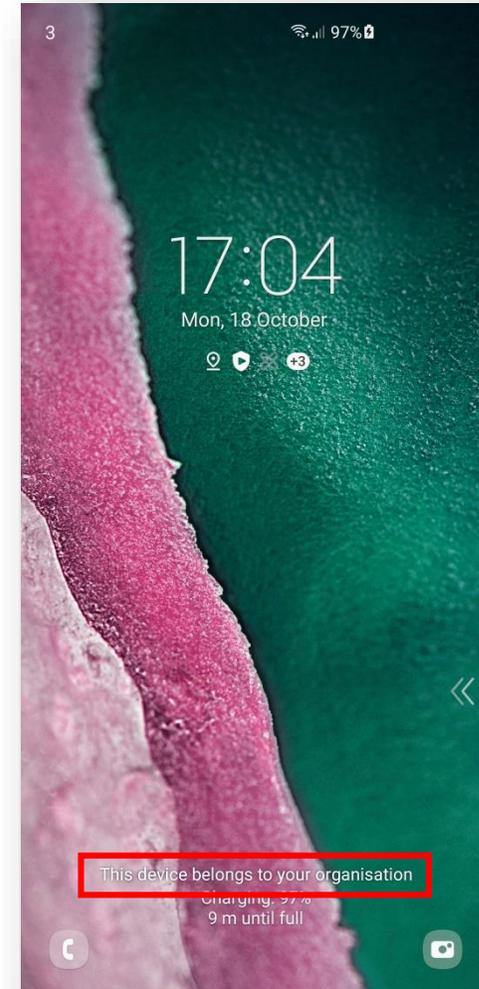
How to tell that Work Profile on a Company Owned Device has been successfully set up:



Personal Tab



Work Tab

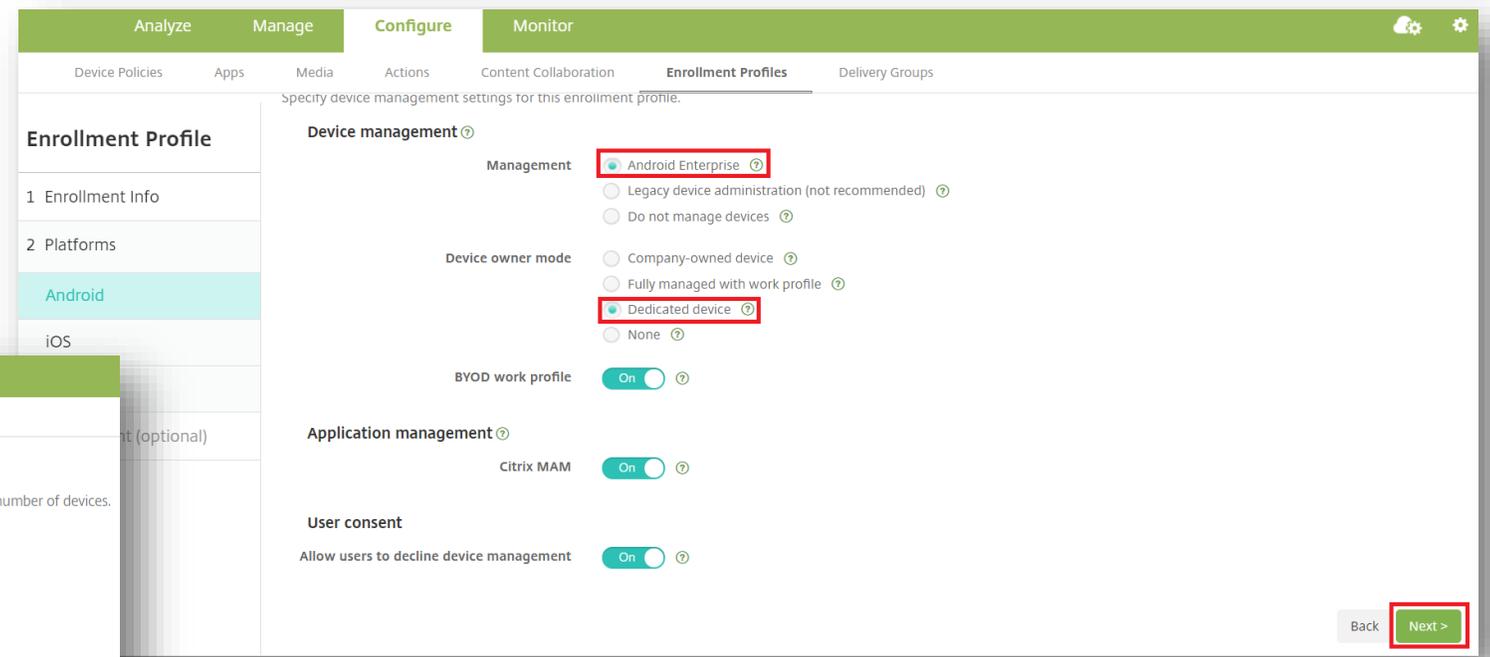
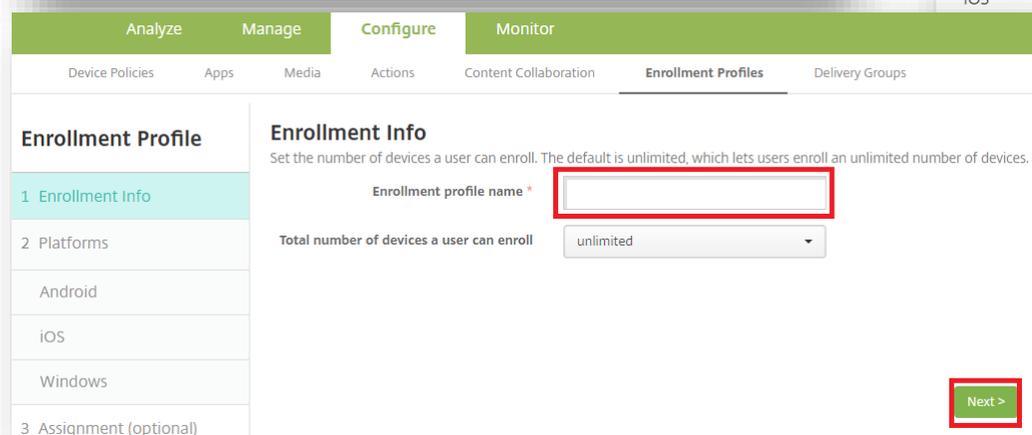
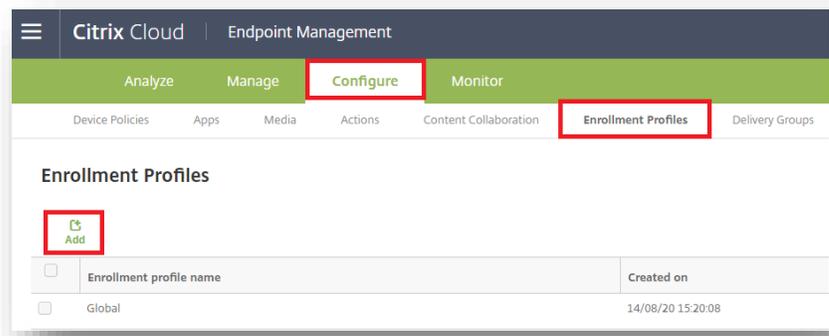


Device belongs to your organization on lock screen

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**



Note: On the latest console, the second Device owner mode now reads:

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 configuration process for different operating systems.

Top Left Screenshot (iOS Configuration): Shows the 'Enrollment Configuration' page for iOS. The 'Device management' section has 'Apple Device enrollment' selected. The 'Application management' section has 'Citrix MAM' set to 'On'. The 'User consent' section has 'Allow users to decline device management' set to 'On'. A red box highlights the 'Next >' button.

Top Right Screenshot (Windows Configuration): Shows the 'Enrollment Configuration' page for Windows. The 'Device management' section has 'Fully managed' selected. 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'. A red box highlights the 'Next >' button.

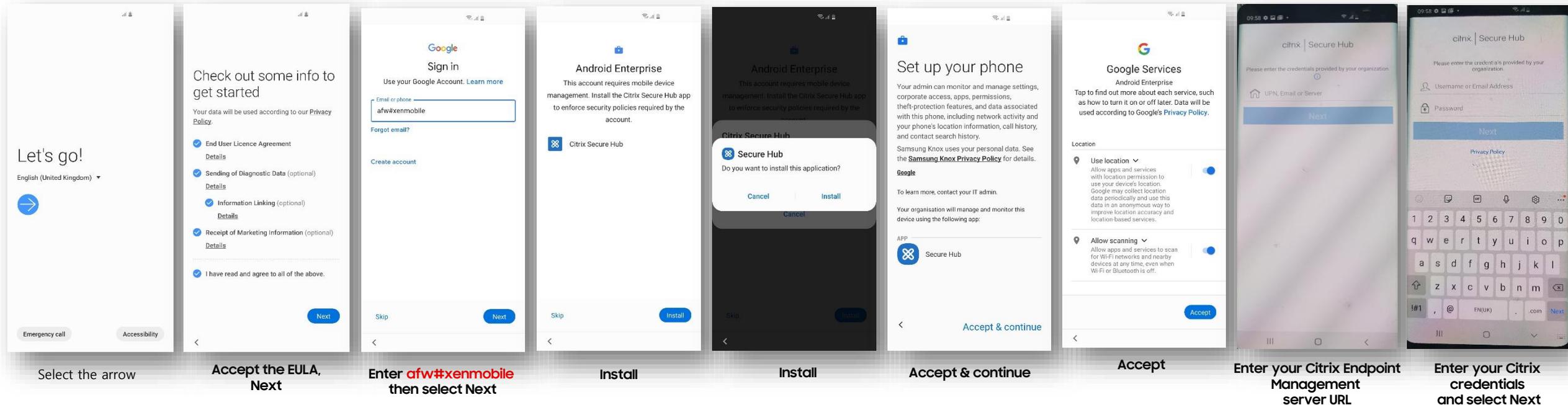
Bottom Screenshot (Delivery Group Assignment): Shows the 'Delivery Group Assignment' dialog box. The 'Choose delivery groups' section has 'TestUser' selected with a red box around the checkbox. The 'Delivery groups to receive app assignment' section shows 'TestUser' listed. A red box highlights the 'Save' button.

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 [FREE or \$ for some special options such as Dual DAR]

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

The screenshot shows the Citrix Cloud Endpoint Management console. The top navigation bar includes 'Citrix Cloud' and 'Endpoint Management'. Below this is a green navigation bar with 'Analyze', 'Manage', 'Configure', and 'Monitor'. Under 'Configure', there are sub-tabs: 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is selected and highlighted with a red box. Below the navigation, the 'Apps' section is displayed. It includes a heading 'Apps' and a sub-heading 'Use the MDX Service on Citrix Cloud to wrap an app for delivery.' Below this, there are three buttons: 'Add', 'Category', and 'Export'. The 'Add' button is highlighted with a red box. Below the buttons is a table with columns: 'Icon', 'App Name', and 'Type'. The table contains one row with a blue 'S' icon, 'Citrix Files' as the app name, and 'MDX' as the type.

Icon	App Name	Type
	Citrix Files	MDX

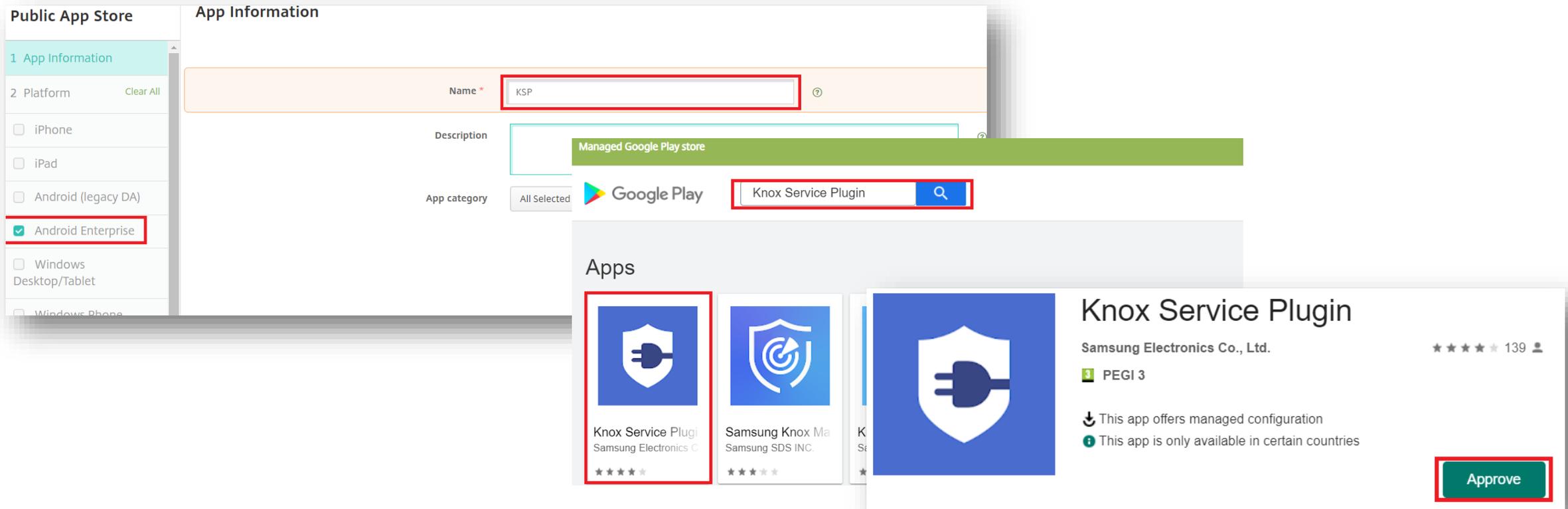
Public App Store

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 'Public App Store' interface with the following elements:

- Public App Store:** A sidebar on the left with a list of platform options:
 - 1 App Information
 - 2 Platform Clear All
 - iPhone
 - iPad
 - Android (legacy DA)
 - Android Enterprise**
 - Windows Desktop/Tablet
 - Windows Phone
- App Information:** A form area where:
 - Name:** A text input field containing 'KSP' is highlighted with a red box.
 - Description:** A text input field containing 'Managed Google Play store' is highlighted with a green box.
 - App category:** A dropdown menu is set to 'Google Play', and a search input field contains 'Knox Service Plugin' with a search icon, highlighted with a red box.
- Apps:** A list of search results showing:
 - Knox Service Plugi** by Samsung Electronics Co. (highlighted with a red box).
 - Samsung Knox Ma** by Samsung SDS INC.
 - Knox Service Plugin** (larger view):
 - Developer: Samsung Electronics Co., Ltd.
 - Rating: ★★★★★ 139
 - Content Rating: PEGI 3
 - Managed configuration: This app offers managed configuration.
 - Availability: This app is only available in certain countries.
 - Approve** button (highlighted with a red box).

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 configuration interface across three main sections:

- Managed Google Play:** A search bar contains the text "com.samsung.android.knox.kpu". Below it, search results for "Knox Service Plugin" by Samsung Electronics are shown, with the result highlighted by a red box.
- Delivery Group Assignments (optional):** This section allows assigning the app to delivery groups. Under "Choose delivery groups", the "TestUser" group is selected with a checked checkbox, highlighted by a red box. The "AllUsers" group is unselected. The "Delivery groups to receive app assignment" list on the right contains "TestUser".
- App Details:** A form for the app configuration. The "Name" field is filled with "Knox Service Plugin" and the "Description" field contains "For enterprise IT Admins to setup Knox policies on Samsung mobile devices." The "Next >" button is highlighted with a red box.

Navigation elements include "Back" and "Save" buttons at the bottom right of the main configuration area, and "Back" and "Next >" buttons at the bottom right of the app details form.

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 console navigation menu with the 'Configure' tab selected. Under 'Configure', 'Device Policies' is highlighted. Below this, the 'Device Policies' section has an 'Add' button highlighted. A table of existing policies is shown below:

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

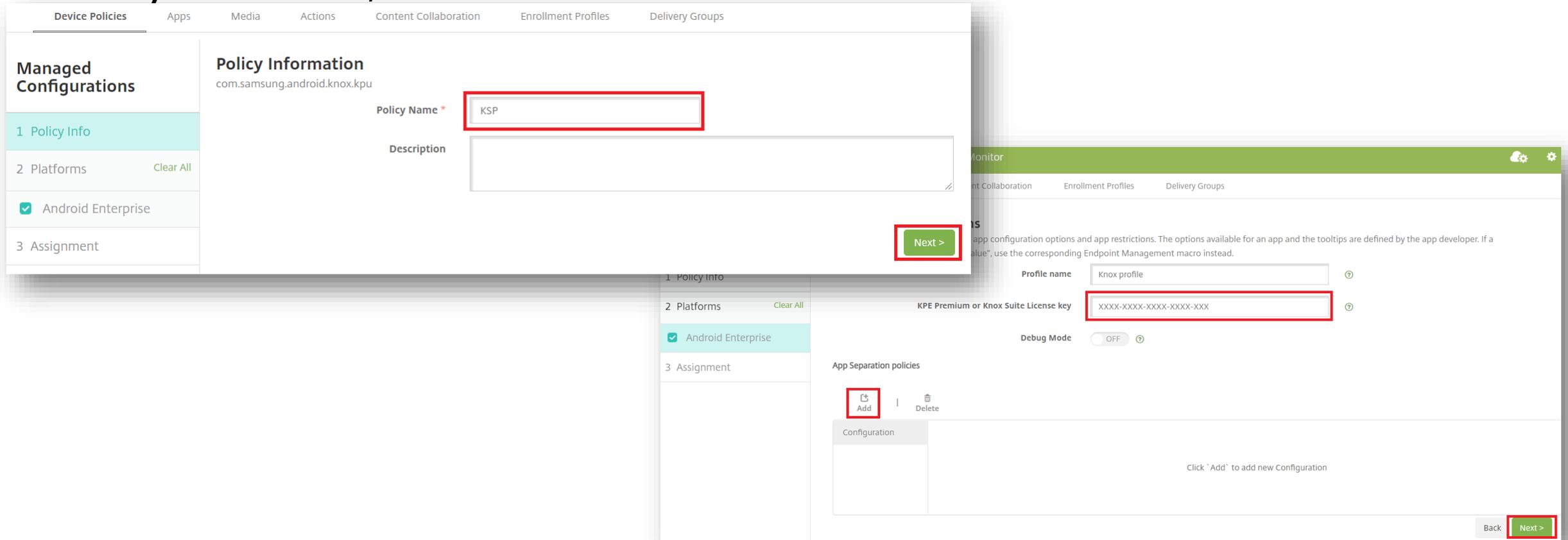
The screenshot shows the 'Add a New Policy' dialog. On the left, the 'Policy Platform' list has 'Android Enterprise' selected. The main dialog shows various policy categories. In the 'Security' section, 'Managed Configurations' is selected. A 'Select Application' modal is overlaid on top, showing the following configuration:

Platform	Android Enterprise
Application	Knox Service Plugin

An 'OK' button is visible at the bottom right of the modal.

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 screenshot displays the Knox configuration interface. The top navigation bar includes 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows 'Managed Configurations' with a list of steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section shows 'Policy Name' set to 'KSP' and a 'Description' field. A 'Next >' button is highlighted in green. The 'App Separation policies' section shows 'Profile name' as 'Knox profile', 'KPE Premium or Knox Suite License key' as 'XXXX-XXXX-XXXX-XXXX-XXXX', and 'Debug Mode' as 'OFF'. An 'Add' button is highlighted in red. The bottom right corner shows a 'Next >' button highlighted in green.

Configure Knox Platform for Enterprise using Knox Service Plugin

- Choose a delivery group
- Select Save

The screenshot displays the Knox configuration interface. The top navigation bar includes 'Analyze', 'Manage', 'Configure' (highlighted with a red box), and 'Monitor'. Below this, a secondary navigation bar lists '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'. The 'Assignment' step is selected in the left sidebar. In the 'Choose delivery groups' section, a search bar is present, and a list of delivery groups includes 'AllUsers' and 'TestUser', with 'TestUser' selected (checkbox checked and highlighted with a red box). The 'Delivery groups to receive app assignment' section on the right contains the text 'TestUser'. At the bottom right, there are 'Back' and 'Save' buttons, with the 'Save' button highlighted with a red box.

This is version 2.1 of this document.

Thank you!

