

Citrix Endpoint Management Knox Platform for Enterprise

October 2021
Samsung R&D Centre UK
(SRUK)

Agenda

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/>

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

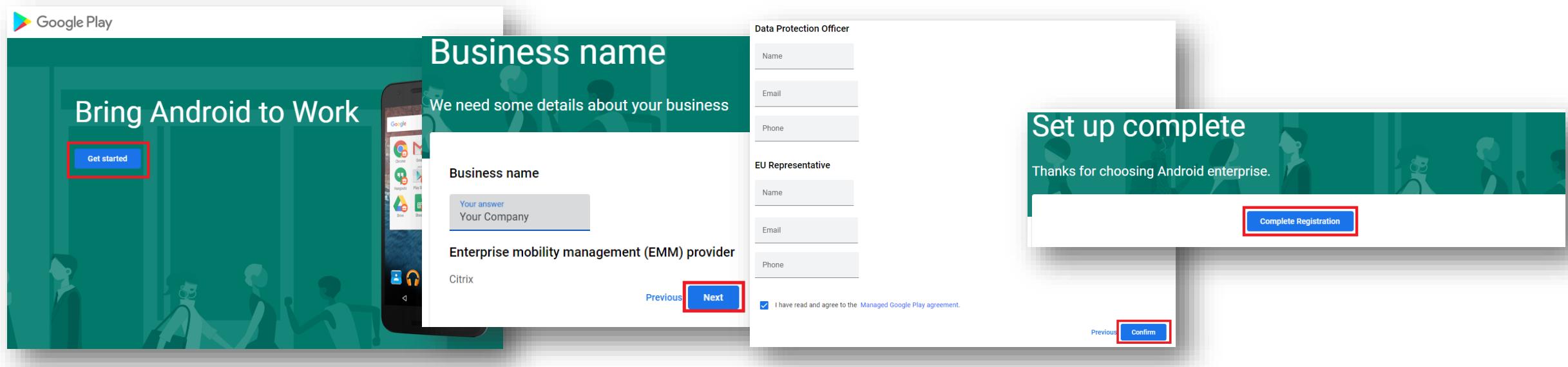
Configure Android Enterprise

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

The screenshot shows the Citrix Endpoint Management console interface. At the top, there's a green navigation bar with tabs: Analyze, Manage, Configure, and Monitor. On the far right of the top bar is a gear icon, which is highlighted with a red box. Below the navigation bar, the main content area has a title 'Settings'. Under 'Authentication', there are links for Derived Credentials for iOS and Identity Provider (IDP). Under 'Certificate Management', there are links for Certificates, Credential Providers, and PKI Entities. Under 'Client', there are links for Client Branding, Client Properties, and Client Support. In the center-left, under 'Notifications', there are links for Carrier SMS Gateway and Notification Server. Under 'Platforms', there are links for Alexa for Business, Android SafetyNet, Apple Configurator, Apple Deployment, and Google Chrome. The link 'Android Enterprise' is highlighted with a red box. To the right, under 'Server', there are links for ActiveSync Gateway, Citrix Gateway, Cloud Connector Allow List, Endpoint Management Tools, Enrollment, Firebase Cloud Messaging, and LDAP. A section titled 'Frequently Accessed Items' lists links for Android Enterprise, Enrollment, Certificates, Identity Provider (IDP), and Release Management. At the bottom, a large callout box contains the heading 'Android Enterprise ▾'. It says: '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 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.' Further down, it says: 'We are taking you out to Google Play to register Citrix as your EMM provider'. It explains: 'When you click Connect, a window opens. If a window doesn't open, check your pop-up settings.' Finally, it says: 'Sign in to Google Play with your corporate Google ID. Enter your organization name and confirm that Citrix is your EMM provider.' A large green 'Connect' button is at the bottom of this callout, also highlighted with a red box.

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



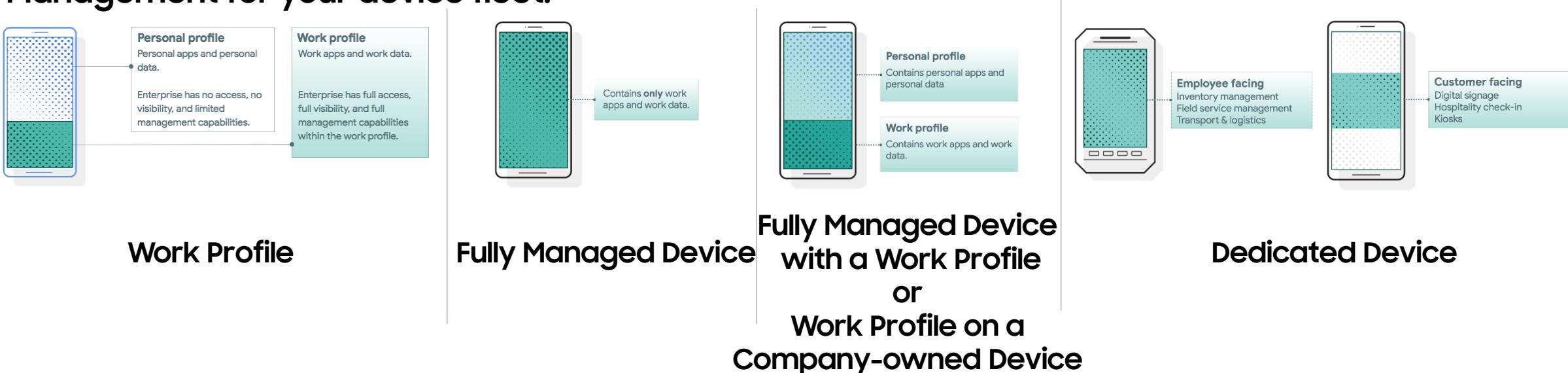
Android Enterprise Deployment Modes

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 shows the Citrix Cloud Endpoint Management interface. The top navigation bar has tabs for Analyze, Manage, Configure (which is highlighted with a red box), and Monitor. Below this, there are sub-tabs for Device Policies, Apps, Media, Actions, Content Collaboration, Enrollment Profiles (which is also highlighted with a red box), and Delivery Groups. On the left, under 'Enrollment Profiles', there is a red box around the 'Add' button. The main content area shows a step-by-step configuration process:

- Enrollment Info:** Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices. The 'Enrollment profile name' field is highlighted with a red box, and the 'Total number of devices a user can enroll' dropdown is set to 'unlimited'.
- Platforms:** Options include Android, iOS, and Windows.
- Assignment (optional):** This step is currently shown as optional.

On the right, the 'Enrollment Configuration' panel is displayed, titled 'Specify device management settings for this enrollment profile'. It includes sections for:

- Device management:** Management is set to 'Android Enterprise' (radio button highlighted with a red box).
- Device owner mode:** 'None' is selected (radio button highlighted with a red box).
- BYOD work profile:** The switch is set to 'On'.
- Application management:** Citrix MAM is set to 'On'.
- User consent:** 'Allow users to decline device management' is set to 'On'.

At the bottom right of the configuration panel is a red box around the 'Next >' button.

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

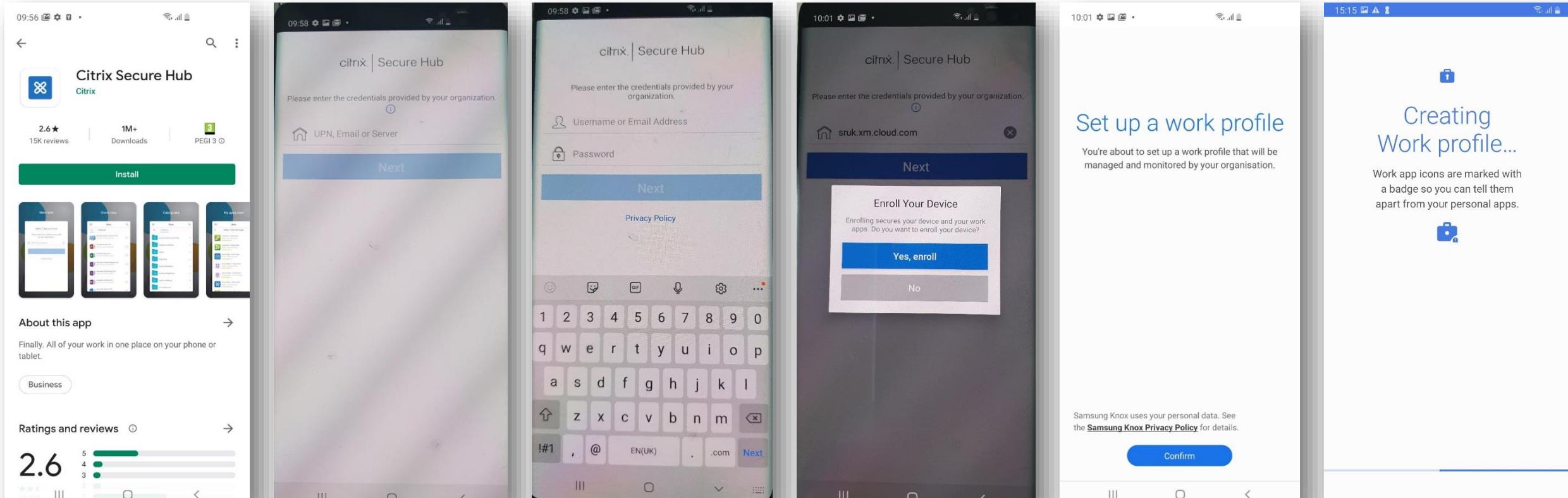
Work Profile Configuration

- 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 figure consists of three screenshots of the Citrix Cloud Endpoint Management interface, illustrating the configuration of an Enrollment Profile:

- Screenshot 1: Enrollment Configuration (iOS Platform)**
 - The "Device management" section shows "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.
 - A red box highlights the "Next >" button at the bottom right.
- Screenshot 2: Enrollment Configuration (Windows Platform)**
 - The "Device management" section shows "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.
 - A red box highlights the "Next >" button at the bottom right.
- Screenshot 3: Delivery Group Assignment (Assignment Step)**
 - The "Choose delivery groups" section shows "TestUser" selected (indicated by a red box).
 - The "Delivery groups to receive app assignment" section lists "TestUser".
 - A red box highlights the "Save" button at the bottom right.

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

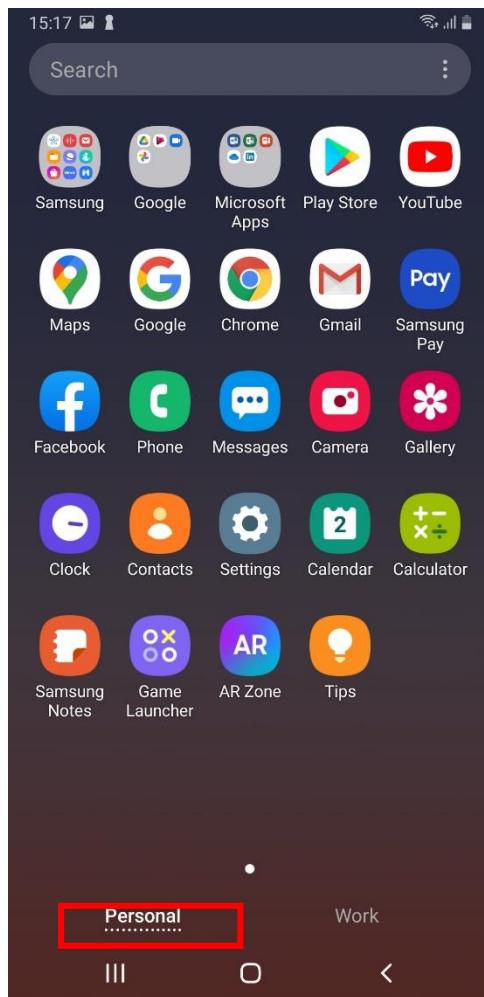
Yes, enroll

Confirm

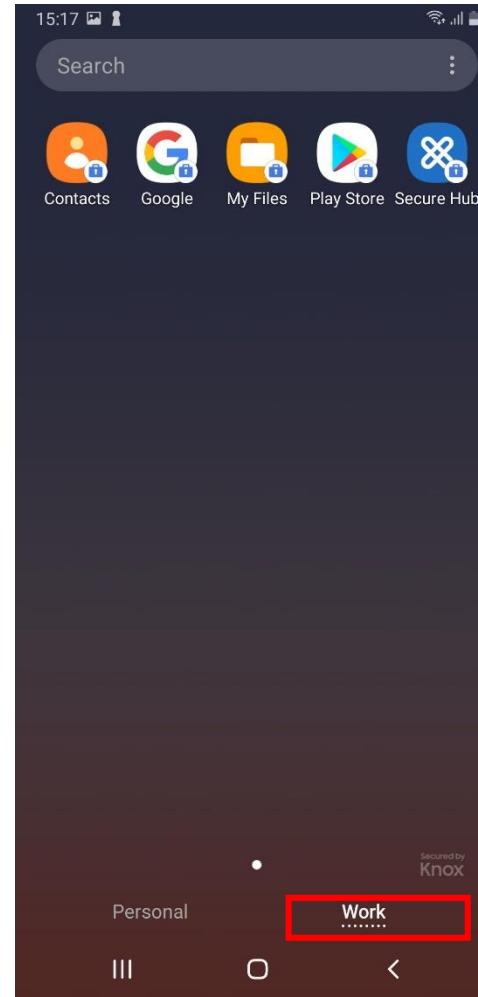
Creating Work profile...

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

Enrollment Profiles

Add

Enrollment profile name	Created on
Global	14/08/20 15:20:08

Enrollment Configuration

Specify device management settings for this enrollment profile.

Device management

Management: Android Enterprise Legacy device administration (not recommended) Do not manage devices

Device owner mode

Company-owned device: Fully managed with work profile Dedicated device None

BYOD work profile Off

Application management

Citrix MAM On

User consent

Allow users to decline device Off

Back **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 consists of three screenshots of the Citrix Cloud Endpoint Management interface, illustrating the steps for creating an enrollment profile.

- Screenshot 1: Enrollment Configuration (iOS Platform)**
Shows the "Enrollment Configuration" step for the iOS platform. It includes sections for "Device management" (Apple Device enrollment selected), "Application management" (Citrix MAM On), and "User consent" (Allow users to decline device management On). A red box highlights the "Next >" button at the bottom right.
- Screenshot 2: Enrollment Configuration (Windows Platform)**
Shows the "Enrollment Configuration" step for the Windows platform. It includes sections for "Device management" (Fully managed selected), "User consent" (Allow users to decline device management On), and "Workspace integration" (Enrollment through Workspace app Off). A red box highlights the "Next >" button at the bottom right.
- Screenshot 3: Delivery Group Assignment**
Shows the "Delivery Group Assignment" step. It lists "Choose delivery groups" with "TestUser" selected (indicated by a red box). A modal window shows "Delivery groups to receive app assignment" containing "TestUser". A red box highlights the "Save" button at the bottom right.

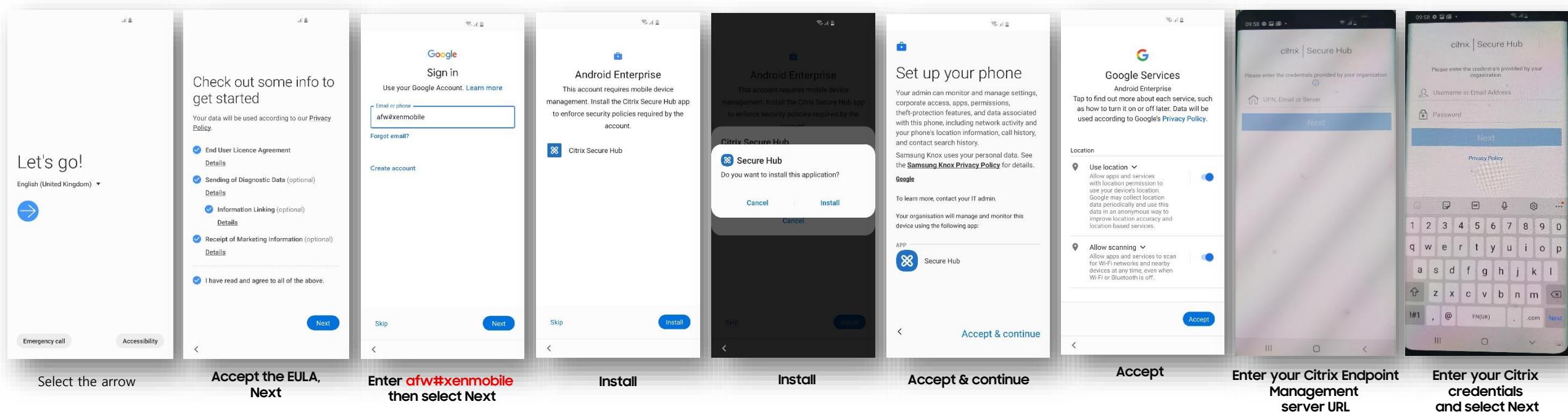
Android Enterprise: Fully Managed Device Enrollment

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.

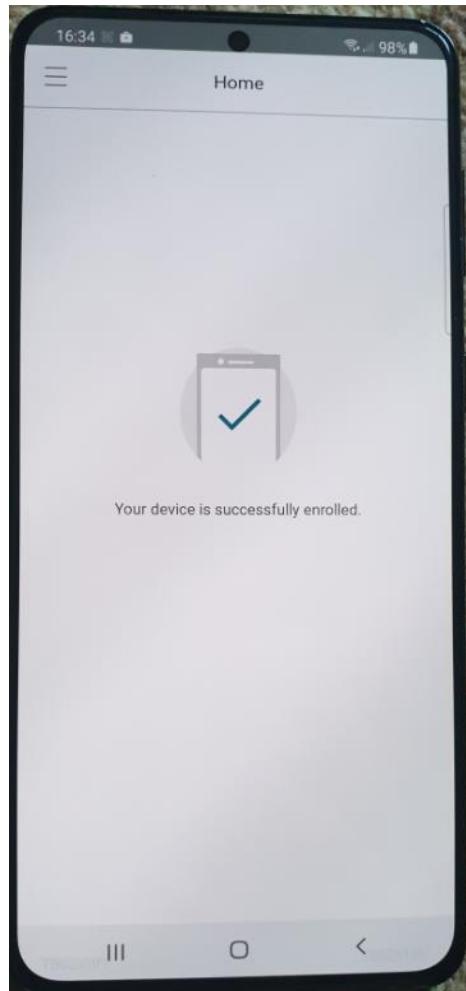
1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**
2. QR Code Enrollment / NFC Enrollment
3. Knox Mobile Enrollment

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

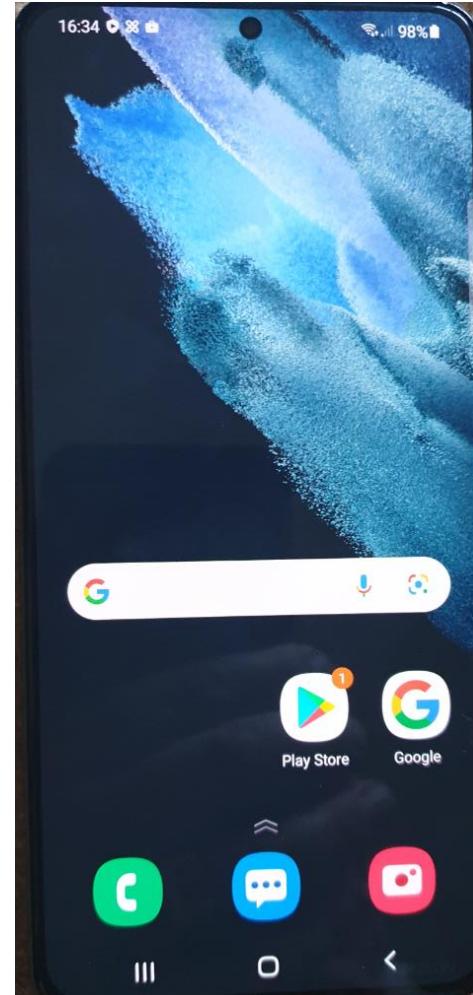


Android Enterprise: Fully Managed Device Enrollment

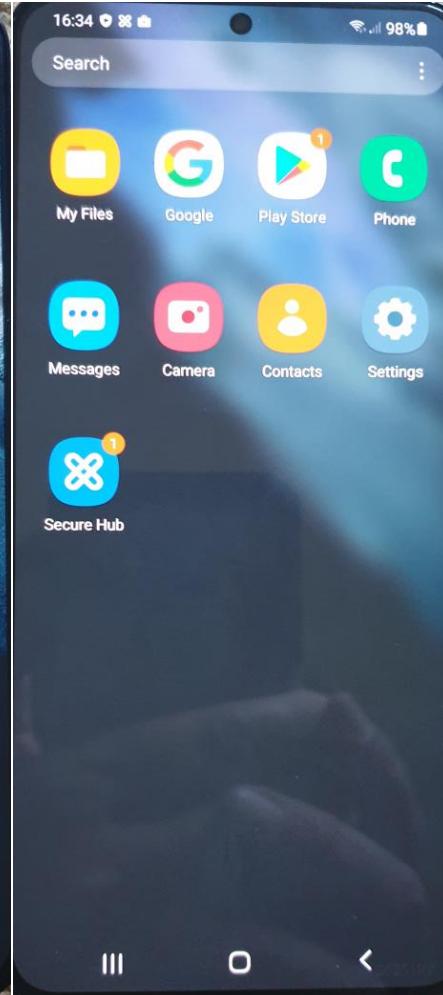
How to tell that a Fully Managed Device has been successfully set up:



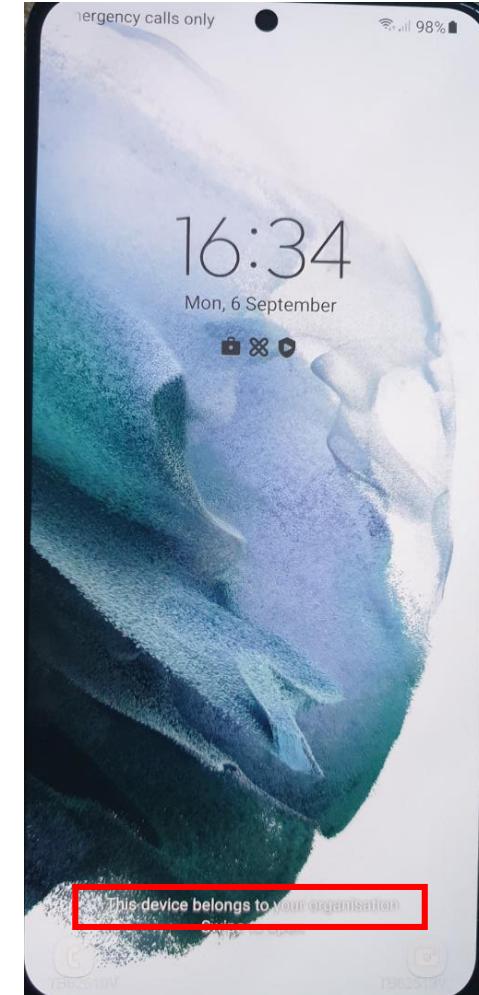
Device is successfully enrolled



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

Citrix Cloud | Endpoint Management

Analyze Manage **Configure** Monitor

Device Policies Apps Media Actions Content Collaboration **Enrollment Profiles** Delivery Groups

Enrollment Profiles

Add

Enrollment profile name	Created on
Global	14/08/20 15:20:08

Analyze Manage **Configure** Monitor

Device Policies Apps Media Actions Content Collaboration **Enrollment Profiles** Delivery Groups

Enrollment Profile

1 Enrollment Info

Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.

Enrollment profile name *

Total number of devices a user can enroll

2 Platforms

Android

iOS

Windows

3 Assignment (optional)

Next >

Citrix Cloud | Endpoint Management

Analyze Manage **Configure** Monitor

Device Policies Apps Media Actions Content Collaboration **Enrollment Profiles** Delivery Groups

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 **Android Enterprise**

Legacy device administration (not recommended)

Do not manage devices

Device owner mode

Fully managed with work profile

Company-owned device

Dedicated device

None

BYOD work profile

Application management

Citrix MAM

User consent

Allow users to decline device

Back **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 consists of three screenshots of the Citrix Cloud Endpoint Management interface, illustrating the steps to configure an enrollment profile:

- Screenshot 1: Enrollment Configuration (iOS Platform)**
Shows the "Enrollment Configuration" step for the iOS platform. It includes sections for "Device management" (Apple Device enrollment selected), "Application management" (Citrix MAM On), and "User consent" (Allow users to decline device management On). A red box highlights the "Next >" button at the bottom right.
- Screenshot 2: Enrollment Configuration (Windows Platform)**
Shows the "Enrollment Configuration" step for the Windows platform. It includes sections for "Device management" (Fully managed selected), "User consent" (Allow users to decline device management On), and "Workspace integration" (Enrollment through Workspace app Off). A red box highlights the "Next >" button at the bottom right.
- Screenshot 3: Delivery Group Assignment (Assignment Step)**
Shows the "Delivery Group Assignment" step. It lists "Choose delivery groups" with "TestUser" selected (indicated by a red box). A modal window shows "Delivery groups to receive app assignment" containing "TestUser". A red box highlights the "Save" button at the bottom right.

Android Enterprise: Fully Managed with a Work Profile Enrollment

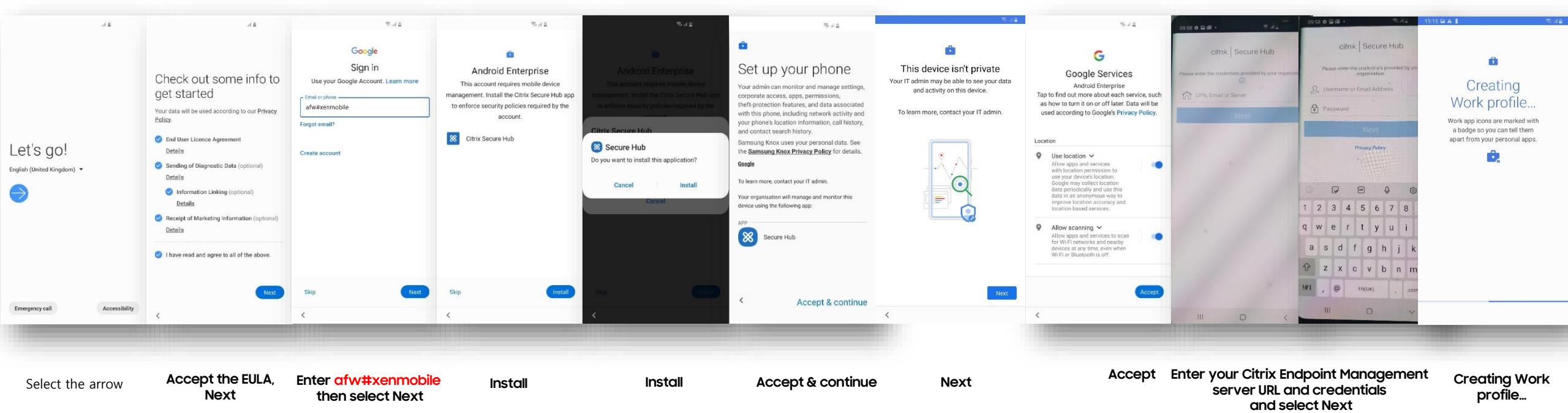
To enroll your device as an Android Enterprise Fully Managed with a Work Profile, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Fully Managed with a Work Profile.

1. DPC Identifier [Also known as the hashtag method] **afw#xenmobile**

2. QR Code Enrollment / NFC Enrollment

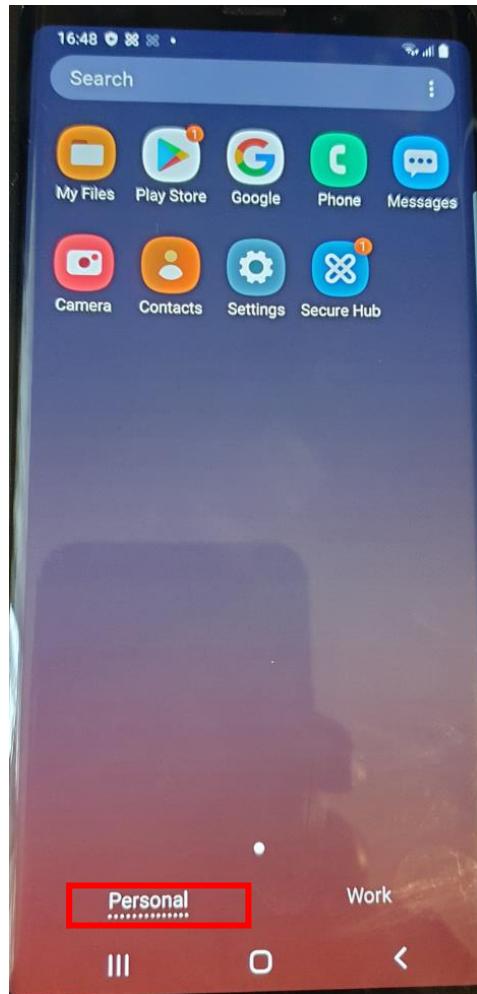
3. Knox Mobile Enrollment

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



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

The screenshot shows two views of the Citrix Cloud Endpoint Management interface. The top view displays the 'Enrollment Profiles' page with a red box around the 'Add' button. The bottom view shows the 'Enrollment Info' step of the enrollment process, where the 'Enrollment profile name' field and the 'Total number of devices a user can enroll' dropdown are highlighted with red boxes. A 'Next >' button at the bottom right is also highlighted with a red box.

The screenshot shows the 'Enrollment Configuration' dialog box. It includes sections for 'Workspace integration', 'Device management', 'Device owner mode', 'BYOD work profile', 'Application management', and 'User consent'. In the 'Device management' section, 'Android Enterprise' is selected under 'Management'. In the 'Device owner mode' section, 'Fully managed with work profile / Work profile on corporate-owned devices' is selected. Both of these options are highlighted with red boxes.

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

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 consists of three screenshots of the Citrix Cloud Endpoint Management interface, illustrating the steps to configure an Enrollment Profile:

- Screenshot 1: Enrollment Configuration (iOS Platform)**
 - Shows Device management (Apple Device enrollment selected), Application management (Citrix MAM On), and User consent (Allow users to decline device management On).
 - A red box highlights the "Next >" button at the bottom right.
- Screenshot 2: Enrollment Configuration (Windows Platform)**
 - Shows Device management (Fully managed selected), User consent (Allow users to decline device management On), and Workspace integration (Enrollment through Workspace app Off).
 - A red box highlights the "Next >" button at the bottom right.
- Screenshot 3: Delivery Group Assignment**
 - Shows the "Choose delivery groups" section with "TestUser" selected (highlighted with a red box).
 - The "Delivery groups to receive app assignment" list contains "TestUser".
 - A red box highlights the "Save" button at the bottom right.

Android Enterprise: Work Profile on a Company Owned Device Enrollment



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:

The first screenshot shows the 'Platform Configurations' section with 'Android' selected. The second screenshot shows the 'Android Enterprise' configuration with 'Connected with Google Play' status and the 'Android Enterprise QR Code' button highlighted.

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:

The screenshot shows the 'Android Enterprise QR Code' generator. It includes fields for Server FQDN (domain.xm.cloud.com), User name (username), and Password (password). To the right, the generated JSON code is displayed, with the 'desiredProvisioningMode' field highlighted. Below the JSON is a 'Generate QR Code' button, and to the far right is a large QR code.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBainzRrrjCQv6L006L10jcxT3-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

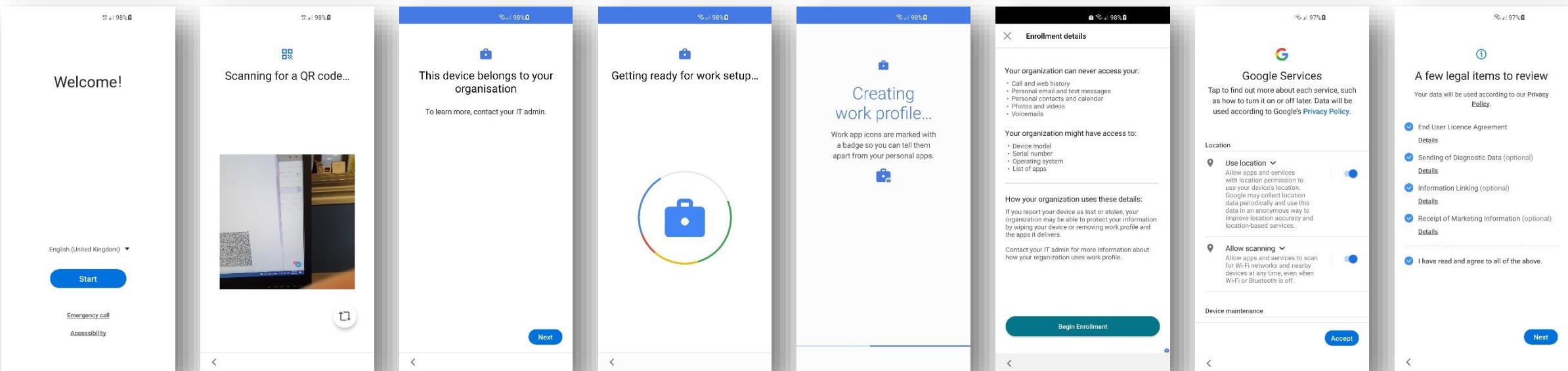


To enroll your device as an Android Enterprise Work Profile on a Company Owned Device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 2 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Work Profile on a Company Owned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

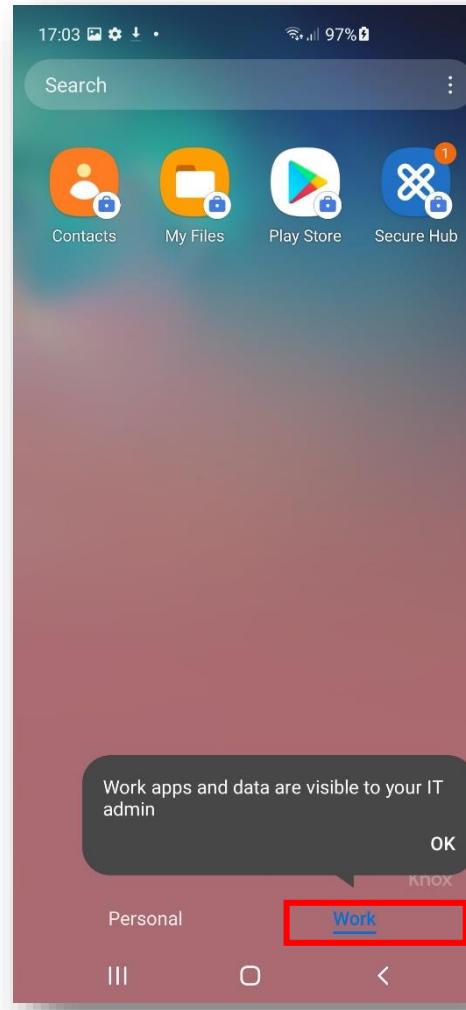
Android Enterprise: Work Profile on a Company Owned Device Enrollment



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

Citrix Cloud | Endpoint Management

Analyze Manage Configure Monitor

Enrollment Profiles

Add

Enrollment profile name	Created on
Global	14/08/20 15:20:08

Analyze Manage Configure Monitor

Device Policies Apps Media Actions Content Collaboration Enrollment Profiles Delivery Groups

Enrollment Profile

1 Enrollment Info

2 Platforms

Android

iOS

Management

Android Enterprise

Legacy device administration (not recommended)

Do not manage devices

Device owner mode

Dedicated device

Company-owned device

Fully managed with work profile

None

BYOD work profile

On

Application management

Citrix MAM

On

User consent

Allow users to decline device management

On

Back 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 consists of three screenshots of the Citrix Cloud Endpoint Management interface, illustrating the steps for creating an enrollment profile and assigning it to a delivery group.

- Screenshot 1: Enrollment Configuration (iOS Platform)**
Shows the "Enrollment Configuration" screen for the iOS platform. It includes sections for "Device management" (Apple Device enrollment selected), "Application management" (Citrix MAM On), and "User consent" (Allow users to decline device management On). A red box highlights the "Next >" button at the bottom right.
- Screenshot 2: Enrollment Configuration (Windows Platform)**
Shows the same "Enrollment Configuration" screen but for the Windows platform. It includes sections for "Device management" (Fully managed selected), "User consent" (Allow users to decline device management On), and "Workspace integration" (Enrollment through Workspace app Off). A red box highlights the "Next >" button at the bottom right.
- Screenshot 3: Delivery Group Assignment**
Shows the "Delivery Group Assignment" dialog. It lists "Choose delivery groups" with "TestUser" selected (indicated by a red box). The "Delivery groups to receive app assignment" section shows "TestUser". A red box highlights the "Save" button at the bottom right.

Android Enterprise: Dedicated Device Enrollment

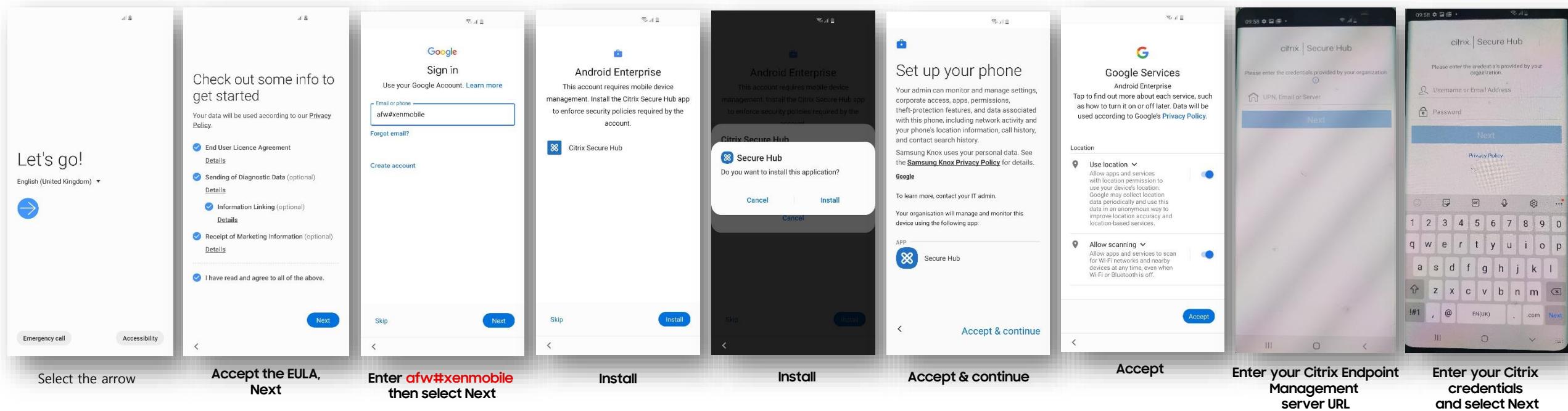
To enroll your device as an Android Enterprise Dedicated device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Citrix Endpoint Management as an Android Enterprise Dedicated device.

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.



Knox Platform for Enterprise

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 interface. The top navigation bar has tabs: Analyze, Manage, **Configure**, and Monitor. The **Configure** tab is highlighted with a red box. Below it, a sub-navigation bar has tabs: Device Policies, **Apps** (which is also highlighted with a red box), Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups. On the left, a sidebar shows a tree structure with 'Apps' selected. The main content area has a heading 'Public App Store'. It contains the text: 'Free or paid apps available in a public app store, such as iTunes or Google Play, for download.' and 'Example: GoToMeeting'. A red box highlights the 'Public App Store' section.

Citrix Cloud | Endpoint Management

Analyze Manage **Configure** Monitor

Device Policies **Apps** Media Actions Content Collaboration Enrollment Profiles Delivery Groups

Apps

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

Add Category Export

	Icon	App Name	Type
<input type="checkbox"/>		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 shows the 'Public App Store' interface for configuring the Knox Service Plugin. On the left, a sidebar lists platforms: iPhone, iPad, Android (legacy DA), **Android Enterprise** (selected and highlighted with a red box), Windows Desktop/Tablet, and Windows Phone. The main area is titled 'App Information' with tabs for '1 App Information' and '2 Platform'. The 'Name' field contains 'KSP' and is highlighted with a red box. The 'Description' field says 'Managed Google Play store'. Under 'App category', 'Google Play' is selected, and 'Knox Service Plugin' is typed into the search bar, which is also highlighted with a red box. Below this, the 'Apps' section shows three results: 'Knox Service Plugin' by Samsung Electronics Co., Ltd. (highlighted with a red box), 'Samsung Knox Ma...' by Samsung SDS INC., and another 'Knox Service Plugin' entry. The right side shows a detailed view of the first result: 'Knox Service Plugin' by Samsung Electronics Co., Ltd., rated 4.5 stars (139 reviews). It includes a note: 'This app offers managed configuration' and 'This app is only available in certain countries'. A large green 'Approve' button is at the bottom right of this card, also 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 shows the Knox Platform for Enterprise configuration interface. The top navigation bar has tabs: Analyze, Manage, Configure (selected), and Monitor. Below the tabs, there are sub-tabs: Device Policies, Apps (selected), Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups.

The main content area is divided into sections:

- Public App Store:** A list of platforms:
 - 2 Platform
 - iPhone
 - iPad
 - Android (legacy DA)
 - Android Enterprise
 - Windows Desktop/Tablet
 - Windows Phone
 - 3 Approvals (optional)
 - 4 Delivery Group Assignments (optional) (highlighted with a red box)
- Delivery Group Assignments (optional):** A section titled "Assign this app to one or more delivery groups." It includes a search bar and a list of delivery groups:
 - AllUsers
 - TestUser (highlighted with a red box)
- Deployment Schedule:** A section with a "Next >" button.
- Managed Google Play:** A search interface with a search bar containing "com.samsung.android.knox.kpu" and a "Search" button. The results show a single item:
 - Knox Service Plugin Samsung Electronics ... (highlighted with a red box)
- App Details:** A form with fields:
 - Name *: Knox Service Plugin
 - Description *: For enterprise IT Admins to setup Knox policies on Samsung mobile devices.
- Buttons:** Back, Next > (highlighted with a red box), Save (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 Platform for Enterprise configuration interface. On the left, there's a navigation bar with tabs: Analyze, Manage, Configure (highlighted with a red box), and Monitor. Below this is a sub-navigation bar with Device Policies (highlighted with a red box), Apps, Media, Actions, and Content Collaboration. Under Device Policies, there's an 'Add' button (highlighted with a red box) and a table listing existing policies: Passcode and App Inventory. On the right, the 'Configure' tab leads to the 'Device Policies' screen. In the top right of this screen, there's a 'Policy Platform' dropdown showing various platforms with counts: iOS (9), Windows Desktop/Tablet (10), Android (legacy DA) (11), macOS (7), and Android Enterprise (20). The 'Android Enterprise' option is selected and highlighted with a red box. Below this is a 'Policies most often used' section with Exchange, Location, Passcode, Restrictions, Scheduling, and WiFi. To the right of these sections are tabs for Security, Apps, and Files. A 'Managed Configurations' section is also visible. A modal window titled 'Select Application' is open in the bottom right, showing a 'Platform' dropdown set to 'Android Enterprise' and an 'Application' dropdown set to 'Knox Service Plugin'. An 'OK' button is 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 shows the Knox Platform for Enterprise configuration interface. It consists of two main windows:

- Top Window (Policy Information):** This window is titled "Policy Information" and shows the "Policy Name" field set to "KSP". The "Description" field is empty. A red box highlights the "Next >" button at the bottom right of this window.
- Bottom Window (KPE Premium or Knox Suite License key):** This window contains the following fields:
 - "Profile name": Set to "Knox profile".
 - "KPE Premium or Knox Suite License key": Set to "XXXX-XXXX-XXXX-XXXX-XXXX".
 - "Debug Mode": Set to "OFF".A red box highlights the "Add" button under "App Separation policies". Another red box highlights the "Next >" button at the bottom right of this window.

Configure Knox Platform for Enterprise using Knox Service Plugin

- Choose a delivery group
- Select Save

The screenshot shows the 'Managed Configurations' screen in the Knox Platform for Enterprise interface. The 'Configure' tab is selected. In the 'Delivery Groups' section, 'TestUser' is selected. The 'Save' button is highlighted with a red box.

Managed Configurations
com.samsung.android.knox.kpu

Choose delivery groups

Type to search

AllUsers

TestUser

Delivery groups to receive app assignment

TestUser

Back

Save

Document Information

This is version 2.1 of this document.

Thank you!

