

Knox Manage

How to use “Shared device”

What is shared device?

Shared device for multiple users:

- Starting with the KM 21.6 release, IT admins can set up devices so that multiple users can share the same device. This feature is particularly useful for devices that are used by visitors, guest users, or shift workers. This feature is available for all Samsung tablet devices and non-Samsung mobile devices running Android 9 OS or higher and Only Work Profile controls in Android Enterprise profile applies to shared device.

Creating “shared device” user.

- To use the phone as “shared device” it will be necessary to create an user as “Staging User”, as shown on the example.
- Insert all the mandatory fields (fields with red star)
- Select the option “Yes” on “Staging User”
- Select the type of “User” that would be created:

Temporary – option to be used by visitors/guest. When “checkout” is done, all the user information will be deleted from phone .

Persistent – option to be used by shift workers. The phone will keep user information when checkout is done. Another employee can use the same phone just entering his user. No information will be shared through users from same phone.

Add User

Enter all required fields to add a user. The user can sign in using the ID and password you entered below.

User ID * @labsouza.samsung.com

Password * ☐ Reset after Sign-in

Confirm Password *

User Name *

Email *

Mobile Number

User Group / Organization * 1 Selected

Name	Type
labsouza.samsung.com(Default Group)	User Group

License * ? ☒ Knox Suite ☐ Knox Manage

Staging User * ? ☒ Yes ☐ No

- Shared Device Type * ? ☐ Temporary ☒ Persistent

Enrolling the device as shared.

- The enroll can be done using KME or QR code or afw#knoxmanage
- Use the Persistent or Temporary account to enroll the device
- The example below was using KME to enroll the Device.

Devices

UPLOADS (5) ALL DEVICES (1) BULK ACTIONS

< Uploaded by Sidi

Upload date: 04 Aug 2021
Order date: Unavailable
Devices: 1 Device

All 1 device(s) on this page selected.

<input checked="" type="checkbox"/>	IMEI / MEID	SERIAL NUMBER	MODEL ▼	USER ID	TAGS
<input checked="" type="checkbox"/>	35250447000	RX2R2010	SM-T575		

352504470006714

Profile assigned

Profile: labsouza

User ID: tab_act_3_shared

Password:

Tags: Add a tag

Modified: 05 Aug 2021 14:28:11 by Luis Souza

Device IMEI: 35250447000

Device SN: RX2R2010

Model: SM-T575

Wi-Fi: Device MAC address: 28:C2:1F:DB:1A:58

Upload ID: 55eb8b9f-aa19-4d56-af16-93f18e9520a6

Order number: -

Uploaded: 04 Aug 2021 11:47:55 by Sidi

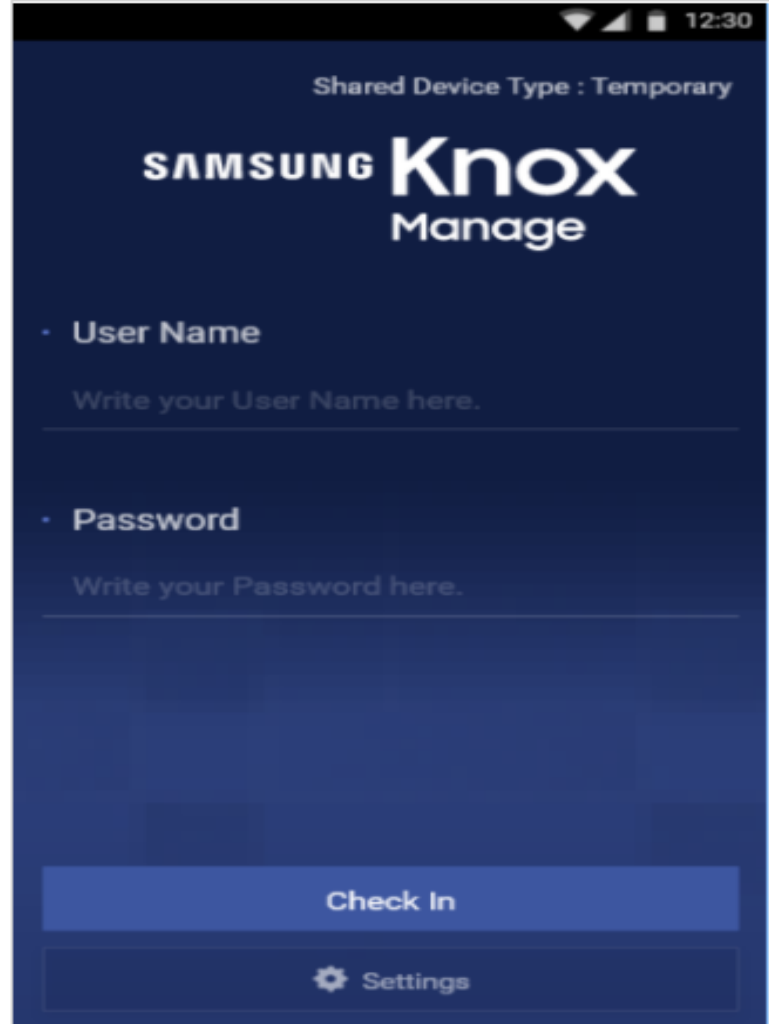
How it is shown on KM console.

- Through “Device” menu from KM console It is possible to confirm that device was successful enrolled as shared device.

<input type="checkbox"/>	Status	Last Seen	Device Name	IMEI / MEID	Serial Number	User Name	Device Tag	Platform & Manage Type	Mobile Number	Enrolled Type	Last Updated
<input type="checkbox"/>	 Enrolled	2m	tab_act_3_shared_Android_1	3525044700	RX2R201	Tab_act_3	-	 Shared (Persistent)	-	KME	08/05/2021 See History.

Check-in screen.

- After complete the enrollment with Persistent account the phone will open a kiosk screen called “Check-in”
- The phone will remain on this screen till a “normal” user (non-shared account) execute the login on the device.



The screenshot shows a mobile device screen with a dark blue background. At the top, the status bar shows signal strength, Wi-Fi, and the time 12:30. Below the status bar, the text "Shared Device Type : Temporary" is displayed. The main heading is "SAMSUNG Knox Manage" in white. There are two input sections: "User Name" with a placeholder "Write your User Name here." and "Password" with a placeholder "Write your Password here.". At the bottom, there are two buttons: "Check In" and "Settings".

Shared Device Type : Temporary

SAMSUNG Knox
Manage

• User Name
Write your User Name here.

• Password
Write your Password here.

Check In

Settings

[Check-in]

Creating normal users to check-in.

- Normal user accounts (non-shared users) should be created to login on the phone. As shown on the example below:

<input type="checkbox"/> User ID ≡	User Name	Status ▾	User Group	Organization	Device ⓘ	Last Updated ≡
<input type="checkbox"/> Employee_2	sidi_employee_2	Active	labsouza.samsung.com(Default Group), user02	Undefined	-	08/05/2021
<input type="checkbox"/> Employee_1	Sidi_employee_1	Active	labsouza.samsung.com(Default Group)	Undefined	-	08/05/2021

Applying policies.

- It is possible to apply different policies to the users, but only work profile policies.

Assigned Profile

Priority	Profile Name	Version	Platform	Registrant
2	Policy_Employee_1	2	Android Enterprise	luis.souza

Category**Policy****Value****Profile Name**

Android Enterprise (Work Profile Controls)

System	Screen Capture	Disallow	Policy_Employee_1
--------	----------------	----------	-------------------

Assigned Profile

Priority	Profile Name	Version	Platform	Registrant
1	Policy_Employee_2	2	Android Enterprise	luis.souza

Category**Policy****Value****Profile Name**

Android Enterprise (Work Profile Controls)

Location	GPS	Disable On	Policy_Employee_2
----------	-----	------------	-------------------

Back

Delete

Assign

Applying Apps.

- It is possible to assign different apps to the users too.

Assign Application



Meu Talking Tom 2 Android Managed Google Play | Public

Target Device ☐ Android Legacy ☒ Android Enterprise ☐ Android Legacy + Enterprise

Android Enterprise Settings

Installation Area ☐ Device + Work Profile

Installation Type ☐ Manual ☒ Automatic (Removable)

Auto-run after Installation ☒ Yes ☐ No

Schedule

Use Deployment Scheduler ☐ Use ☒ Do not use

Deployment Starts At

Target

Target Type ☒ Group ☐ Organization

☒ 1 item(s) selected | Total 5

<input type="checkbox"/> Group Name	Type	User	Device	Device Type
<input checked="" type="checkbox"/> Employee_2	User	1	0	

Shared Device Detail

Employee_2_Android_1

Enrolled | 0 minutes

Android Shared (Persistent)

IMEI / MEID	35399696024
Serial Number	R9XNB00
Model Name	Galaxy Tab A7 (SM-T505)
Agent Version	21.7(2.4.3.03)
User Name	Sidi_Employee_2 Detail

Security Device Information Network Application Profile Content Group/Organization

Installed Application **Assigned Application** Controlled Application

Total 1 | 10 per page

Application Name	Version	Platform & Source
Meu Talking Tom 2 com.outfit7.mytalkingtom2	2.7.6.7	Android Managed Google Play

Checking which user is logged in.

- It is possible to check which account is using the tablet through -> “Device details” -> “Shared device”, as shown on the example below

Device Detail

tab_act_3_shared_Android_1

Enrolled | 3 hours

Android Shared (Persistent)

IMEI / MEID	3525044700	Last Updated	08/05/2021
Serial Number	RX2R201	Last Connected	08/05/2021
Model Name	Galaxy Tab Active3 (SM-T575)	Last Inventory Synced	08/05/2021
Agent Version	21.7(2.4.3.03)	Enrolled Type	KME
User Name	Tab_act_3		

Security

Device Information

Network

Application

Content

Group/Organization

Command History

Shared Device

Shared Device User

Shared Device Log

Total 2 | 10 per page

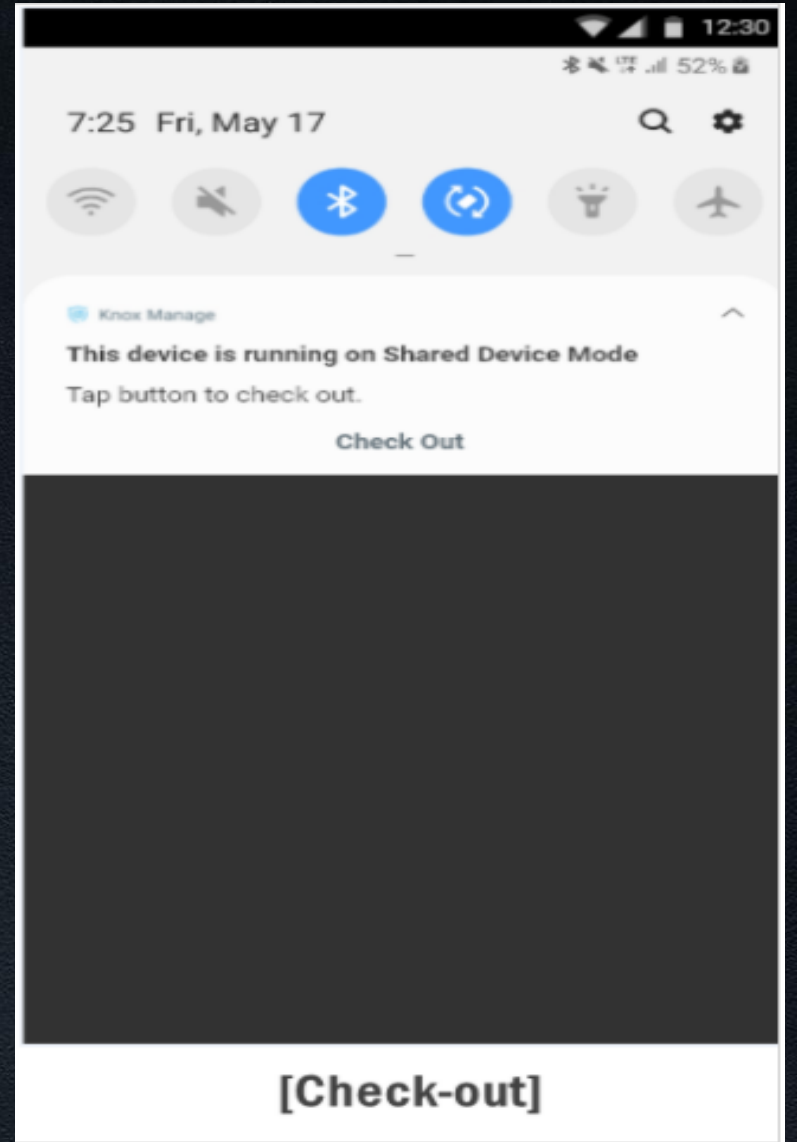
Device Command

Search by User ID or User Name

Status	User ID	User Name	Last Updated	
Checked-In	Employee_2	sidi_employee_2	08/05/2021 18:35:48	Detail
Checked-Out	Employee_1	Sidi_employee_1	08/05/2021 18:33:47	Detail

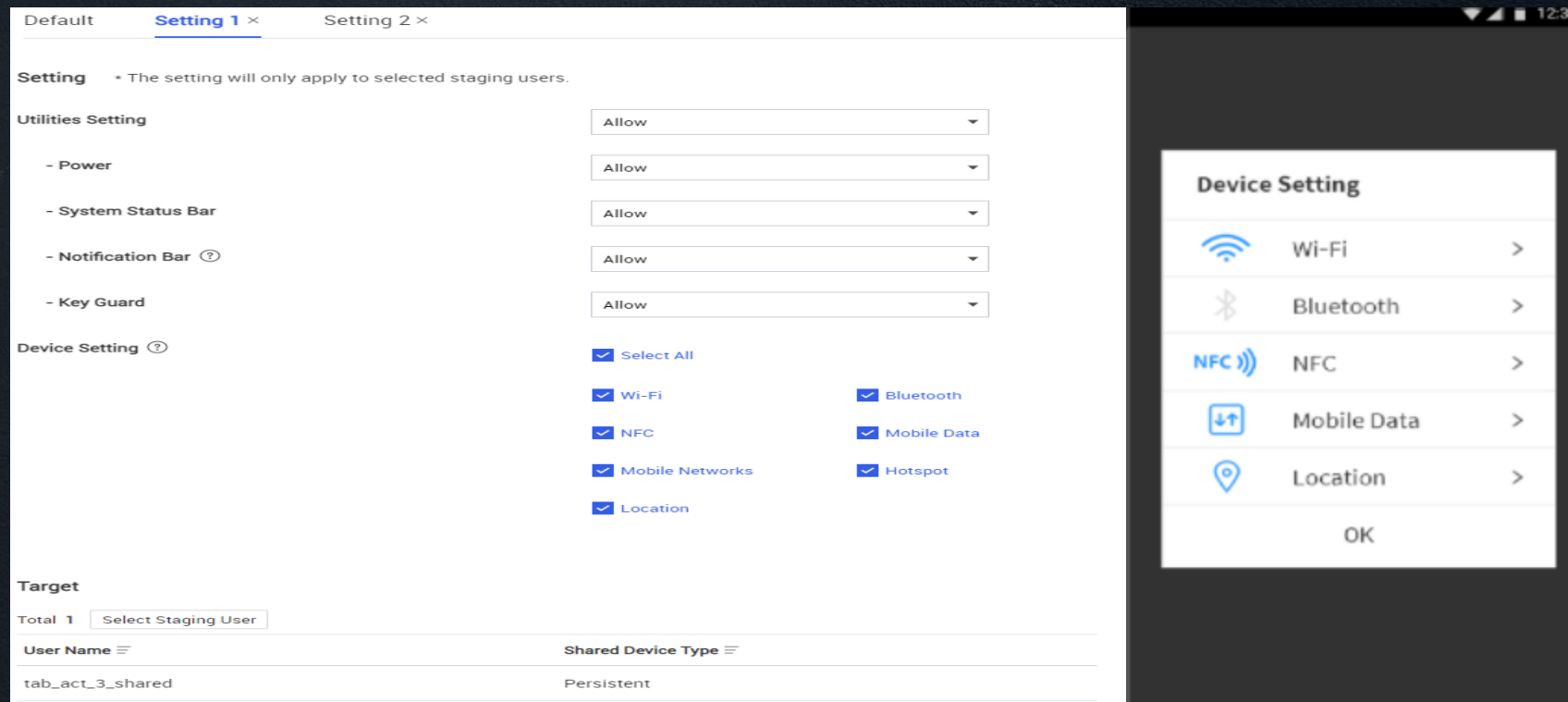
Check-out screen and shifting users.

- To change the user it is necessary to check-out from phone using the option available on notification bar.
- The phone will return to “Check-in” screen and a new employee will be able to login on the phone.



Settings allowed on kiosk shared screen

- The IT admins can send further instructions to control the network and other UI options available to the shared device using the Device Settings page.
- To go to this page, on the Knox Manage console, go to **Settings > Configuration > Staging and Shared Device**.
- The allowed settings can be applied per Stage user, as shown on the example (Setting_1, Setting_2...)



Exiting from Shared Device Kiosk

- The shared device also has an option to **Exit Shared Device Mode** that the device user can use to exit out of the shared mode in case of emergencies or issues with the shared device mode. To exit the shared device mode, the device user uses a passcode that is given by the IT admin. Once all the issues are resolved, the IT admin can apply the shared device mode again using the Device Command functionality.

Device Detail

tab_act_3_shared_Android_2

Enrolled | 9 minutes

Android Shared (Persistent)

IMEI / MEID	3525044
Serial Number	RX2R20
Model Name	Galaxy T
Agent Version	21.7 (2.4
User Name	tab_act

Security

Device Information

Network

Application

Content

Group/Org

Lock Device

Device Password Policy Compliance

Device Password Failure Count

Knox Manage Agent Sign-in Failure Count

Temporary Password - Lock Screen

Temporary Password - Work Profile

Unenrollment Code

Keepalive

SafetyNet Attestation

Compromised OS

Compromised App

Unauthorized Container

Shared Device Mode Status

Unlocked | Unlock Code 398183345

Unlock Mo

-

0/- | Password Failure Policy -

0/5 | Signin Failure Policy None

-

-

QI0G-5V2K-2ZIG-O2CE

-

-

Normal

Normal

-

Normal | Exit Shared Device Code 649755318

Settings

Device Setting

Exit Shared Device Mode

OK

Exit Shared Device Mode

Enter the 9-digit code given from your admin to exit Shared Device.

1 2 3 4 5 6 7 8 9

User Name
test123

Device Name
test123_Android_1

IMEI/MEID
123456789876543

Cancel

OK