

**Samsung Knox™ Configure
Shared Device**

July 2017

Samsung Knox™ shared device

A Samsung Knox™ *shared device* enables multiple users, or employees, to access the same device without sharing data across multiple devices. Individual settings, accounts, applications, and policies are utilized exclusively to a single user account. Data does not share with other employees, and is wiped from the device when the user logs out. Each employee can log in to a separate account with their *Active Directory* (AD) credentials and manage their own unique set of files and apps. Shared device functionality is optional and not a requirement for Knox Configure profile creation.

Using a Knox shared device is simple, just log into the device as you would a personal device. When powering on a device, shared device users immediately receive a prompt to log into their AD credentials. You must log in to AD to access the device's resources.

With the *single-sign on* (SSO) feature, the user can then have access to all necessary resources without having to log in to each application. Once an employee is done, log out and hand the device to the next user who then enters their own credentials.

Note: To log into a shared device, users must maintain an active connection to the corporate Wi-Fi network or VPN. Shared device functionality does not work on devices utilizing a Knox container. Ensure device containers are removed prior to activating a shared device.

IT admins can also manage a Knox shared device by utilizing advanced security features. They can remotely find, lock, and wipe misplaced devices. IT admins can also manage security policies, install apps, and restrict device functionality to business use only.

The following prerequisites are required to utilize the Knox shared device functionality:

- Active Directory
 - End user credentials
 - Kerberos (port 88) must be enabled for the shared device authentication
- A supported Samsung device running Knox version 2.6 or above

Deploying Samsung Kerberos Single Sign On (SSO)

There are several ways enterprises can utilize Samsung Kerberos SSO when creating a shared device supported profile in KC, including:

Internet Sites – Using Sbrowser to access intranet sites

Applications

- Obtain a Samsung Kerberos token by integrating with the Samsung Kerberos SSO SDK (<https://seap.samsung.com/sdk/knox-ss0-android>).
- Integrate with Sbrowser custom tabs (<http://developer.samsung.com/internet/android/web-guide>)

Preventing users from performing a factory reset

Samsung recommends utilizing a KC policy that prevents users from factory resetting their device. By default, users can factory reset their device after logging in to their shared device account. After factory resetting the device, the Knox shared device APK is removed. Users can then use the device as a regular Android device with no restrictions.

Preventing users from stopping the Knox shared device app

If stopping the Knox shared device app, the device converts to a regular Android device without restrictions beyond the policies that you have already deployed. By default, users can stop the Knox shared device app once it has started by navigating to **Settings > Application Manager**.

Samsung recommends blocking the **Force Stop** and **Clear Data** options for the Knox shared device. Consider deploying policies to prevent users from going to **Application Manager** and using the **Force Stop or Clear Data** options to prevent a shared device app from running properly.

If you programmatically manage a Knox shared device, call the APIs referenced below and pass

`com.sec.enterprise.knox.shareddevice` and

`com.sec.enterprise.knox.shareddevice.keyguard` as the `packageList` input parameter:

- `addPackagesToForceStopBlackList (List <String> packageList)`
- `addPackagesToClearDataBlackList (List <String> packageList)`
- `addPackagesToClearCacheBlackList (List <String> packageList)`
- `setApplicationUninstallationDisabled (List <String> packageName)`

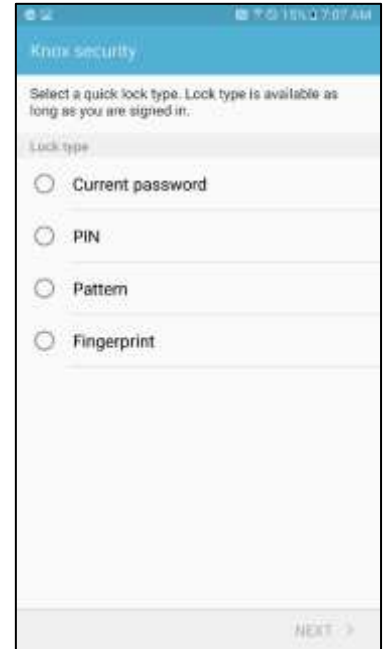
End user configuration

Refer to the following information to setup and login into a Knox shared device, and if necessary uninstall Knox shared device.

Setup Knox shared device

To configure Knox shared device support on the actual device:

1. Enter the following credentials provided by your IT admin, then tap **Sign in**.
 - Domain name
 - Username
 - Password
2. Select an unlock method.
 - Current password
 - PIN
 - Pattern
 - Fingerprint
3. Select and confirm the unlock method.



Sign into Knox shared device

Note: Once enrolled in Knox shared device, you cannot use the device without signing in to your account.

To sign into Knox shared device:

1. Enter the following credentials provided by your IT admin.
 - Domain name
 - Username
 - Password
2. Tap **Sign in**.



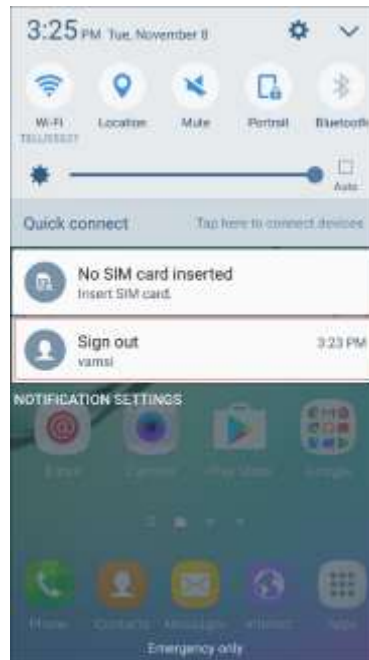
Sign out of Knox shared device

To sign out of a Knox shared device:

1. Swipe down from the top of the screen to display the status bar.
2. Tap **Sign out** on the notification pane with your Knox Shared Device username.

OR

1. Lock the device.
2. Tap **SIGN OUT** from the top right-hand corner of the device.



Uninstall Knox shared device

If you attempt to uninstall Knox shared device without factory resetting the device, some user data may remain on the device.

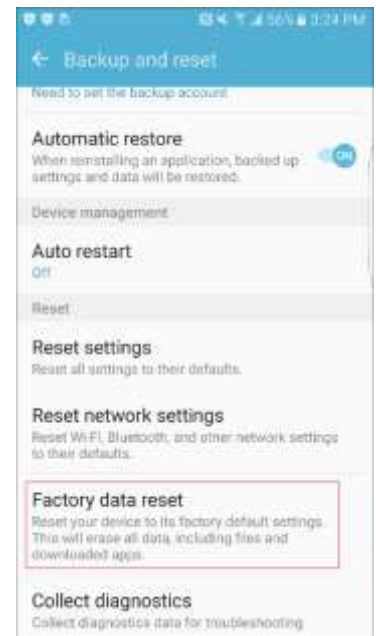
Note: Samsung recommends you deploy a policy to prevent users from factory resetting their device. Otherwise, they may accidentally uninstall Knox shared device.

To uninstall Knox shared device:

1. Deploy a factory reset policy to the device,

OR

1. Log in to your Knox shared device account.
2. Navigate to **Settings > Backup and reset > Factory data reset**.
3. Tap **RESET DEVICE**.

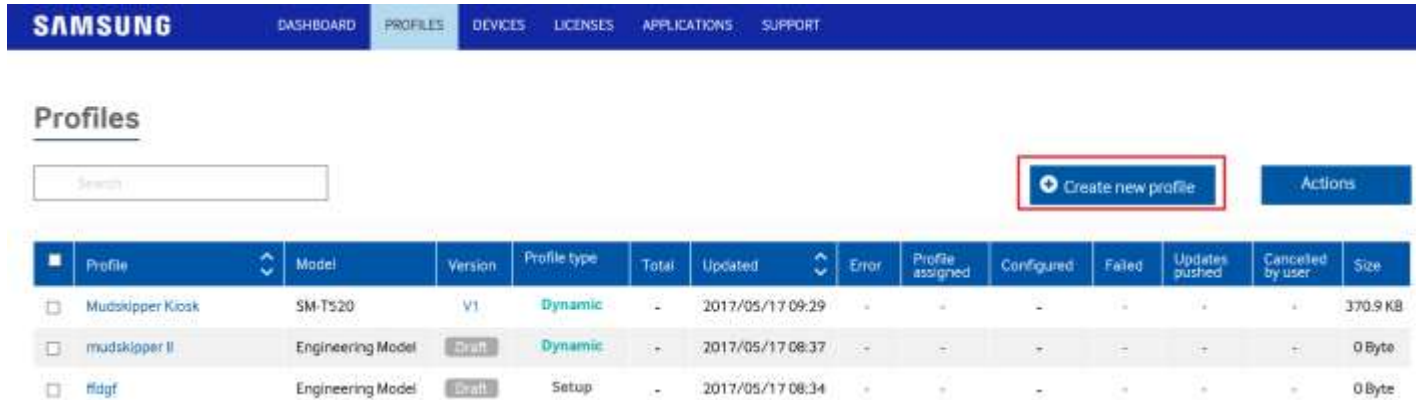


Define a shared device supported KC policy

To support Knox shared device functionality, a KC profile requires creation with shared device functionally specifically set. Additionally, KC profile creation affords an IT admin a unique opportunity to customize device settings, company name and branding, device lock mechanisms, applications, booting sequence, animation, setup wizard cancellation, Kiosk Mode and hard key remapping.

To configure a shared device profile in KC:

1. Log into KC and navigate to the **Profiles** tab.
2. Select **Create new profile** from the upper-right portion of the screen.

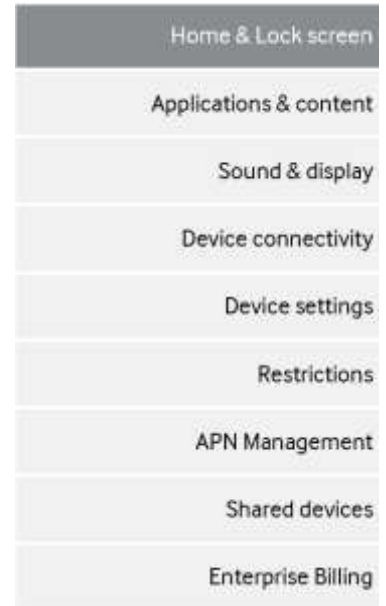


The screenshot shows the Samsung Knox Configure interface. At the top, there is a navigation bar with the Samsung logo and tabs for DASHBOARD, PROFILES, DEVICES, LICENSES, APPLICATIONS, and SUPPORT. The 'PROFILES' tab is selected. Below the navigation bar, the page title is 'Profiles'. There is a search bar on the left and a 'Create new profile' button on the right, which is highlighted with a red box. Below the search bar and button is a table with the following columns: Profile, Model, Version, Profile type, Total, Updated, Error, Profile assigned, Configured, Failed, Updates pushed, Canceled by user, and Size. The table contains three rows of profile data.

Profile	Model	Version	Profile type	Total	Updated	Error	Profile assigned	Configured	Failed	Updates pushed	Canceled by user	Size
Mudskipper Kiosk	SM-T520	V1	Dynamic	-	2017/05/17 09:29	-	-	-	-	-	-	370.9 KB
mudskipper II	Engineering Model	Draft	Dynamic	-	2017/05/17 08:37	-	-	-	-	-	-	0 Byte
flgdt	Engineering Model	Draft	Setup	-	2017/05/17 08:34	-	-	-	-	-	-	0 Byte

3. Ensure you select **Dynamic edition** as the profile type, as shared device support is not available in a KC's setup edition option.
4. Complete the profile creation process by adding the desired configuration attributes you would like to apply to the device.

Navigate to the *Home & Lock screen*, *Applications & content*, *Sound & display*, *Device connectivity*, *Device settings*, *Restrictions* and *APN Management* tabs and set the intended configuration for the shared device. Select **Next** within each screen to proceed once each screen is populated for the shared device profile.



5. Once you have completed the profile configuration down to **Shared devices**, set the following settings to enable multiple users, or employees, to access and share a single device:

The screenshot displays the 'Shared devices' configuration page in the Samsung Knox Configure Shared Device Administrators interface. The page is divided into a sidebar menu on the left and a main content area. The sidebar menu includes options like 'Profile information', 'Licenses', 'Applications', 'Home & Lock screen', 'Applications & content', 'Sound & display', 'Device connectivity', 'Device settings', 'Restrictions', 'APN Management', 'Shared devices' (highlighted), 'Enterprise Billing', and 'Devices'. The main content area is titled 'Shared devices' and contains several sections:

- Upload Shared Device agent:** A section with a 'Select' button to choose an existing agent or a link to upload a new one.
- Background image:** A section with a 'Select' button to choose a background image for the lock screen.
- SSO authentication:** A section with a checkbox labeled 'SSO authentication'. Below it are two 'Upload' buttons: 'Upload XML configuration file' and 'Upload Samsung (Kerberos) SSO authenticator'. A link 'Click here for sample xml file' is provided next to the XML upload button.
- Enterprise branding information:** A section with a 'Company logo' field (with image requirements: less than 1MB, BMP, JPEG, PNG; recommended dimensions: 450px by 450px) and a 'Company name (max. 20 characters)' field.

A smartphone image is shown on the right side of the interface, displaying a 'SIGN IN' screen with an 'EMERGENCY CALL' button at the bottom. The interface also includes a 'Dynamic' dropdown menu, an 'Edit' button, and a 'Clear all' button at the bottom right.

- If you have an existing shared device agent, choose the **Select** button to apply it. Otherwise, select the **Upload Shared Device agent** link to download an available version. Choose **Select** to upload the APK on to the target device.
- Samsung recommends the Samsung Kerberos SSO authenticator for validating shared devices. Select the **SSO authentication** checkbox. Selecting this option enables both the required **Upload XML configuration file** and **Upload Samsung (Kerberos) SSO authenticator** configuration options.
- Choose the **Select** button and upload the XML formatted configuration file to utilize with the shared device configuration. If you do not have a XML configuration file, select the **Click here for sample XML file** link to display a sample file.
- If you have a Kerberos SSO authenticator, choose the **Select** button to apply it. Otherwise, select the **Upload Samsung Kerberos SSO authenticator** link to download an authenticator. Extract the zip package and choose **Select** to upload the APK on to the target device. Select **Next** to continue.

- 6) Optionally navigate to the **Summary** screen to review the attributes of the newly created shared device KC profile.

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales exceeding KRW 201 trillion.

For more information about Samsung Knox, visit <http://www.samsungknox.com/>.

Copyright © 2017 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trademark of Samsung Electronics Co. Ltd. Specifications and designs are subject to change without notice. Non-metric weights and measurements are approximate. All data were deemed correct at time of creation. Samsung is not liable for errors or omissions. Android and Google Play are trademarks of Google Inc. ARM and TrustZone are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

Samsung Electronics Co., Ltd.
416, Maetan 3-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772, Korea