



# SureLock for Android

## User Guide

Ver 21.09.16

All the information contained in this document is the property of 42Gears and meant only for the intended recipient. The contents of the document shall not be used, copied, altered, published, or redistributed without the prior written consent of 42Gears Mobility Systems Pvt. Ltd

## Table of Contents

<b>Introduction</b>	<b>5</b>
<b>Getting Started with SureLock</b>	<b>9</b>
<b>Admin Settings</b>	<b>11</b>
<b>Quick Settings</b>	<b>11</b>
<b>Allowed Applications</b>	<b>12</b>
Add Allowed Applications	12
Edit Allowed Application	21
Remove Allowed Applications	22
Add a folder	23
Edit or remove a folder	23
<b>Allowed Websites</b>	<b>24</b>
<b>SureLock Settings</b>	<b>24</b>
Wallpaper Settings	24
Display Settings	25
Row and Column Size	25
Icon Size	26
Font Size	26
Use Classic Calculation	26
Spacing between the Icons	26
Text Color	27
Apps Order	27
Allow Icon Relocation	27
Detect Network Connection	27
Full Screen Mode	27
Notification Badge	28
Hide App Title	28
Floating Buttons Settings	28
Single Application Mode	29
Application Launch Delay	31
Run Only Once	31
Create Single App Mode Exit File	31
SureLock Settings	31
Change Password	31
User Security	32
Admin Users	33

Multi-User Mode	35
Disable Bottom Bar	36
Hide Bottom Bar	37
Disable Hardware Keys	37
Disable Soft Navigation Keys	37
Assign SureLock System Permission	37
Peripheral Settings	38
Camera Settings	38
Wi-Fi Settings	38
Mobile Data Settings	38
Prefer Mobile Data Settings	39
Wifi Hotspot Settings	39
NFC Mode Settings	39
GPS Settings	39
Bluetooth Settings	40
Sound Settings	40
Loudspeaker Settings	40
Volume Settings	40
Airplane Mode Settings	41
Flashlight Settings	41
SureLock Homescreen Orientation	41
Rotation Settings	42
Brightness Settings	42
Set Custom Toast Message	42
Enable Toast Message	43
Set Custom Access Denied Message	43
Watchdog Service	43
Kill Unallowed Application	44
Disable Clipboard	44
Lock Safe Mode	44
Disable Safe Mode	45
On Launch of Unallowed Application	45
On USB state change go to Home	45
Auto Power On When Charger is Connected	46
Auto Power Off When Charger is Disconnected	46
Clear Data on Home Screen Load	46
Suppress Notification Panel	46
Hide Quick Settings Tile	47

Block Notifications	47
Disable Status Bar	47
Disable Factory Reset	47
Disable USB	47
USB Connectivity Preference	48
Disable OTG/External SD Card	48
Suppress Power Button/Keyboard	48
Enable SureKeyboard	48
Driver Safety	49
Bootup Delay	51
Timeout Settings	51
Schedule Reboot	54
Widget Settings	54
Title Bar Settings	55
Status Bar Color	56
SureLock Analytics	56
Power Saving Settings	57
Battery Popup Notification	58
Miscellaneous Settings	58
Number of Taps	58
Access Settings Timeout	58
Admin Login Security	59
Send Notification On Exit	60
Set Usage Access Warning	60
Enable Log	61
Send Error Report	61
Use Advance Hide Bottom Bar	61
On Press of Home Button	61
Disable Touch Input	61
Use SDP Calculation	62
Memory Settings	62
Screensaver Settings	62
Disable Applications	63
Disable Wi-Fi /Mobile Data Access	63
Unrestricted Data Usage	63
Default Runtime Permissions for Allowed Apps	63
Diagnostic Settings	64
<b>Samsung Knox Settings</b>	<b>64</b>

Set Custom Boot Animation	66
Set Custom Shutdown Animation	66
Disable Other Home Screens	66
Disable Safe Mode	66
Disable Factory Reset	67
Disable Multi Window	67
Disable USB	67
Wipe Recent Apps	67
Disable S Voice	67
NFC Mode	68
Disable Air View Mode	68
Disable Air Command Mode	68
Disable Smart Clip Mode	68
Allow Multiple Users	68
Disable OTA Upgrade	68
Disable SD card	69
Disable Hardware Keys	69
Disable Custom Hardware Keys	69
Disable Power Off	69
Disable Application Installation	69
Disable Application Uninstallation	69
Disable Edge Screen Functionality	70
Hide Status Bar (Samsung Knox)	70
Hide Navigation Bar (Samsung Knox)	70
<b>Allowed Widgets</b>	<b>70</b>
Add Widget	70
Edit/Remove Widget	71
<b>Manage Shortcuts</b>	<b>71</b>
<b>Phone Settings</b>	<b>73</b>
<b>Multi-User Profile Settings</b>	<b>75</b>
Profile Management	75
User Management	76
Server Configuration	77
Display Last Logged In User	78
<b>System Settings</b>	<b>78</b>
Setup SureLock Permissions	79
<b>Import/Export Settings</b>	<b>80</b>
Export Settings	80

Import Settings	81
Reset Settings	82
Automatic Import	82
Schedule Automatic Import	82
Advanced Settings	83
<b>Remotely Configure SureLock Settings</b>	<b>83</b>
<b>Exit SureLock</b>	<b>83</b>
<b>Uninstall SureLock</b>	<b>84</b>
<b>About SureLock</b>	<b>84</b>

## Introduction

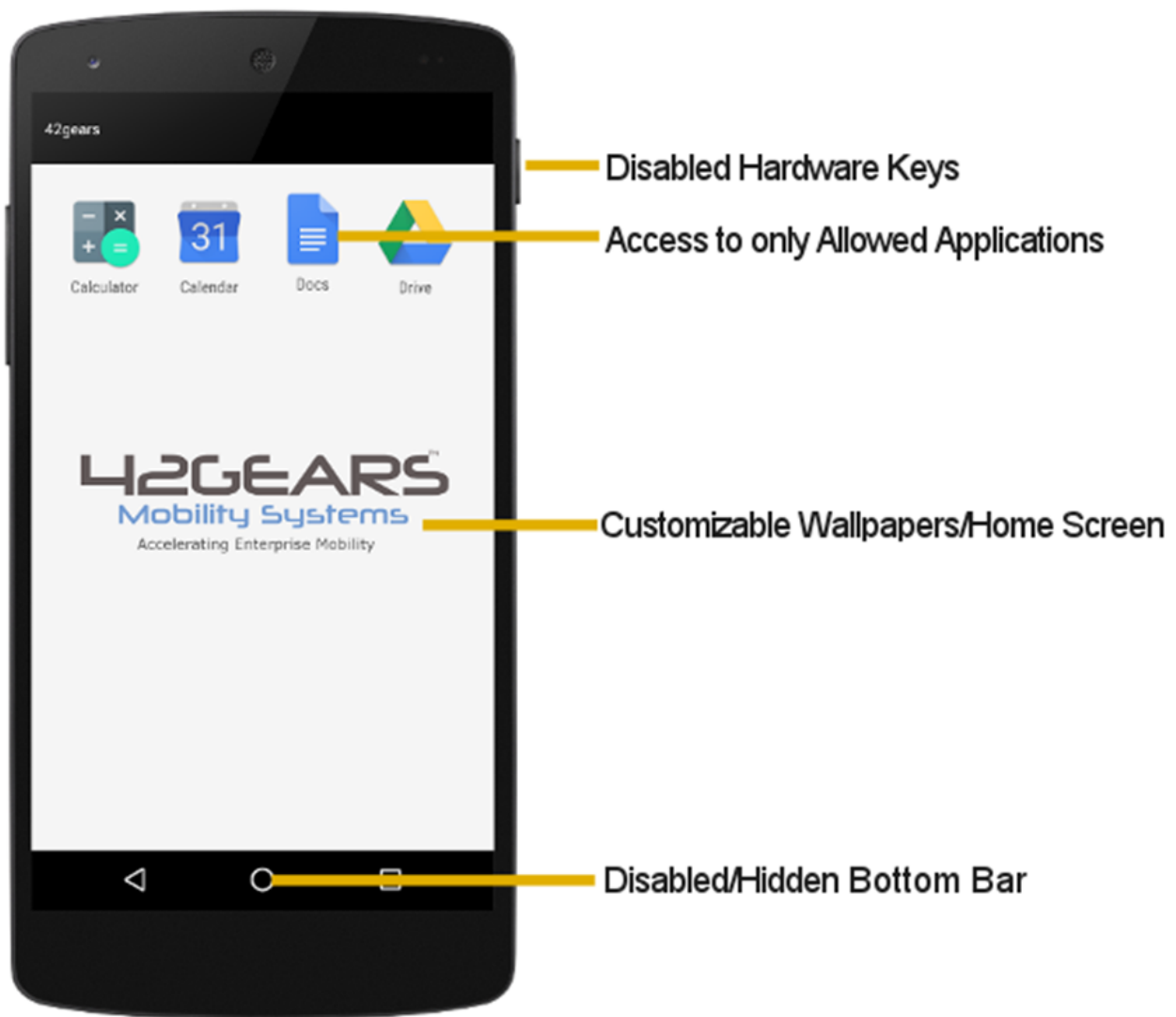
### What is SureLock?

Businesses with mobile workforce require secured and locked mobile device to ensure responsible usage, improved productivity and reduced device maintenance cost. One of the ways to achieve above mentioned objectives is by allowing access to only required applications for users and preventing them from making any unwanted changes in the device. With **SureLock**, only the approved applications are allowed to run on the device and only the administrator can access the password protected settings to either modify settings or exit lockdown.

### How does it work?

Download and install **SureLock** on your Android device. Access the password protected **SureLock Admin Settings** and specify the applications you wish to approve. Return to **SureLock Home Screen**, only the approved applications will be listed on the screen. This confines the device users to only **SureLock Home Screen** with approved applications and is restricted from accessing device home screen, device settings and **SureLock** lockdown settings.

## Key Features



- Lock down Android smartphones and tablets in Kiosk Mode
- Restrict users to only Allowed Applications
- Block user from playing games, browsing or installing unapproved applications
- Hide or Disable Bottom Bar
- Show only selected Widgets (e.g. battery, Wi-Fi, weather etc.) on **SureLock Home Screen**
- Arrange Allowed Applications in categories on **SureLock Home Screen**
- Block user from changing Device Settings
- Selectively allow or block individual child windows of any application



- Password protect launch of Allowed Applications
- Brand SureLock with your own corporate logo/wallpaper
- Auto launch application(s) at Startup
- Custom title for Allowed Applications on Home Screen
- Hide icon of an Allowed Application on Home Screen
- Peripheral Lockdown (Wi-Fi, Bluetooth, Auto-orientation, Flight Mode, Audio, GPS, Mobile Data)
- Modify SureLock Settings using MDM solution like **SureMDM**
- Option to allowlist/blacklist phone numbers
- Relocate icons anywhere on the screen using drag and drop
- Import/Export SureLock Settings
- Remotely deploy SureLock configuration (http/cloud/file transfer)
- Driver Safety features
- Easily integrates SureFox (Special lockdown browser to restrict browsing to only certain websites)
- Multi Users feature to enable multiple users sharing single device with respective lockdown profiles

## Getting Started with SureLock

SureLock can be downloaded from following sources:

- [Google Play](#)
- [Direct Download](#) from 42Gears website

### Launch SureLock

To launch **SureLock**, follow these steps:

1. Tap the **SureLock** icon to launch.
  2. On **SureLock Kiosk Lockdown** welcome screen, go through the details and select **SureLock** as the home app.
  3. On **Setup SureLock Permissions** screen, select **Set SureLock as Default Launcher** and tap **Continue**. To know more about **SureLock Permissions**, see [Setup SureLock Permissions](#).
- SureLock Home Screen** will appear on the screen.



### Access SureLock Admin Settings

To access **SureLock Admin Settings**, follow these steps:

1. Launch **SureLock**.
2. Tap **SureLock Home Screen** 5 times within 3 seconds to launch the password prompt.
3. On the password prompt, enter **SureLock** default password as **0000** (four zeros) and tap **GoTo Admin Settings**. To change the password, see [Change Password](#).



**Note:** *Exit SureLock* option will be available only for trial version of **SureLock**.

 **Password**


Default password is 0000

Enter Password...

GO TO ADMIN SETTINGS

EXIT SURELOCK

On successful login, **SureLock Admin Settings** screen will appear.



**Note:**

- i. Alternate option to access **SureLock Admin Settings** is to tap the **Back** button 5 times.
- ii. If **SureLock** is continued to be in the trial version, each time when the user enters the password, a pop-up appears to indicate the user to avail **SureLock's** free full feature trial version for 7 days. Tap **Sign up for FREE full feature trial** option and fill the relevant details and then tap **Submit** or **Sign up using Google/Facebook/LinkedIn** to get a free trial for 7 days.

## Admin Settings

**Admin Settings** provides options to manage and control the lockdown settings.

### Quick Settings

**Quick Settings** option helps the user to quickly lockdown the device with approved applications and configure basic settings.

To lockdown the device using **Quick Settings**, follow these steps:

1. Launch **SureLock**
2. On **SureLock Admin Settings** screen, tap **Quick Settings**.  
All installed applications will get listed.
3. Select the desired application for the lockdown.
4. Go to **Peripheral Settings** using the arrow at top right corner of the screen.
5. Select the desired **Peripheral Settings** and apply changes.
6. Go to **Home Screen Settings** using the arrow at top right corner of the screen.
7. Select **Application Icon Size**.
8. Enter the **Title** for **Home Screen**.
9. Select the **Wallpaper** for **Home Screen**.
10. Go to **Finish** screen using the arrow at top right corner of the screen.
11. Tap **Launch** icon/button.
12. On the successful launch, **SureLock Home Screen** will appear.



**Note:** *Quick Settings* is enabled for single user mode only. It will not support **Multi-user mode**.

## Allowed Applications

**Allowed Applications** option displays the list of applications that are approved on the **SureLock Home Screen**. The admins have the options to approve and allow more applications, edit, or organize the allowed ones by assigning them to a specific folder.

### Add Allowed Applications

**Add App** option lists all the installed applications on the device. The user can use this list to select and allow **approved** applications.

To add an **Allowed Application(s)**, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On Admin Settings screen, tap Allowed Applications.
3. On Allowed Applications screen, tap Add App to launch the list of installed applications.
4. Select the required application(s) to allow from the list and tap Done.

List of all approved applications will be displayed under Allowed Applications screen.



**Note:** The apps in the device are listed under different categories such as **All Apps**, **Downloaded Apps**, **System Apps**, **Services**, **Plugin Apps**.

5. Tap **Done** to return to **Admin Settings**.

Once done, the user can see the icons along with titles of all allowed applications on **SureLock Home Screen**.

### Plug-in Apps

Few plug-in apps come preinstalled with SureLock such as Wi-Fi Center and Bluetooth Manager. Admins can allow access to these plug-in apps by adding them to the allowed applications and use it like any other applications on SureLock Home Screen. These apps are helpful when the admin wants to give access to only specific device settings. For example, if

the locked device is always on the move and has to connect to different Wi-Fi networks, the admin can allow plug-in app called Wi-Fi Center which enables the device users to use Wi-Fi settings without accessing device settings.

Following Plug-in apps are available in SureLock:

**Bluetooth Manager** – With this plug-in app, the admin can allow the user to have access to following Bluetooth functionalities on the device:

- Turn ON/OFF Bluetooth option.
- Pair with the devices under **Available Devices**.
- Change password to access Bluetooth functionalities

To configure Bluetooth settings in **Bluetooth Manager** plug-in app, follow these steps:

1. On the **SureLock Home Screen**, launch **Bluetooth Manager**.
2. On the **Bluetooth Manager** screen, tap **Settings** icon.
3. Enter the password and click **OK**.
4. Configure **Bluetooth Settings**:

**Device Types** - Allow or block access to various device types (Phone/Wearable/Toy and more) those are connected to Bluetooth.

**Change Password** - Change the default/existing password to the desired password.

**Brightness Settings** – With this plug-in app, admin can allow the user to have access to set phone brightness levels of the device screen.

**Security Manager** – With this plug-in app, the admin can allow the user to set or change the device pin to access the device.

**Settings Manager** – With this plug-in app, the admin can allow the user to perform the following actions:

- Turn Airplane mode ON or OFF

**Note:**

1. *This feature is supported on the platform signed devices along with the EA system plugin app.*
2. *If Airplane mode is kept as Always On or Always Off in Peripheral Settings then the Airplane mode option in Settings Manager will be greyed out.*

- Turn Mobile Data ON or OFF
- Turn Data Roaming ON or OFF
- Switch between the SIM's



**Note:** *This feature will be supported only on platform signed devices.*

- Configure Screen Timeout
- Auto-rotate screen - Rotate the screen orientation from portrait to landscape or vice-versa.



**Note:** *This feature is supported on Marshmallow or above devices.*

- Reading Mode Intensity - User can adjust the reading mode intensity based on the available lighting.

To access the above-mentioned settings, navigate to **SureLock Admin Settings > Allowed Applications > Plugin Apps > Settings Manager**.

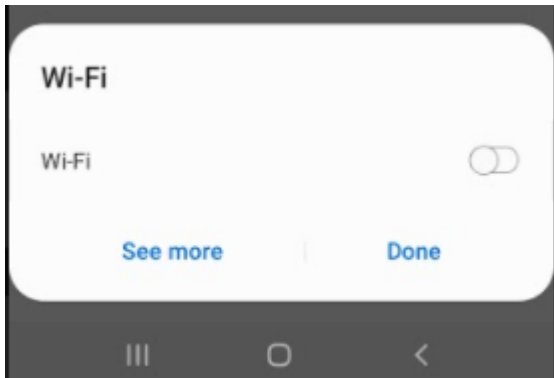
**Phone Manager** – With this plug-in app, admin allows configuring only the whitelisted contacts in the **Phone Settings**.

**WiFi Center** – With this plug-in app, admin allows the user to access certain Wi-Fi related functionalities on the device. They can use this plug-in app to configure multiple network connections. To configure WiFi Center settings, follow these steps:

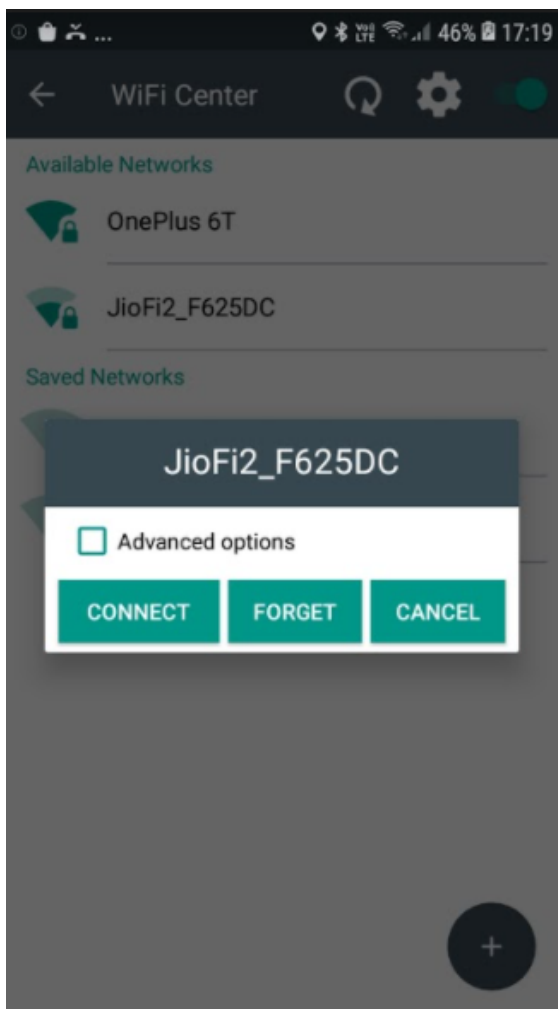
1. On the SureLock Home Screen, launch WiFi Center plug-in app.
2. Turn on the WiFi Center toggle button.



**Note:** Once the **WiFi Center** toggle button is On, a prompt appears to connect to the available WiFi network. This prompt will appear only on the devices running Android 10 or later devices.



A list of available / saved SSID's will be displayed on the screen.



3. Select the appropriate SSID and tap **Connect**.





**Note:** You cannot **Forget** (disconnect) a network when it is configured in SureLock. This is applicable only for the devices running Android version Marshmallow or later.

4. On the **WiFi Center** screen, tap **Settings** icon.
5. Enter the password.
6. Configure the following **WiFi Center Settings**.

Settings	Description
<b>Load default URL when connected to open network</b>	Select this option to launch the default URL when connected to an open network.
<b>Launch webpage when connected to open network</b>	Select this option to launch the specified webpage URL when connected to an open network.
<b>Webpage URL</b>	Enter the Webpage URL that will be launched when connected to an open network.
<b>Change Password</b>	Change the default or existing password to the desired password to access <b>WiFi Center Settings</b> .
<b>Hide Forget Button</b>	Hides <b>Forget Button</b> for the connected network.
<b>Hide IP Settings</b>	Hides <b>IP Settings</b> option for the connected network.
<b>Hide Use Proxy Settings</b>	Hides <b>Use Proxy Settings</b> option for the connected network.
<b>Allow Connection to Open Network</b>	Allows connecting to an open network.
<b>Launch WiFi Center on loss of WiFi connectivity</b>	Allows launching of WiFi Center within the specified time when WiFi connection is lost.
<b>Turn ON Mobile Data on loss of WiFi Connectivity</b>	Allows connecting the network through mobile data when WiFi connection is lost.



**Note:** This feature will be supported only on platform signed devices.

## Configure a Wi-Fi network

Admins can add and configure multiple Wi-Fi networks.

To add a new Wi-Fi network, follow these steps:

1. On the **SureLock Home Screen**, launch **WiFi Center** plug-in app.
2. On the WiFi Center screen tap Add icon.
3. On the **Wi-Fi network** prompt,
  - Enter the **Network SSID**.
  - Select a **Security** option from the following:
    - None**
    - WEP**
    - WPA/WPA2 PSK**
    - 802.1xEAP**
  - Hidden Network - Use this option if you want to make this specific SSID as hidden network.
  - Under **Advanced options**,
    1. Select **Use Proxy** and enter the proxy details such as **Proxy hostname**, **Proxy Port**, **Bypass proxy for**.
    2. Select **IP settings > DHCP / Static**.

**Flashlight Manager** - With this plug-in app, admin allows the user to use the flashlight on their device.



**Note:** This feature is supported on the devices that have flashlight option.

**Hotspot Manager** - With this plug-in app, admin allows the user to create or configure a Hotspot network on the device. Users can use this plug-in app to configure hotspot settings.

To configure Hotspot settings, follow these steps:

1. On the **SureLock Home Screen**, launch **Hotspot Manager** plug-in app.
2. On the **Hotspot Manager** page, configure the following settings and tap **Save**.

Settings	Description
<b>Portable Wi-Fi Hotspot</b>	Turn ON/OFF portable Wi-Fi Hotspot network.
<b>Setup Wi-Fi Hotspot</b>	<ul style="list-style-type: none"> <li>• Enter the <b>Network SSID</b></li> <li>• Select the <b>Security: Open / WPA/WPA2 PSK</b></li> <li>• Enter the <b>Password</b>.</li> </ul>



**Note:** Users can only Turn ON/OFF the Hotspot network, but modifications on the configuration are not allowed on the below-mentioned devices:

- Android version Oreo onwards
- Non-Samsung devices
- Non-Signed devices

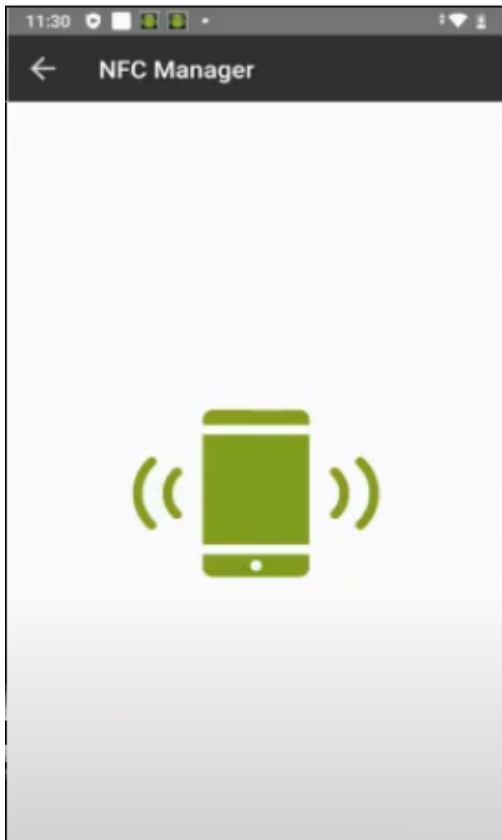
**Hotspot Manager** - With this plug-in app, the admin can allow the user to transfer files between devices without exiting from SureLock.

To enable NFC to transfer files,

1. Go to **SureLock Admin Settings > Allowed Application > Plugin Apps** and select **NFC Manager**.

The NFC Manager app will be added to the SureLock home screen.

2. Tap **NFC Manager** app and you can see the device is ready to connect with other device for file transfer.



**Note:** Both the devices should support the NFC mode setting.

If you again tap on the green icon, NFC will get disconnected, and the file transfer will be interrupted.

**Volume Control** - With this plug-in app, the admin can allow the user to control the volume of the device's media, alarm, notification, ringtone, and call.

To configure volume settings of a device using the Volume Control plugin app,

1. On the **SureLock Home Screen**, launch **Volume Control**.
2. On the **Volume Control** screen, tap the **Settings** icon.
3. Enter the password and click **OK**.
4. Allow/deny the user to adjust the volume control for the following :
  - Enable Media Volume
  - Enable Alarm Volume

- Enable Notification Volume
- Enable Ringtone Volume
- Enable Call Volume
- Enable Sound Mode (Ring/Vibrate/Silent)
- Change Password - Use this option to change the password (from default '0000' to the desired password) to access volume control settings

**Note:**

1. *If the sound mode is already set in the Sound Settings of the device, then the user cannot switch between sound modes in the Volume Control plugin app.*
2. *If the volume threshold is already configured in the Volume Settings then the user can change the volume level within the set threshold limit on the Volume Control plugin app.*

**APN Manager** - With this plug-in app, the admin can allow the user to create or configure the **Access Point Name (APN)**.

To configure APN settings of a device using the **APN Manager** plugin app, follow these steps:

1. On the **SureLock Home Screen**, launch **APN Manager**.
2. On the **APN Manager** screen, tap the **Settings** icon.
3. Enter the password and click **OK**.
4. Enable/disable the following settings to create or configure the APN.
  - **Insert Override APN** - Create a new APN by adding the required details.
  - **Configure Override APN** - Edit or delete the created APN.
  - **Enable Override APN** - Use this option to enable/disable the APNs created.
  - **Change Password** - Use this option to change the password (from default '0000' to the desired password) to access APN Manager settings.

**Note:**

1. *APN Manager is supported only when the device has Integrated SureLock and Device Owner privilege.*
2. *This plug-in app will be supported only when there is a SIM inserted in the device.*

### Edit Allowed Application

The user can edit different aspects of allowed applications such as **Label, Icon, Password,**

#### Hide Icon in Home Screen.

To edit an **Allowed Application**, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Applications**.
3. On **Allowed Applications** screen, tap **Edit** icon of the application.
4. On **Application Settings** screen, the user can edit the following options:

**Label** - Name of the application

**Icon** - Icon image for the application

**Password** - Access application by setting a password

**Hide Icon in Home Screen** - Hide applications' icon in **Home Screen**

**Launch at Startup** - Launch the application when the device is switched ON

**Restart app on relaunch** - Restart the application on its relaunch

**Clear Data on Launch** - Clear the data on application launch



**Note:** To enable **Clear Data on Launch** requires device rooting/platform permission.

**Runtime Permissions** – Admin can restrict or allow the following runtime permissions for the application:

- Camera
- Microphone
- Location
- Contacts
- Storage



**Note:** This feature is available for the devices running Android Marshmallow and above / Samsung Knox/ Platform Signed.

**Allow Child Windows** - Restrict or allow the access to a specific child windows of the application.

For example, **Camera** app can be used to capture both photo and video. The admins can use this feature to restrict the video camera by disabling the video camera child windows.

**Current Path** - Path of the folder in which the application is saved. This is helpful if the allowed applications are arranged in folders.

**App Idle Timeout** - Configure a specific period of device inactive time after which **SureLock** will auto- redirect the device screen to **SureLock Home Screen**.



**Note:** To configure App Idle Timeout, enable Idle Timeout option under Admin Settings > SureLock Settings > TimeOut Settings.

5. Tap **Done** to complete

### **Remove Allowed Applications**

To remove an allowed application from **SureLock Home Screen**, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Applications**.

3. On **Allowed Applications** screen, tap the application to remove.
4. On **Application Settings** screen, tap **Remove** to complete.

### Add a folder

**Add Folder** option allows the admins to create folders on **SureLock Home Screen**. The admins can assign and organize approved applications in these folders.

To arrange approved applications in a folder, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Applications**.
3. On **Allowed Applications** screen, tap **Add Folder** and enter a name for the folder.
4. Tap **Ok** to create a folder.
5. Tap on the folder to open and follow steps mentioned in [Add Allowed applications](#) to the folder.

The folder created will reflect on **SureLock Home Screen** with approved applications.



**Note:** To move an existing approved application to a folder, edit **Current Path** of the application to that of the desired folder.

### Edit or remove a folder

To edit or remove an existing folder, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Applications**.
3. On **Allowed Applications** screen, long tap on the folder.
4. On **Folder Settings** screen, edit the following options:



**Label** - Name of the folder

**Icon** - Icon image for the folder

**Landscape Wallpaper** - Wallpaper for folder when in landscape mode

**Portrait Wallpaper** - Wallpaper for folder when in portrait mode

**Password** - Lock password for the folder

5. Tap **Ok** to edit the folder.
6. Tap **Remove** to delete the folder.

## Allowed Websites

**Allowed Websites** helps the admins to install **SureFox** application on the device home screen.

**SureFox** can be downloaded from following sources:

- [Google Play](#)
- [Direct Download](#) from 42Gears website

## SureLock Settings

**SureLock Settings** offers features to customize **SureLock Home Screen** such as advance lockdown of a device, peripherals settings, timeout settings and more.

### Wallpaper Settings

**SureLock Home Screen** can be personalized with a wallpaper. The admins can set two different wallpapers for **SureLock Home Screen: Landscape** and **Portrait**.

**Wallpaper Settings** has following options:

1. **Wallpaper** - Use **Wallpaper** option to set wallpaper for **SureLock Home Screen** and Device **Lock Screen**. The user has the option to set same or two different wallpapers for **Landscape** and **Portrait** mode and also set wallpaper for the Lock screen.

To configure a wallpaper, follow these steps:

1. On **Admin Settings** screen, tap **Sure Lock Settings**.
  2. Select **SureLock Settings > Home Screen Settings > Wallpaper**.
  3. Tap **Landscape** or **Portrait Wallpaper**.
  4. Tap on browse icon to select a wallpaper image from **Drive/Gallery/Photos**.
  5. Tap **Lock screen Wallpaper** to browse and select the desired image from **Drive/Gallery/Photos**.
  6. Tap **Customize Loading Screen** to change loading screen message and enable progress bar and spinning wheel.
2. **Wallpaper Position** - Use **Wallpaper Position** option to specify and set the position of the wallpaper. The user has the following options to select from:
    - Center
    - Fill
  3. Use **System Wallpaper** - Select **Use System Wallpaper** to set system wallpaper as **SureLock Home Screen** wallpaper.
  4. **Background Color** – Enter **Hex** color code or select a color from the color picker to apply background color for **SureLock Home Screen**.

## Display Settings

**Display Settings** offers a range of features that can be used to customize the look and feel of **SureLock Home Screen** and approved applications.

## Row and Column Size

**Row and Column Size** option will change the **SureLock Home Screen** grid size to specified value. This option is available for both **Portrait** and **Landscape** mode.



### **Note:**

- i. *The values for the **row and column size** can range between 0 and 11.*
- ii. *Widgets option should be in disable mode to enable this feature.*
- iii. ***Icon Size, Font Size, Use Classic Calculation, Spacing between the icons** are disabled when **Row and Column Size** option is enabled.*

## Icon Size

**Icon Size** option will set the size of approved applications' icons on **SureLock Home Screen**.

The user has following options to select from:

- Small (50%)
- Medium (100%)
- Large (200%)
- Extra Large (400%)
- Custom - Enter the desired value for the icon size can range between 10 and 600.
- Original - Displays icon with the actual resolution.

## Font Size

**Font Size** option will set the font size of approved applications' titles on **SureLock Home Screen**. The user has the following options to select from:

- Same Icon size
- Small (50%)
- Medium (75%)
- Large (100%)

- Custom Font Size - Enter the desired value for the text size

## Use Classic Calculation

**Classic Calculation** option will use the older algorithm to calculate icon size.

## Spacing between the Icons

The **Spacing between the icons** option will allow the user to specify space between the approved applications' icons on **SureLock Home Screen**.



**Note:** The value for the **spacing between the icons** can range between 1 and 50.

## Text Color

**Text Color** option will set text color for approved applications' titles on **Surelock Home Screen**.

## Apps Order

Admin can set the order of apps on the **SureLock Home Screen** with following options:

- **Alphabetical** - Allowed applications will be displayed in alphabetical order on the **SureLock Home Screen**.
- **Sequential** - Allowed Applications will be displayed in the sequence of applications added to the allowed applications list on **SureLock Home Screen**.

## Allow Icon Relocation

**Allow Icon Relocation** option will allow relocation of the icon on the **SureLock Home Screen**. This option once enabled will let the user drag and organize icons on the home screen.

Admin can enable this option, arrange the home screen and later disable it to retain the layout on the device.

## Detect Network Connection

**Detect Network Connection** option once enabled will redirect the user to **SureLock Home Screen** when an offline device connects to a network and goes online.

## Full Screen Mode

**Full Screen Mode** option will auto hide **Status Bar** and extend the display to fit the complete screen of the device.



**Note:** ***Status Bar** is the bar on top of the device screen which shows details about battery level, network strength and time.*

## Notification Badge

Use **Notification Badge** to enable a small red notification count badge on the application icon. This icon will notify the user of new messages/emails/call count.

The purpose of this feature is to let the user know the number of unread alerts or notifications for allowed applications.



**Note:**

- i. *This feature is supported only on Samsung KNOX devices (KitKat and above).*
- ii. *This option will be in disable mode by default.*

## Hide App Title

Allowed applications will display as icons with their respective titles on **SureLock Home Screen**. Use **Hide App Title** option to hide the title and display only icons of the approved applications on **SureLock Home Screen**.

## Floating Buttons Settings

Floating buttons are icons floating above the user interface on the screen. **SureLock** offers the feature to add a floating button on the screen with following options:

**Home, Back, Print and Recent.**



**Note:** *Floating Back and Print buttons are supported only on Samsung KNOX devices, rooted devices or devices with platform signature.*

To add **Floating Buttons** on the screen,

1. Access [SureLock Admin Settings](#).
2. On **SureLock Settings**, tap **Floating Buttons Setting**.
3. On **Floating Buttons Settings** screen, select the following:
  - a. Enable **Floating Back Button** and select desired options from the following:
    - **Floating Back Button**
    - **Floating Home Button**
    - **Floating Recent Button**
    - **Floating Print Button**
  - b. Tap **Floating Buttons Color** to pick a color for the icons.
  - c. Tap **Floating Buttons Size** option to set the floating button size  
(**Small/Medium/Large/Extra Large/ Custom** (desired value)) that will be displayed on SureLock home screen.
  - d. Tap **Allow Relocation of Floating Buttons** to allow relocation of floating buttons anywhere on the screen.
4. Tap **Done**.

### **Single Application Mode**

**Single Application Mode** refers to a state of device lockdown in which there is only one application on the screen. With just one application in the foreground, access to **Home Screen Settings** or other apps will be blocked at all time.

To enable **Single Application Mode**, follow these steps:

1. Launch **SureLock**.
2. Access [SureLock Admin Settings](#).
3. Go to **SureLock Settings > Single Application Mode**.
4. Enable **Single Application Mode**.



**Note:** To enable this feature, only one approved application should be visible on the **SureLock** home screen. To know how to add an allowed application on the SureLock home screen, see [here](#).

5. Go to **SureLock Settings > Single Application Mode** and select **Enable Single Application Mode**.
6. Select an application that you want to run in the **Single Application** mode.
7. Tap **Ok > Done**.



**Note:**

- i. If there are more than one application added to the **Allowed Applications**, a prompt appears to remove or hide other apps from the SureLock home screen.
  - ii. Please read the precautionary message before you tap **Ok**.
8. Go back to **SureLock Home Screen**.

The approved application with a green dot indicates that the application runs on **Single Application Mode**.

### Exit Single Application Mode

To exit from **Single Application Mode**, follow these steps:

1. Reboot the device.
2. When **SureLock** is loading, tap on the screen for 5 times within 3 secs to launch the password prompt.

Or

Tap 10 times on foreground application to launch the password prompt.



**Note:** These options are available only once and to activate it again, the user has to reboot the device.

3. On Admin Settings screen, tap SureLock Settings > Single Application Mode.
4. Disable Single Application Mode option to complete.

## Application Launch Delay

**SureLock** allows the user to delay the launch of **Single Application Mode** after the specified time.



**Note:** The default time set for the delay of the launch of **Single Application Mode** will be **500ms**.

## Run Only Once

Once this option is enabled will allow running of **Single Application Mode** only once. On reboot of the device, **Single Application Mode** will automatically get disabled.

## Create Single App Mode Exit File

This option will create **Single App Mode Exit File** and gets saved in the specified path. This file can be pushed using MDM solution like **SureMDM**. Once the user creates this file and pushes to the device, **Single Application Mode** will be disabled for first 10 minutes.

## Enable Password Prompt

This option will enable the user to launch password prompt by tapping 10 times anywhere on the screen when an application is running in the foreground on **Single Application Mode**.

## SureLock Settings

**SureLock Settings** allows the admins to edit and set general settings in **SureLock**.

## Change Password

Password to access SureLock Admin Settings can be changed using **Change Password**.





**Note:** In case of forgotten password, the user has to factory reset the device.

To change the Password, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **SureLock Settings** screen > **SureLock Settings** > **Change Password**.
3. Enter the existing **Old Password**.
4. Enter the **New Password**.
5. Enter the **New Password** again in **Confirmation** field.
6. Tap **Change** to complete.

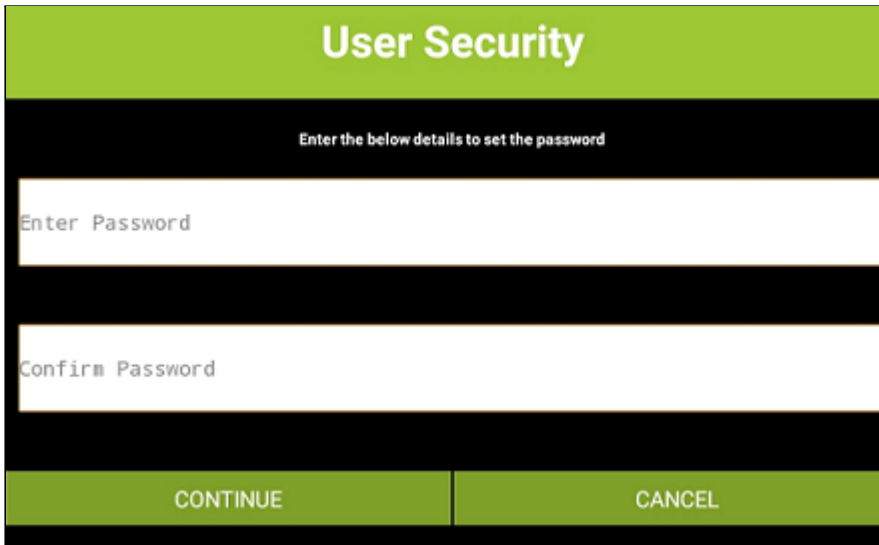
## User Security

**SureLock** will force the user to set a password to access the **Home Screen** when **User Security** option is enabled. User login screen will be displayed after the specified idle timeout interval and the user can access **SureLock Home Screen** only after entering the valid password.

To set a password to access the **SureLock Home Screen**, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **SureLock Settings** screen, select **User Security**.
3. On **User Security** prompt, select **Enable** and tap **Done**.

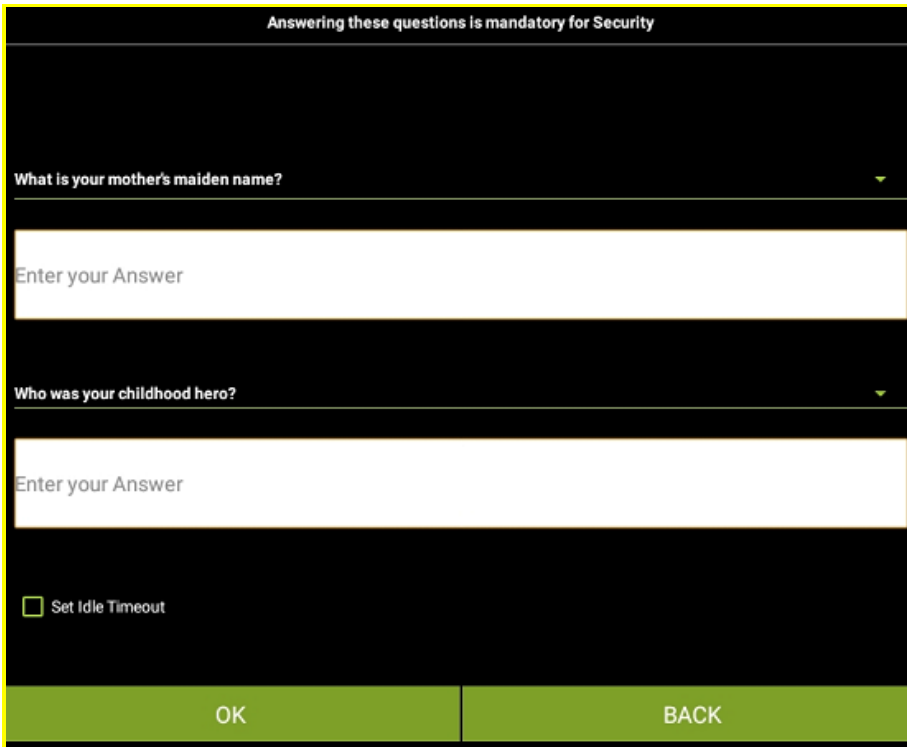
**User Security** screen will appear.



The 'User Security' screen has a green header with the title 'User Security'. Below the header, a black bar contains the instruction 'Enter the below details to set the password'. The main area is white and contains two text input fields: 'Enter Password' and 'Confirm Password'. At the bottom, there are two green buttons: 'CONTINUE' and 'CANCEL'.

4. Enter desired **Password** and type same password in **Confirm Password** field and tap **Continue**.

Security questions will appear as shown below:



The 'Security questions' screen has a black header with the instruction 'Answering these questions is mandatory for Security'. The main area is white and contains two drop-down menus with questions: 'What is your mother's maiden name?' and 'Who was your childhood hero?'. Below each question is a text input field with the placeholder 'Enter your Answer'. At the bottom, there is a checkbox labeled 'Set Idle Timeout'. At the very bottom, there are two green buttons: 'OK' and 'BACK'.

5. Select desired questions from the drop-down list and enter the relevant answers.
6. Select **Set Idle Timeout** and enter the value in **seconds / minutes** and tap **Ok**.



**Note:** User login screen will appear after the specified idle timeout.

## Admin Users

**SureLock** can be accessed by more than one admin user to configure the device and lockdown settings. Multiple admin profiles with different passwords can be created for multiple admin users. They can use their respective passwords to access SureLock Admin Settings to edit or update settings.

**Admin Users** will have access to all settings except for following five options under **SureLock Admin Settings**:

- Exit SureLock
- Uninstall SureLock
- Change Password
- Admin Users
- System Settings

## Add an Admin User

To add Admin users, follow these steps:

1. On **SureLock Settings**, tap **Admin Users**.
2. On **Admin User Settings** screen, tap **Add User**.
3. Enter the **Name**, **Description**, and **Password**.
4. Tap **Save** to complete.

## Edit an Admin User

To edit Admin user details, follow these steps:

1. On **SureLock Settings**, tap **Admin Users**.
2. On **Admin User Settings** screen, tap Admin User.

3. On **Admin Users** screen, tap on the specific admin user.

The details of the selected **Admin User** will appear.

4. Tap on the specific fields to edit the details.
5. Tap **Save** to complete.

### Delete an Admin User

To delete Admin Users, follow these steps:

1. On **SureLock Settings**, tap **Admin Users**.
2. On **Admin Users** screen, tap on the specific admin user.

The details of the selected **Admin User** will appear.

3. Tap **Remove** to complete.

### Multi-User Mode

Multi-User Mode option is helpful to maintain applications separately for different users. A single device can be shared among multiple users with the option to switch between different work profiles.

### Enable Multi-User Mode

To add multiple users, download **SureLock** and follow these steps:

1. Launch **SureLock**.
2. Tap **SureLock Home Screen** for **5** times within **3** seconds.
3. On the password prompt, enter SureLock default password as **0000** (four zeros) to access SureLock Admin Settings.
4. Tap **SureLock Settings**.
5. On **SureLock Settings** screen, enable **Multi-User Mode**.
6. Tap **Done** to go back to **Admin Settings** screen.

7. Tap **Allowed Applications**.
8. On **Allowed Applications** screen, tap **Add User**.
9. Enter the **User Name** and tap **Ok**.
10. To add multiple users, repeat steps 7 to 9.
11. Tap **Done** to complete.

### Add Allowed Applications to a specific user

To add an **Allowed Application** to a specific user, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Application**.
3. Tap **User Name**.
4. To add Allowed Applications to the user, see [Add Allowed Applications](#).

Once done and return to **SureLock Home Screen**, the user will now see separate icons with different users. The device users just have to tap their respective icon and assigned work profile to log in using their respective password.



**Note:** The default password for any user profile will be four zeros '**0000**'. To set a different password, follow these steps:

- i. Access [SureLock Admin Settings](#).
- ii. On **Admin Settings** screen, long tap on a specific user.
- iii. Type the password in **Password field**.

To log out or switch to another user profile, tap **Back** button.

### Delete a user

To delete a user, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Allowed Applications** screen, long tap on a specific user.

3. Tap **Remove** to complete.

## Disable Bottom Bar

Most of the Android devices have an on-screen bar at the bottom of the screen with options to navigate back, home, take screenshots and see recently used applications. Select **Disable Bottom Bar** option to disable this bar. This option will only disable the bottom bar and not hide it.



**Note:** *Disable Bottom Bar may not work for certain applications.*

## Hide Bottom Bar

Most of the Android devices have an on-screen bar at the bottom of the screen with options to navigate back, home, take screenshots and see recently used applications. Select **Hide Bottom Bar** option to completely hide from the screen.



**Note:**

- i. On selecting **Hide Bottom Bar**, the user has to reboot the device immediately or later.
- ii. This feature is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.

## Disable Hardware Keys

Hardware Keys includes Power Button, Home Button, Recent Apps Button and Volume keys of devices (smartphone or tablet). Select **Disable Hardware Keys** option to disable these hardware keys of the device.



**Note:** *This feature is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.*

## Disable Soft Navigation Keys

Soft Navigation keys are Home Button, Recent Apps Button and Back button on the devices (smartphone or tablet). Select **Disable Soft Navigation Keys** option to disable these keys on the device.



**Note:** *This feature is supported only on platform signed devices.*

## Assign SureLock System Permission

Use **Assign SureLock System Permission** option to copy SureLock.apk (setup file) to the system folder.



**Note:**

- i. On selecting **Assign SureLock System Permission** option, the user has to reboot the device.
- ii. This option will avoid users to break the lockdown by enabling safe mode or factory reset of the device and is supported only on rooted devices.

## Peripheral Settings

**Peripheral Settings** allows the admins to restrict or allow the use of Android device peripherals such as **camera, WiFi, Mobile Data** etc.

### Camera Settings

To disable camera from functioning, select **Always Disable** from the following options:

- Don't Care
- Always Disable

### Wi-Fi Settings

To disable Wi-Fi from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off

## Mobile Data Settings

To disable mobile data from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This feature is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.

## Prefer Mobile Data Settings

Select this option to use **Mobile Data** as connection preference even when connected to **Wi-Fi** network.

## Wifi Hotspot Settings

To disable Wi-Fi Hotspot from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off

## NFC Mode Settings

To disable NFC mode from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This feature is supported only on platform signed devices and have support for NFC mode feature on the device.

## GPS Settings



To disable GPS from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This feature is supported only on Samsung KNOX devices, rooted devices or platform signed devices.

## Bluetooth Settings

To disable Bluetooth from functioning, select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off

## Sound Settings

Use **Sound Settings** option to set a default sound setting for the device. It has following sound options:

- Don't Care
- Normal Mode
- Vibrate Mode
- Silent Mode

## Loudspeaker Settings

Use **Loudspeaker Settings** option to set the speaker settings of the device.



**Note:** **Loudspeaker Settings** option is enabled when SIM card is present in the device.

## Volume Settings

Admin can configure the following volume settings on the device:

- **Set Volume Level** – Set the desired volume level for Alarm, Ringtone, Media, Voice on the device using **Volume Slide Bar**.



**Note:** Minimum value to set for the volume will be **10**.

- **Set Range of Volume Level** - Set the desired volume range for Alarm, Ringtone, Media, Voice on the device using **Volume Slide Bar**. Once the range is specified the user can adjust the volume of the device only within the set range.

## Airplane Mode Settings

To enable **Airplane Mode**, select **Always On** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This feature is supported only on Samsung KNOX devices, rooted devices or platform signed devices.

## Flashlight Settings

To enable **Flashlight settings**, select **Always On** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This feature is supported on the devices that have flashlight option.

## SureLock Homescreen Orientation

**SureLock Homescreen Orientation** option will set the **SureLock Home Screen** orientation to either **Landscape** or **Portrait** using following options:

- Don't Care
- Landscape
- Portrait
- Reverse Landscape
- Reverse Portrait
- Auto Landscape
- Auto Portrait

## Rotation Settings

Use **Rotation Settings** to enable or disable rotation of device screen.

To disable screen rotation, turn the device in the desired screen orientation, access **SureLock Settings** and select **Always Off** from the following options:

- Don't Care
- Always On
- Always Off



**Note:** This option will be enabled only when **Watchdog Service** is enabled.

## Brightness Settings

Use **Brightness Settings** to adjust and set the brightness of the device screen. The following options are available to select from:

- Don't Care
- Force Auto Brightness
- Fix Minimum Brightness

- Fix Maximum Brightness
- Lock Current Brightness



**Note:** This option will be enabled only when **Watchdog Service** is enabled.

## Set Custom Toast Message

Admin can customize the toast message that appears when the user tries to access the unallowed application.

## Enable Toast Message

**Toast Messages** are small notification pop-ups which appear on the screen notifying the users. Once **Enable Toast Message** is selected, **SureLock** will notify the users with a toast message when any unallowed application is accessed.



**Note:** This option will be enabled only when **Watchdog Service** is enabled.

## Set Custom Access Denied Message

Use this option to enable a custom toast message instead of default Access Denied message.



**Note:** This option will be enabled only when **Watchdog Service** is enabled.

## Watchdog Service

**Watchdog Service** enables advance lockdown of the device by restricting access to any unallowed application from an allowed application. For example, if **Camera** is among the allowed applications, users may access gallery or share the picture using available options on the Camera screen. In this scenario, enable **Watchdog Service** to restrict the users to access only approved applications and nothing else.

- **Watchdog Service** enables the following settings:
- Rotation of Screen Brightness on Screen

- Enable Toast Message
- Set Custom Access Denied Message
- Kill unallowed Application
- On launch of unallowed Application
- Diagnostic Settings

## Kill Unallowed Application

When an Android device is locked down using **SureLock** and an unallowed application is launched, **SureLock** blocks the application however, the application remains launched in the background.

Select **Kill Unallowed Application** option will block all unallowed applications running in the background.



**Note:** This feature is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.

## Disable Clipboard

Admin can disable copy or paste option in **SureLock**.



**Note:** This feature is supported only on specific Zebra devices.

## Lock Safe Mode

Like in Windows OS, **Safe Mode** in Android runs only required settings and applications on the device and does not allow running of any other downloaded apps on the device. Getting into Safe Mode on an Android phone is as easy as pressing and holding phone's power button for a few seconds. This option will clear the password set for the device and allows any user to access the device.

**Lock Safe Mode** option in **SureLock** prevents the user from entering Safe Mode by locking it with a password. When the user tries to enter Safe Mode, SureLock will ask for the password, without which the Safe Mode won't be accessible. The admin can also set a password for the device as an additional security feature.



**Note:** This feature is available for devices running Android Marshmallow and below.

To enable **Lock Safe Mode**, follow these steps:

1. Login to **SureLock Admin Settings**.
2. On **Admin Settings** screen, tap **SureLock Settings**.
3. On **SureLock Settings** screen, tap and enable **Lock Safe Mode**.
4. On **Activate Device Administrator** prompt, tap **Activate**.
5. On the prompt, enter/select the following details:
  - Safe Mode Password
  - Confirmation
  - Add Device Password
  - Device Password
  - Confirmation
6. Tap **Change** to complete.

## Disable Safe Mode

This feature will disable **Safe Mode** option on the device.



**Note:** This feature is supported only on specific Zebra and LG devices.

## On Launch of Unallowed Application

Use **On Launch of Unallowed Application** option will redirect the user to any of the following screens:

- Home Screen
- Resume Previous Application
- Relaunch Previous Application



**Note:** This option will be enabled only when **Watchdog Service** is enabled.

## On USB state change go to Home

If the user wants to automatically redirect the screen to SureLock Home Screen when an external device (like the charger) is connected to the USB port, then enable On USB state change go to Home option.

## Auto Power On When Charger is Connected

Using this option admin can allow the end-user device to power On automatically when the USB charger is connected to the device.



**Note:** The device must be Lenovo CSDK (Pie or above) /running OEM agent V1.14 onwards for this setting to work.

## Auto Power Off When Charger is Disconnected

Use this option to set a time (in minutes/seconds) to delay the device from turning Off after the USB charger is disconnected from the device.



**Note:**

- The device must run in Device Owner mode/ Enterprise Agent or CSDK installed for this setting to work.
- This feature doesn't work on the Knox or other devices.

## Clear Data on Home Screen Load

Select this option to clear the data of the application (**launched in SureLock**) running in the background when the user returns to the **SureLock Home Screen**.

## Suppress Notification Panel

**Notification Panel** refers to a panel that displays the general notifications which can be accessed by simply dragging down the screen from the top.

Select **Suppress Notification Panel** to suppress the notification panel. Once enabled, the users will be restricted from viewing the Notification Panel.

## Hide Quick Settings Tile

This option will hide the Quick settings tiles from the Notification panel on Signed and Rooted devices.



**Note:** This feature is available for devices running Android Lollipop and above.

## Block Notifications

Admin can block all applications' notifications from **Notification Panel** on **SureLock Home Screen**.



**Note:** This feature is supported on all platform signed devices/ all lollipop and above devices.

## Disable Status Bar

**Status Bar** refers to the bar at top of the screen which displays date, time, battery level, network strength, and notifications. The device users can use this bar to access device settings or applications. It has following options:

- None - Status Bar will not be disabled. This setting will be applicable for all devices
- Legacy Mode - Status Bar will be disabled. This setting will be applicable for all devices
- Advanced Mode - Status Bar will be disabled. This setting will be applicable for only platform signed devices.



## Disable Factory Reset

**Factory Reset** allows the user to erase complete data stored in the device. Enable this feature to restrict the users from factory resetting the device.



**Note:** This feature is supported only on platform signed Lollipop devices / specific Zebra and LG devices.

## Disable USB

Enable this option to disable USB storage and USB debugging.



**Note:** This feature is supported only on Samsung KNOX/Rooted/Platform signed/ specific Zebra devices.

## USB Connectivity Preference

This option helps the admin to set the connectivity preference when USB is plugged-in with the device. It has the following options:

- **Don't Care**
- **File Transfer** - Allow transferring different types of files only.
- **Photo Transfer** - Allow transferring images or videos only.



**Note:** This feature is supported only on Platform signed devices.

## Disable OTG/External SD Card

This option disables the usage of **OTG/ External SD card**.



**Note:** This feature is supported only on platform signed/ specific Zebra devices.

## Suppress Power Button/Keyboard

Use this option **Suppress Power Button/Keyboard** to prevent shut down of the device and also disable keyboard of the device.

## Keyboard Settings

Some Android devices allow the use of USB port to attach external keyboards. When an external keyboard is attached to a device, the on-screen soft keyboard is disabled.

Select **Keyboard Settings** option to enable on-screen soft keyboard even when an external keyboard is plugged in using the USB port.



**Note:** This feature is not supported by Android Lollipop and above.

## Enable SureKeyboard

While using the device keyboard, the users will have the option to long-press Settings key (from the device) and can alter the device settings or exit from the lockdown state. SureLock allows the admin to set SureKeyboard as a default keyboard instead of the device keyboard that prevents the users exiting from lockdown state. On enabling SureKeyboard, Settings key option will not be available for the user.

To enable SureKeyboard, follow these steps:

1. Launch **SureLock**.
2. Navigate to **Admin Settings > SureLock Settings > Enable SureKeyboard**.

## Driver Safety

**Driver Safety** locks the device screen completely to stop driver's interaction with the device while driving at a particular speed. This function works in coordination with GPS and allows the user to set a speed threshold for the vehicle to auto lock and restrict all device functionalities.



**Note:** GPS should be **ON** and set to **High Accuracy**.

## Enable Driver Safety

**Enable Driver Safety** option helps the admin to set Driver Safety settings.

Following are the options available in Driver Safety feature:

## Enable Driver Safety Overlay

Select this option to display an overlay on the screen when the vehicle speed exceeds the set overlay threshold.

Enable Driver Safety Overlay option enables the following settings:

- **Allow Running Background Applications** - Allows applications to run in the background even when driver safety overlay appears on the screen.
- **Set Driver Safety Overlay Threshold** - Enter the value for **Driver Safety Overlay Threshold** in **Miles/Km**. When the vehicle speed exceeds the specified **Overlay Threshold** then an overlay appears on the screen and will restrict the driver from accessing the device functionalities.

## Allow Transparent Overlay

Select **Allow Transparent Overlay** option to show a transparent overlay on the screen when the driver exceeds the speed threshold set by admin. If driver tries to tap on the screen, driver safety overlay will be visible for only few seconds.

## Enable Email Alert

Select **Enable Email Alert** option to enable email alert service to the admins.

Enable Email Alert option enables the following settings:

- **Set Email Alert Threshold** - Enter the value for **Set Email Alert Threshold** in **Miles/Km**. When the vehicle speed exceeds the **Set Email Alert Threshold** then an email alert is sent to the admin.
- **Alert Email Address** - Enter the admins' email address to send an alert email to the user when the vehicle speed exceeds the specified **Email Alert Threshold**.

## Enable Driver Safety Profile

Driver Profile has to be configured before selecting **Enable Driver Safety Profile** option.

Admin can select and enter a path to import new settings when the vehicle speed exceeds the specified **Driver Safety Profile Threshold**.

**Enable Driver Safety Profile** option enables the following settings:

- **Set Driver Safety Profile Threshold** - Enter the value for **Set Driver Safety Profile Threshold** in **Miles/Km**. When the vehicle speed exceeds **Set Driver Safety Threshold** then **SureLock** will import alternate driver profile settings file with specific applications allowed to the user.
- **Set Driver Safety Profile Delay (secs)** - Enter the value in **secs**. Admin can set the delay on applying **Driver Safety Profile** settings on the device.
- **Location update interval**- Enter the value for **Location update interval** in **secs**. **SureLock** receives the location update at the specified time interval.

## Bootup Delay

There might be instances where multiple applications approved in **SureLock** will need time for proper booting.

**Bootup Delay** option in **SureLock** will delay the bootup process to allow proper booting of all approved applications.

## Timeout Settings

**Timeout Settings** offers a range of features which can be used for configuring time-based lockdown and device behavior like preventing the device from suspending or redirection activity on idle timeout.

## Prevent Suspend Mode

Android device screen goes into sleep mode when the device is idle for a specific period of time depending on the device settings. Enable **Prevent Suspend Mode** to keep the device screen always **On** when **SureLock** is running.



**Note:** *Prevent Suspend Mode enables **AC Power Prevent Suspend** and **Schedule Prevent Suspend Mode** and disables **Keep CPU On** option.*

### Keep CPU On

Use **Keep CPU On** option to keep CPU ON when **SureLock** is running.

### AC Power Prevent Suspend

Enable **AC Power Prevent Suspend** feature to prevent the device screen from going off when **SureLock** is running and the device is plugged into **AC Power**.



**Note:** *AC Power Prevent Suspend disables **Schedule Prevent Suspend Mode**.*

### Schedule Prevent Suspend Mode

Use **Schedule Prevent Suspend Mode** feature if the user wants the device running **SureLock** to get into **Prevent Suspend Mode** on a specific time and days of the week. This feature gives the option to specify following details:

- Start At
- End At
- Days of the week

### Pause Prevent Suspend on Low Battery

Select this option and set the required battery threshold. When the battery percentage of the device reaches the specified threshold, then the **Prevent Suspend Mode** option will be paused automatically.

### Prevent Suspend Only for Selected Apps

Admin can enable **Prevent Suspend Mode** on specific apps using this option. There are two options under this feature:

**Only for the selected apps** – Select this option to enable **Prevent Suspend Mode** on selected apps only when running in the foreground.

**Except for the selected apps** – Select this option to enable **Prevent Suspend Mode** on all allowed apps except for the selected apps when running in the foreground.

### Idle Timeout

Select **Idle Timeout** feature to set a period of time for the device to be inactive after which **SureLock** redirects the device screen to **SureLock Home Screen**.

### Idle Timeout Application

Select **Idle Timeout Application** feature to select an approved application to be inactive after which **SureLock** redirects the screen to an option given below instead of **SureLock**

#### Home Screen:

- **Chrome** – Redirects to the Chrome browser
- **Logout** – Logout from SureLock

### Enable Sleep Mode After Idle Timeout Action

With this setting, admin can allow an application that can run as a screensaver in SureLock.

To configure an application that will run as a screensaver, follow these steps:

1. Add an allowed application (that can run as a screensaver).
2. Configure screensaver timeout for the application.
3. Access [SureLock Admin Settings](#).
4. Tap Timeout Settings and enable **Idle Timeout**.
5. Go to **Idle Timeout Application** and select **None**.

## 6. Select **Enable Sleep Mode Idle Timeout Action**.



**Note:** *Idle Timeout value should be higher than the screensaver timeout value for this setting to work.*

For example: Let us imagine, when idle timeout is set for 10mins in SureLock and screensaver timeout is set for 5mins for the application, beyond the device's idle timeout (i.e 10mins) the screen redirects to the SureLock home screen and after 5mins of screensaver timeout, the screensaver will appear.

### **Restart App on Idle Timeout**

Enable **Restart App on Idle Timeout** option if the user wants the locked Android device to wake up after the idle timeout with refreshed app screen.

### **Reset Brightness Timer on Idle TimeOut**

**SureLock** has multiple features which once enabled save battery consumption by specifying auto adjusting of brightness on device inactivity or redirecting to **SureLock Home Screen** on device inactivity.

This feature once enabled will reset the timer specified in **Brightness on Inactivity** to **0** (zero) when the device is inactive.

**Example:** *If **Idle Timeout** is set as **10** seconds and **Brightness on inactivity** is set as **15** seconds, the timer for both the activities will start together. When the device is inactive for **10** seconds, it gets into **Idle Timeout mode** and resets the timer of **Brightness on Inactivity** to **0** (zero). This cycle continues till the device is in the inactive state.*

### **Schedule Reboot**

Use this feature to reboot the device on specified days and time. Select **Enable schedule Reboot** option to select **Change schedule reboot time** and **watch dog** for the device to auto reboot on the scheduled time and days.



**Note:** This feature is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.

## Widget Settings

The user can organize the approved widgets in **SureLock Home Screen**.

**Widget Settings** has following customization options:

To apply the **Widget Settings** on the device, follow these steps:

1. Select **Display Widget(s)** to apply settings for the Widget.
2. Select **Widget App/ Shortcut Title**.
3. Tap on the position (**Top/Bottom/Left/Right**) to display the Widget on the **SureLock Home Screen**.
4. Select **Widget Settings** as **Show** or **Hide**.
5. Select **Widget alignment** as **Vertical** or **Horizontal**.
6. Select **Show Widget Tray** to display the tray on the **SureLock Home Screen**.
7. Select **Landscape Widget Area** (in pixels) using the slider.
8. Select **Portrait Widget Area** (in pixels) using the slider.
9. Tap **Done** to complete.

## Title Bar Settings

Select **Title Bar Settings** to enable and customize title bar on **SureLock Home Screen**.

**SureLock Title Bar Settings** has following customization options:

- **Text** - Enter the **Name** to display on Title bar





**Note:** *Title Bar* text can be customized by adding **SureLock** version to it.

- **Font Color** - Select the desired **Font Color** from options displayed
- **Font Size** - Enter the **Font Size** (in numeric)
- **Font Style** - Select the desired **Font Style** from the options displayed
- **Font Family** - Select the desired **Font Family** from the options displayed
- **Position** - Select the desired **Position** for the text to display
- **Enable Gradient** - Select **Enable Gradient**
- **Color** - Select the desired background color from **Pick a Color bar**
- **Size** - Enter the **Title Bar Size** (in numeric)
- **Preview** - The user can view the settings applied to the **Title Bar**

### Status Bar Color

The user has the option to change the **Status Bar Color** by selecting a color from the Color Bar.



**Note:**

- i. **Status Bar Color** will be enabled only when **Full Screen Mode** is disabled.
- ii. This feature is supported only for Android versions Lollipop and above devices.

### SureLock Analytics

**SureLock Analytics** option will record **SureLock** activities such as the name of applications accessed, time spent on the applications, unallowed applications that are blocked and more.

The user can also export the records in **.csv** format.

The export and clearing of analytics data can also be scheduled on a specific day and time using **Schedule Export** feature under **SureLock Analytics**.

The following are the options available in **Analytics Settings**:

- **SureLock Analytics** - Enable this option to configure SureLock Analytics
- **Export Analytics Data** - Browse and select the location to export the analytics data in .csv format
- **Clear Analytics Data** - Clears all stored analytics data
- **Schedule Export** - Enable this option to schedule export of analytics data to **File / Mail / SureMDM**.



**Note:** Analytics report can be generated from SureMDM Web Console.

- **Export At** - Set a scheduled time for the export of analytics data
- **Days of the week** - Select the required days of the week for scheduled export
- **Schedule Export to Mail** - Enable scheduled export of analytics to configured email id
- **Configure Email** - Analytics Data will be exported to the configured email
- **Clear Analytics Data After Export** - Clears all analytics data after export from the device

## Power Saving Settings

**Power Saving Settings** will save on power consumption by adjusting and setting the brightness of the device.



**Note:** **Power Saving Settings** option is enabled when **Brightness Settings** is set to **Don't Care**.

There are following options available in **Power Saving Settings**:

- **Enable Power Saving** - Enables power saving option
- **Default Brightness** - Set the default values for the brightness when the device is connected to **Battery/AC Power**.



**Note:** Brightness values should range between 0 and 255.

- **Brightness On Inactivity**- Set the value of the brightness when the device becomes inactive after the specified time.
- **Brightness On Battery Level** - Set screen brightness based on the battery level
- **Disable Brightness Change On Third-Party App** - Brightness settings on Third party Apps can be disabled.



**Note:** *Disable Brightness Change on Third-Party App* option is supported only on Jellybean and KitKat devices.

### Battery Popup Notification

This feature helps the user to show popup notifications and sound alerts when the device battery reaches the specified threshold.

- **Battery Popup Notification** has following options:
- **Show Low Battery Popup** - Enable this option to configure Battery Notifications
- **Configure Popup** - Configure the following popup settings:

**Battery Popup Threshold (%)** - Enter the value for **Battery Popup Threshold**. When the battery level reaches the specified threshold, device user will be notified with an alert message.

**After Every % Drop In Battery (%)** - Enter the value for **After Every % Drop In Battery (%)**. When the specified battery percentage drops from the set threshold, device user will be notified with an alert message.

**Alert Message** - Enter the message to display when battery percentage goes below the specified threshold.

### Miscellaneous Settings

## Number of Taps

**SureLock Settings** password prompt by default can be launched with 5 taps on the screen.

**Number of Taps** option allows admins to change this default **5 taps** to a desired number of taps.



**Note:** The value entered for **Number of Taps** should range between **4** and **60**.

## Access Settings Timeout

The admins can restrict the access to SureLock Admin Settings after a specified time period.

Once Access Settings Timeout option is enabled, the password prompt will not appear even if the user taps the required numbers within a specified time.



**Note:** Once this feature is enabled, to login to **SureLock Admin Settings**, the device needs to be rebooted.

## Admin Login Security

**SureLock** offers following admin related features. Some of these features require lockdown device which needs to be enrolled in [SureMDM](#).

**Admin Login Security** - Select this option to enable **Admin Login Security features**.

**Block Admin Access after loading SureLock** - When this feature is enabled, access to **SureLock Admin Settings** will be blocked after loading **SureLock**. The only way to access **SureLock Admin Settings** is to reboot the device and tap for **5** times while loading.

**Send Mail to SureMDM** - This option will be greyed out if the locked device is not enrolled in **SureMDM**. Once this feature is enabled, the admins get email notifications when the user tries to access **SureLock Admin Settings** and fails.

- **Block login until reboot** - Enable this option to reboot the device to access **SureLock Admin Settings**, when the user exceeds the number of failed attempts specified in **Login Threshold**.
- **Block Login for a specified time** - Enable this option to block the **SureLock** login for a specified time that is set in the **Set Prevent Login Time**, when the user exceeds the number of failed attempts specified in **Login Threshold**.
- **Block Login until SureMDM notifies** - Enable this option to block access to **SureLock Admin Settings** when the user exceeds the number of failed attempts specified in **Login Threshold**. SureLock will block access to **SureLock Admin Settings** until the admins use **SureMDM** to push the grant login access run script to the device.

A run script job with the following command should be pushed to the device to grant login access.

**For Blank password:** *am broadcast -a com.gears42.surelock.COMMUNICATOR -e "command" "allowlogin"*

**For Other passwords:** *am broadcast -a com.gears42.surelock.COMMUNICATOR -e "command" "allowlogin" -e "password" "0000"*

- **Login Threshold** - Use this option to set value for the maximum number of failed attempts by the device users, after which the set features under **Admin Login Security** gets triggered.
- **Send Daily Login Report** - Once this option is enabled, **SureLock** will send daily login report for successful and failed Attempts to **SureMDM**.
- **Send At** - Set the time for the **Daily Login Report** to be sent to **SureMDM Web Console**.

### Send Notification On Exit

Use this option to enable a notification to be sent to following options when the user exits

#### **SureLock:**

- **Notify Through Mail** - Enable this option to notify the admins through the email.
- **Notify Through SureMDM** - Enable this option to notify the admins through SureMDM.

#### **Set Usage Access Warning**

This option will be available when **Enable Usage Access** is disabled under **Setup SureLock Permissions**. The warning message can be customized as per the requirement.



**Note:** This feature is supported only on Android versions 5.1.1 and above devices.

#### **Enable Log**

Enable this feature to record logging activities of **SureLock**. Log File records all the events and activities of **SureLock** and gets saved at a specified location.

**Set Log File Path** - Browse and select a location for the log file to save.

#### **Send Error Report**

This option enables **SureLock** to collect and send logs and diagnostic information to enterprises' server whenever an error occurs.

#### **Use Advance Hide Bottom Bar**

This feature is similar to **Hide Bottom Bar** which completely hides the bottom bar of the device. Unlike **Hide Bottom Bar** option, to enable this feature the device does not require a reboot.



**Note:** This feature is supported only on devices with Android KitKat or below versions.

#### **On Press of Home Button**

This option will redirect the users to either **Last Accessed Folder** or **Home Screen** when **Home** button is tapped.



**Note:** This option is helpful when multiple approved applications are arranged in folders.

## Disable Touch Input

Enable this feature to disable touch input on the screen when **SureLock** is on. Once this option is enabled, the user can only launch **SureLock Password Prompt** by tapping 5 times on the screen.



**Note:**

- i. Launching of **SureLock Password Prompt** by tapping on screen 5 times will work even if **SureLock** is not in focus.
- ii. **Disable Touch Input** is enabled only when **Idle Timeout** and **Brightness on Inactivity** are disabled.

## Use SDP Calculation

Enable **Use SDP Calculation** option to use advanced calculation for icon size and font size. This option works based on the different versions of Android.



**Note:** The user can see the difference in the **Font** and **Icon** size when Android is upgraded to Marshmallow and above.

## Memory Settings

Use **Memory Settings** to track memory usage by allowed applications. Once enabled and a **Memory Threshold** is set, SureLock will automatically clear the open application if the free memory is less than the specified threshold. Admin has the option to hide all prompts on SureLock Home Screen when background processes are being killed.

## Screensaver Settings

Use **Screensaver Settings** option on device inactivity. This option allows only an image or GIF to be set as a screensaver and has the following options:

- **Enable Screensaver** - enables screensaver option
- **Use System Wallpaper** - uses wallpaper of the device as the screensaver
- **Select Screensaver Media or Webpage** - allows the user to browse and select an image /enter webpage URL for the screensaver
- **Screensaver Timeout** - allows user to set a time of inactivity for the screensaver to appear



**Note:** The time (in secs) set for **Idle Timeout** should be higher than **Screensaver Timeout**.

- **Load Page In Background** - allows loading the page in background even if screensaver is running

## Disable Applications

Use **Disable Applications** to disable launch of any non-native/third-party applications including the ones that are allowed in **SureLock**.



**Note:** This option will not list the system applications/native applications and is supported only on Samsung KNOX devices, rooted devices or devices which are platform signed.

## Disable Wi-Fi /Mobile Data Access

Admin can activate or deactivate the connectivity preference (**WiFi / Mobile Data**) for the specific apps.

## Unrestricted Data Usage

When Data Saver is ON, device will restrict the data access for all apps in the device. Enable this setting to allow unrestricted data access for the specific apps.





**Note:** *This feature is supported only on Nougat and above signed devices.*

## Default Runtime Permissions for Allowed Apps

Admin can grant/deny all the runtime permissions for Allowed Applications from SureLock Admin Settings.

To grant all permissions for the allowed applications, select **Grant All** from the following options:

- Don't Care
- Grant all
- Deny All



**Note:**

- This feature is supported only on Marshmallow & above devices and it should be either Knox/Platform Signed devices.*
- In Platform signed devices, **Deny All** option is not available.*

## Diagnostic Settings

**Diagnostic Log** refers to the log that has the list of all events when **SureLock** blocks unallowed applications.

Enabling **Diagnostic Log** also enables, following options:

- **Enable Diagnostic Log** - Diagnostic log once enabled will log all activities of allowed/blocked applications and notifies whenever any icon unallowed application is blocked.
- **Set Diagnostic Log Path** - Browse and select a folder to save the diagnostic logs.
- **View Diagnostic Log** - Use **View Diagnostic Log** option to view the log of all activities in SureLock.

- **Clear Diagnostic Log** - Use **Clear Diagnostic Log** option to clear the log entries.

## Samsung Knox Settings

**Samsung KNOX** feature in **SureLock** is available only for **Samsung Android** devices with **Android 4.2.2** and above. Once enabled this feature in **SureLock** will provide advance lockdown functionalities for the device without rooting.

There is no rooting required to enable advanced lockdown features in Samsung Knox enabled devices. Select **Enable Samsung Knox options** to enable the following features:

Set Custom Boot Animation

Set Custom Shutdown Animation

Disable Other Home Screens

Disable Safe Mode

Disable Factory Reset

Disable Multi Window

Disable USB

Wipe Recent Apps

Disable S Voice

NFC Mode

Disable Air View Mode

Disable Air Command Mode

Disable Smart Clip Mode

Allow Multiple Users

Disable OTA Upgrade

Disable SD card

Disable Hardware Keys

Disable Custom Hardware Keys

Disable Power Off

Disable Application Installation

Disable Application Uninstallation

Disable Edge Screen Functionality

Hide status Bar

Hide Navigation Bar

### **Set Custom Boot Animation**

Samsung devices display an animation of Samsung logo when the device is booting.

Select **Set Custom Boot Animation** option to play the desired animation file while booting the device.



**Note:** This feature is supported only when **Samsung Enterprise Agent** is installed on the device and custom **KNOX** license key file is placed in the root folder of the SD Card.

### **Set Custom Shutdown Animation**

Samsung devices display an animation of Samsung logo during the shutdown.

Select **Set Custom Shutdown Animation** option to play a desired animation file during the shutdown.



**Note:** This feature is supported only when **Samsung Enterprise Agent** is installed on the device and custom **KNOX** license key file is placed in the root folder of the SD Card.

### **Disable Other Home Screens**

Android devices can have more than one home screens; inbuilt and downloaded. When

**Home** button is pressed, the user gets an option to select home screen from the available

options. Once **Disable Other Home Screen** option is enabled, it disables all other installed home screens along with device's default home screen and directs the user to **SureLock Home Screen**.

### *Disable Safe Mode*

**Safe Mode** is a diagnostic mode and lets the user boot the Android device with disabled third-party applications. An user can manually enter **Safe Mode** by using the **Power** and **Volume** buttons. Once the user enters **Safe Mode**, third-party applications can be disabled and uninstalled.

Use **Disable Safe Mode** option to prevent users from entering **Safe Mode** using device hardware keys by password protecting the access.

### *Disable Factory Reset*

This option prevents users from resetting the device to factory settings. This is helpful if **Settings** is allowed as an approved application and do not want the user to factory reset the device. Once this option is enabled, **Factory Reset** option gets grayed out.

### *Disable Multi Window*

Multi-window option is accessed through the draggable vertical bar on the left side of the device screen. This option is used for launching applications and arranging them in multi-window view.

Once **Disable Multi Window** option is enabled, the multi-window accessing option on the devices will be disabled.

### *Disable USB*

This option disables following two ways of USB usages:

- Mass Storage - restricts access to the stored files on the device
- USB Debugging - restricts access to device using Command Prompt

### *Wipe Recent Apps*

Once **Wipe Recent Apps** option is enabled, on the launch of **SureLock**, the recent applications accessed by the user on the device gets auto wiped.

### *Disable S Voice*

**S Voice** feature is a virtual mobile personal assistant which is capable of running a large number of tasks through voice command.

This option disables **S Voice** feature on Samsung devices.

### *NFC Mode*

**NFC** (Near Field Communication) is a means of passing data from one device to another over radio waves by touching them or putting them closer.

Use this option in Samsung devices to keep the NFC mode of the device as always **ON** or always **OFF**.

### *Disable Air View Mode*

This option disables the Air View which allows the user to get a preview of certain types of content without having to actually touch the display.

### *Disable Air Command Mode*

This option disables Air Command gestures which gives access to **S Pen** features like **Smart select**, **Screen write**, and **Samsung Notes**.

### *Disable Smart Clip Mode*

The user has the option to block **Smart Clip** feature on the device. If it set to false, the user will not be able to use the stylus pen, smart clip, copy/paste.

### ***Allow Multiple Users***

Use this option to disable Multiple users functionality which allows multiple user spaces on shareable devices such as tablets.

### ***Disable OTA Upgrade***

Use this option to disable **Over the air upgrades** in Samsung devices.

### ***Disable SD card***

This option disables SD card if present in the Samsung devices.

### ***Disable Hardware Keys***

This option disables all the hardware keys of the device. These hardware keys include Home, Volume Down, Back, Volume Up, Menu, Recent Apps and Power Button.

### ***Disable Custom Hardware Keys***

This option disables the hardware keys (includes Volume Up, Volume Down, Home, Flash key) of the device.

To disable the hardware key, follow these steps:

1. Access **SureLock Settings**
2. Tap **Samsung Knox > Disable Custom Hardware Keys**.
3. Tap **Add New Key**.
4. On **Add New Hardware Key** prompt, enter a keycode or press and hold the hardware key and tap **OK**.

### **Disable Power Off**

Select this option to block the user from switching off the device or restart the device.

### **Disable Application Installation**

This option disables the user from installing new applications on Samsung devices.

### **Disable Application Uninstallation**

This option disables the user from uninstalling applications in Samsung devices.

### **Disable Edge Screen Functionality**

This option disables the edge screen functionality on the Samsung devices.



**Note:** This feature is supported only on Samsung Edge devices (for example: Samsung S8 Edge, Samsung S9 Edge etc.).

### **Hide Status Bar (Samsung Knox)**

This option will hide the status bar (refers to the bar at top of the screen which displays date, time, battery level, network strength, and notifications) of a device.



**Note:** This option will be disabled when Hide Bottom Bar is selected.

### **Hide Navigation Bar (Samsung Knox)**

This option will hide the navigation buttons (refers to the Back, Home, Recent buttons) on a device.



**Note:** This option will be disabled when **Hide Bottom Bar** is selected.

## **Allowed Widgets**

**Widgets** refer to the application's extension which resides on Android Home Screen for quick access.

**SureLock** allows the user to create a similar setting on **SureLock Home Screen**. The user can use options under **Allowed Widgets** to add and modify app or shortcut widgets.

### Add Widget

The user can add the widgets to the **SureLock Home Screen**.

To add a Widget, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Widgets**.
3. On **Allowed Widgets** screen, tap **Add Widget** to list all App Widgets.
4. Select the desired application(s) widget to allow from the list, and tap **Done**.

List of all allowed widgets will get displayed on the **Widget Tray** of **SureLock Home Screen**.



**Note:** The Applications that are added in the **Allowed Applications** can only be added to the **Widgets**.

### Edit/Remove Widget

Widgets that are added to the Home Screen can be edited or removed.

Widget properties such as **Landscape Margin**, **Portrait Margin**, **Select Widget Size** can be edited in this option. Only **Widget Position** can be changed from **Admin Settings >**

**SureLock Settings > Widget Settings**.

To remove an allowed widget, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Allowed Widgets**.
3. On **Allowed Widgets** screen, tap on the widget from the list.
5. On **Widget Details** screen, tap **Remove** to complete.



## Manage Shortcuts

Shortcuts are links which provide quick access to files, applications or settings.

**SureLock** provides a way to create shortcuts for system settings, documents & applications on its home screen.

### Add a Shortcut

To add a Shortcut, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Manage Shortcuts**.
3. On **Manage Shortcuts** screen, select the following options:
  - **Allow New Application Shortcuts on Home Screen** - Select this option to display the newly created application shortcut on the **SureLock Home Screen**.
  - **Show New Application Shortcuts on Home Screen** - Show or hide the application shortcut on the **SureLock Home Screen**.
  - **Remove Shortcuts on App Uninstall** - Select this option to remove the application shortcut when the app is uninstalled.
4. Tap **Add Shortcut**.

Two types of shortcuts can be created:

#### System Settings Shortcut:

- a. Tap **Add Settings Shortcut** for System Settings.
- b. Select a shortcut for Android Settings from the list.

Shortcut configuration for the System Settings will be populated.

#### Application Shortcut:

- a. Tap **Add App Shortcut** for Applications.

- b. Select an app from the list.

Shortcut configuration for the App will be populated.

5. Edit the attributes for **Icon, Action, Category, Package Name, Class Name, URI, Extras, and Flags.**
6. Enter the **Password** to access the shortcut.
7. Select appropriate options: a. **Restart app on relaunch** b. **Launch at Startup** c. **Hide Icon in Home Screen.**
8. Browse and select **Current Path** to locate the folder and **Move** the shortcut to it.
9. Once done with configuring the shortcut, tap **Test Shortcut** to test the shortcut.
10. Tap **Save and Done** to complete.

Newly created shortcut will be displayed on the **SureLock Home Screen.**



**Note:** The user needs to add the Application or Package to the list of Allowed Applications for the shortcut to work.

- **Deny Shortcut** - Admin can blacklist a specific application downloaded from Play Store.

Tap **Deny Shortcut** and enter the package name to be blacklisted. If the user tries to download the denied package or application from Play Store, shortcut for the denied package will not be created and the user can see the denied toast message on the screen.

## Delete a Shortcut

To delete a Shortcut, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Manage Shortcuts**.
3. On **Manage Shortcuts** screen, tap on the desired shortcut.
1. Details of the Shortcut (Settings/App) will be displayed on the screen.

4. Tap **Delete** to complete.

## Phone Settings

Phone Settings option allows to manage calls and SMSs on the locked device.

**Phone Settings** has following options:

- **Call Progress Screen** - If the device has calling option and **SureLock** is running, the user can receive calls but **Call progress screen** may not be visible, which has all the information and options for the ongoing call. Enable **Call Progress Screen** to make call progress screen visible on the device.
- **Block All Incoming Call** - Use **Block All Incoming Call** feature to block all incoming calls.
- **Block All Outgoing Call** - Use **Block All Outgoing Call** feature to block all outgoing calls.
- **Automatically Allowlist New Contact** - Use this option to automatically add newly added contacts to the allowlist phone numbers.
- **Blocklisted Phone Number** - Add phone numbers in **Blocklisted Phone Number** if the admins have allowed all incoming or outgoing calls in a device and wish to block incoming or outgoing calls for selective phone numbers.
- **Allowlisted Phone Number** - Add phone numbers in **Allowlisted Phone Number** if the admins have blocked all incoming or outgoing calls in a device and wish to allow incoming or outgoing calls for selective phone numbers.
- **Block All Incoming SMS** - Use Block All Incoming SMS feature to block all incoming SMS.
- **Block All Outgoing SMS** - Use Block All Outgoing SMS feature to block all outgoing SMS.
- **Block All Incoming MMS** - Use Block All Incoming MMS feature to block all incoming MMS.

- **Block All Outgoing MMS** - Use Block All Outgoing MMS feature to block all outgoing MMS.
- **SMS Command Password** - Use this feature to enable **SureLock** specific SMS commands. This is very useful to reset the device password using SMS, when Nix is offline on the devices.

**Note:**

- Phone Settings** options will be enabled when **SureLock** is installed in sim supported devices.*
- SMS and MMS options are supported only on Samsung Knox devices.*

## Multi-User Profile Settings

A single device can be shared with multiple users. Each user will be assigned to different set of applications and configurations. Users and Profiles are added from **Multi-User Profile Settings**.



**Note:** Multiple users can be assigned with the same profile.

Tap **Enable Multi-User Profile** to activate the following options:

- Profile Management
- User Management
- Server Configuration

### Profile Management

Multiple Profiles can be added with the different set of applications and configurations on the **Profile Management** screen.

To create a profile, follow these steps:

1. Access [SureLock Admin Settings](#).

2. On **Admin Settings** screen, tap **Multi-User Profile Settings**.
3. On **Profile Management** screen, tap **Add** and enter the **Profile Name**.
5. Tap **Ok** to complete.
6. To add more profiles, repeat steps 3-4.

**Note:**

- i. **Default Profile** will be active by default.
- ii. The admins have the option to **Add, Clone, Delete** and **Edit** the profiles.

**Activate a profile and add applications to the profile**

To activate a profile and add applications to the profile, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Multi-User Profile Settings**.
3. On **Profile Management** screen, tap **More** options button of the profile that the user wants to activate.
4. Tap **Activate**.
5. Go back to **Admin Settings** and follow the steps mentioned in [Add Allowed Applications](#) to add applications to the profile.

The approved applications will get listed on the **SureLock Home Screen**.

**User Management**

Admin can add multiple users and associate same or different profile for each user from User Management.

**Add Users and assign profile to the Users**

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Multi-User Profile Settings**.

3. On **Multi-User Profile Settings** screen, tap **User Management**.
4. On **User Management** screen, tap **Add**.
5. On **Add User** prompt, enter **Username, Password , Email Id** and select the profile from the drop-down list.
6. Tap **Save** to complete.

The newly created user will get listed on **User Management** screen.

7. To add more users and assign the profile to the users, repeat steps 3-5.



**Note:** Admins have the option to **Add, Delete** and **Edit** the users.

The login screen will be displayed on **SureLock Home screen**. When the user login with the valid credentials, specified profile gets applied to the device.



**Note:** In case the user forgets password, enter the **User Name** and tap **Forgot Password**. Existing password details will be sent to the configured email.

## Server Configuration

The admins can configure LDAP server details on the **Server Configuration** screen. Use LDAP server for user authentication and apply profile based on the meta tag key.

To configure **LDAP** server details, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **Admin Settings** screen, tap **Multi-User Profile Settings**.
3. On **Multi-User Profile Settings** screen, tap **Server Configuration**.
4. On **Server Details screen**, enter the **Server Path, Port Number, Distinguished Names, Profile Meta Tag key**.



**Note:** The admins should create profiles in **Profile Management** screen with the value given in **Profile Meta Tag Key**. If any user login with valid credentials, the desired profile (value given in **Profile Meta Tag Key**) will be applied to the device.

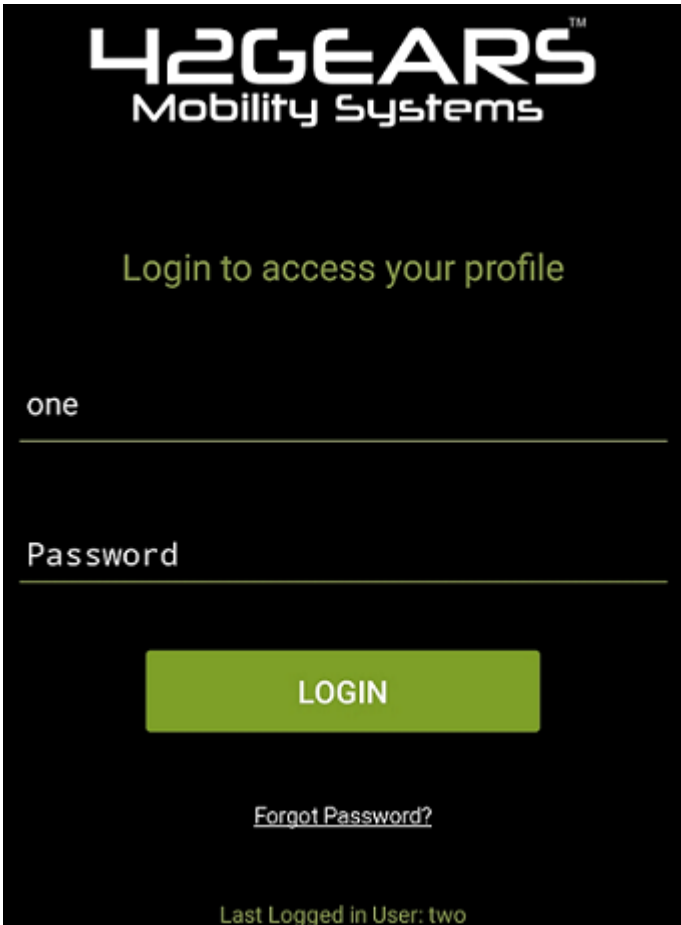
5. **Revoke Access When No Meta Tag/Profile is Found:**

- i. **Enable** - Enable this option if **Profile Meta Tag Key** is not available for the user to avoid the user from logging.
- ii. **Disable** - Disable this option if **Profile Meta Tag Key** is not available for the user to apply the **Default Profile** to the device.

6. Tap **Validate** to enter user credentials and authenticate the server details. Then save the server configuration on successful validation.

### **Display Last Logged In User**

Select this option to view Username of the user who was last logged into the Multi-User login screen.



The image shows a login screen for 42GEARS Mobility Systems. At the top is the logo. Below it, the text 'Login to access your profile' is displayed. There are two input fields: one for the username (containing 'one') and one for the password (containing 'Password'). A green 'LOGIN' button is centered below the fields. A link for 'Forgot Password?' is located below the button. At the bottom, it says 'Last Logged in User: two'.

## System Settings

The user can make changes in the system settings without exiting **SureLock** using **System Settings** option under **SureLock Admin Settings**.

## Setup SureLock Permissions

The admins can activate certain permissions anytime in **SureLock**. The following options are available under **Setup SureLock Permissions**:

- **Set SureLock as Default Launcher** - This option will set SureLock as default Home screen.



- **Activate Device Admin - SureLock** needs Android administrator permission for the advanced lockdown features such as

- **Disable Camera**
- **Disable Lock Screen**
- **Encrypt device**
- **Set Password Expiry**
- **Lock Device**
- **Set Password Restrictions**
- **Reset Device Password**
- **Monitor unauthorized Login**
- **Wipe Device**

Select this option to activate all the advanced lockdown features.

- **Enable Usage Access** - Select this option and then enable Usage Access for **SureLock**.  
The lockdown features of **SureLock** will not work until this option is enabled.
- **Install and Setup Enterprise Agent** - This option will download and install **Enterprise Agent** on the supported device.
- **Enable Samsung Knox** - Select this option to enable Samsung Knox features. This feature is available only for Samsung Knox devices.
- **Disable USB Debugging** - Select this option to restrict access to the device using Command prompt.
- **Disable Automatic Update From Play Store** - Select this option to stop auto-updating all the installed applications from Play Store.

## Import/Export Settings

**SureLock's** feature of **Import/ Export Settings** helps in making the gruesome task of configuring multiple devices with identical settings, quick and easy.

With the option of export or import settings using cloud/file/http, the user can mass configure the devices in almost quarter of the time, generally required. Configuring of multiple devices at a time with cloud option is achieved by just typing unique **Cloud ID** and tapping on **Import**.

### **Export Settings**

Admins can configure **SureLock** settings on multiple devices and export it to a File or Cloud.

#### **Export to File**

If the admins want to configure multiple devices with identical **SureLock Settings**, use **Export to File** option to export the settings to a file which can be imported into other devices for configuration using external storage device.

#### **Export to Cloud**

Select **Export to Cloud** option to export the settings to the Cloud, if admins don't want to save the exported settings to an external storage device.

To export the settings to cloud, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **SureLock Admin Settings** screen, tap **Import/Export Settings**.
3. On **Import/Export Settings** screen, tap **Export to Cloud**.
4. On **Export Settings To Cloud** screen, tap and select one of the following options:

**Export Settings To a New Cloud ID** - Export the **SureLock** settings to a new Cloud ID

**Use Existing Cloud ID** - Export the **SureLock** settings to an existing Cloud ID

**Export Settings to Cloud and generate QR Code** - Export the **SureLock** settings to the **Cloud** and generate **QR Code** and can save it to a file.

On successful export to the cloud, a **Cloud ID** is generated which can be referred while importing the settings.



**Note:** **Cloud ID** created will reflect in user **Cloud ID History** unless it is manually cleared.

## Import Settings

Admins can import the **SureLock** settings from File or Cloud.

### Import from File

Use **Import from File** option to import **SureLock Settings** from a file.

### Import from Cloud

To import settings from the cloud for multiple devices, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **SureLock Admin Settings** screen, tap **Import/Export Settings**.
3. On **Import/Export Settings** screen, tap **Import from Cloud**
5. Following are the options available in **Import Settings** screen,

**Import** - Enter the **Cloud ID** and tap **Import** or select the **Cloud ID** from the **History**

**Scan QR** - Tap **Scan QR** to scan the settings from other devices

**Show QR** - Display the **QR** code generated for the selected Cloud ID

**Clear History** - Clears all the Cloud histories that are created.

The admins will receive a confirmation on the import of **SureLock Settings**.



**Note:** Alternate option to Import the settings from **Cloud** and **QR Code** is available on the **SureLock**

**Home Screen.**

## Reset Settings

**Reset Settings** option will reset all settings in **SureLock** including **Allowed Applications** list.

### *Automatic Import*

Automatic Import option will import **SureLock Settings** automatically from a specified **File** or **Cloud ID**.

Automatic Import Cloud has the following options:

- **Enable Automatic Import** - Enables Automatic Import option from **File** or **Cloud**
- **Auto Import From** - This option will import **SureLock** settings from **File** or **Cloud ID**.
- **Periodically Check** - This option is to specify a time period for **SureLock** to check for new settings to import.

### *Schedule Automatic Import*

Admins can use **Schedule Automatic Import** to import new settings automatically within a specified period of time.

**Schedule Automatic Import** has the following options:

**Enable Scheduled Automatic Import** - Enables the Scheduled Automatic Import option

**Start At** - Set time to start scheduled import

**End At** - Set time to end scheduled import

### *Advanced Settings*

**Advanced Settings** has more advanced options on **Import / Export Settings**.

- **Export Activation Code** - While exporting the settings to the file, the activation code of the **SureLock** will be in the encrypted format.

- **Export Auto-Import Settings** - The settings file will have all the settings of **SureLock** except the **Import /Export** settings. Enable this option to include **Import/Export** settings in the settings file.
- **Force activate license on import settings** - While importing **SureLock** Settings in any device, the **SureLock** gets automatically activated in the specific device.
- **SureLock Settings Identifier** - Enter the name for the **Settings Identifier** for the **SureLock** settings. The admins can identify the applied **SureLock** Settings with the **SureLock Settings Identifier** on **SureMDM** console.
- **Export Permissions Check List Status** - On selecting this option, while importing **SureLock** permissions on multiple devices, a force prompt of permissions checklist appears for the admins to select appropriately.

## Remotely Configure SureLock Settings

Admins can remotely manage the **SureLock** applications through **SureMDM** Console. If **SureMDM** is not installed in the device, it will enable Integrated Nix Agent on tapping **Remotely Configure SureLock Settings**.

## Exit SureLock

This option will logout from **SureLock**.

To exit from **SureLock**, follow these steps:

1. Access [SureLock Admin Settings](#).
2. On **SureLock Admin Settings** screen, tap **Exit SureLock**.
3. Tap **Exit** to complete.

On successful exit of **SureLock**, the home screen of the device will be visible.

## Uninstall SureLock

Select **Uninstall SureLock** to uninstall **SureLock** and its settings permanently from the device.



**Note:** While uninstalling SureLock, current system settings of the device will not be altered.

## About SureLock

**About SureLock** provides **General, Device, License** and **Diagnostics** information of the SureLock Application.

- **About SureLock** has following details:
- **SureLock Version** - Displays SureLock version installed
- **Activate** - Option to activate SureLock
- **Buy Now** - Option to buy the product from **google in-app purchase**
- **Free Upgrade available till** - Displays the date till which user will receive free upgrades
- **IMEI 1 /IMEI 2** - Unique preferred activation IDs of the device
- **IMSI** - Unique number to identify user of a cellular network
- **MAC (WiFi)** - a unique identifier assigned to network interfaces for communications on the physical network segment
- **MAC (Bluetooth)** - a unique identifier assigned to network interfaces for communications on the physical network segment
- **GUID** - Unique reference number used as an identifier in computer software
- **Android ID** - a unique alphanumeric code, specifically used for identification purpose.
- **Serial Number** – a unique alphanumeric code that is given by manufacturer
- **Preferred Activation ID** - Option to specify ID used for activation

- **Deactivate** - Option to deactivate SureLock
- **Export Log Files to Cloud** - Use this feature to export SureLock's Device Logs, Settings File, and Diagnostic Logs to Cloud. Once the user exports the log files to Cloud will get a Cloud ID which can be shared. Using this Cloud ID, the log file can be accessed anytime, anywhere.
- **Documentation** – Option to link the [online help](#) documentation of SureLock



**Note:** Admins can also activate the licenses using IMEI1, IMEI2, Serial Number and Android ID.