Lenovo

ThinkShield

ThinkShield Edge Mobile Management

Mobile Application User Guide

December 2019

Table of Contents

ThinkShield Edge Mobile Management Application Overview

Lenovo ThinkSystem SE350 Edge server (hereinafter Device) is supplied to customers in locked state for security reasons. ThinkShield mobile application provides a configuration utility for SE350 service Ethernet port.

The application provides clear instruction for the end user as to how to connect the device and activate it.

The application also provides the opportunity to read Activation Code from the Device, change its network settings, view and update user's personal data and receive additional information on support page.
A user with Service User role can also view and update Public Key.

The application is available **worldwide**.

ThinkShield Edge Mobile Mgmt for iOS (available **worldwide**).

Mobile Platform: native iOS and Android application.

Supported devices:

- Android supported devices: Android mobile devices with OS 5.0 - 9.0, hdpi screens full support, xhdpi, xxhdpi, xxxhdpi partial support (adaptive layout); portrait screen orientation.
- iOS supported devices: all officially supported iPhone with iOS 12.x and 13; portrait screen orientation.

Supported languages:

- English
- Brazilian Portuguese
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean
- French
- German
- Italian
- Spanish
- Russian
- Thai

Roles vs Capabilities

Roles for users of the ThinkShield Edge Mobile Management Application are assigned within the ThinkShield Key Vault Portal by the Organization Admin(s).

Roles → Function ⋁	No credentials	Has a Lenovo ID	Base User	Edge User	Maintenance User	Org Admin
Can Login to ThinkShield Edge Mobile Management App			x	x	x	x
Mobile Profile			x	x	x	x
Logout			x	x	x	x
Access to an Organization			x	x	x	x
View device lockdown status			x	x	x	x
Show Activation Code	x	x	x	x	x	x
View Mobile Support	x	x	x	x	x	x
Activate Device				**x**	**x**	**x**
Update Key					**x**	
Network Configuration				**x**		**x**
Device Management						**x**
Transfer Devices (Group)						x
Activate System Lockdown Mode						x
Re-sync				x	x	x

Capabilities

The following features are available based on Role vs Capabilities:

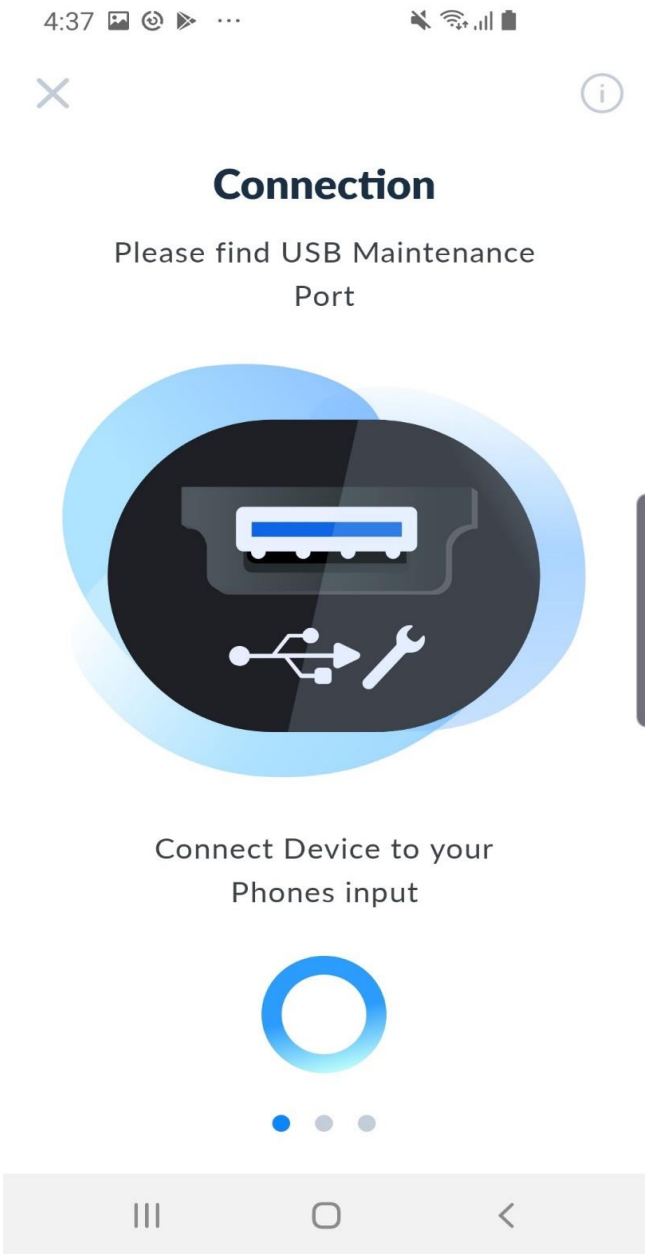
1. Show Activation Code (used for retrieving Secure Activation Code)
2. Device Activation/ Re-activation
3. Network Configuration
4. Re-sync
5. View Mobile Support
6. View and Update Mobile Profile
7. Logout
8. View device lockdown status
9. Update Key
10. Transfer Devices (Group)
11. Activate System Lockdown Mode

Connection to Device

In order to interact with the Device you must go through Connection to Device steps.

Plug USB cable into Maintenance Port of the Device. Then connect the Device to your Phones input.

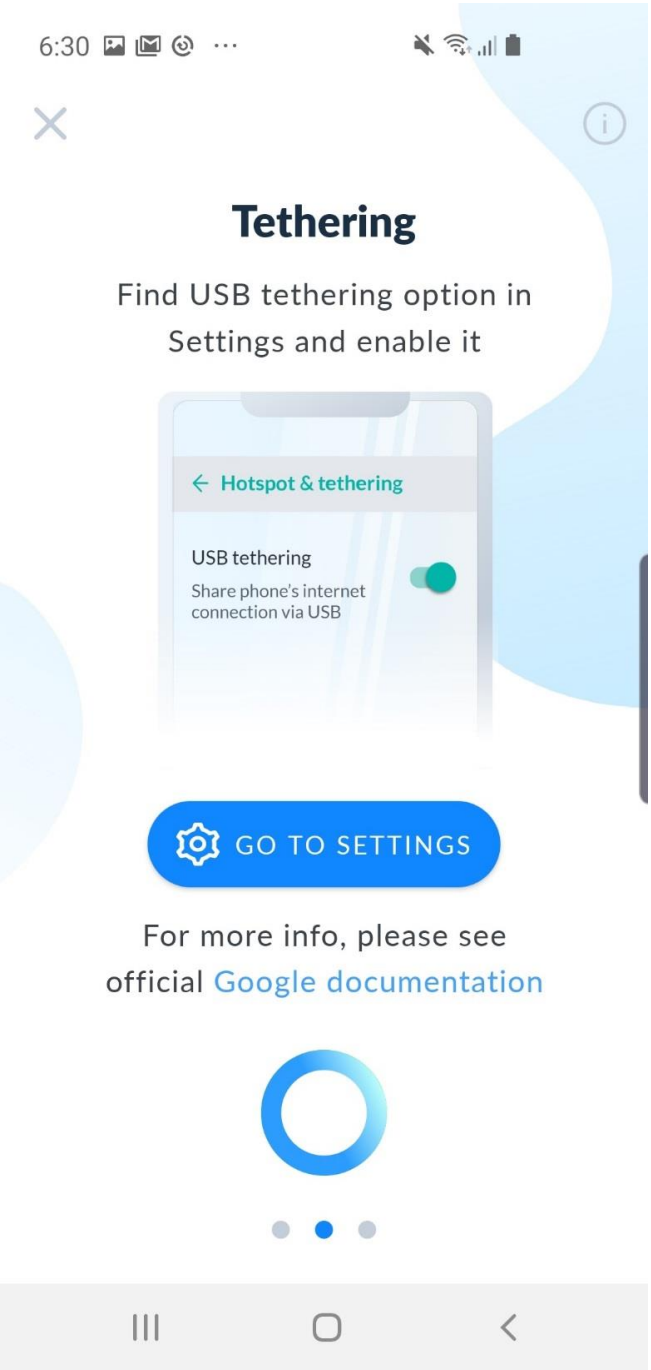
Note: The spinning cycle shows the connection progress. As soon as the step is executed user is redirected to the next screen automatically. If the connection fails, user gets an error message "Connection failed" and "Retry" button appears on the screen.



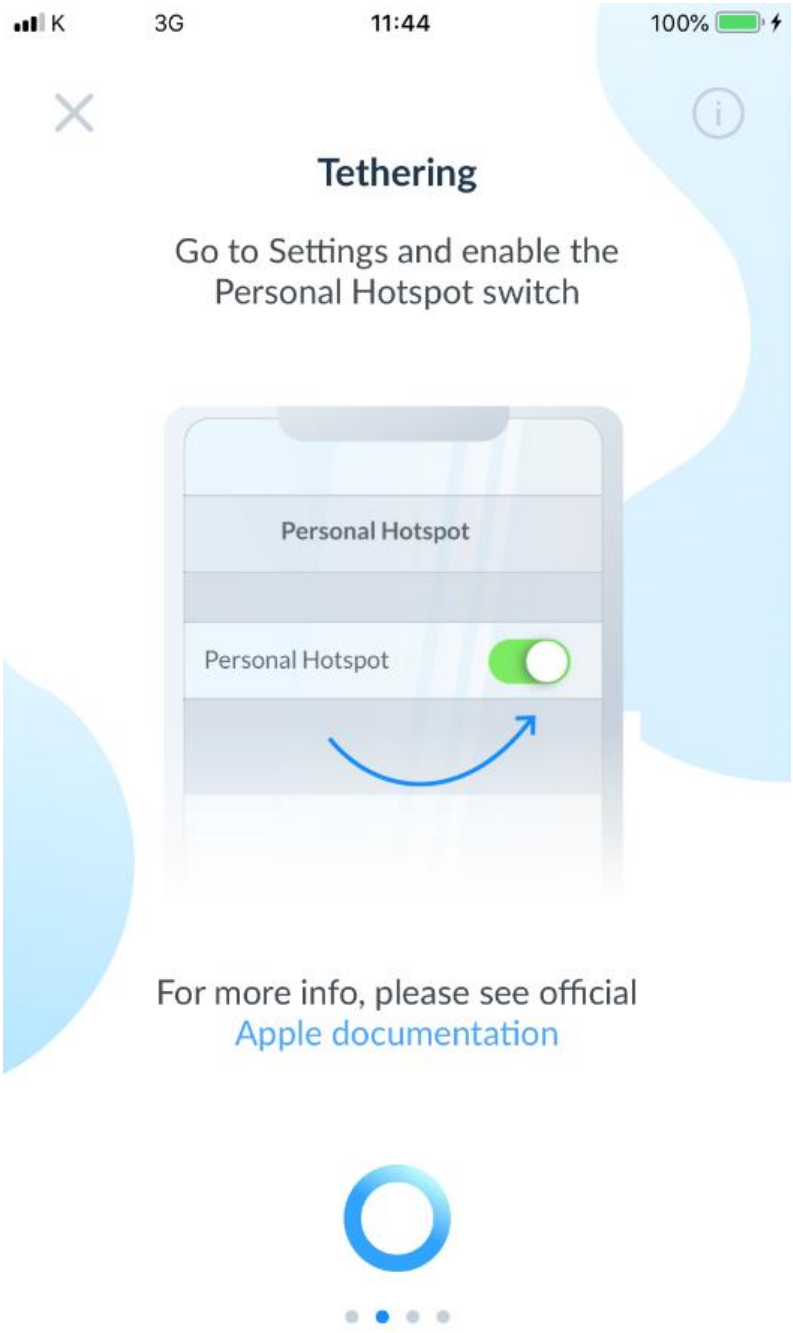
Make sure you select ‘Trust’ on ‘Trust This Computer’ pop-up after the cable was plugged in, you may be requested to enter your devices pin code if pin enabled.

Enable Tethering on your phone.

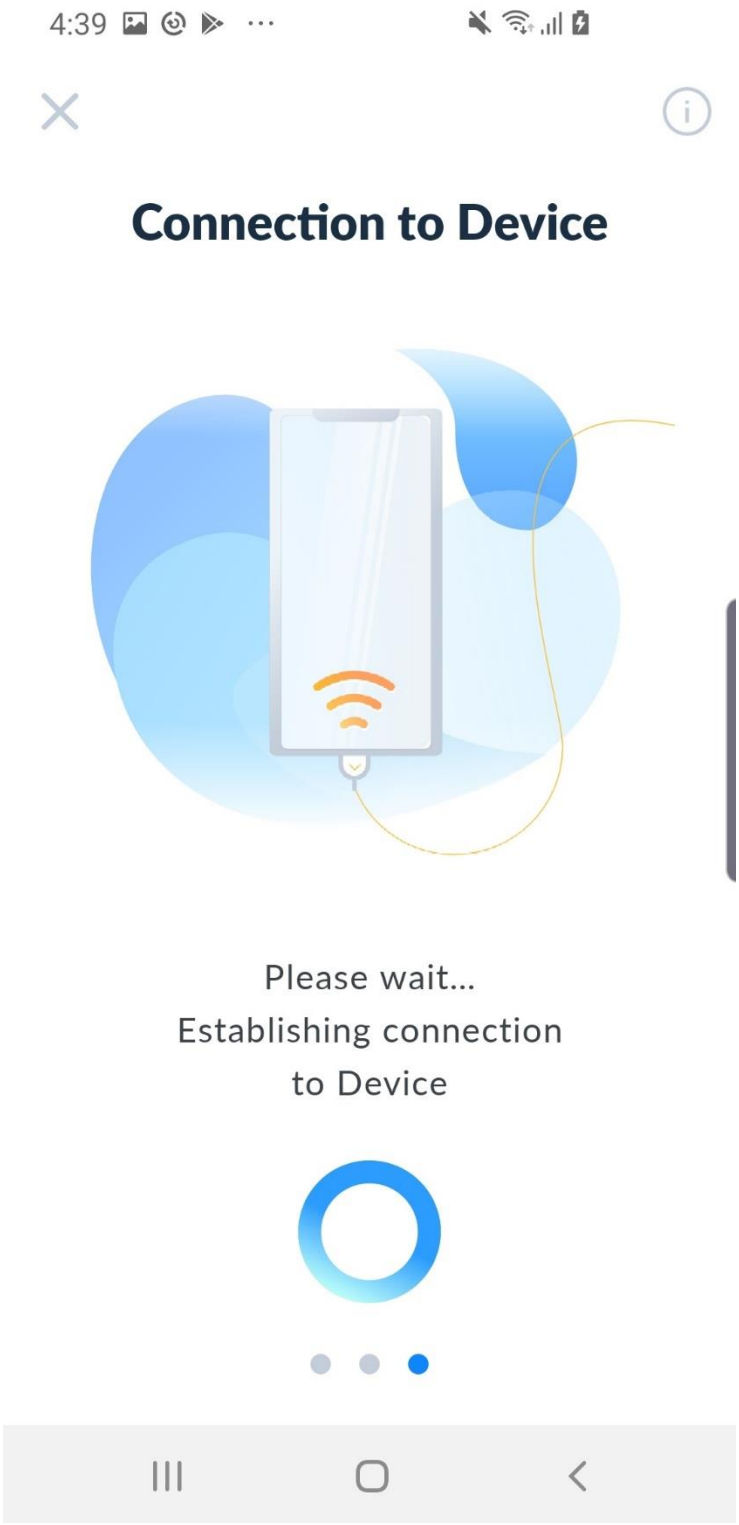
Android Tethering Screen: there is a direct link to Settings screen where tethering can be enabled. Information regarding tethering option can be found at https://support.google.com/android/answer/9059108?hl=en



iOS Personal Hotspot: there is NO direct link to Settings screen where tethering can be enabled due to platform constrains.
Information regarding tethering option can be found at https://support.apple.com/en-us/HT204023



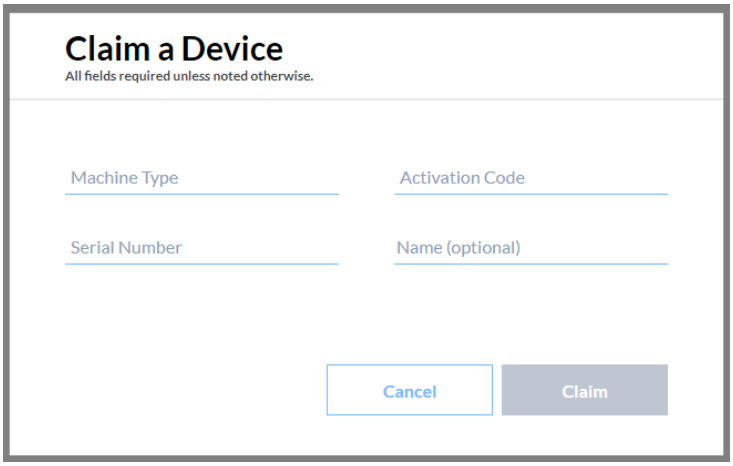
Wait until connection to the Device establishes.



Show Activation Code

The SE350 secure activation code is used to claim a device prior to activation within the ThinkShield Key Vault Portal (hereinafter Portal). The secure activation code is printed on in-packaging materials, but you can also retrieve it from the ThinkShield Edge Mobile Management mobile application. The secure activation code retrieved by the mobile application may not match the code printed on in-packaging materials. Both codes are valid for system claiming.

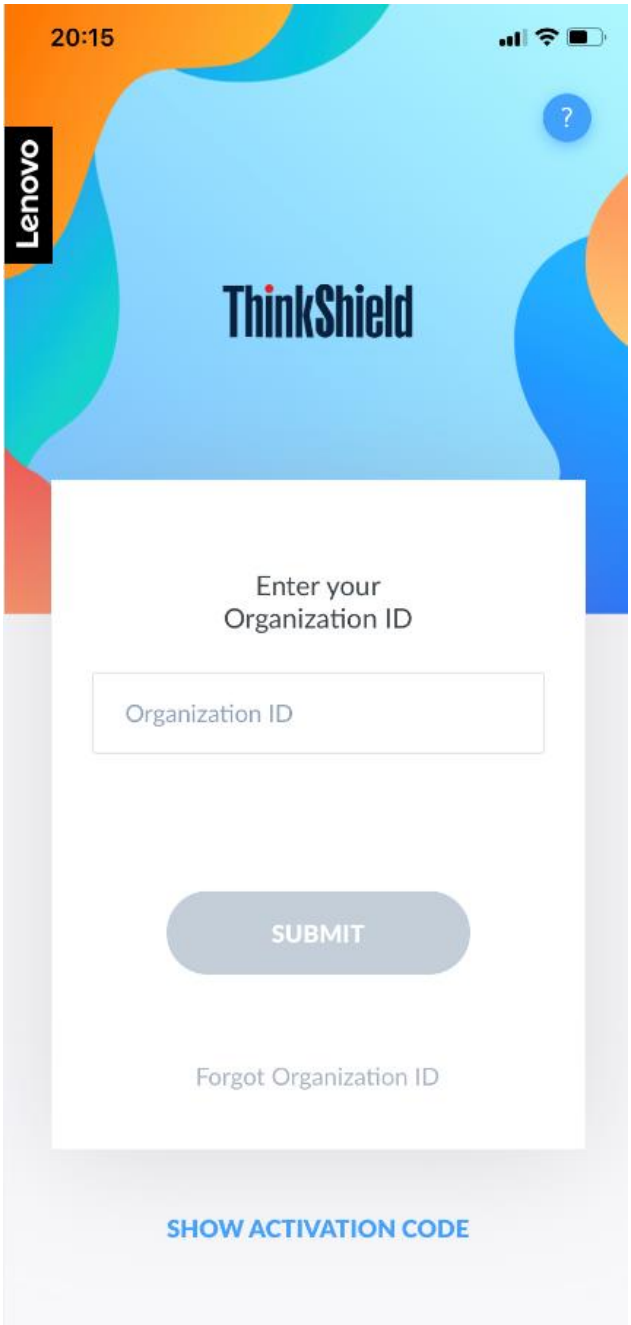
***Note**: The claiming process associates your device with you and your organization. This code is used during claiming process within your devices page on the web portal here:*



Show Activation Code Flow

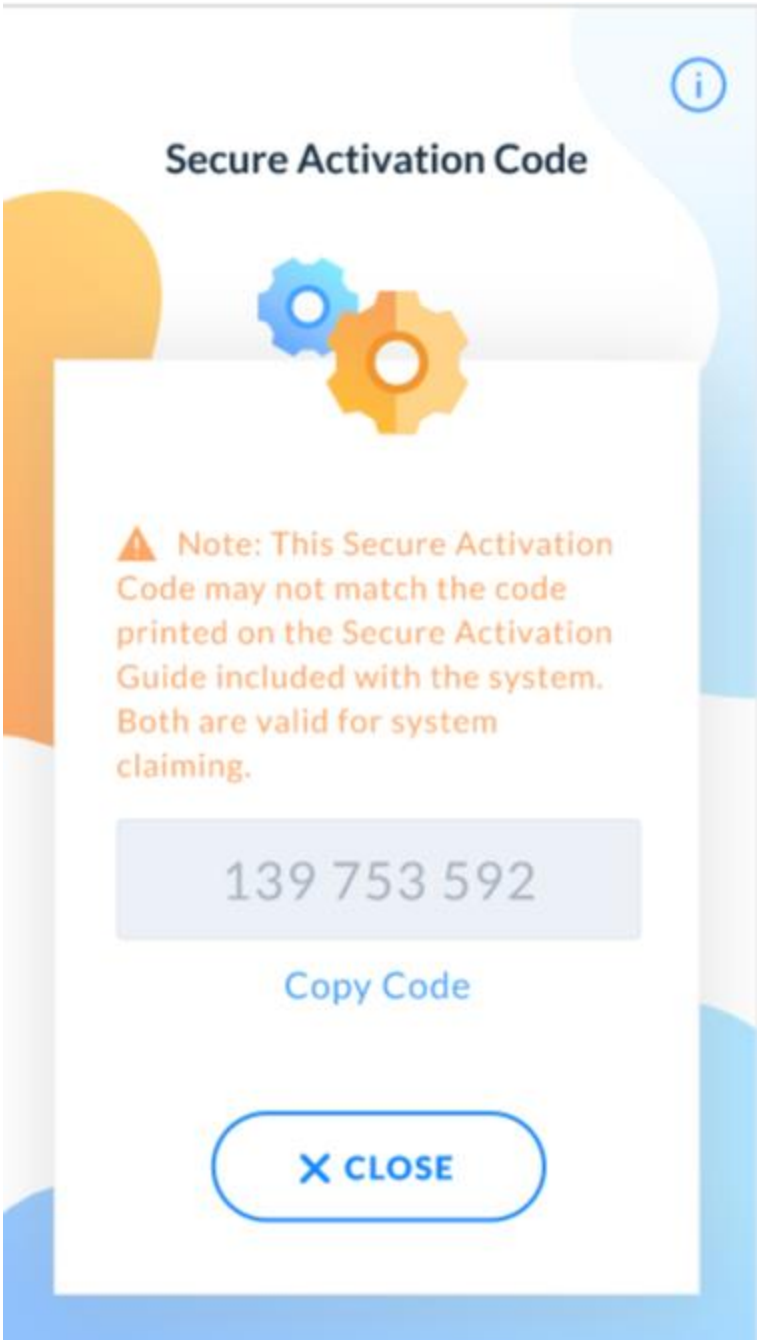
Tap on ‘SHOW ACTIVATION CODE’ at the bottom of the screen. If needed go through connection to Device steps (see Connection to Device for details).

Note, you do not need to log in in order to retrieve Activation Code.



Check Security Activation Code on the screen.

Note: Activation Code is unique for each Device.

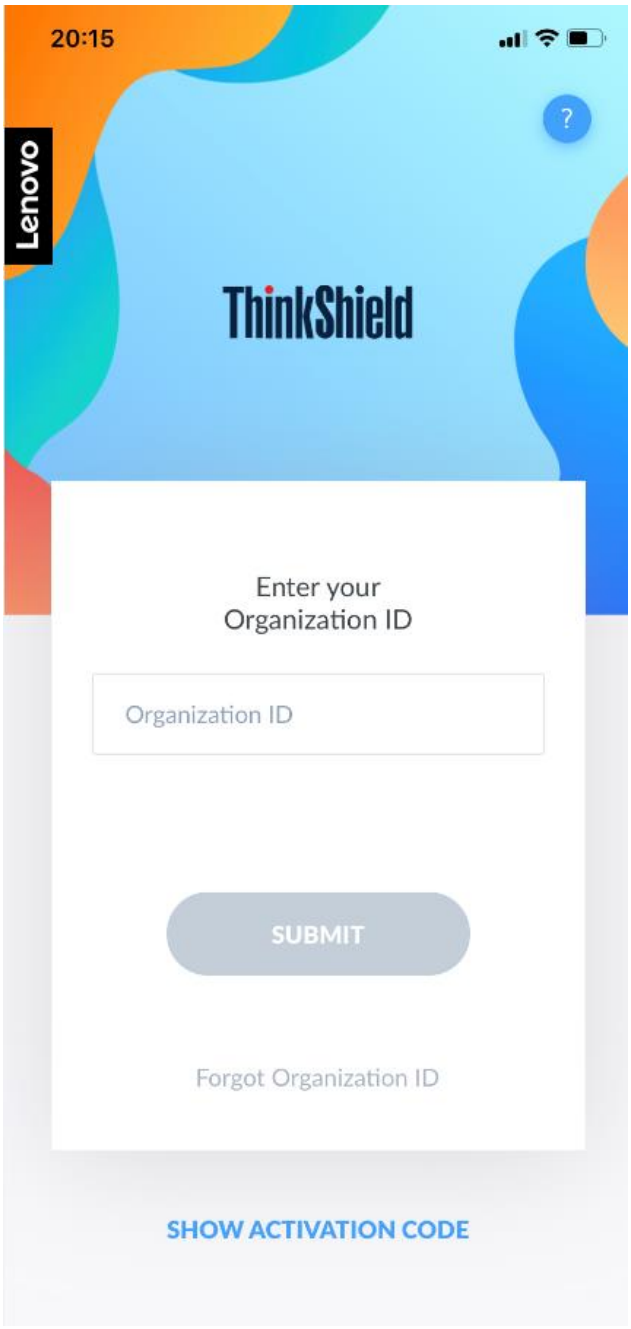


Device Activation/Re-activation Flow

Securely activating a device from the mobile application will claim your device to your organization within the Portal and allow your device to boot from its locked factory state. Follow the on-screen steps to proceed with activation. If SE350 device is locked due to tamper event, please follow these steps again for reactivation.

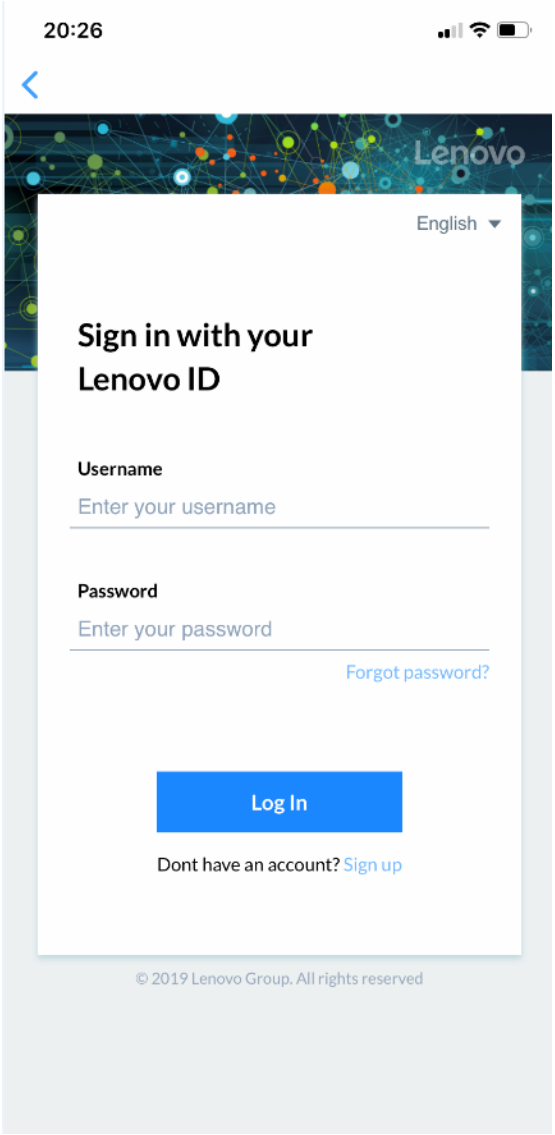
Please note, that only logged in user can perform Device Activation.

Provide your Organization ID into ‘Organization ID’ field and tap on ‘SUBMIT’ button.

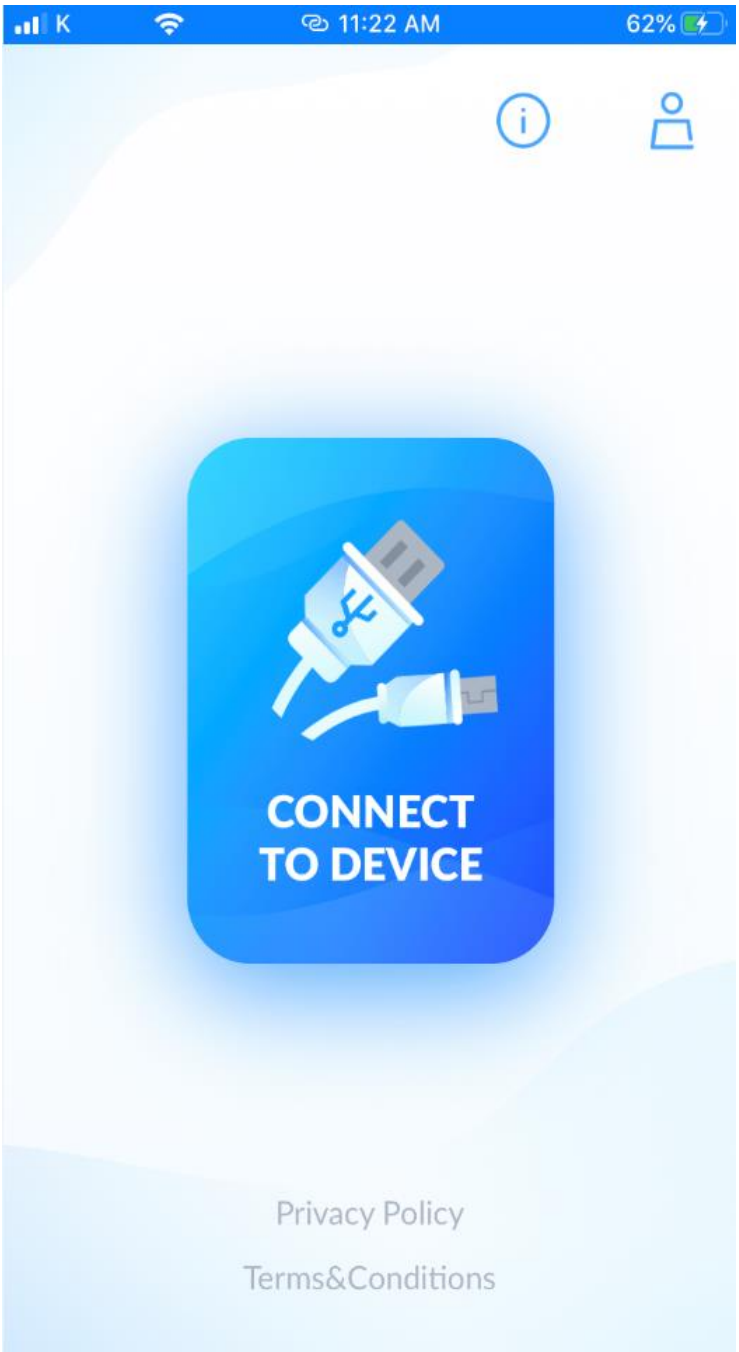


Provide your Lenovo ID or Active Directory credentials and tap on ‘Log In’ button.

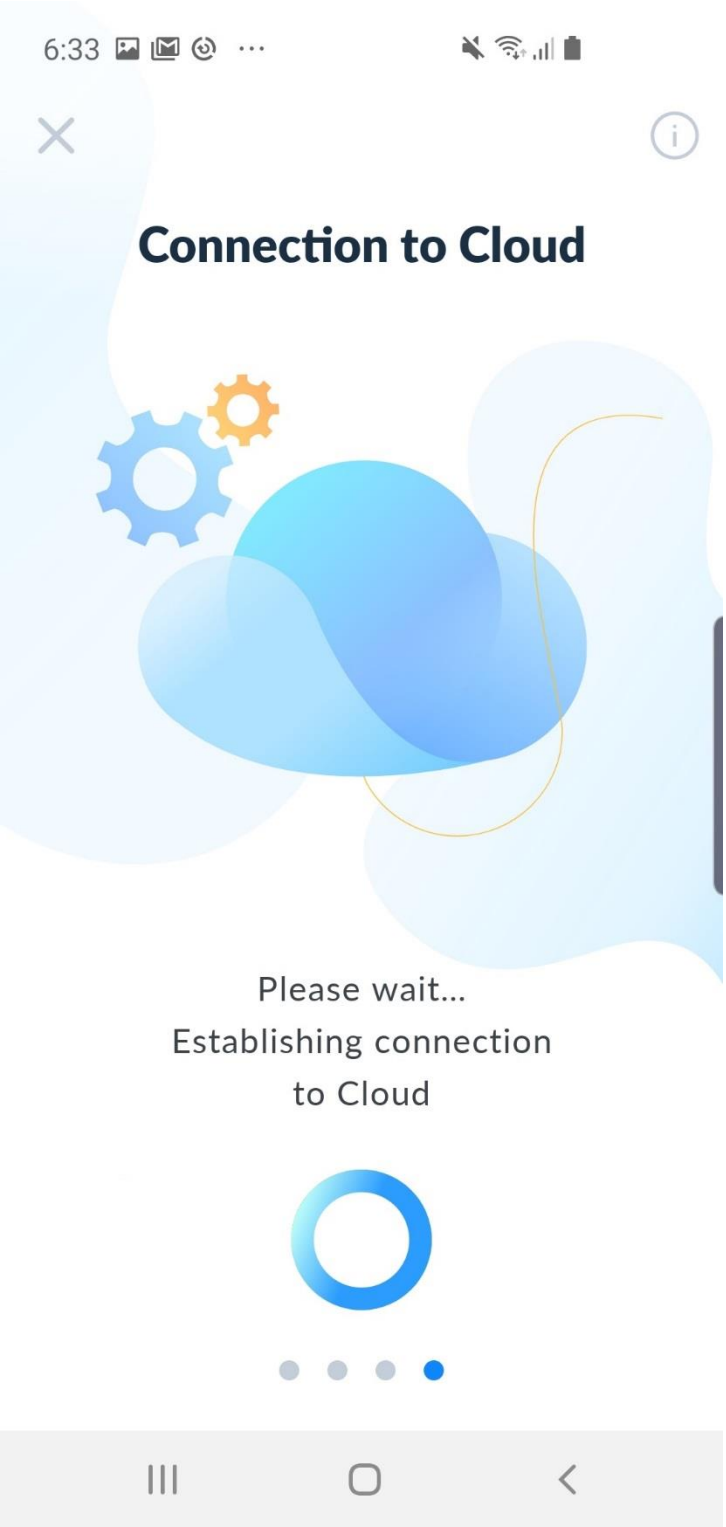
Note: In case you provide Active Directory credentials, you will be redirected to your service provider website to log in.



Tap on ‘Connect to Device’ on Landing screen. If needed go through connection to Device steps (see Connection to Device for details).

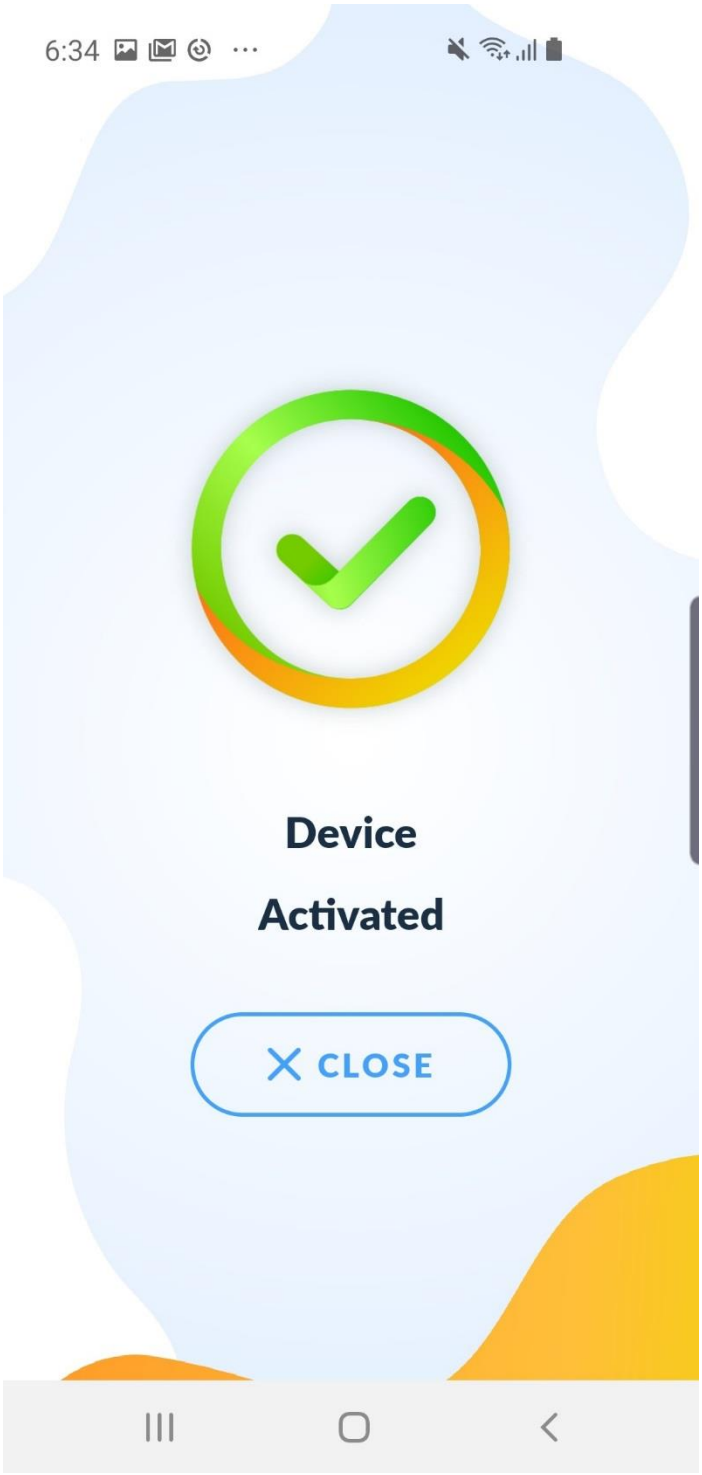


As soon as the connection is established the Device will be connecting to the Cloud. Wait until this connection establishes.



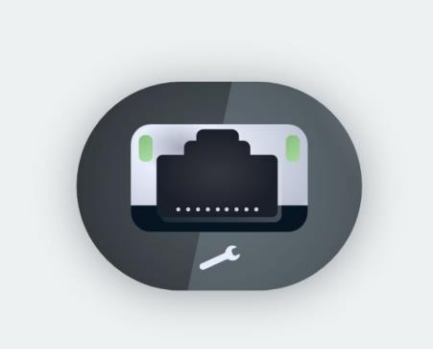
When the connection is established, click ‘Activate Device’ on Menu screen.

‘Device Activated’ message will be shown if the Device was successfully activated.



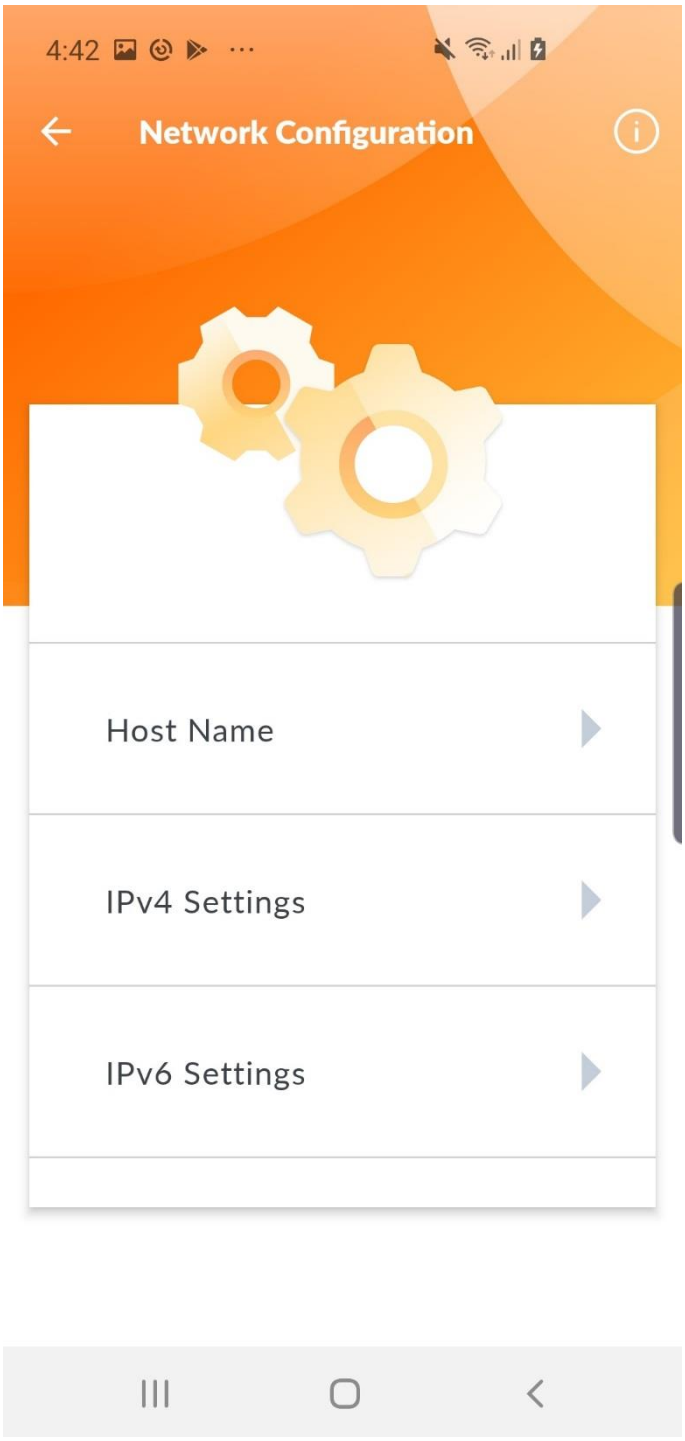
Network Configuration

The network configuration tool allows for configuration of XClarity management networking ports. These ports can be identified by the following logo on the device.

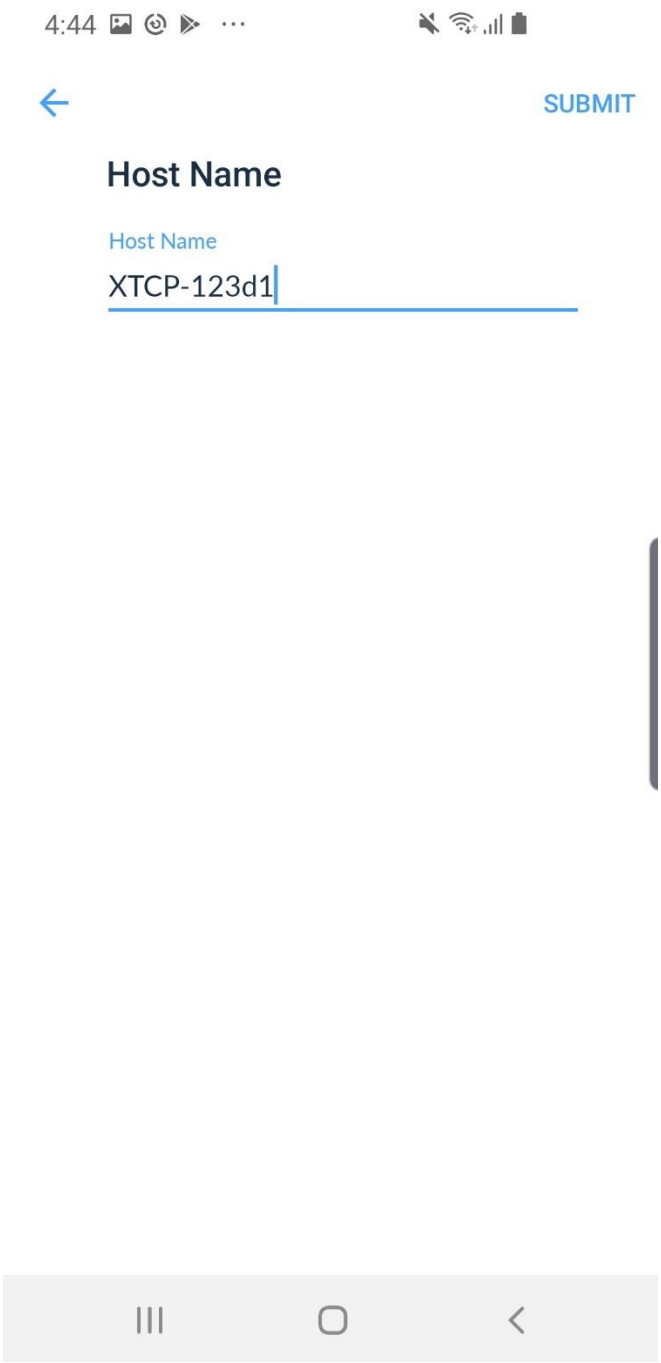


Tap on ‘Network Configuration’ on Menu screen, if needed Connect the Device to the Phone (see Connection to Device for details).

Tap on the item that needs to be modified.



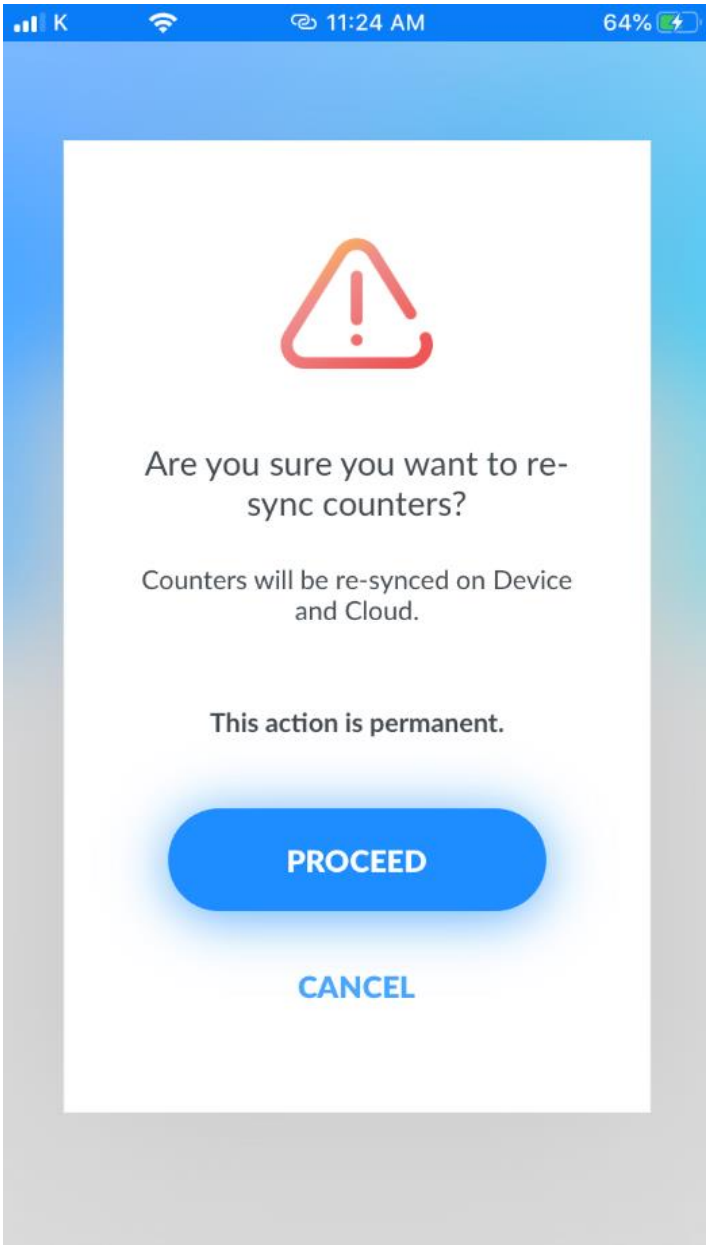
‘Submit’ button becomes active as soon as any changes are done on the screen (i.e. User changes Host Name). Tap on ‘Submit’ after providing necessary data and it is sent to the Device, you will be notified with a pop-up message (at the bottom of the screen) whether submission was successful or not.



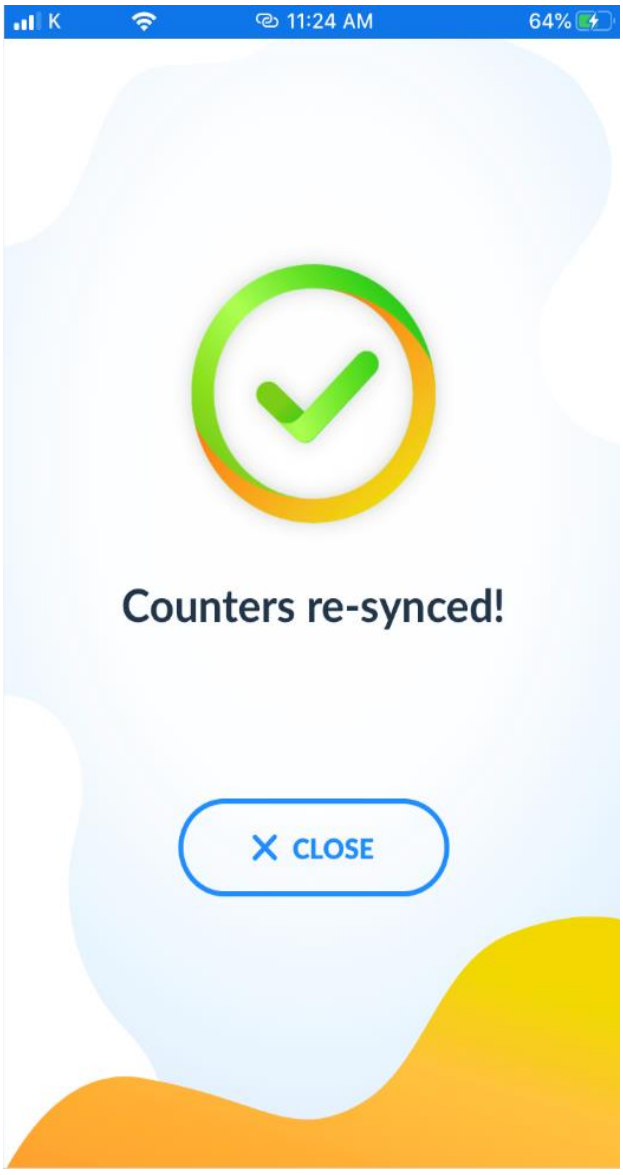
Re-sync

To reset the counters on a Device, click ‘Re-sync’ on Menu screen.

Confirm the action by clicking ‘Proceed’ on the pop-up window.



‘Counters re-synced’ message will be shown if the counters on Device and Cloud were successfully re-synced.

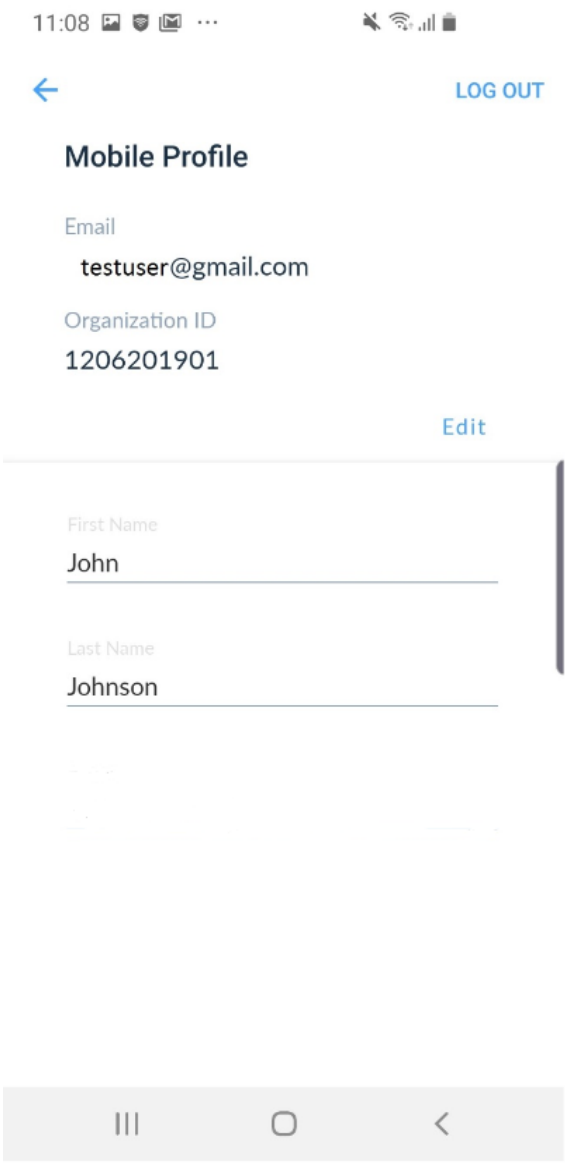


Mobile Profile

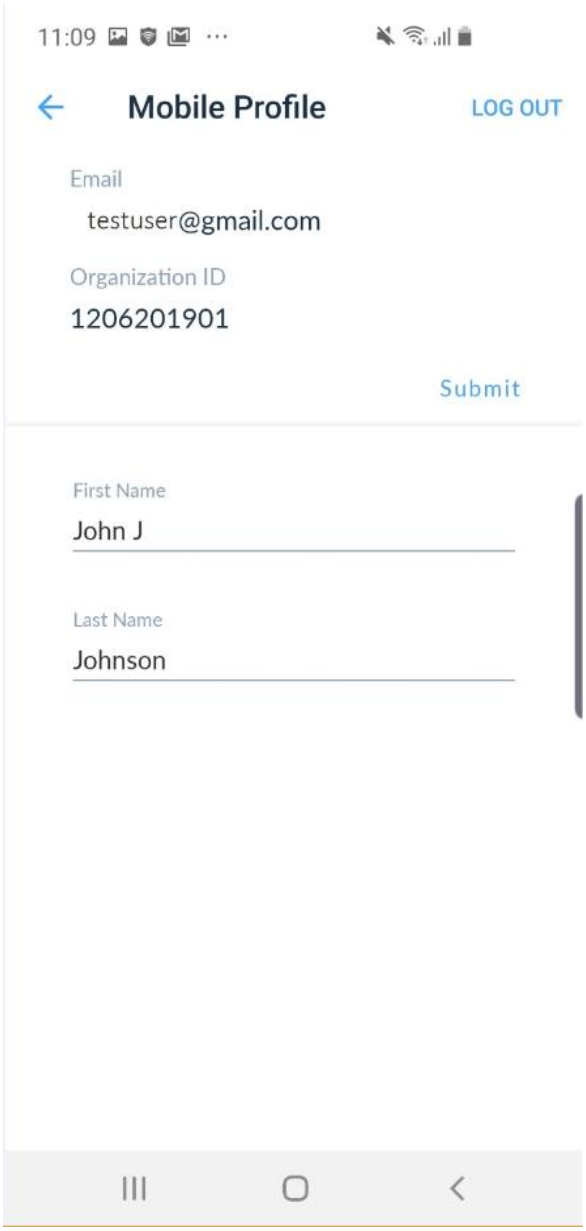
Edge User can view and update their personal information. The information is read from the Portal.

Tap on ‘Edit’ to change information.

Note that Email and Organization ID are not editable fields.

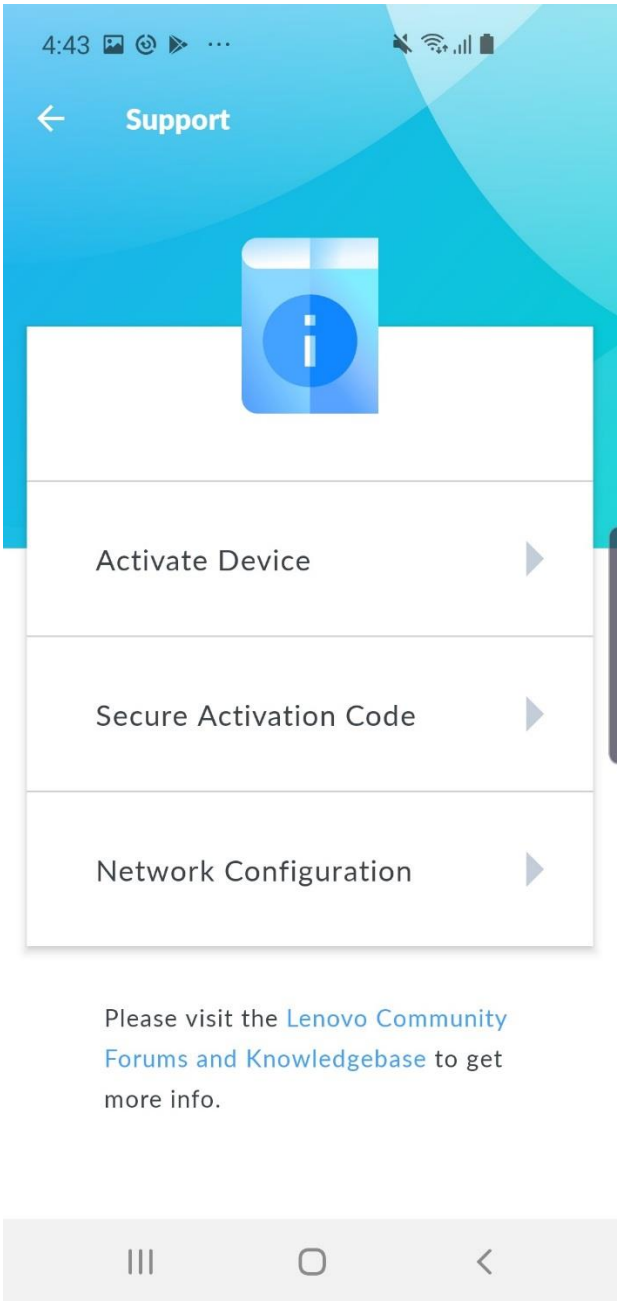


Tap on ‘Submit’ after necessary changes were provided. Data will be sent to the Portal. You will be notified with a pop-up message (at the bottom of the screen) whether submission was successful or not.



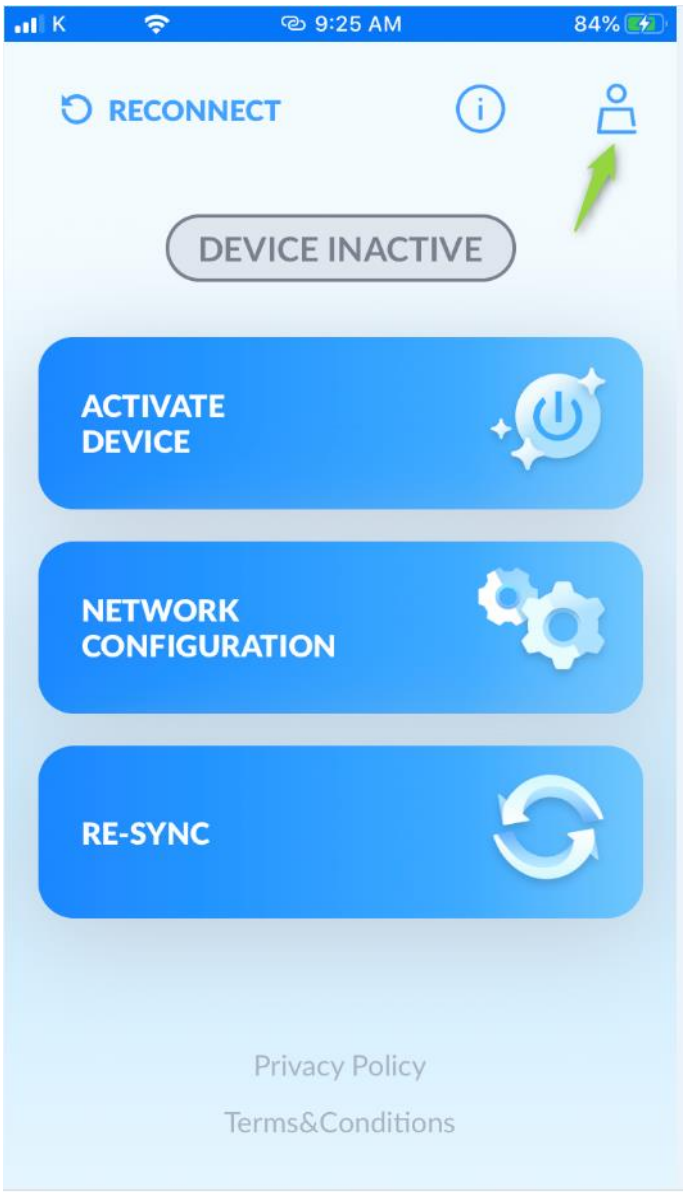
View Mobile Support

Mobile Support is intended to provide additional information. Tap on the issue you want to get additional information about. If more information is needed tap on ‘Lenovo Community Forums and Knowledge’ at the bottom of the screen.

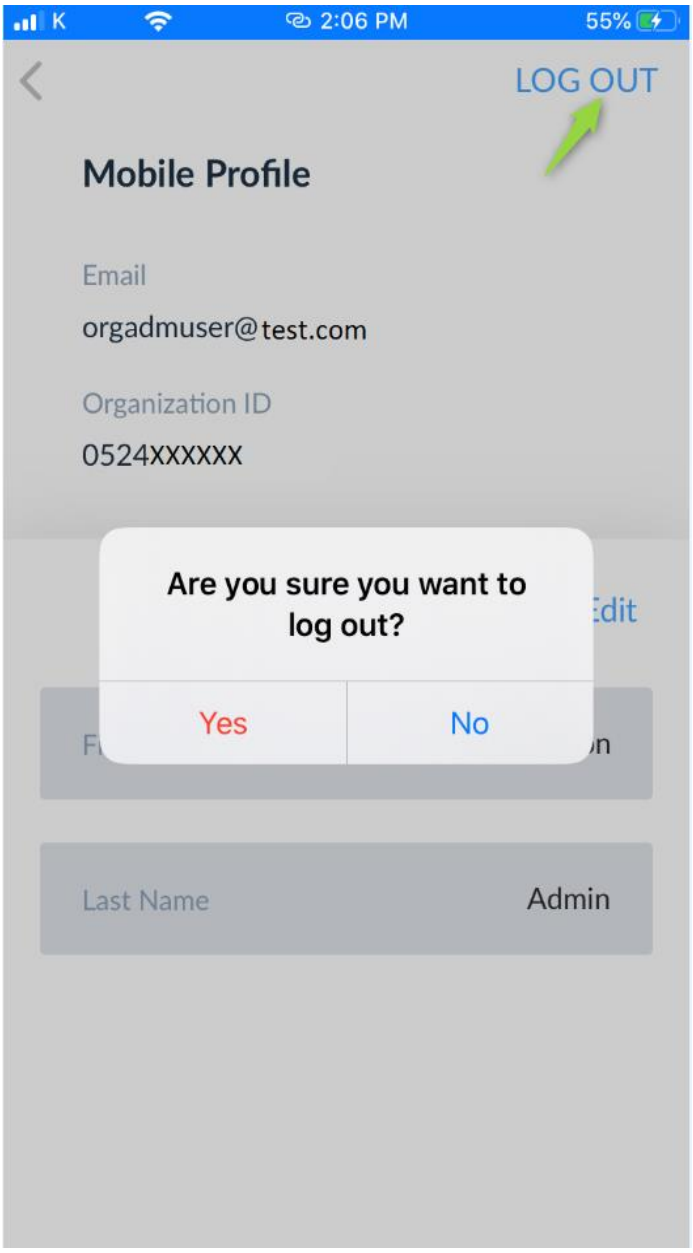


Logout

Tap on the ‘User’ icon in the right upper corner of the screen.



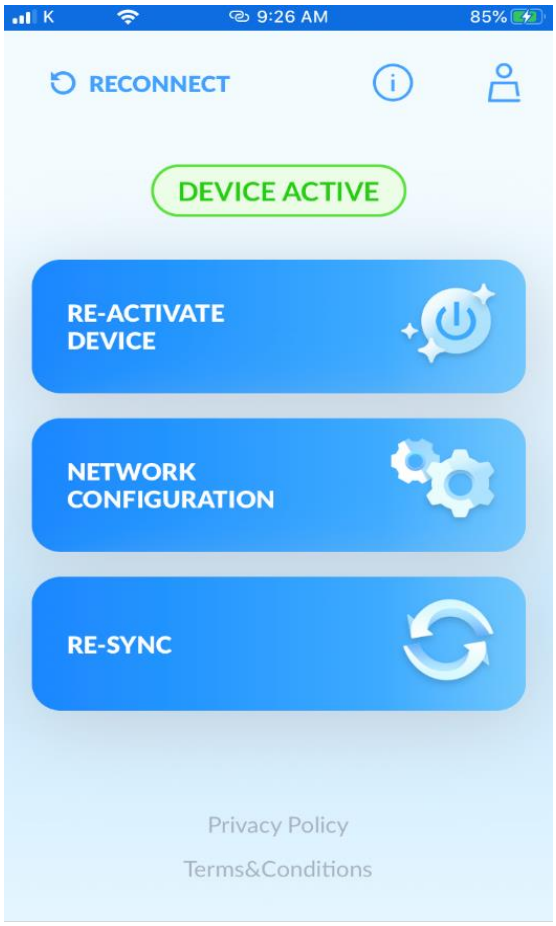
On ‘Mobile Profile’ screen tap on ‘Log Out’ and confirm the action by clicking ‘Yes’ on the pop-up window.



View Device Lockdown Status

Tap on ‘Connect to Device’ on Landing screen. If needed go through connection to Device steps (see Connection to Device for details).

The status of the Device is displayed on Menu screen. ‘Active’ status shows that a Device is active. ‘Inactive’ status shows that a Device is asserted to Lockdown Mode.



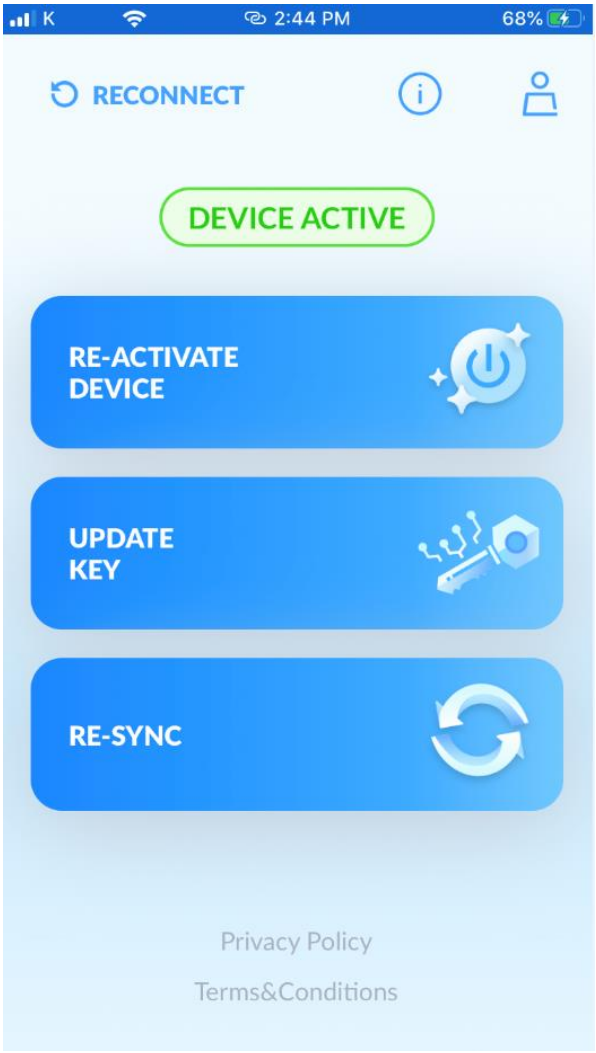
Update Key

The mobile application provides the opportunity to Maintenance User to update Public Key in case a system board of a Device has been replaced or exchanged.

In case of exchange of system board on failure, the new system board part will be programmed from the factory with new public / private key information, however at time of install to the existing machine it needs to be associated with existing device Machine Type and Serial Number.

Tap on 'Connect to Device' on Landing screen. If needed go through connection to Device steps (see Connection to Device for details).

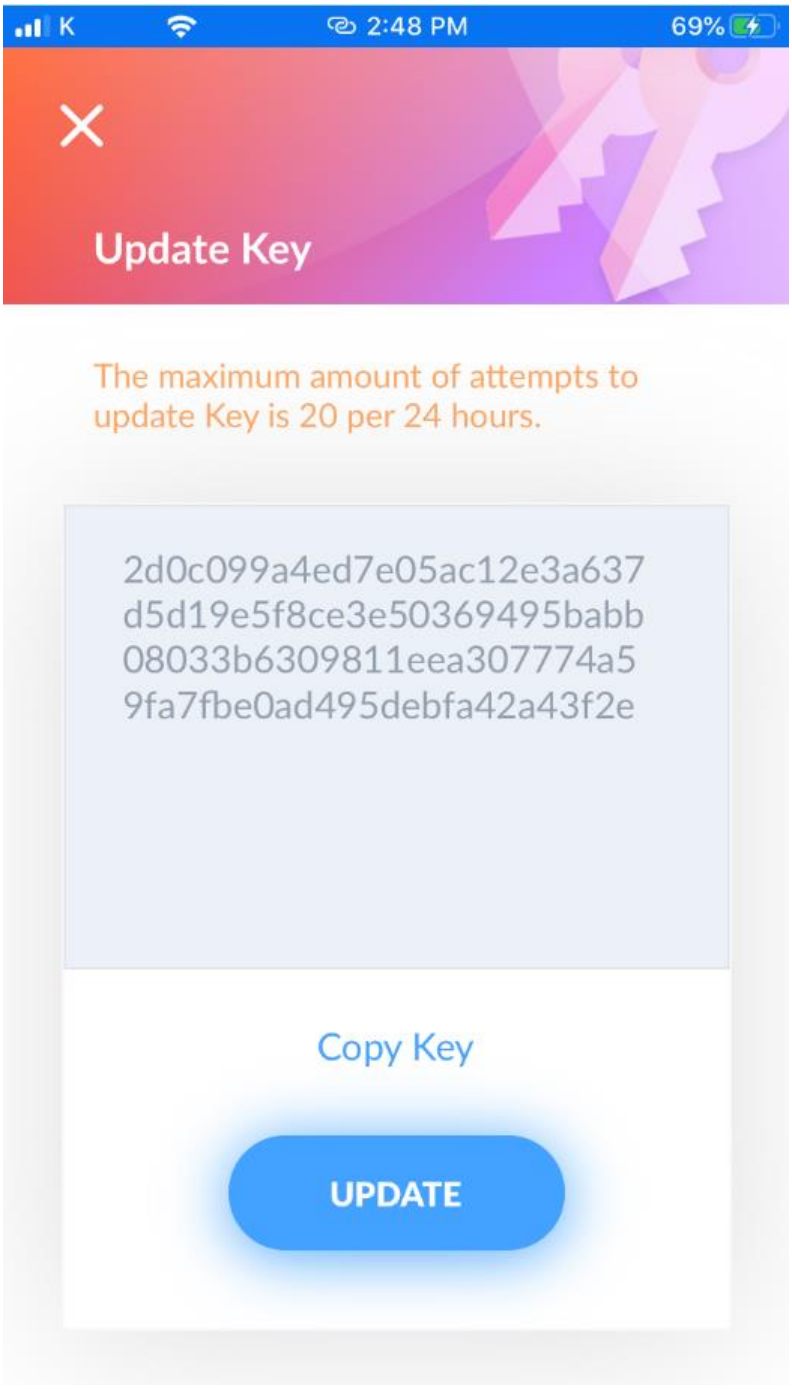
Tap on 'Update Key' on Menu screen.



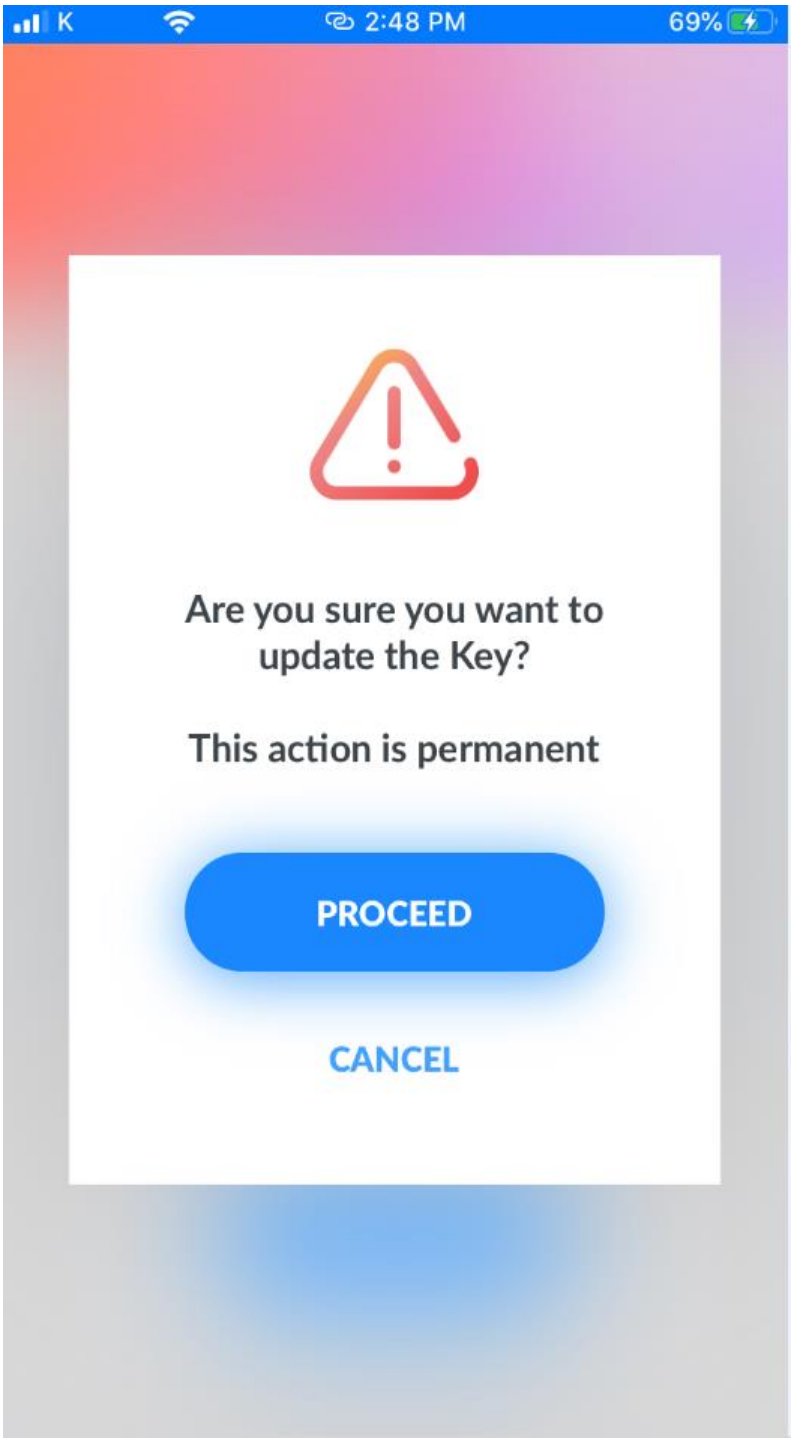
Tap on ‘Update’ on Update Key screen.

Note: The maximum amount of attempts to update Key is 20 per 24 hours.

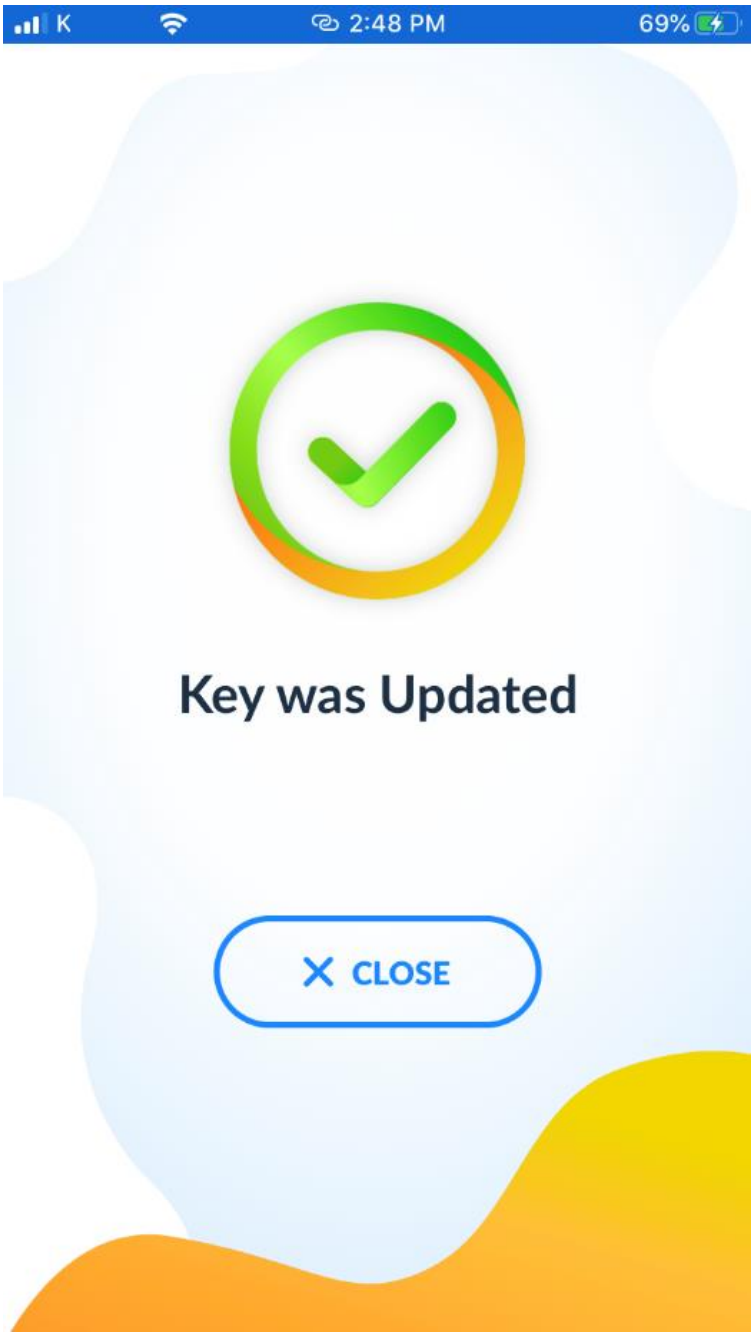
Tap on ‘Copy Key’ to copy the key to the clipboard.



Confirm the action by clicking ‘Procced’ on ‘Are you sure…?’ pop-up window.



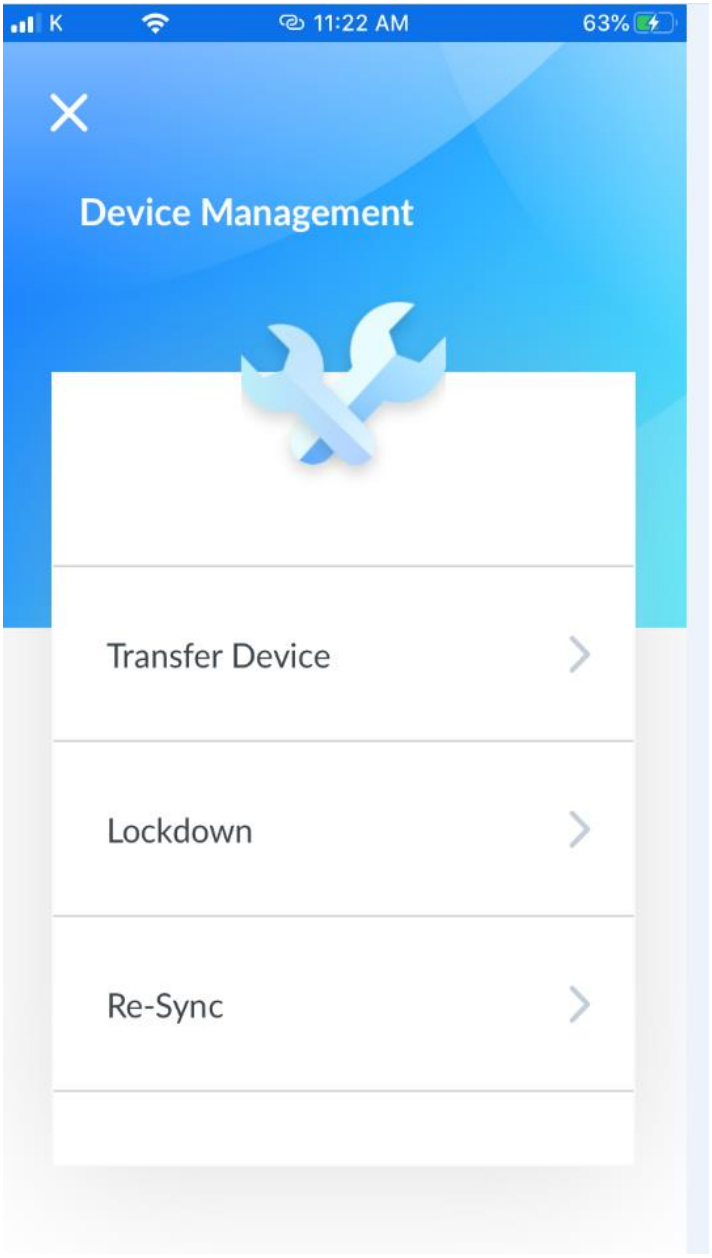
The Key is successfully updated. Tap on ‘Close’ to return to Menu screen.



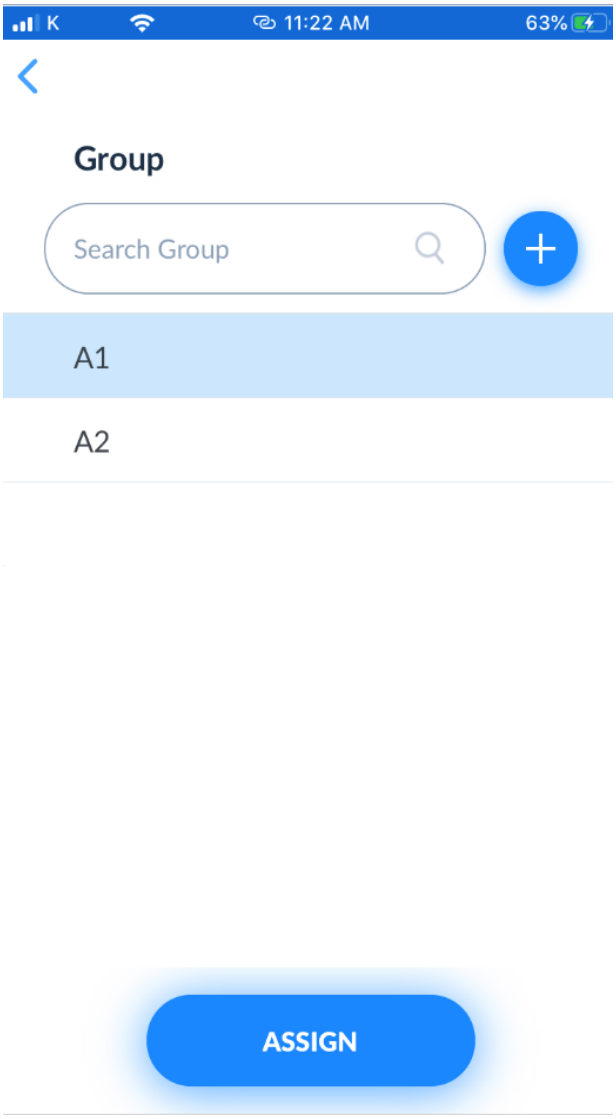
Transfer Devices (Group)

Tap on ‘Connect to Device’ on Landing screen. If needed go through connection to Device steps (see Connection to Device for details).

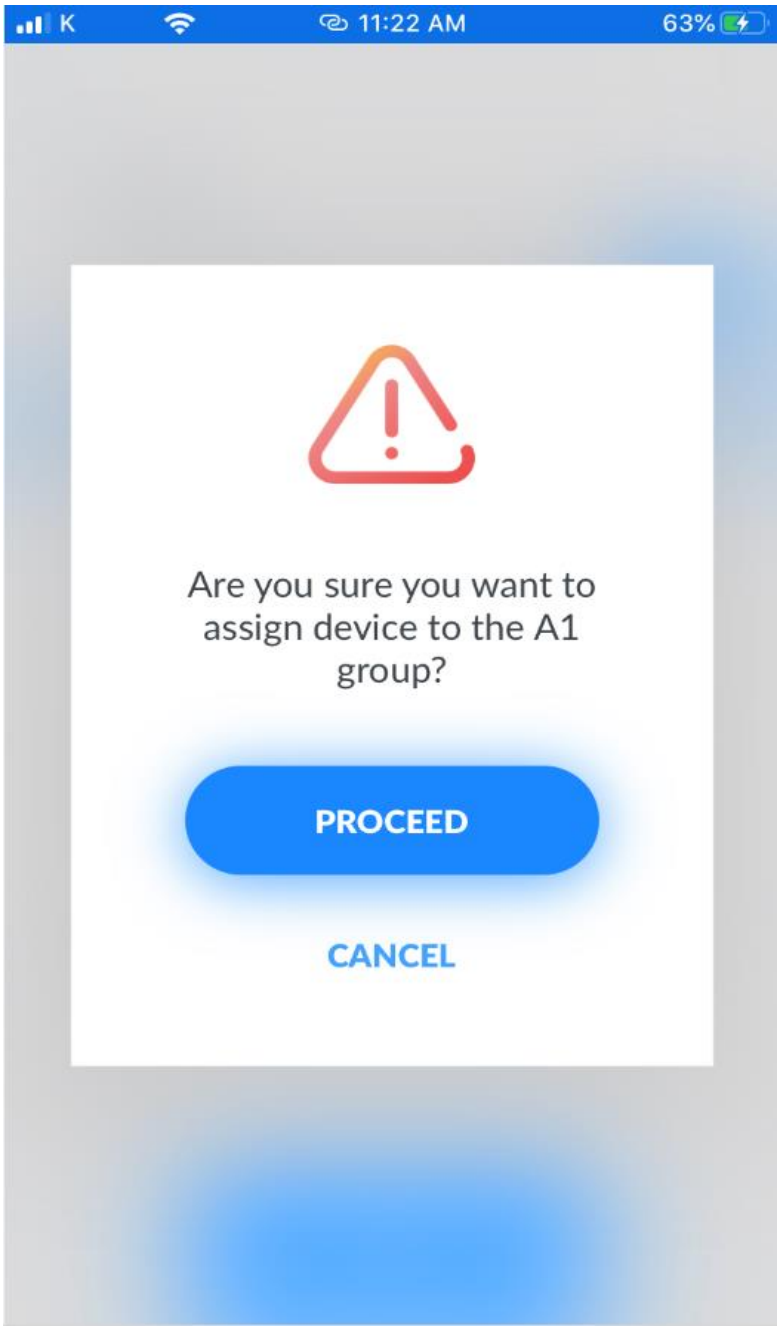
Tap on ‘Transfer Device’ on ‘Device Management’ tab.



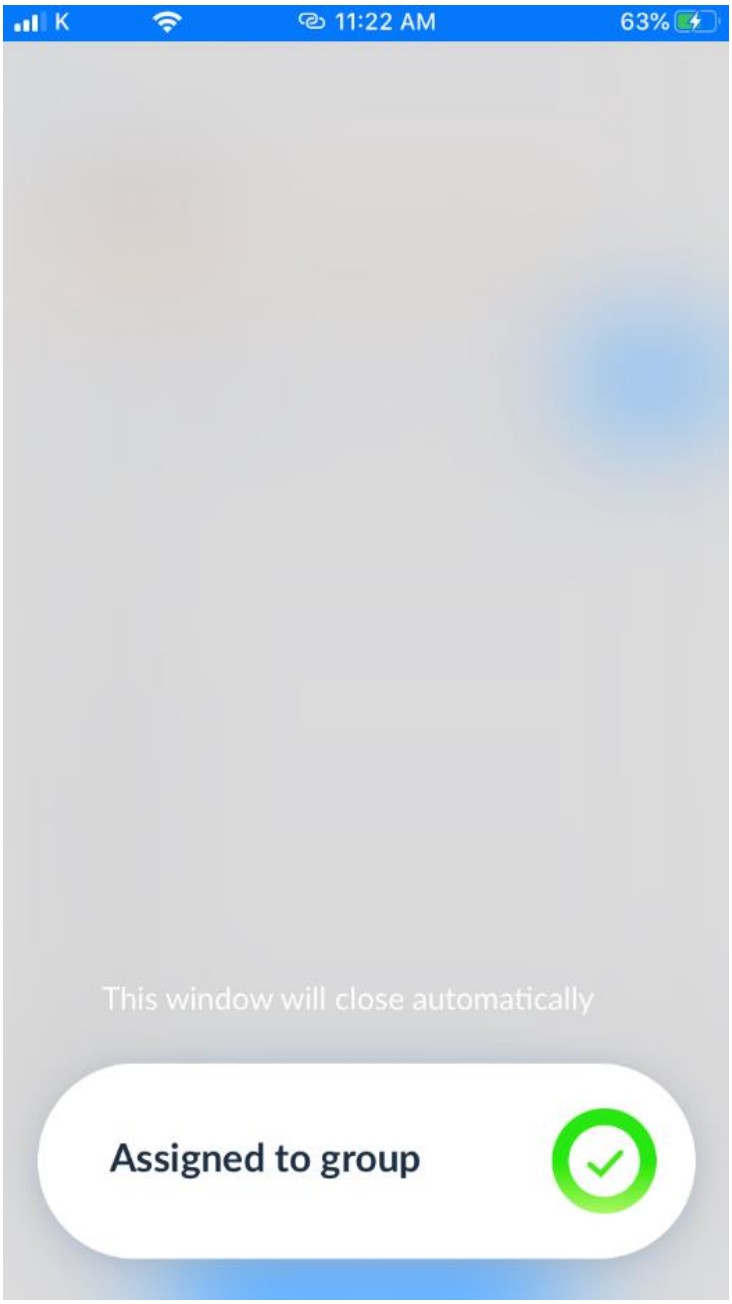
In order to assign a Device to a Group select a Group you want to assign a Device to and tap on ‘Assign’. To find a Group in the list start typing the name of the Group into the Search field and tap on ‘Magnifying glass’ icon.



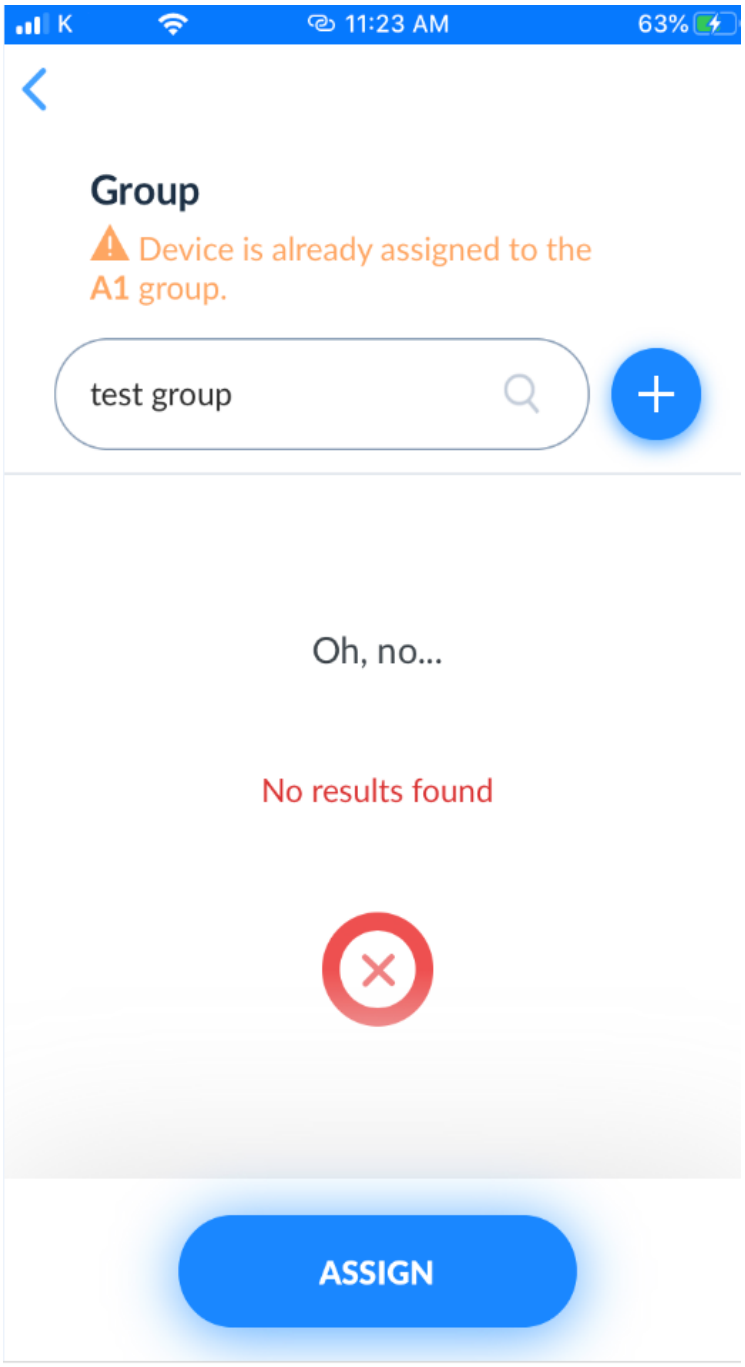
Confirm the action by clicking ‘Procced’ on ‘Are you sure…?’ pop-up window.



A Device is successfully assigned to the Group.

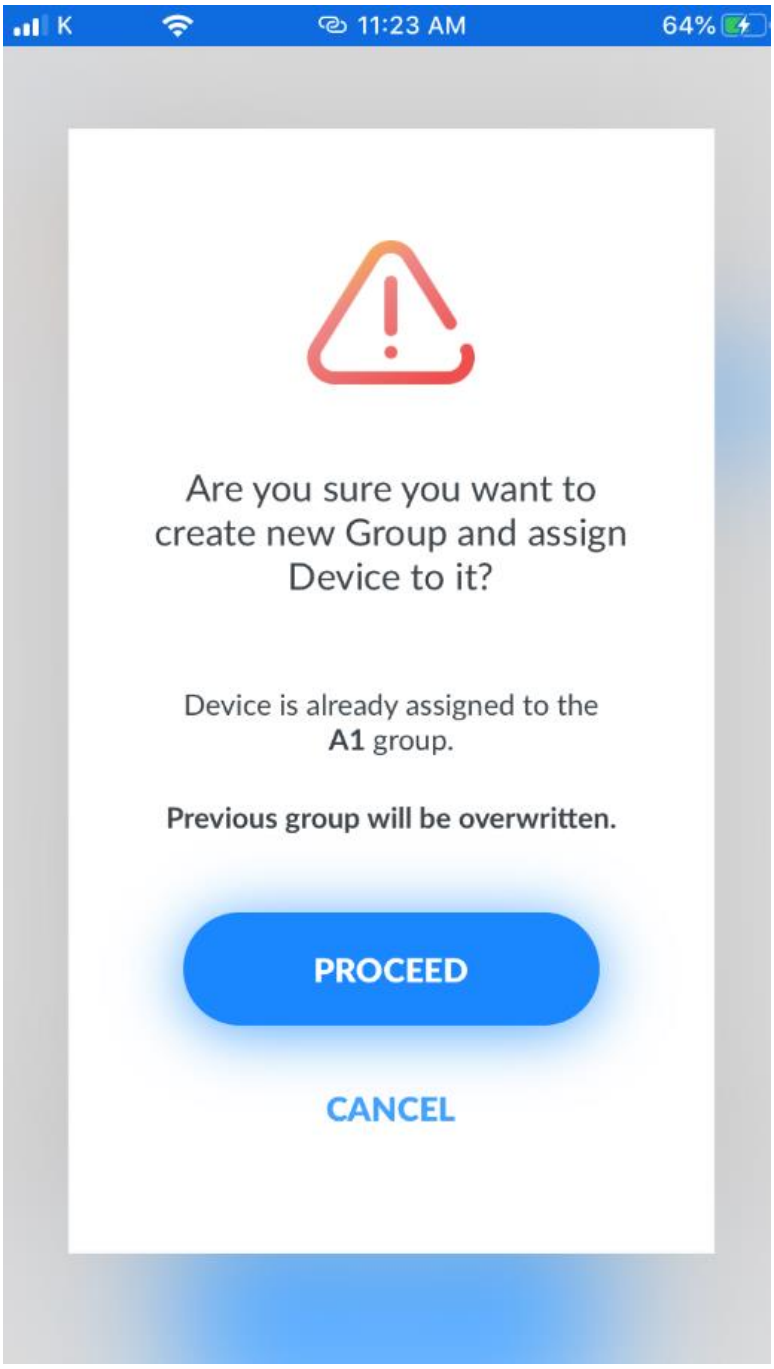


In order to create a new Group tap ‘+’ icon next to the Search field.

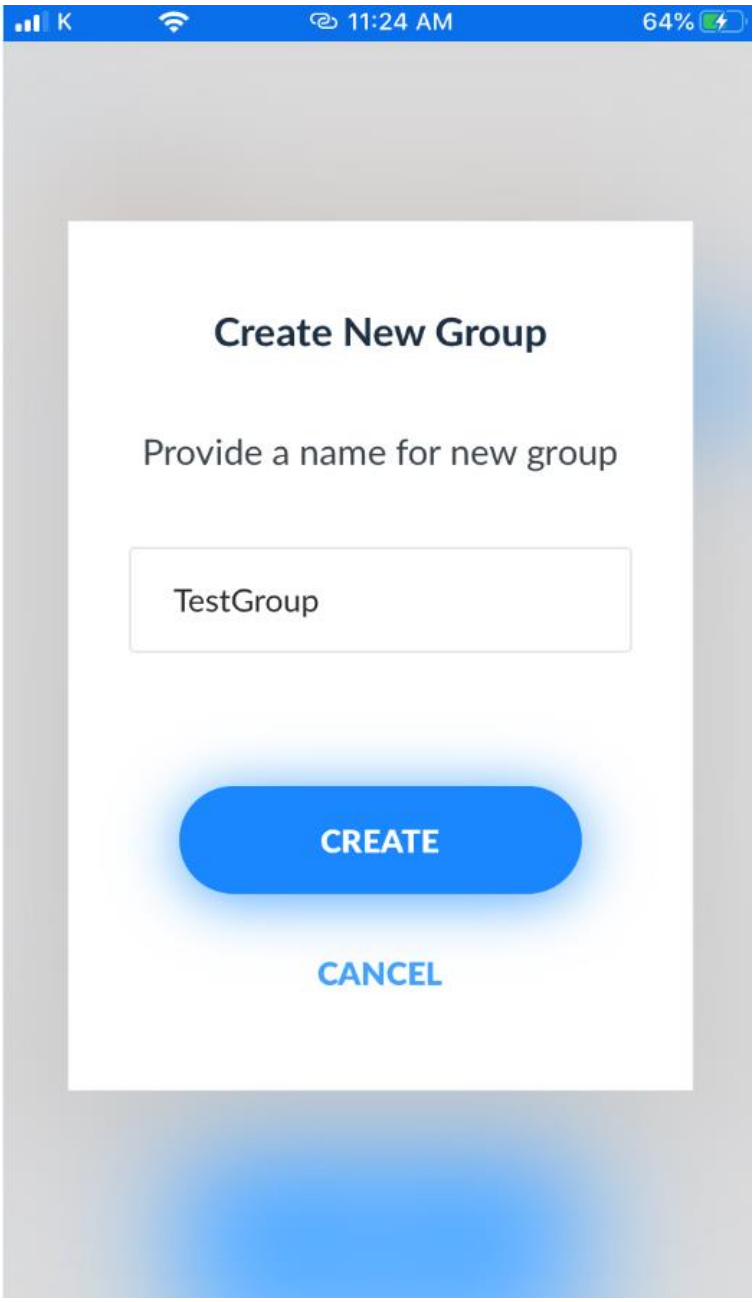


Confirm the action by clicking ‘Proceed’ on ‘Are you sure…?’ pop-up window.

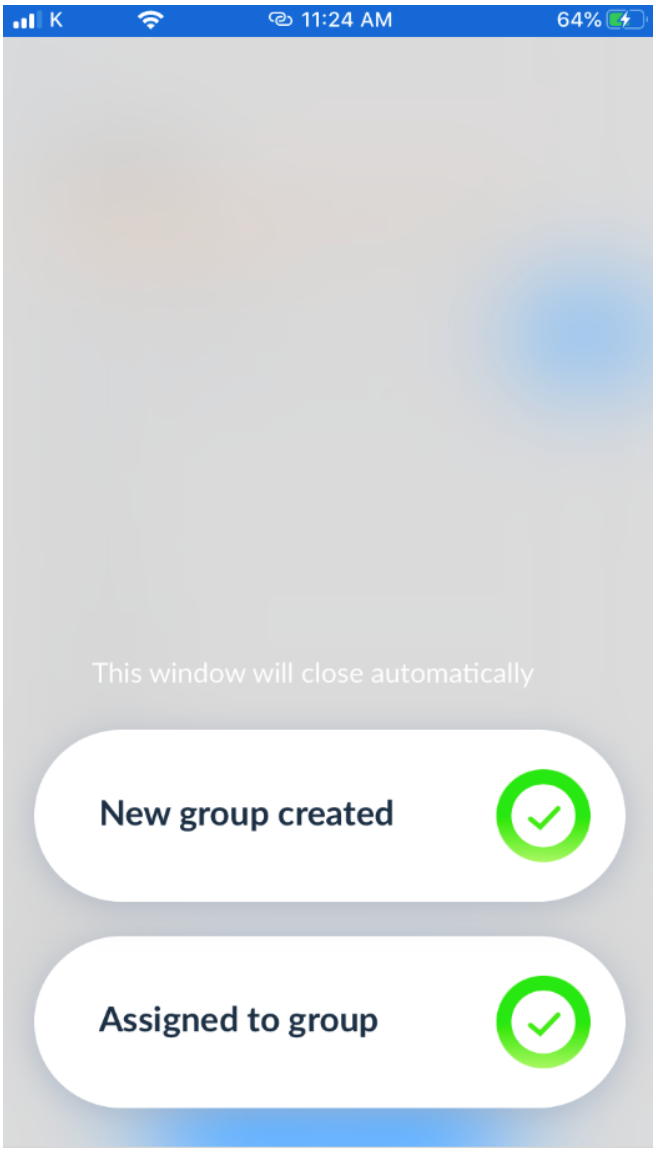
Note: If a Device is already assigned to another Group the previous Group will be overwritten.



Provide a new Group name and tap on ‘Create’.



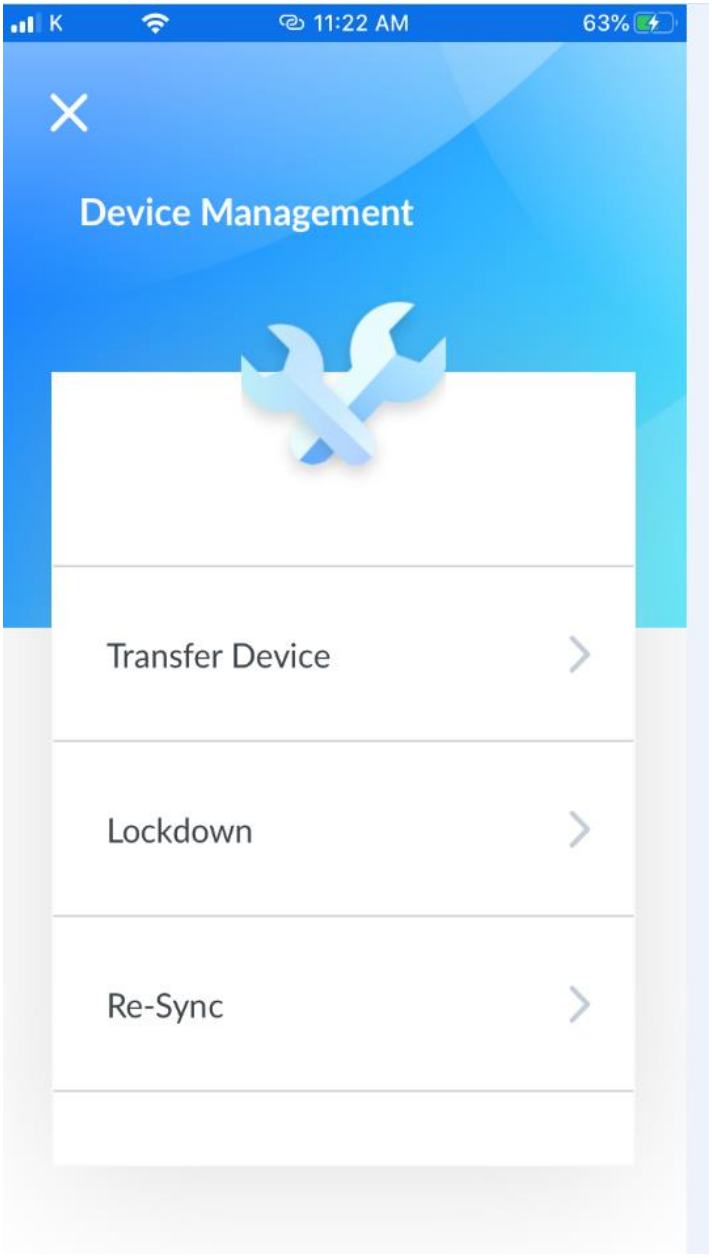
A new Group is successfully created. A Device is assigned to a new Group.



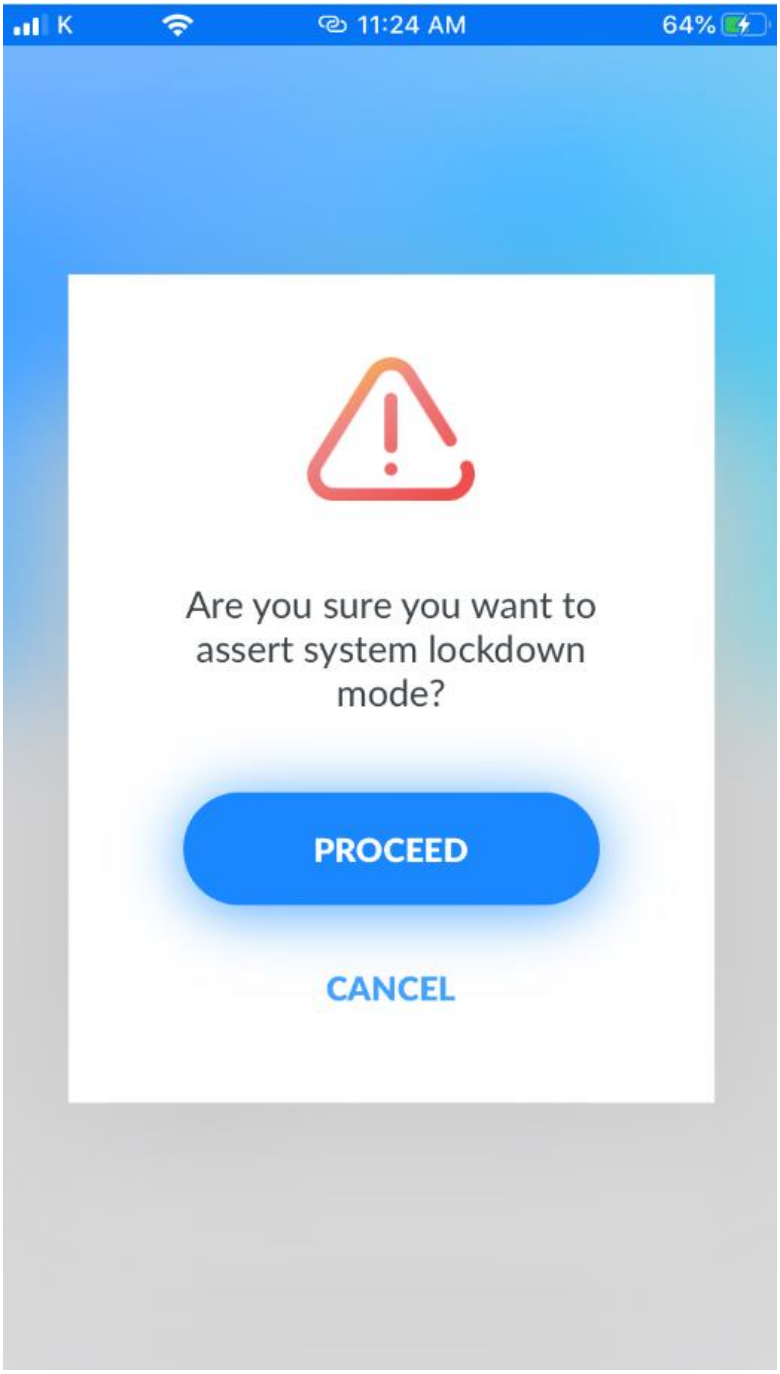
Activate System Lockdown Mode

Tap on ‘Connect to Device’ on Landing screen. If needed go through connection to Device steps (see Connection to Device for details).

Tap on ‘Lockdown’ on ‘Device Management’ tab.



Confirm the action by clicking ‘Procced’ on ‘Are you sure…?’ pop-up window.



A system Lockdown mode is asserted successfully. The status of a Device changes to ‘Inactive’. Click ‘Close’ to return to Menu screen.