ThinkShield Mobile application

User roles and app functionality

ThinkShield Mobile application overview

The SE350 mobile app is called ThinkShield Mobile application, and it is available in both Android and iOS versions. The supported devices are as follows:

- 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 iPhones 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, and Thai.

ThinkShield Mobile application user roles and capabilities

ThinkShield Mobile application user roles are assigned within the ThinkShield Key Vault Portal by the Organization Admin(s).

Scroll down for more information.

Capabilities / Roles	No credentials	Has a Lenovo ID	Base user	Edge user	Maintenance user	Org Admin
Can log in to or log out of the ThinkShield Mobile application			V	V	V	V
Mobile profile			V	V	V	V
Access to an organization			V	V	V	V
View device lockdown status			V	V	V	V
Show Activation Code	V	V	V	V	V	V
View Mobile Support	V	V	V	V	V	V
Activate device				V	V	V
Update key					V	

ThinkShield Mobile application user roles and capabilities

ThinkShield Mobile application user roles are assigned within the ThinkShield Key Vault Portal by the Organization Admin(s).

Scroll down for more information.

Capabilities / Roles	No credentials	Has a Lenovo ID	Base user	Edge user	Maintenance user	Org Admin
Show Activation Code	V	V	V	V	V	V
View Mobile Support	V	V	V	V	V	V
Activate device				V	V	V
Update key					V	
Network configuration				V		V
Device Management						V
Transfer devices (group)						V
Activate system lockdown mode						V
Re-sync				V	V	V

Connecting to a device

To interact with a device, you must go through the following connection steps.

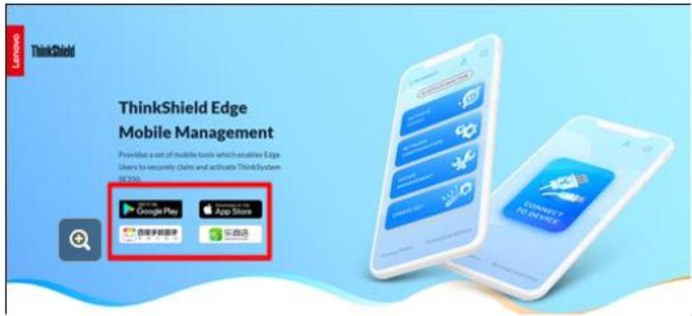
Click each number in turn to see the procedure.

Step 1 2 3 4 5 6

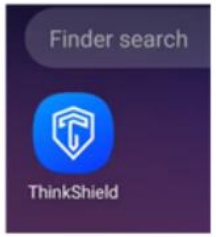
ThinkShield Mobile application

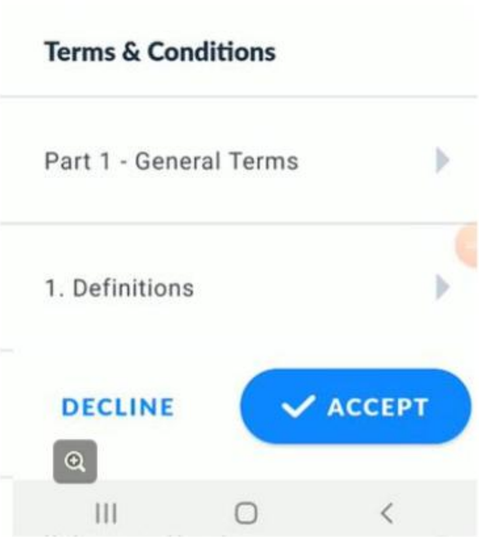
Connecting to a device

- Go to ThinkShield App to download and install the **ThinkShield Edge Mobile Management** app.
- Launch the **ThinkShield** app.
- Accept the **Terms and Conditions**.
- Log in to the app using the email and password assigned by the organization admin.


ThinkShield Edge Mobile Management

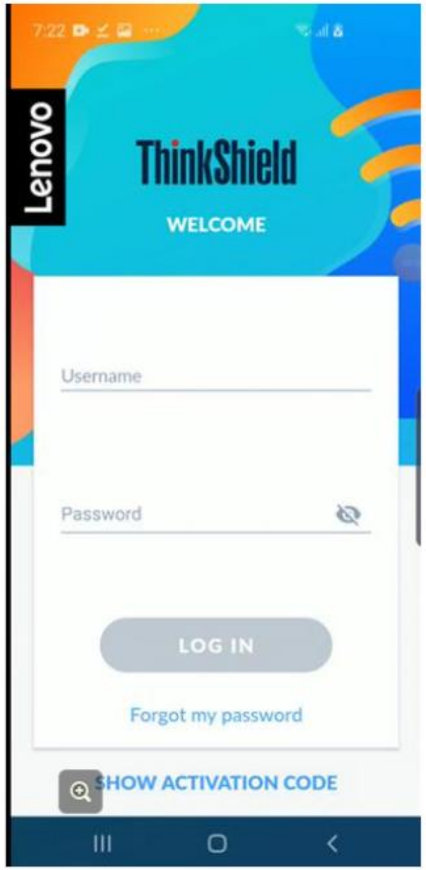
Provides a set of mobile tools which enables Edge Users to securely claim and activate ThinkSystem SE350.




Terms & Conditions

Part 1 - General Terms

1. Definitions

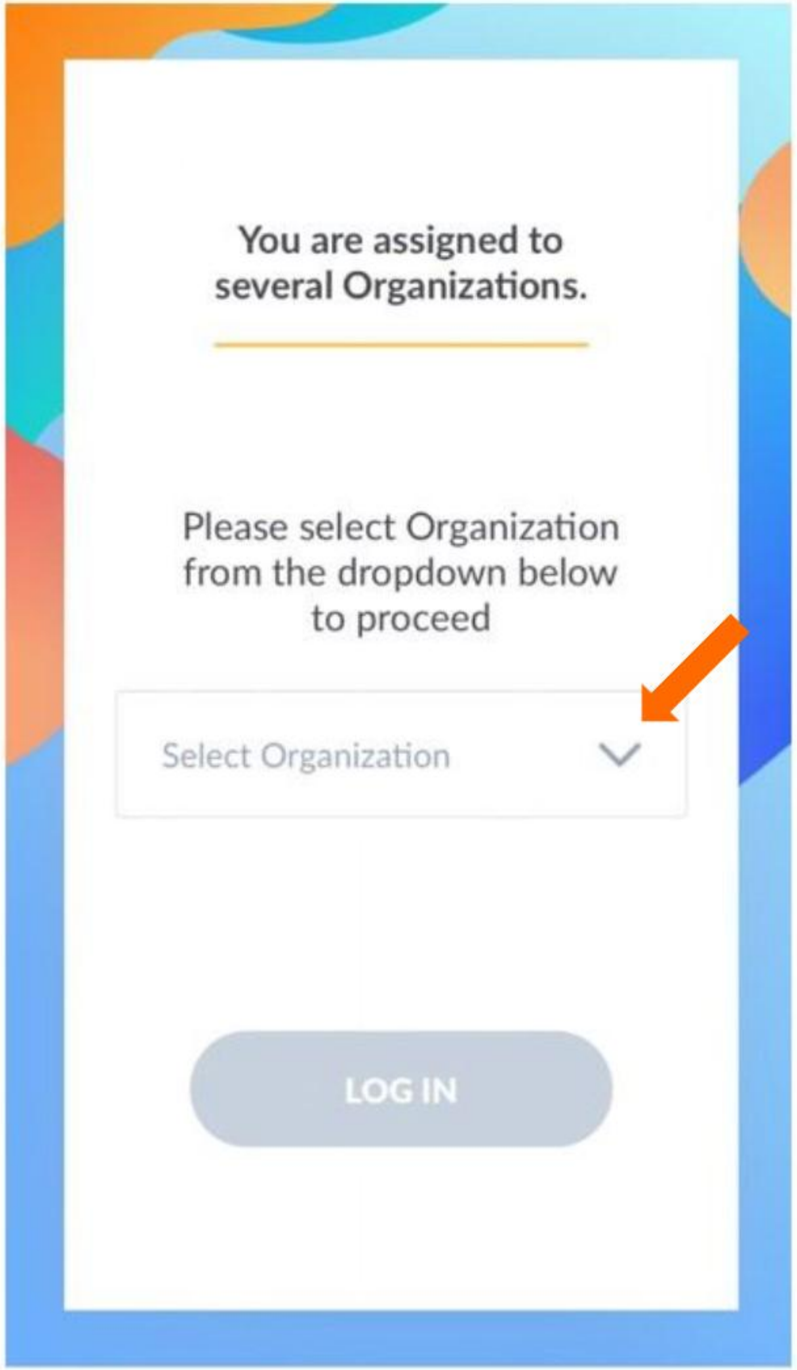


Step 1 2 3 4 5 6

Connecting to a device

If a user is assigned to several organizations, they will be asked to select the organization they want to act on behalf of.
Select an organization from the drop-down menu and tap **LOG IN**.

Step 1 — 2 — 3 — 4 — 5 — 6

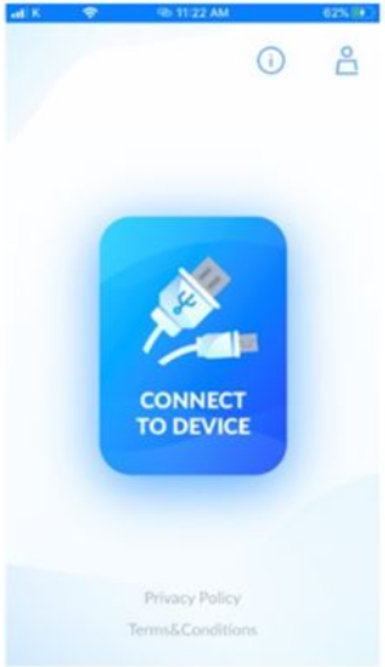


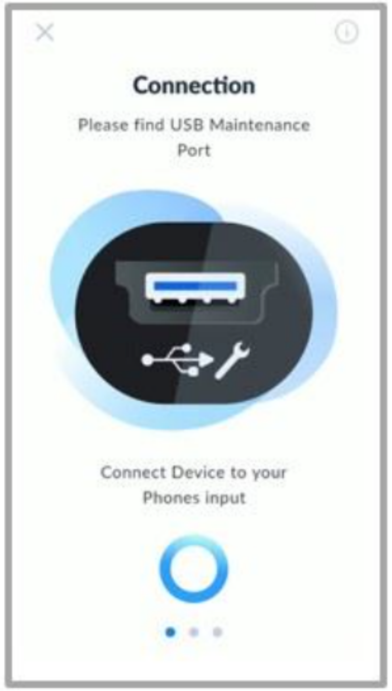
You are assigned to several Organizations.

Please select Organization from the dropdown below to proceed

Connecting to a device

- Tap **CONNECT TO DEVICE** on the landing screen, and the **Connection** indication screen will be displayed.
- Using your own mobile phone charging and data cable and the mini USB cable shipped with the system, connect the mobile phone to the server's XClarity Controller mini USB connector as shown below.

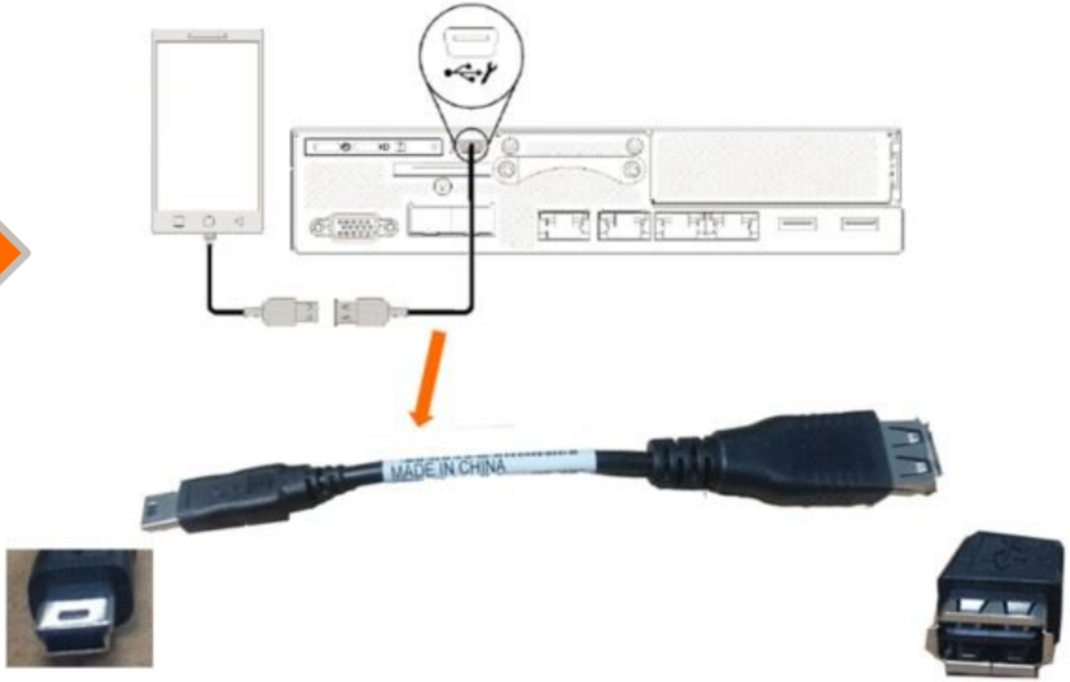




Connection

Please find USB Maintenance Port

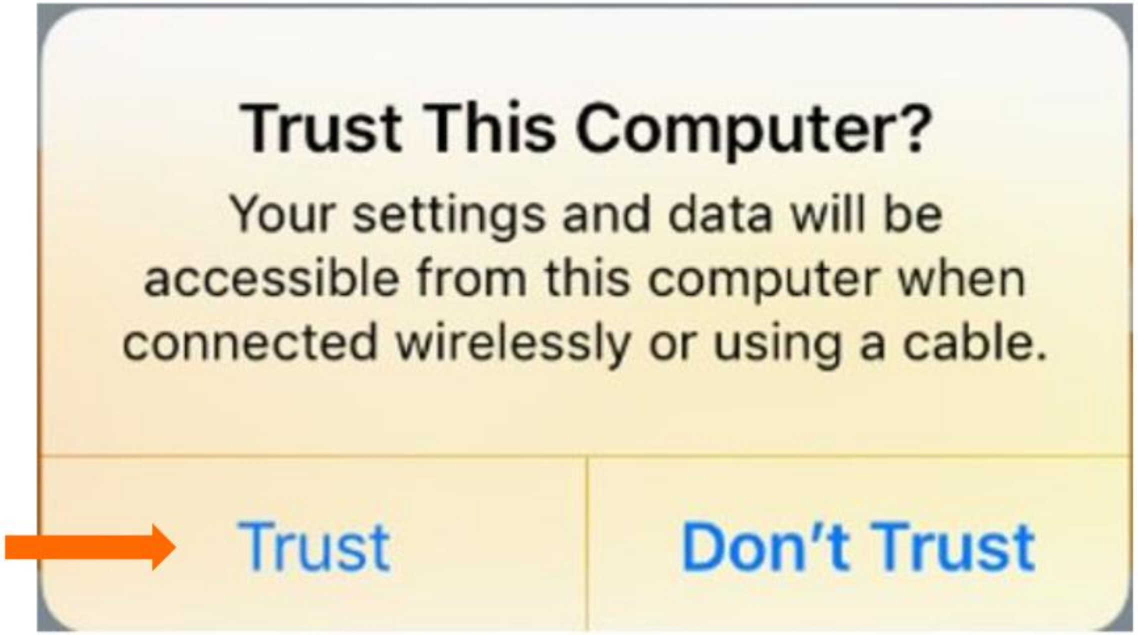
Connect Device to your Phones input



Step 1 — 2 — 3 — 4 — 5 — 6

Connecting to a device

After plugging in the cable, a **Trust This Computer** pop-up window will be displayed. Tap **Trust**. If your PIN is enabled, you may be asked to enter your device’s PIN.



Trust This Computer?

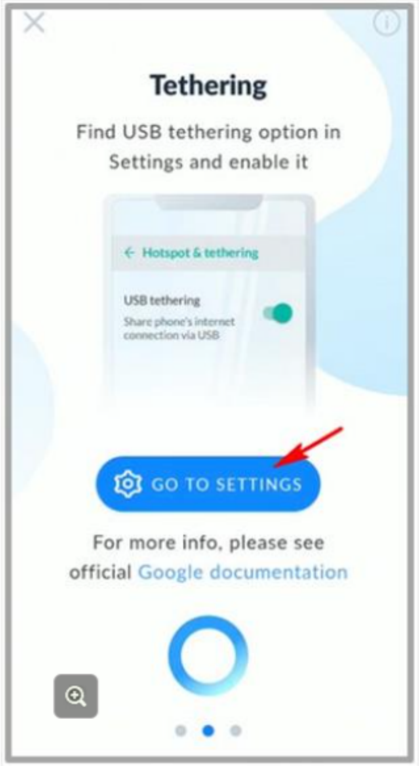
Your settings and data will be accessible from this computer when connected wirelessly or using a cable.

Step 1 2 3 4 5 6

Connecting to a device

Enable tethering on your phone.

- For Android phones, tap **GO TO SETTINGS** on the screen, and then enable **USB tethering**.
- The connection will succeed if there are no errors.

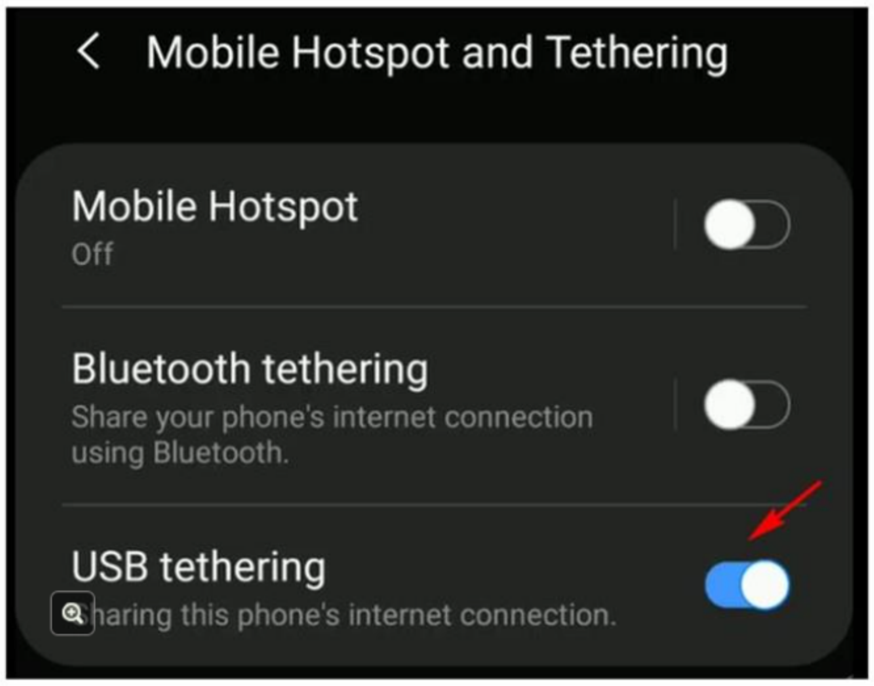


Tethering

Find USB tethering option in Settings and enable it

GO TO SETTINGS

For more info, please see official Google documentation

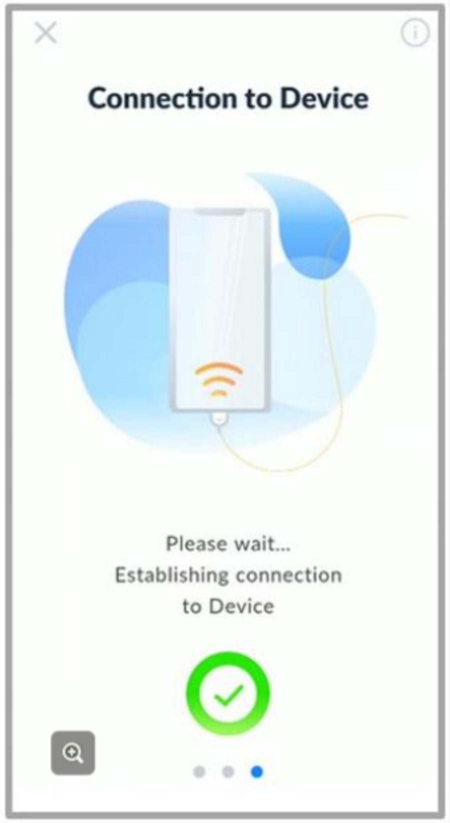


Mobile Hotspot and Tethering

Mobile Hotspot
Off

Bluetooth tethering
Share your phone's internet connection using Bluetooth.

USB tethering
Sharing this phone's internet connection.



Connection to Device

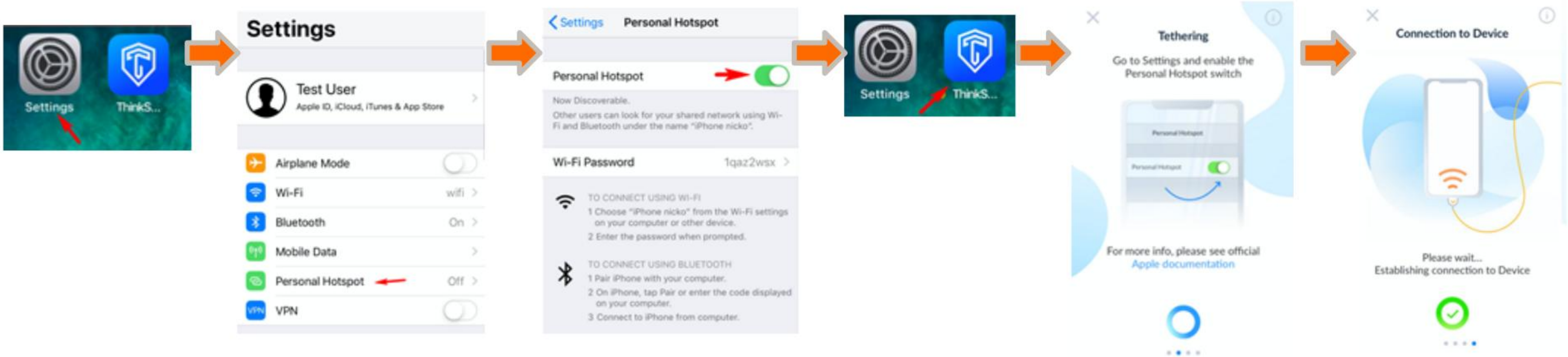
Please wait...
Establishing connection to Device

Step 1 — 2 — 3 — 4 — 5 — 6

Connecting to a device

Enable tethering on your phone.

- For iOS phones, go to **Settings** and enable **Personal Hotspot**.
- The connection will succeed if there are no errors.



Settings

Test User
Apple ID, iCloud, iTunes & App Store

Airplane Mode
Wi-Fi wifi
Bluetooth On
Mobile Data
Personal Hotspot Off
VPN

Settings | Personal Hotspot

Personal Hotspot

Now Discoverable.
Other users can look for your shared network using Wi-Fi and Bluetooth under the name "iPhone nicko".

Wi-Fi Password 1qaz2wsx

TO CONNECT USING WI-FI
1 Choose "iPhone nicko" from the Wi-Fi settings on your computer or other device.
2 Enter the password when prompted.

TO CONNECT USING BLUETOOTH
1 Pair iPhone with your computer.
2 On iPhone, tap Pair or enter the code displayed on your computer.
3 Connect to iPhone from computer.

Tethering

Go to Settings and enable the Personal Hotspot switch

For more info, please see official Apple documentation

Connection to Device

Please wait...
Establishing connection to Device

Step 1 2 3 4 5 6

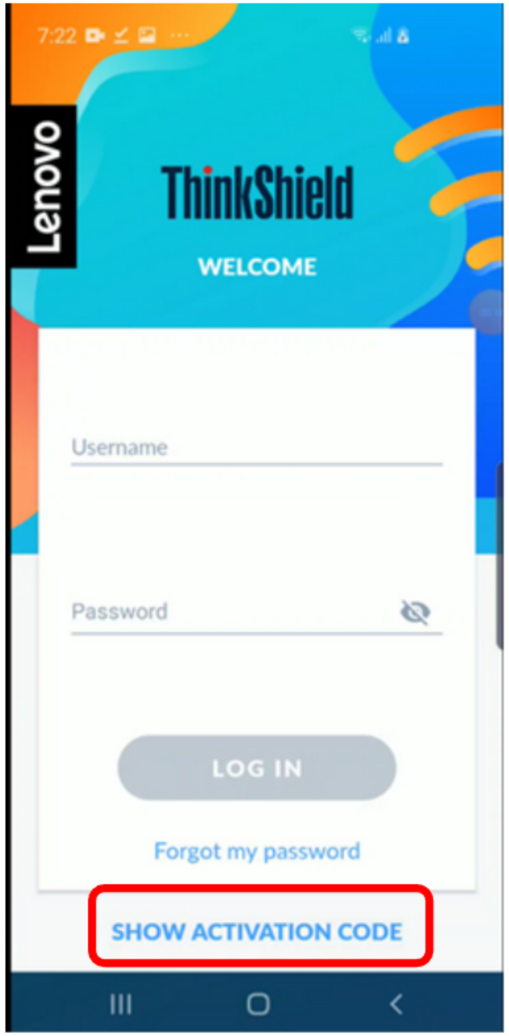
Show Activation Code

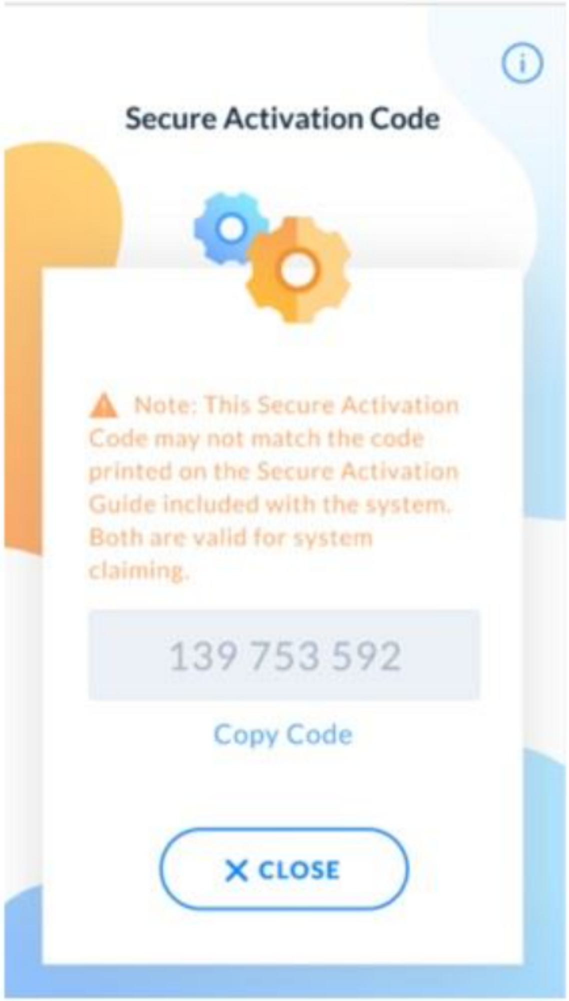
The following section will show you the SE350 ThinkShield Mobile app functionality. Make sure you have already read the **Connecting to a device** section of this course.

When the ThinkShield Mobile app has been installed and launched:

1. Tap **SHOW ACTIVATION CODE** at the bottom of the screen.
2. Plug a USB cable into the device maintenance port and your phone.
3. Ensure tethering is enabled on your phone. (Refer to the **Connecting to a device** section for the procedure).
4. The security Activation Code will be shown on the screen.

> **Note:** You do not need to log in to retrieve the Activation Code.



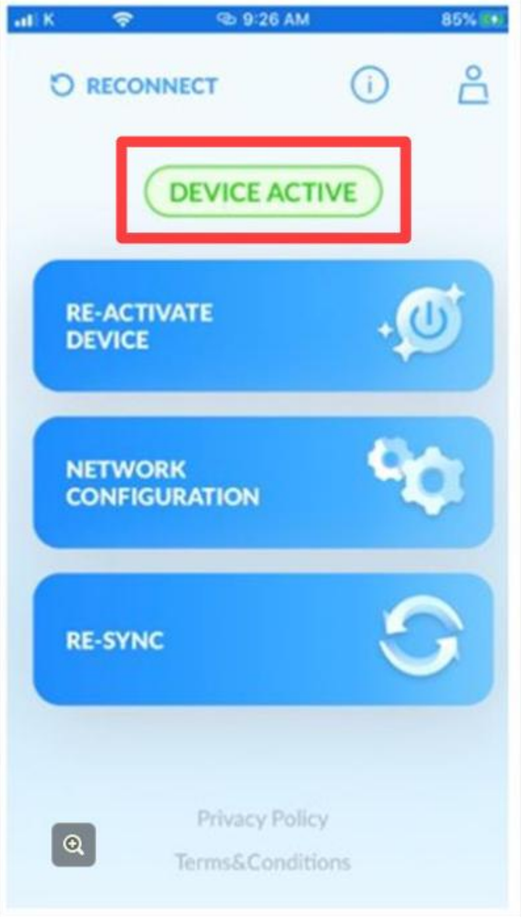


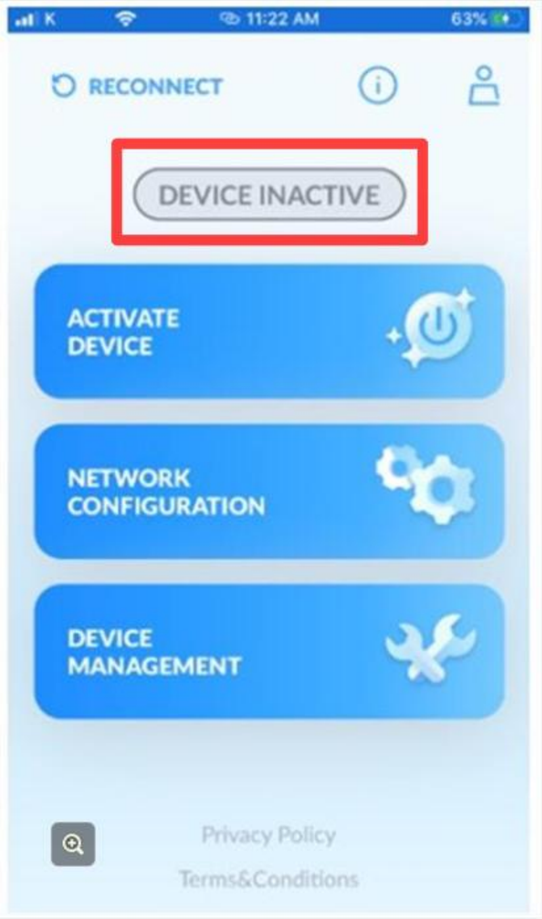
⚠ Note: This Secure Activation Code may not match the code printed on the Secure Activation Guide included with the system. Both are valid for system claiming.

139 753 592

Checking device lockdown status

- Make sure you have already read the **Connecting to a device** section of this course.
- Device status is displayed on the menu screen. If a device is in lockdown mode, the status will be **DEVICE INACTIVE**.





Mobile app activation

As part of the mobile app activation process, the app will automatically claim the device and then complete the activation process. The process should run as follows:

- The customer IT admin needs to register an onsite user first.
    - IT admin delegates activation authority
- The onsite user logs in to the mobile app.
    - This is authentication
- The onsite user taps **Activate**.
- The mobile app automatically retrieves the MT/SN/Activation Code from the SE350 and sends it to the ThinkShield Key Vault Portal. The Portal then registers the device.
    - This is claiming
- The mobile app runs the activation process with the Portal.
    - This is activation

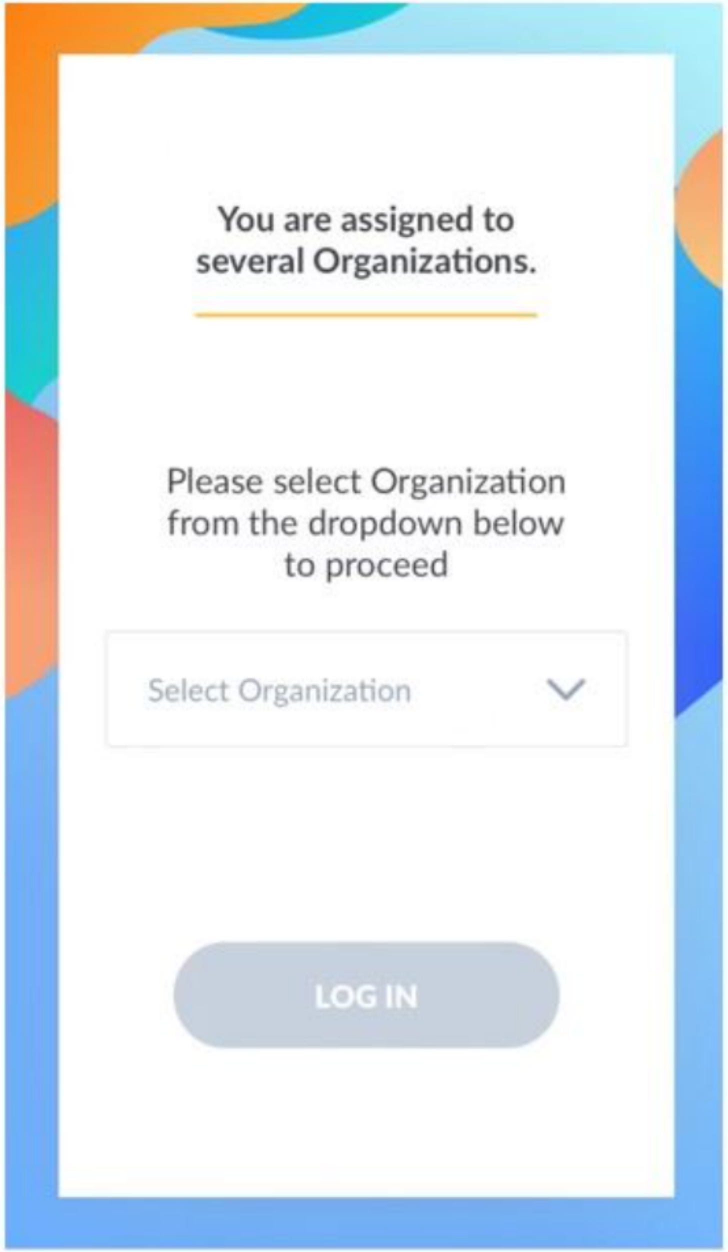
Click each number in turn to see the procedure.

Step 1 2 3

Mobile app activation

Make sure you have read the **ThinkShield Mobile application - Connecting to a device** section of this course.

- Select an organization from the drop-down menu and tap **LOG IN**.
    - **Note**: The device will be claimed to the selected organization during Activation flow.
- If the device was already assigned to another organization, the user will receive an error message at the end of the flow because this is not allowed.



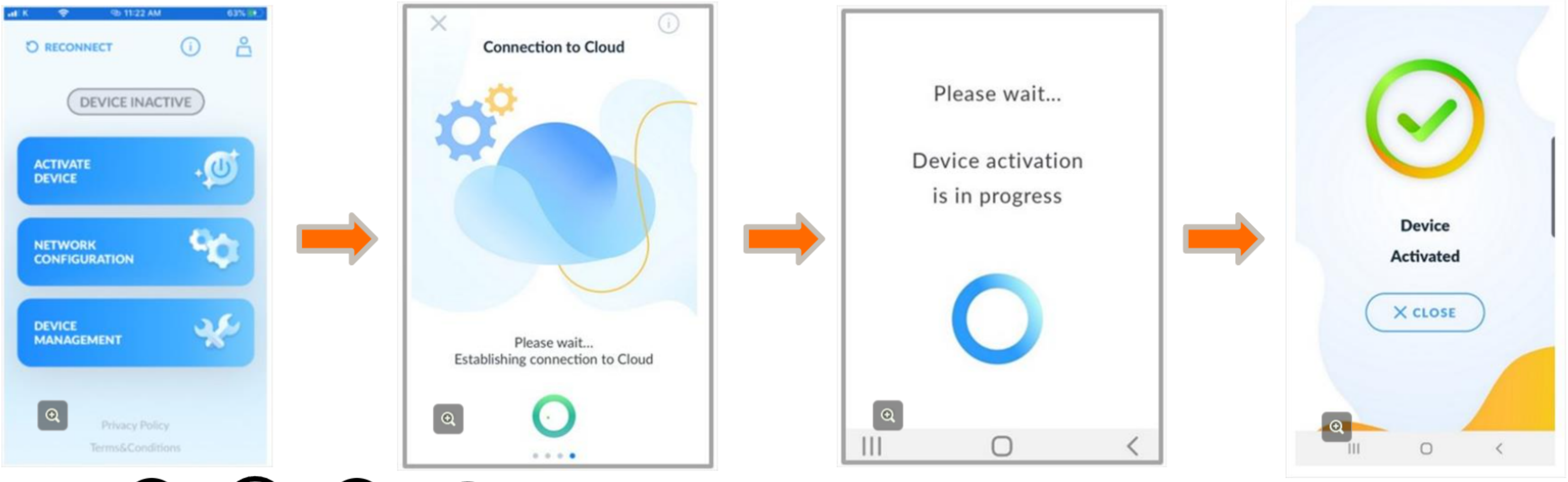
You are assigned to several Organizations.

Please select Organization from the dropdown below to proceed

Step 1 2 3

Mobile app activation

- When the connection is established, tap **ACTIVATE DEVICE**.
- Wait until a **Connection to Cloud** is established.
- A **Device activation is in progress** message will then be displayed.
- A **Device Activated** message will be shown if the device was successfully activated.



RECONNECT

DEVICE INACTIVE

ACTIVATE DEVICE

NETWORK CONFIGURATION

DEVICE MANAGEMENT

Privacy Policy

Terms&Conditions

Connection to Cloud

Please wait...
Establishing connection to Cloud

Please wait...

Device activation is in progress

Device Activated

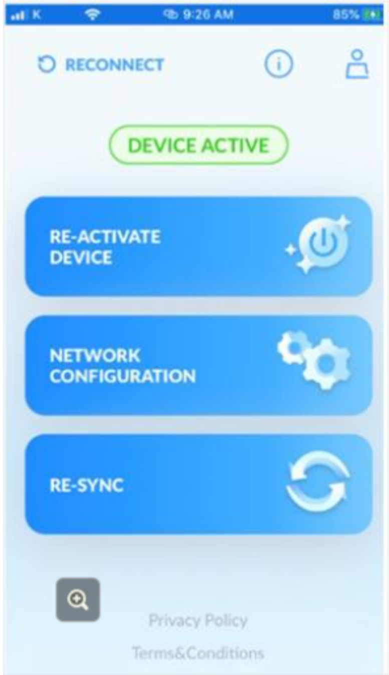
CLOSE

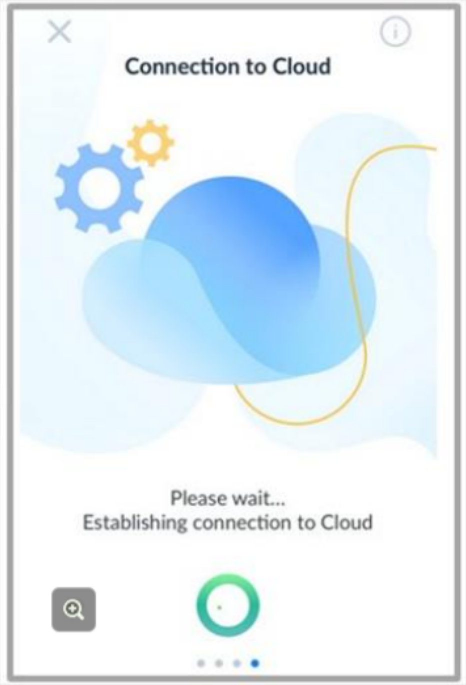
Step 1 — 2 — 3

Mobile app activation

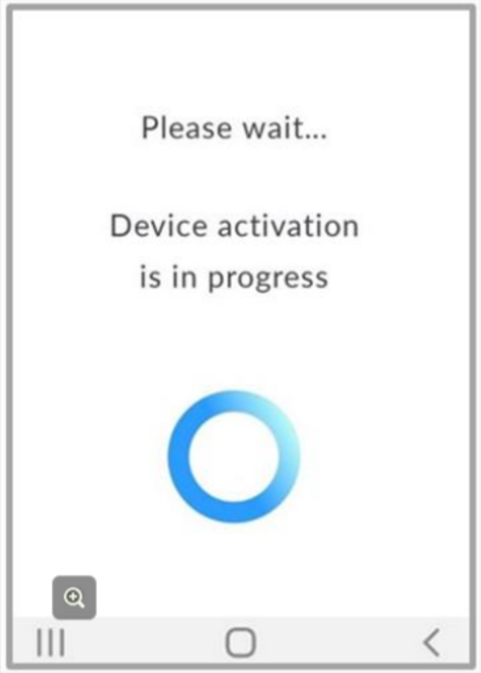
If the SE350 device is locked due to tamper event, follow these steps for reactivation.

- Tap **RE-ACTIVATE DEVICE**.
- Wait until a **Connection to Cloud** is established.
- A **Device activation is in progress** message will then be displayed.
- A **Device Activated** message will be shown if the device was successfully activated.

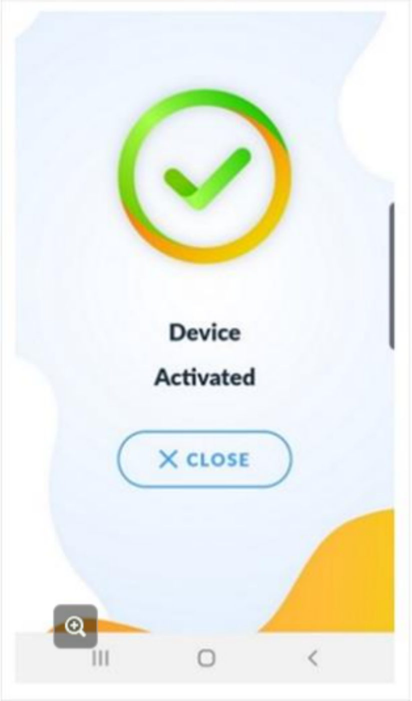



Connection to Cloud

Please wait...
Establishing connection to Cloud


Please wait...

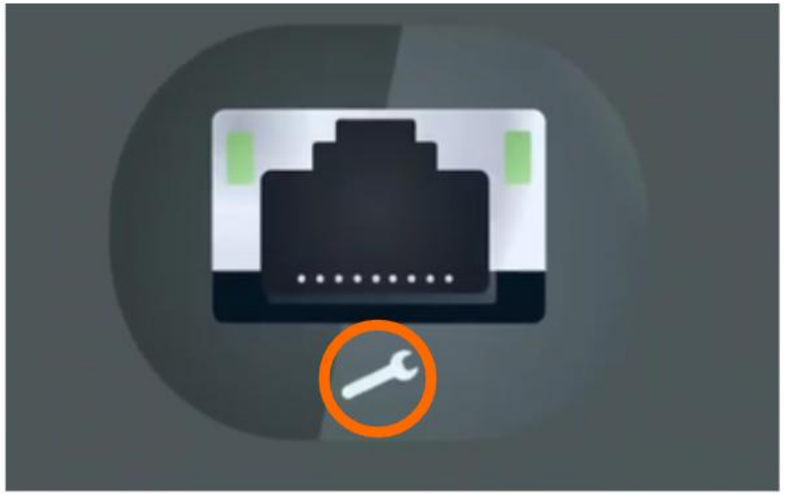
Device activation is in progress


Device Activated

Step 1 2 3

Network configuration

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

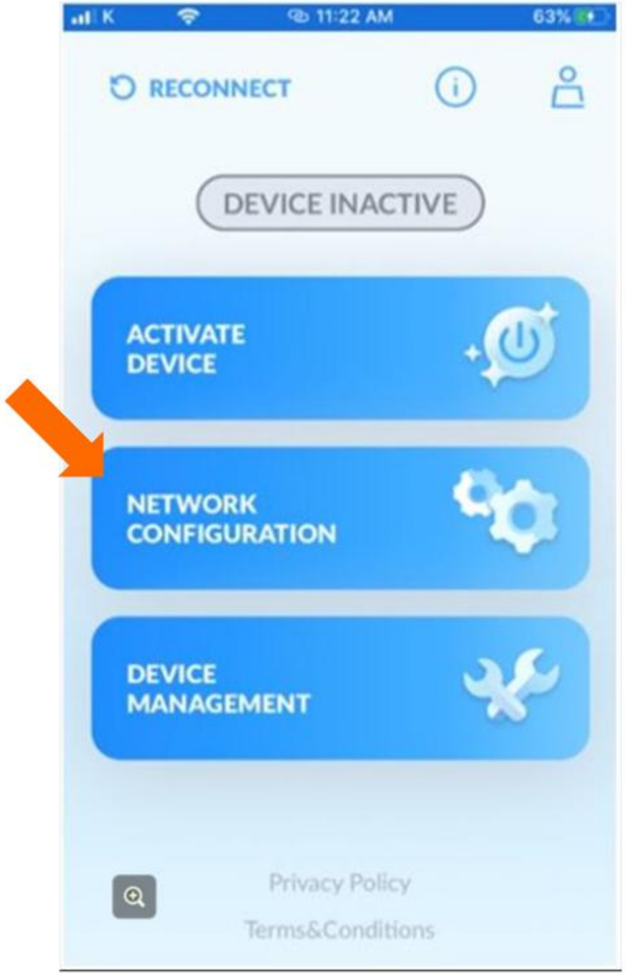


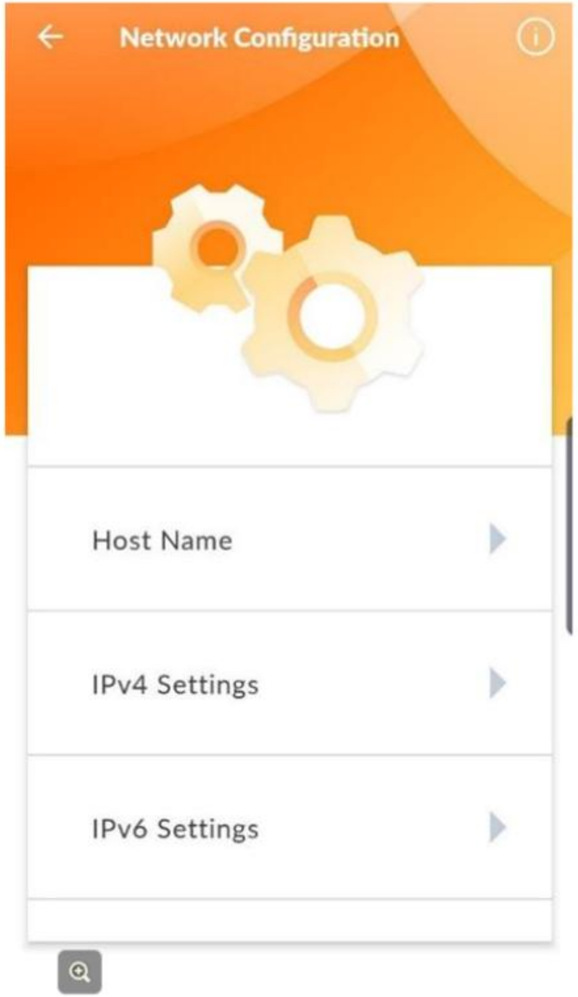
Click each number in turn to see the procedure.

Step 1 — 2 — 3 — 4

Network configuration

- Log in to the ThinkShield app
- Tap **Network Configuration** on the landing screen.
- Plug a USB cable into the device maintenance port and your phone.
- Ensure tethering is enabled on your phone. (Refer to the **Connecting to a device** section for the procedure.)
- The **Network Configuration** screen will be displayed if the connection is successful.
- Tap the item that needs to be modified.



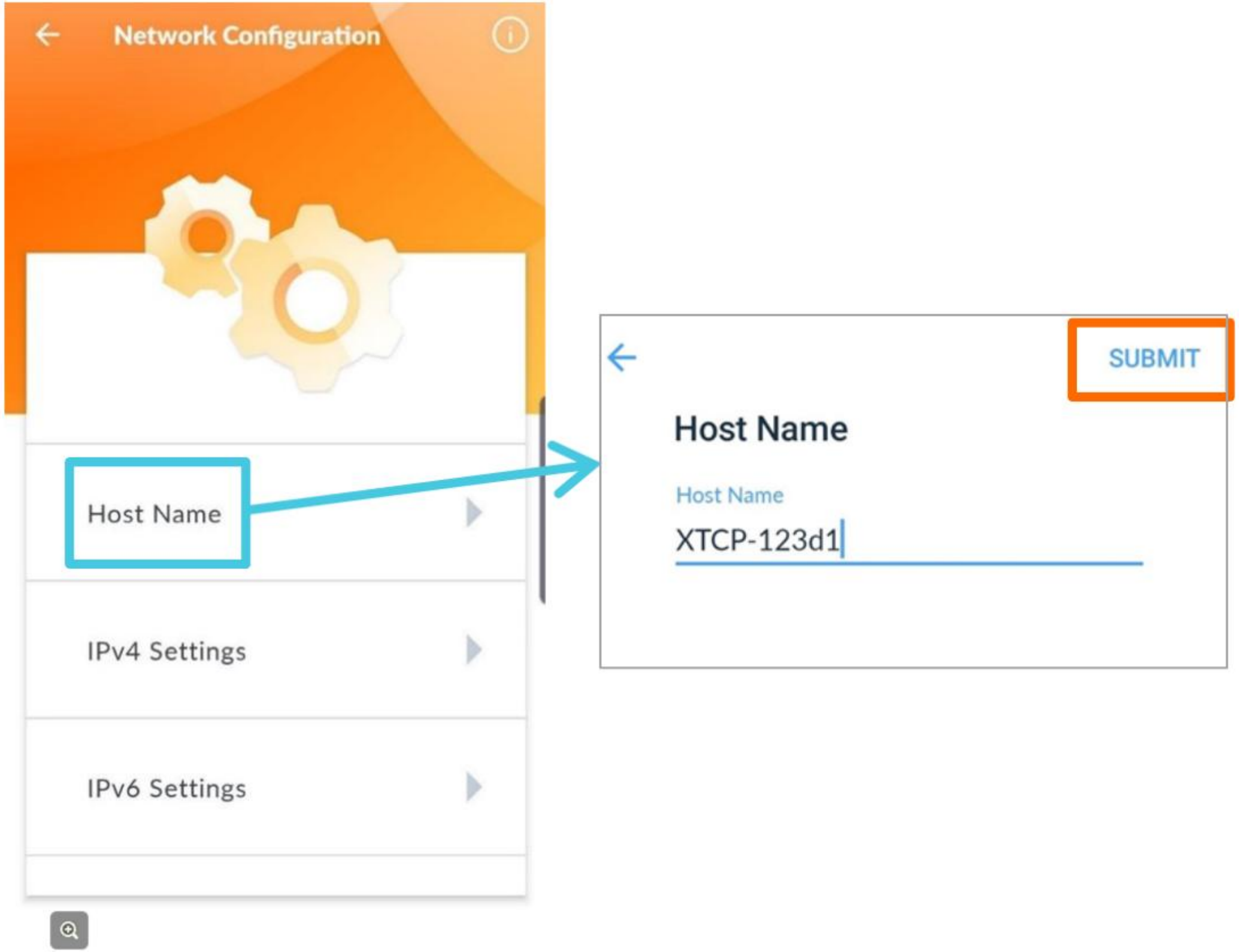


Step 1 2 3 4

Network configuration

The **SUBMIT** button will become active as soon as any changes are entered.

Tap **SUBMIT** after making any necessary changes. Data will be sent to the ThinkShield Portal. A pop-up message at the bottom of the screen will state whether the submission was successful or not.



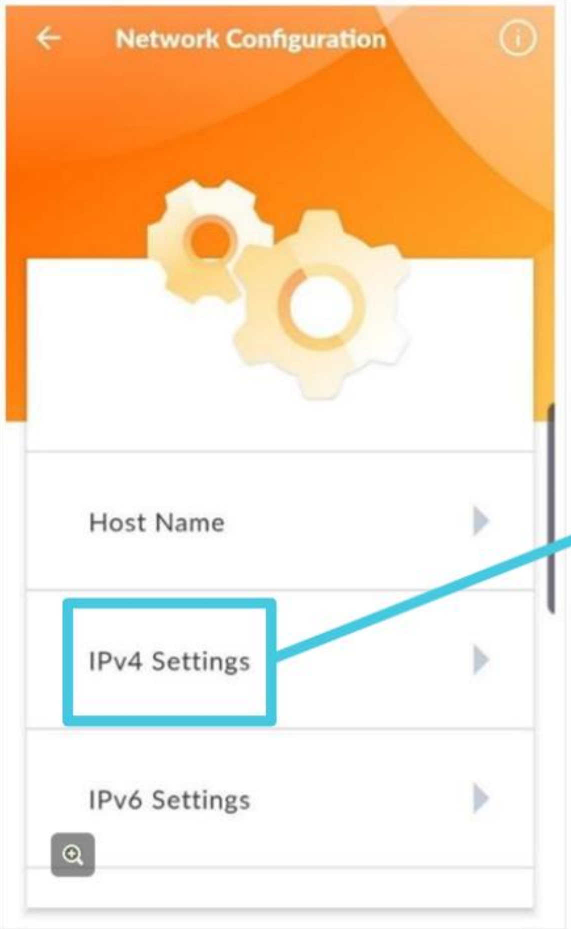
Host Name

Host Name: XTCP-123d1

Step 1 2 3 4

ThinkShield Mobile application

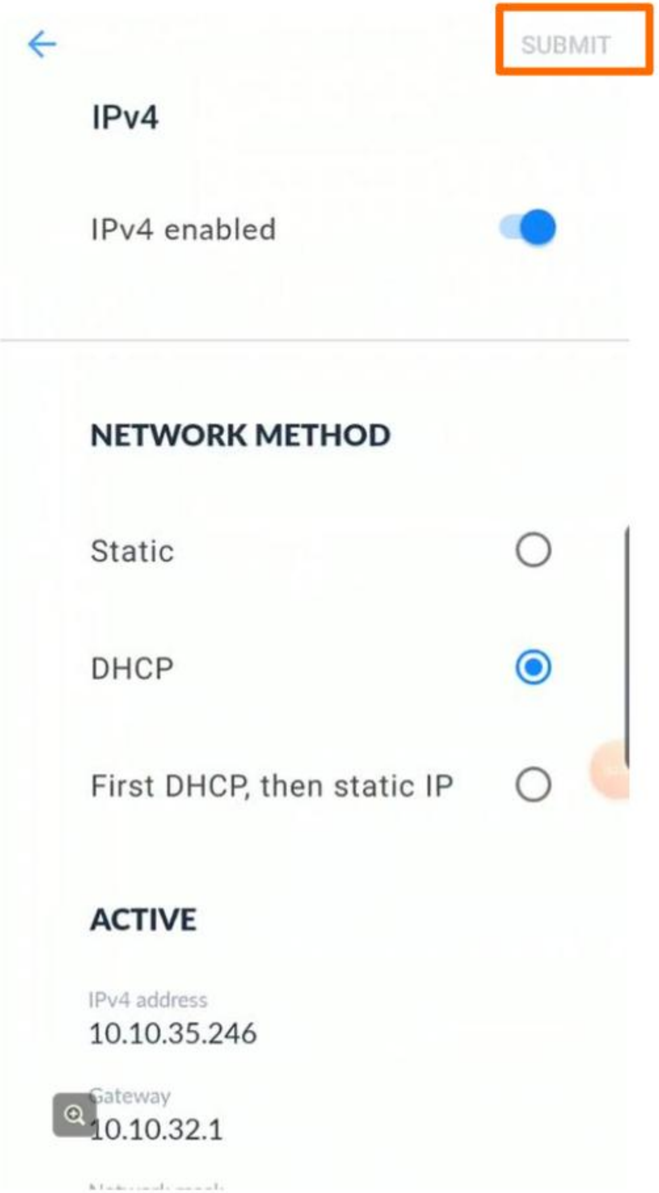
Network configuration


Network Configuration

Host Name

IPv4 Settings

IPv6 Settings


SUBMIT

IPv4

IPv4 enabled ●

NETWORK METHOD

Static ○

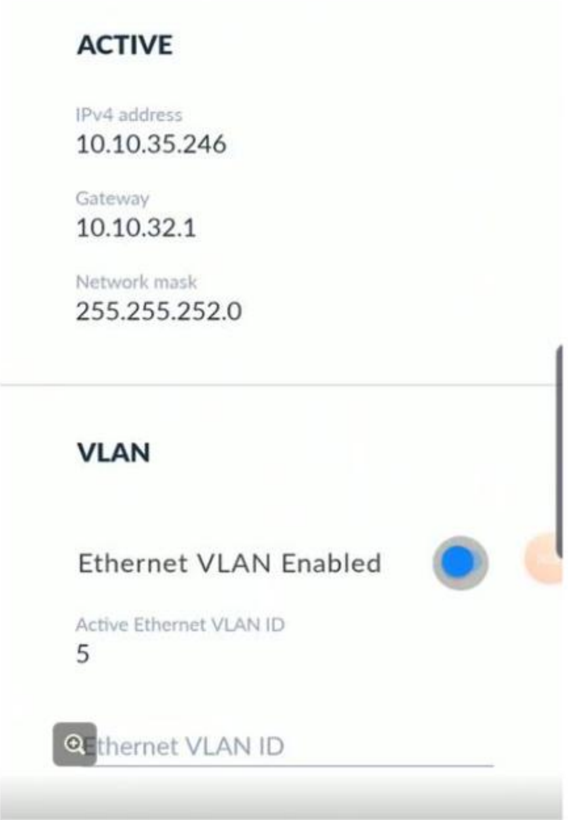
DHCP ●

First DHCP, then static IP ○

ACTIVE

IPv4 address
10.10.35.246

Gateway
10.10.32.1


ACTIVE

IPv4 address
10.10.35.246

Gateway
10.10.32.1

Network mask
255.255.252.0

VLAN

Ethernet VLAN Enabled ●

Active Ethernet VLAN ID
5

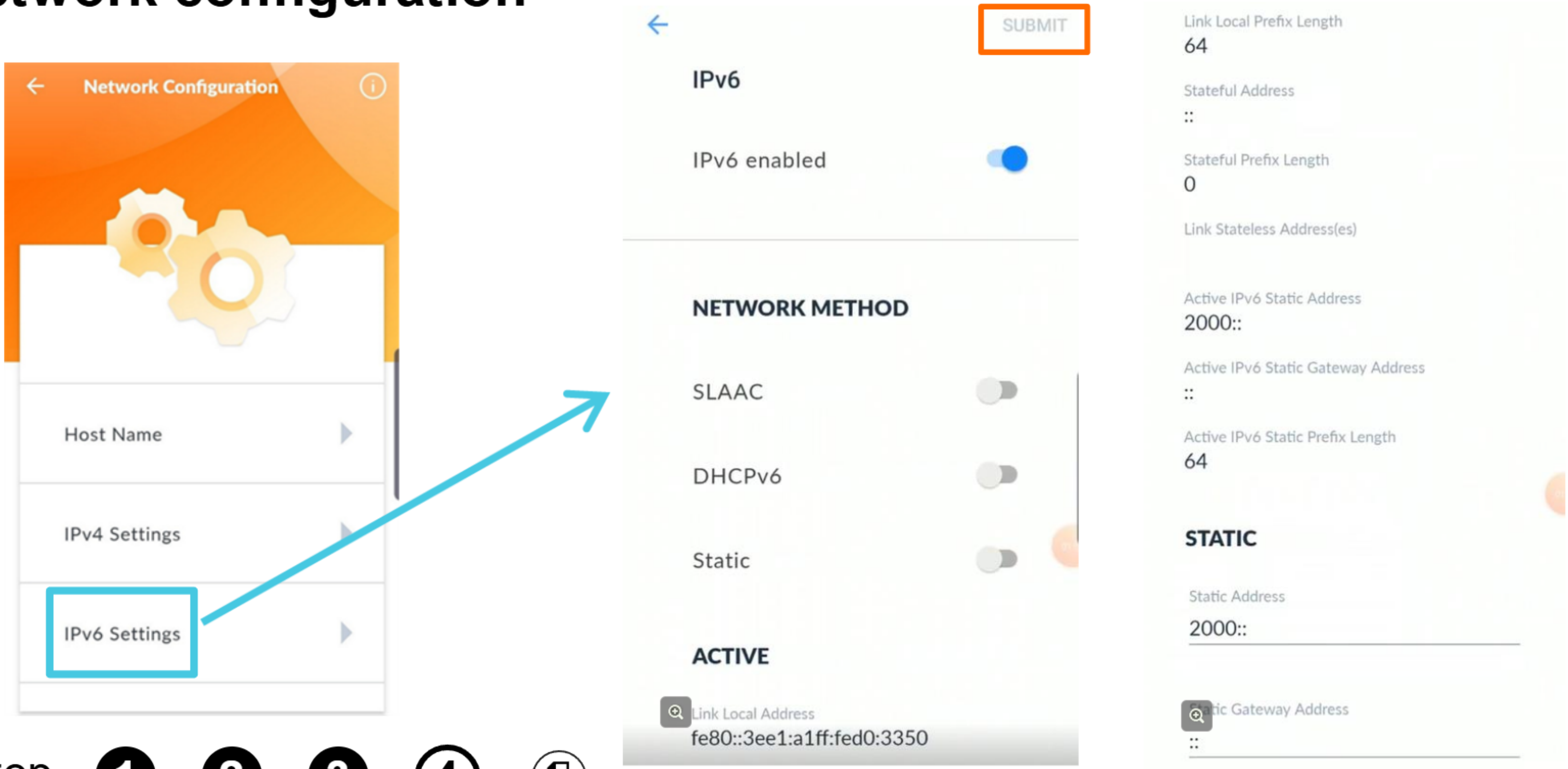
Ethernet VLAN ID

Step 1 — 2 — 3 — 4

Lenovo

ThinkShield Mobile application

Network configuration



IPv6

IPv6 enabled ●

NETWORK METHOD

SLAAC ○

DHCPv6 ○

Static ○

ACTIVE

Link Local Address
fe80::3ee1:a1ff:fed0:3350

Link Local Prefix Length
64

Stateful Address
::

Stateful Prefix Length
0

Link Stateless Address(es)

Active IPv6 Static Address
2000::

Active IPv6 Static Gateway Address
::

Active IPv6 Static Prefix Length
64

STATIC

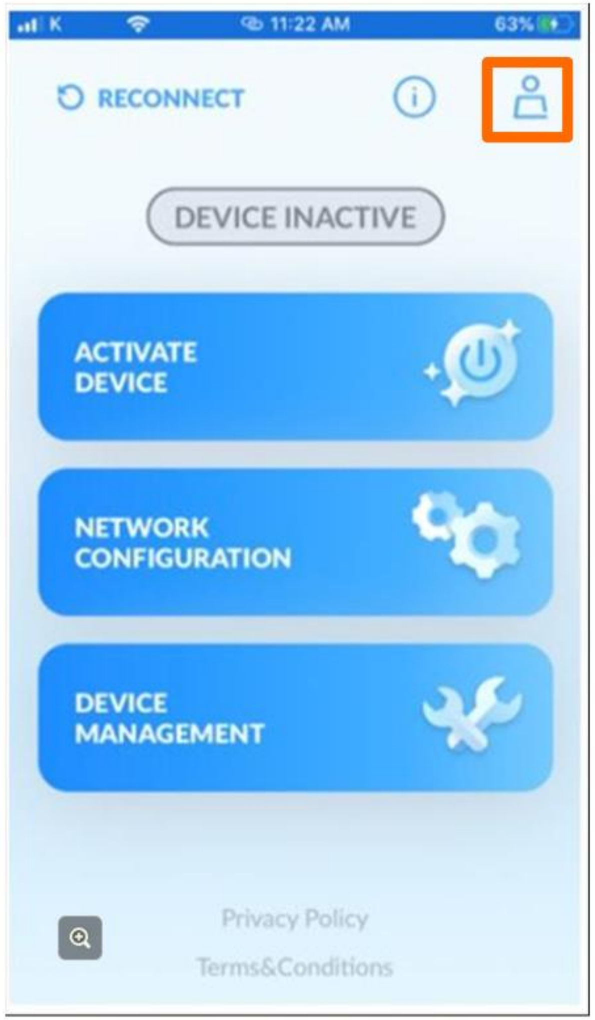
Static Address
2000::

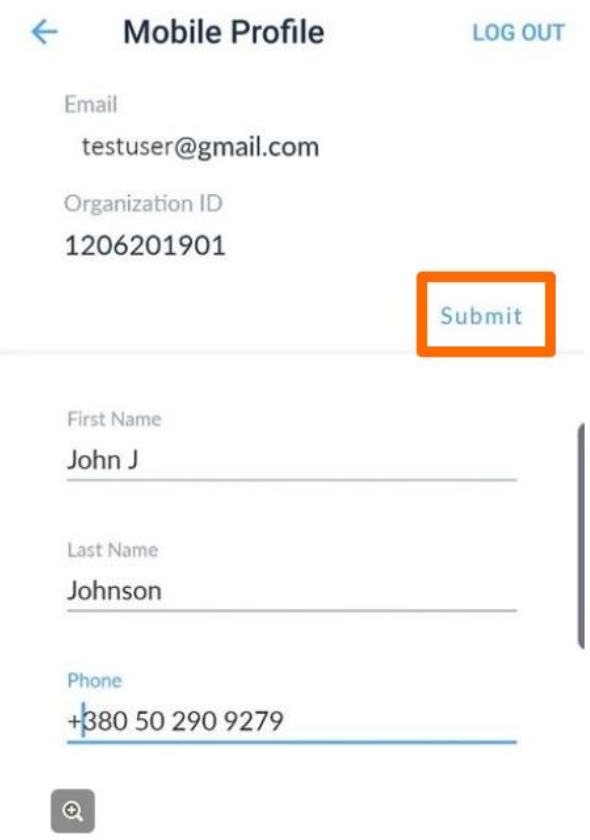
Static Gateway Address
::

Step 1 2 3 4

View and update your mobile profile

Select the user icon at the top of the screen to see the Edge user profile. The user profile can be updated by tapping **Submit** after entering any necessary changes.





Email
testuser@gmail.com

Organization ID
1206201901

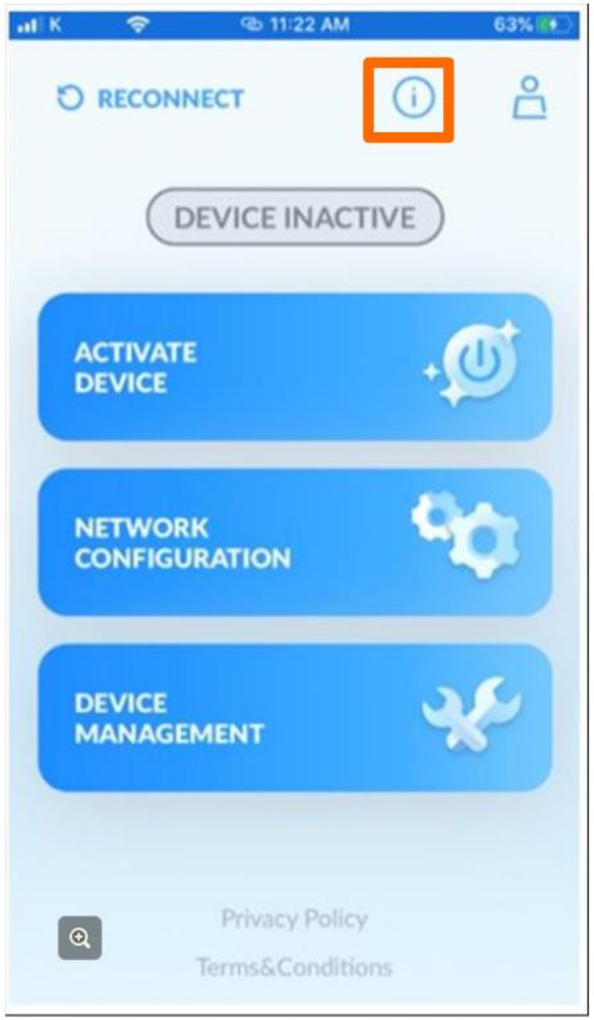
First Name
John J

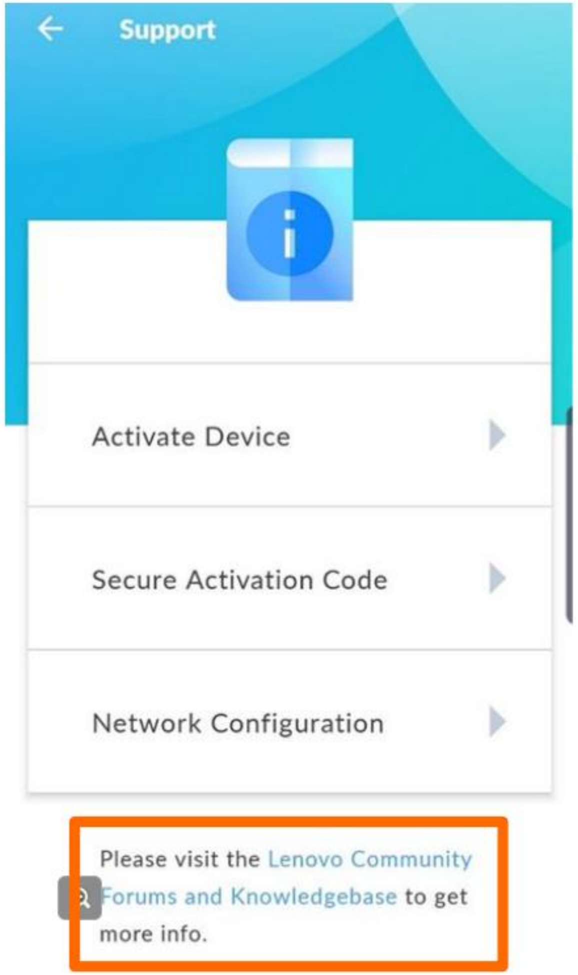
Last Name
Johnson

Phone
+380 50 290 9279

View Mobile Support

Select the information icon at the top of the screen to see Mobile Support.
Mobile Support provides additional information.
If more information is needed, tap **Lenovo Community Forums and Knowledge** at the bottom of the screen.

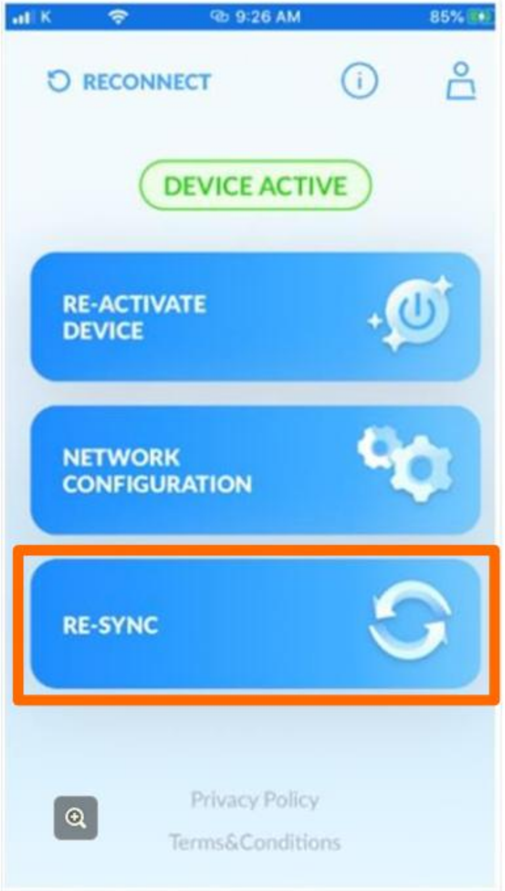


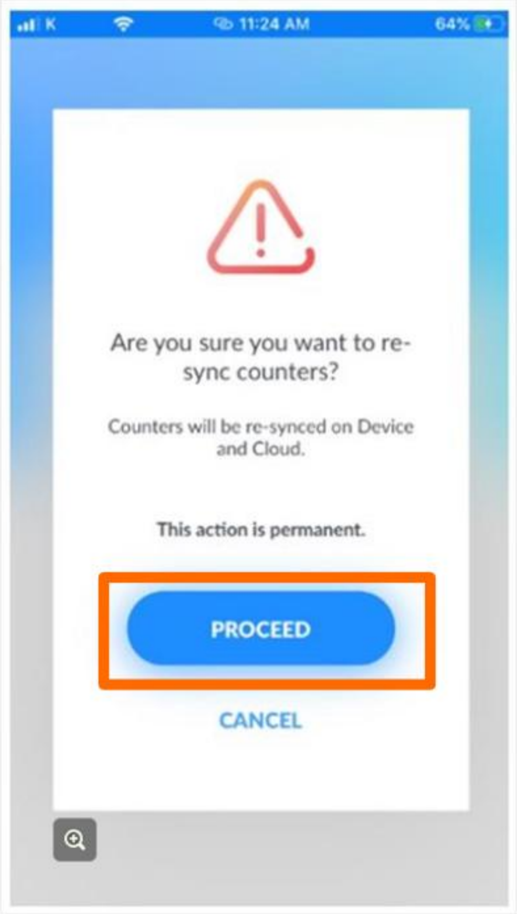


Please visit the Lenovo Community Forums and Knowledgebase to get more info.

Re-sync

- To reset the counters on a device, tap **RE-SYNC** on the Menu screen. This action is useful when an **Activation code is not valid** error occurs.
- Confirm the action by tapping **PROCEED** on the pop-up window.
- A **Counters re-synced** message will be displayed if the counters were successfully re-synced.

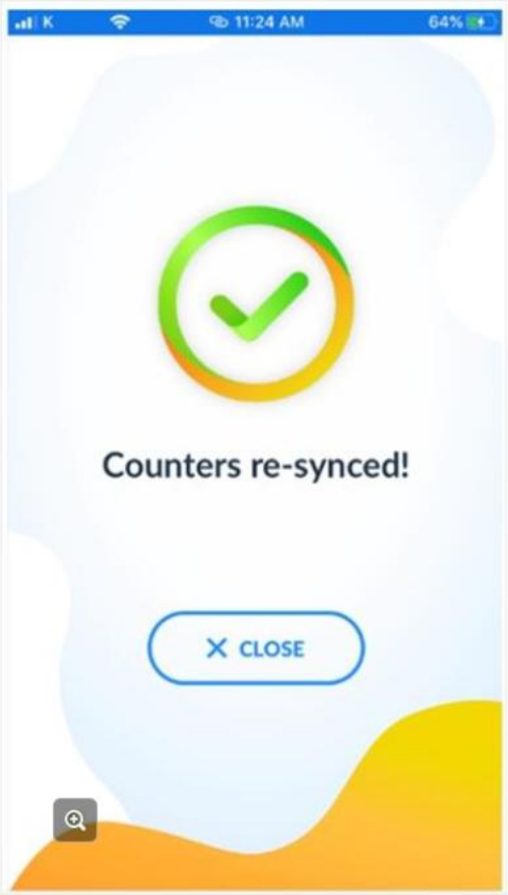




Are you sure you want to re-sync counters?

Counters will be re-synced on Device and Cloud.

This action is permanent.



Counters re-synced!

Checking and updating the Device key

All system boards are programmed at the factory with public and private key information. When installing a replacement system board, it will need to be associated with the existing device MT and SN. The association of the new Device key (public key) with the MT and SN is a highly automated workflow done with the help of the ThinkShield Mobile application.

Attention: This function is available for ThinkShield Service Support users. Anyone servicing an SE350 should send an email to thinkshield@lenovo.com to have a ThinkShield Service Support user account created. If the Mobile app cannot be accessed, contact thinkshield@lenovo.com for a manual update Activation Code.

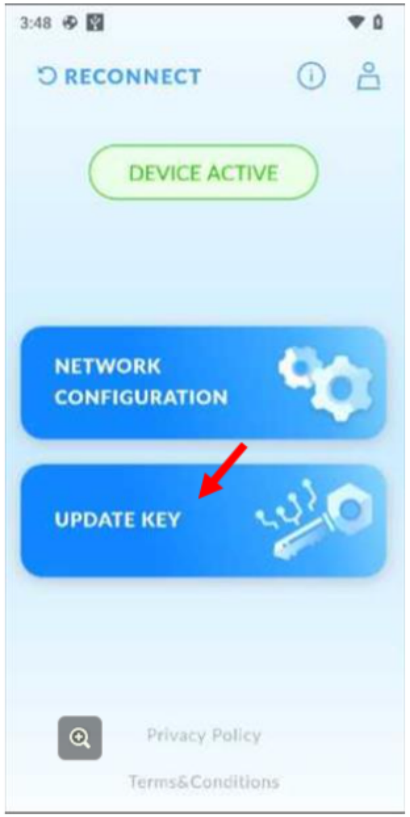
Attention: If the SSR's cell phone cannot be used, use the customer's cell phone and log in to customer's organization with the Maintenance User account to update the Device key. Note that the customer will first need to create a user with a Maintenance User role. For details of how to create different user roles, refer to the Creating users for the mobile connection feature section in this course.

Click each number in turn to see the procedure.

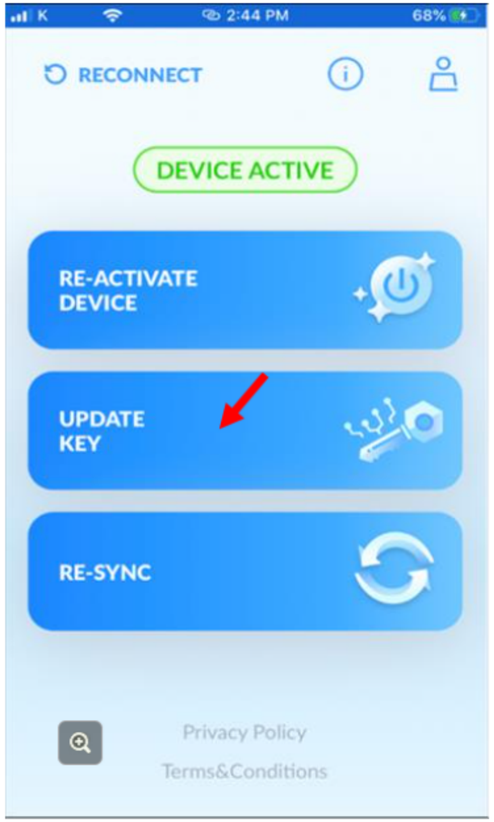
Step 1 — 2 — 3

Checking and updating the Device key

- Using the ThinkShield Service Support credentials, log in to the **TSServiceSupport** organization on the ThinkShield Mobile application.
  - If the SSR can't user their cell phone, use the customer's cell phone and log in to the customer's organization with Maintenance User credentials.
- Make sure you have already read the ThinkShield Mobile application - Connecting to a device section of this course.
- Tap **UPDATE KEY**.



From SSR's phone



From customer's phone

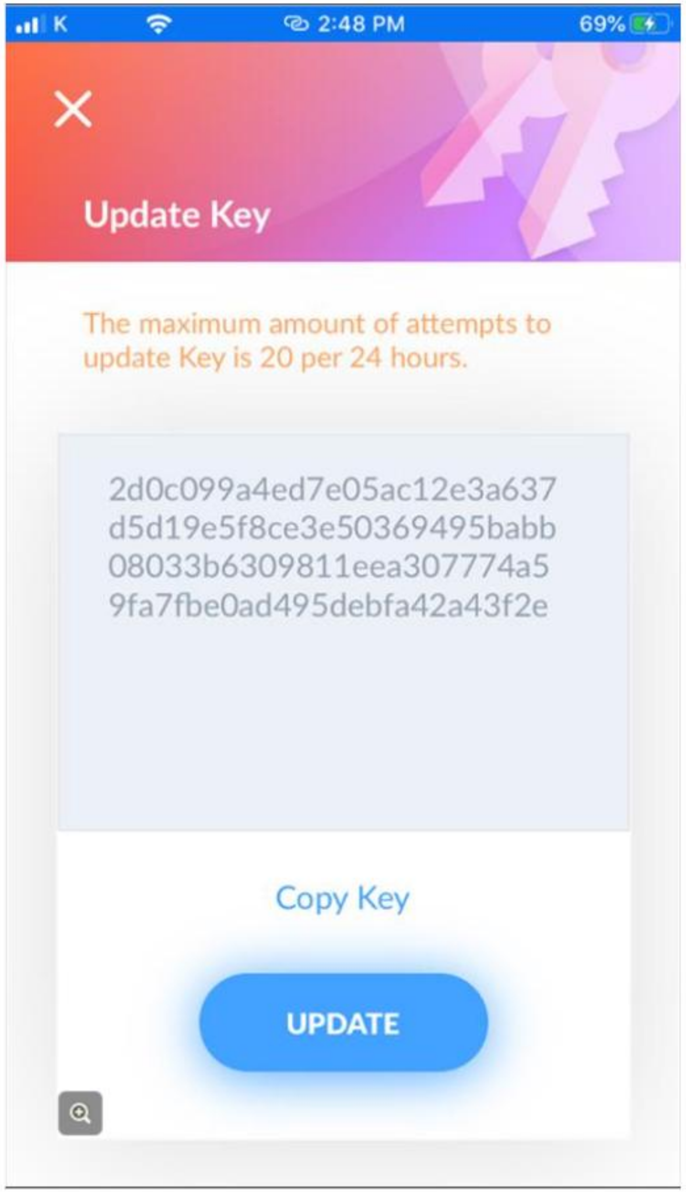
Step 1 2 3

Checking and updating the Device key

- If the connection is successful, the **Update Key** screen will be displayed.
- Copy the key by tapping **Copy Key**. It can be pasted into a personal message or an email to the Organization Admin.
- Tap **UPDATE** to update the key.

Note: You cannot attempt to update the key more than 20 times every 24 hours.

Step ❶—②—❸



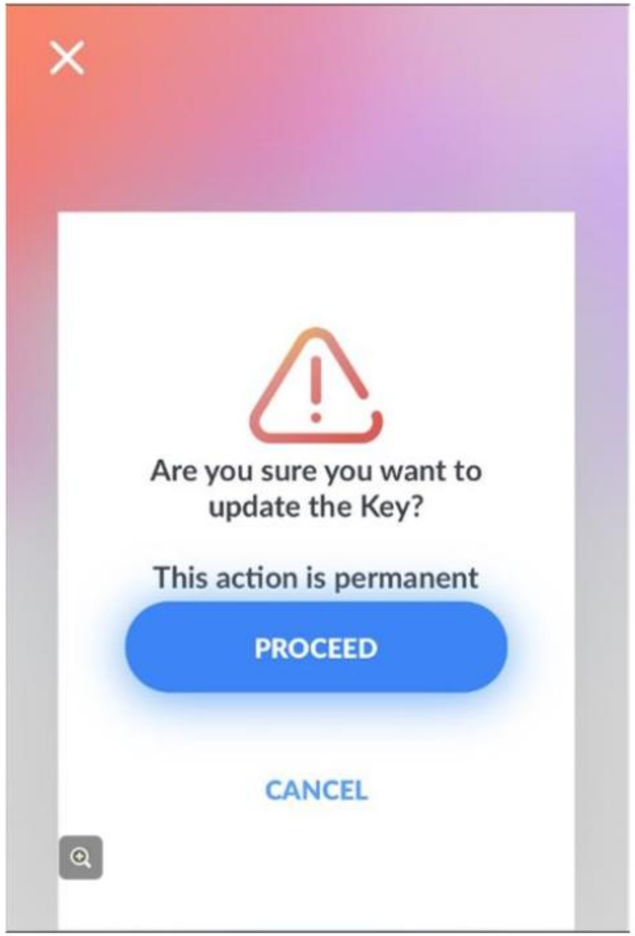
The maximum amount of attempts to update Key is 20 per 24 hours.

2d0c099a4ed7e05ac12e3a637
d5d19e5f8ce3e50369495babb
08033b6309811eea307774a5
9fa7fbe0ad495debfa42a43f2e

Checking and updating the Device key

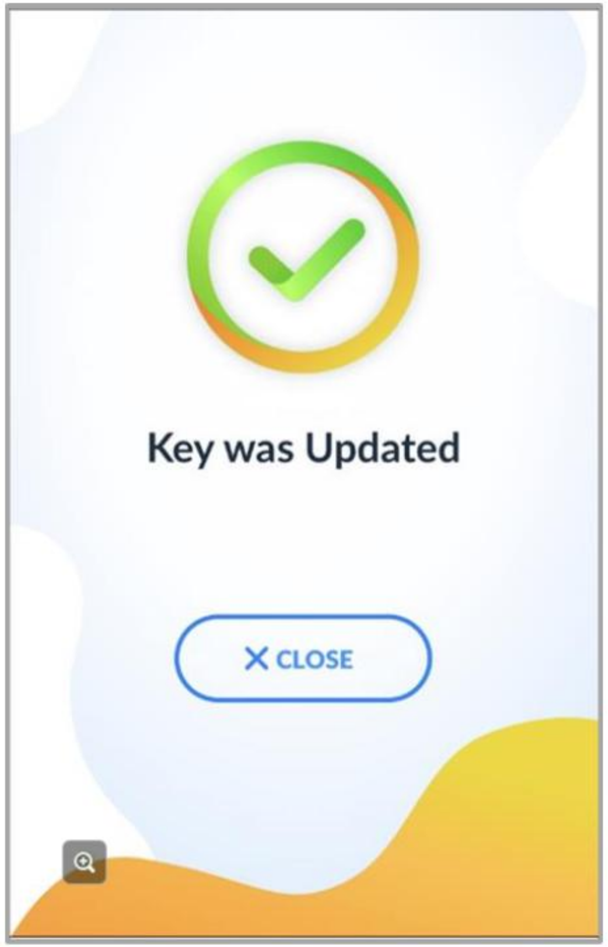
- Confirm the action by tapping **PROCEED**.
- A **Key was Updated** message will be shown if the update was successful. The key will be sent to the Portal and saved in the database.

Attention: The Mobile application **Update Key** will automatically set up the device personality (either Standard or Security Pack).



Are you sure you want to update the Key?

This action is permanent



Key was Updated

Step 1 2 3

Transfer device

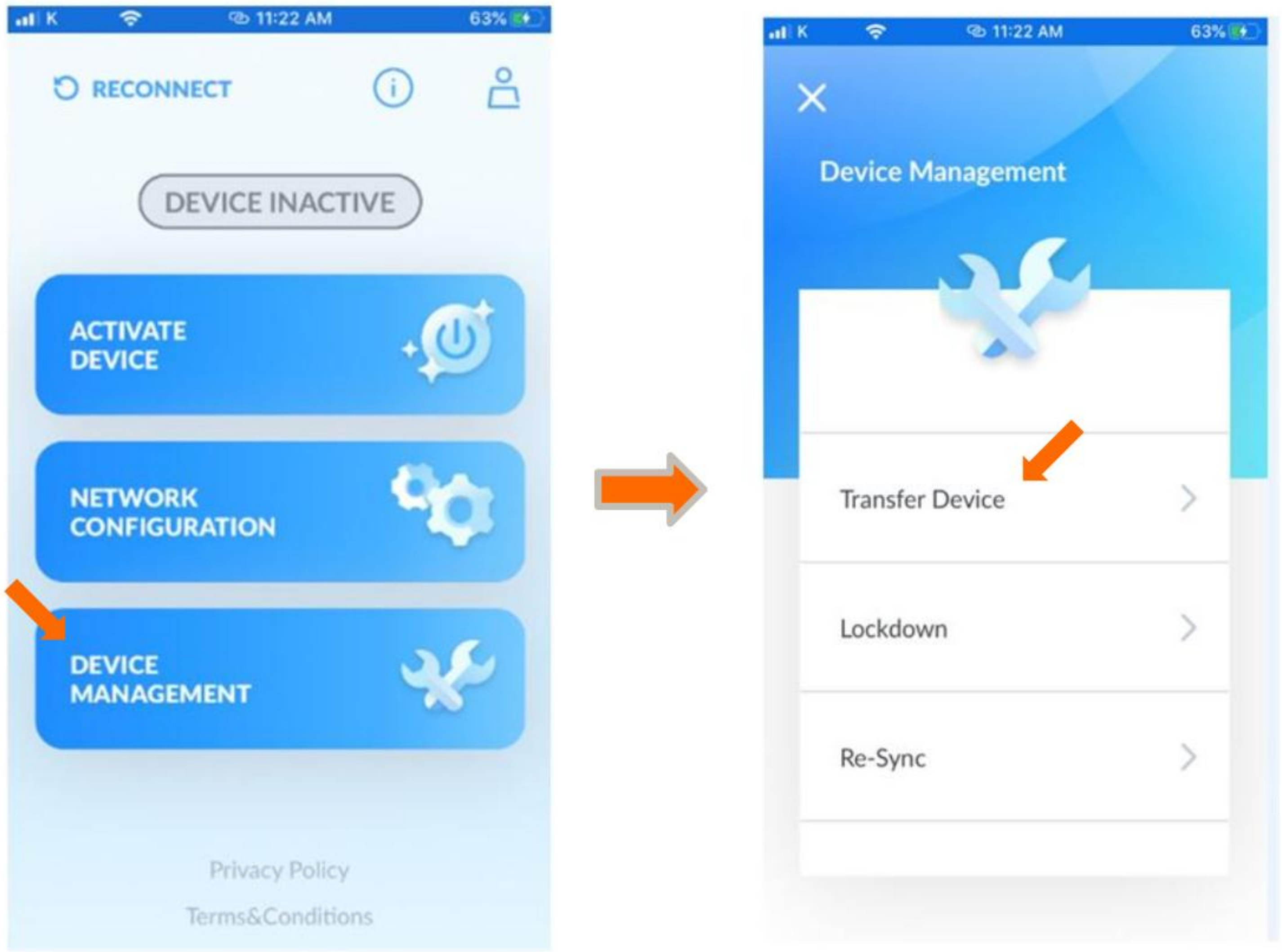
The **Transfer** option allows users to send one or more devices to another organization.

Click each number in turn to see the procedure.

Step 1 2 3 4

Transfer device

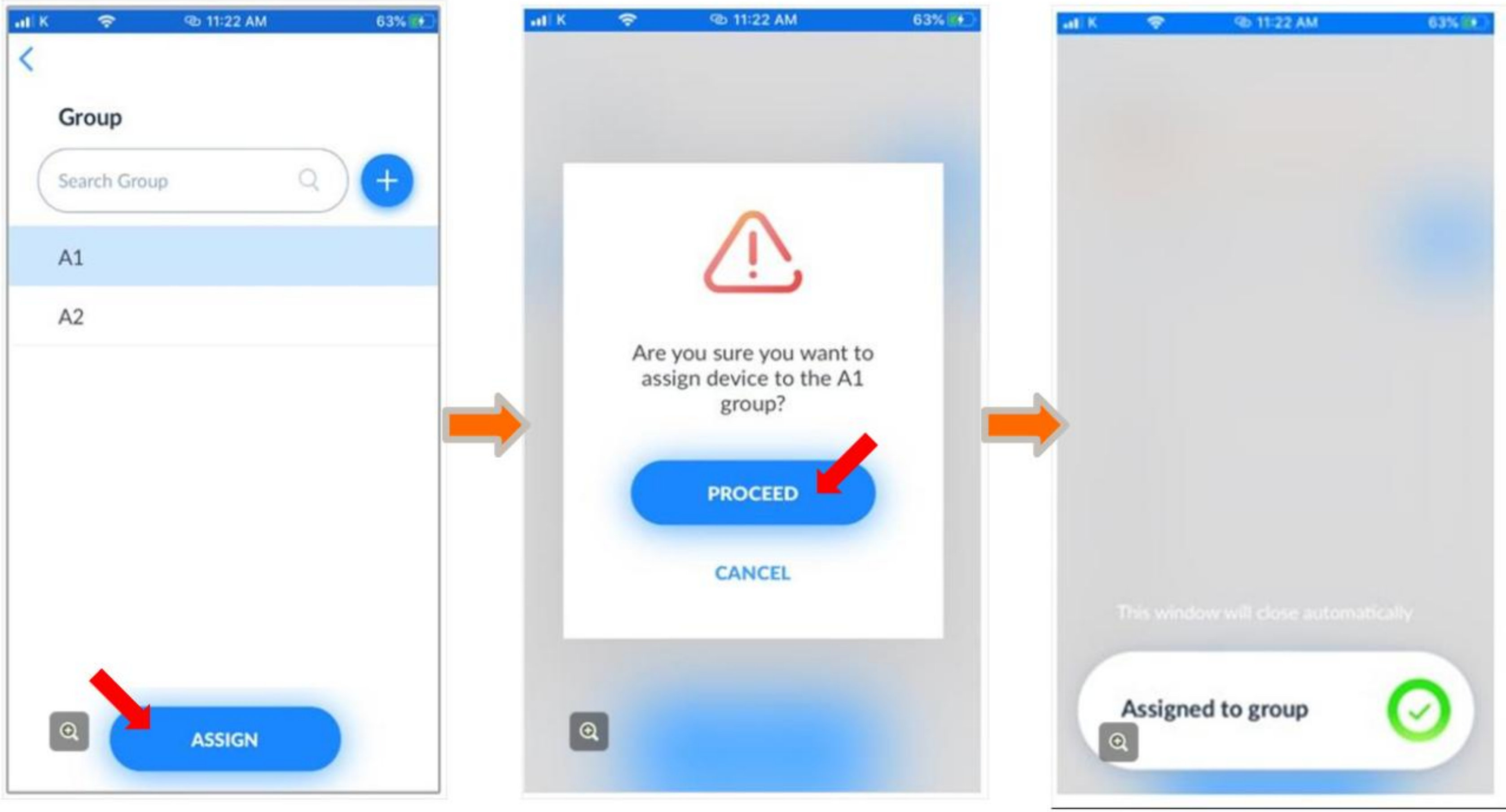
- Make sure you have read the **Connecting to a device** section of this course.
- Tap **DEVICE MANAGEMENT**.
- Tap **Transfer Device**.



Step ① ❷ ❸ ❹

Transfer device

- To assign a device to a group, select the group you want to assign a device to, and tap **ASSIGN**. You can also type the name of the group into the **Search Group** field and tap the **Magnifying glass** icon to find the group from the list.
- Confirm the action by tapping **Proceed** in the pop-up window.
- An **Assigned to group** message will be displayed to show that the action was successful.



Are you sure you want to assign device to the A1 group?

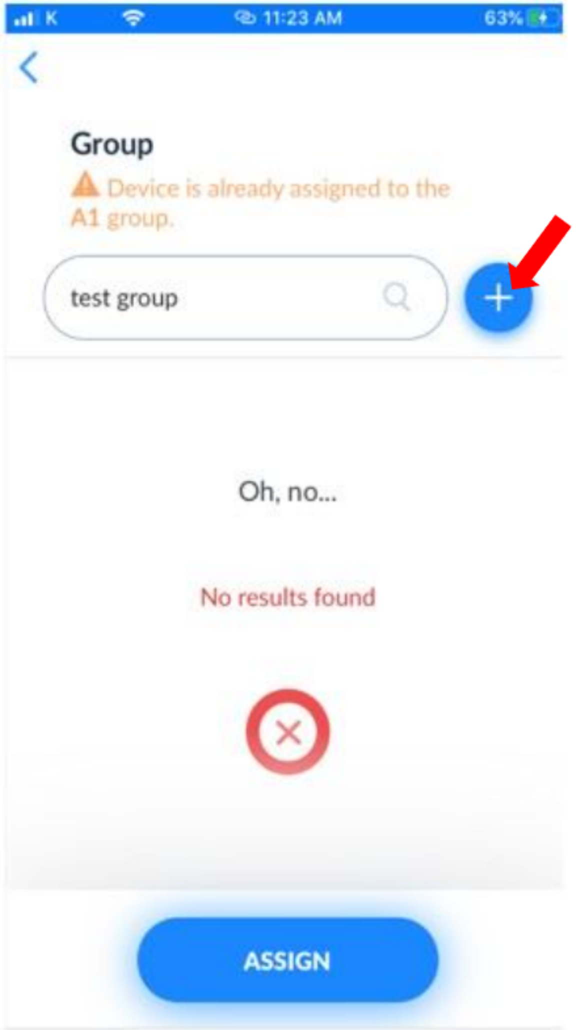
This window will close automatically

Assigned to group

Step 1 2 3 4

Transfer device

- You can create a new group by tapping the **+** icon next to the search field.
- Confirm the action by tapping **PROCEED** in the pop-up window.
    - **Note**: If a device is already assigned to another group, the previous group will be overwritten.



11:23 AM 63%

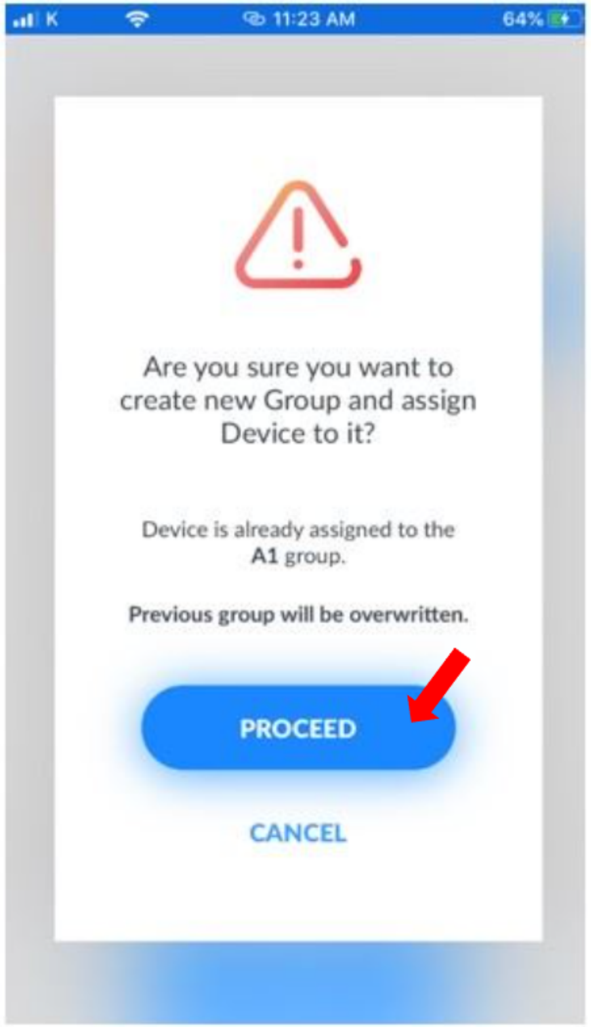
Group

⚠ Device is already assigned to the A1 group.

test group

Oh, no...

No results found



11:23 AM 64%

Are you sure you want to create new Group and assign Device to it?

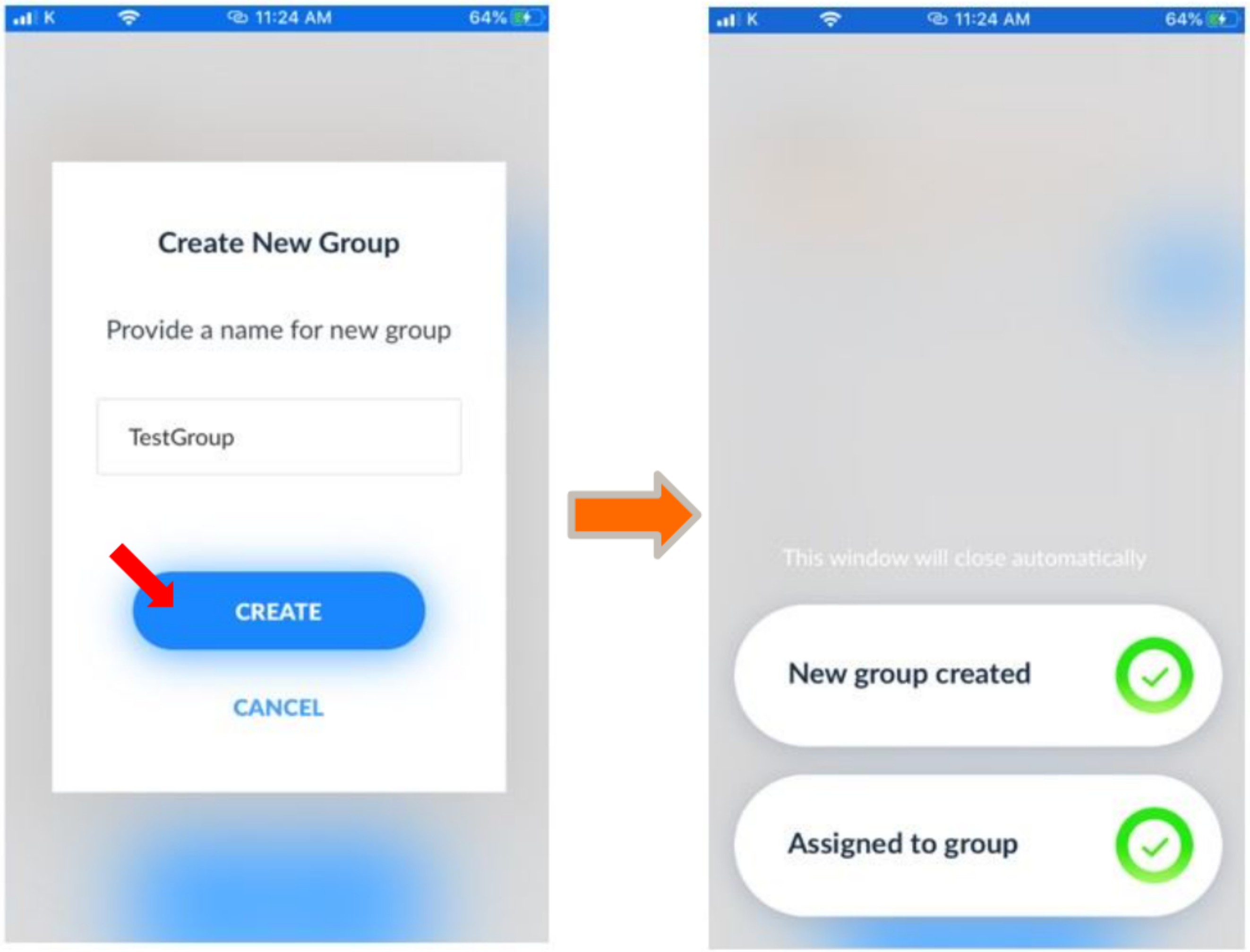
Device is already assigned to the A1 group.

Previous group will be overwritten.

Step 1 — 2 — 3 — 4

Transfer device

- Enter a name for the new group, and tap **CREATE**.
- Messages will be displayed to show that the new group was created and that a device was assigned to the new group.



Create New Group

Provide a name for new group

TestGroup

This window will close automatically

New group created

Assigned to group

Step 1 2 3 4

Activate system lockdown mode

The **lockdown** option allows users to put a device in lockdown mode for transportation (for security reasons). This is an option for devices that have already been activated and had value added to them but which then need to be shipped to a business partner.

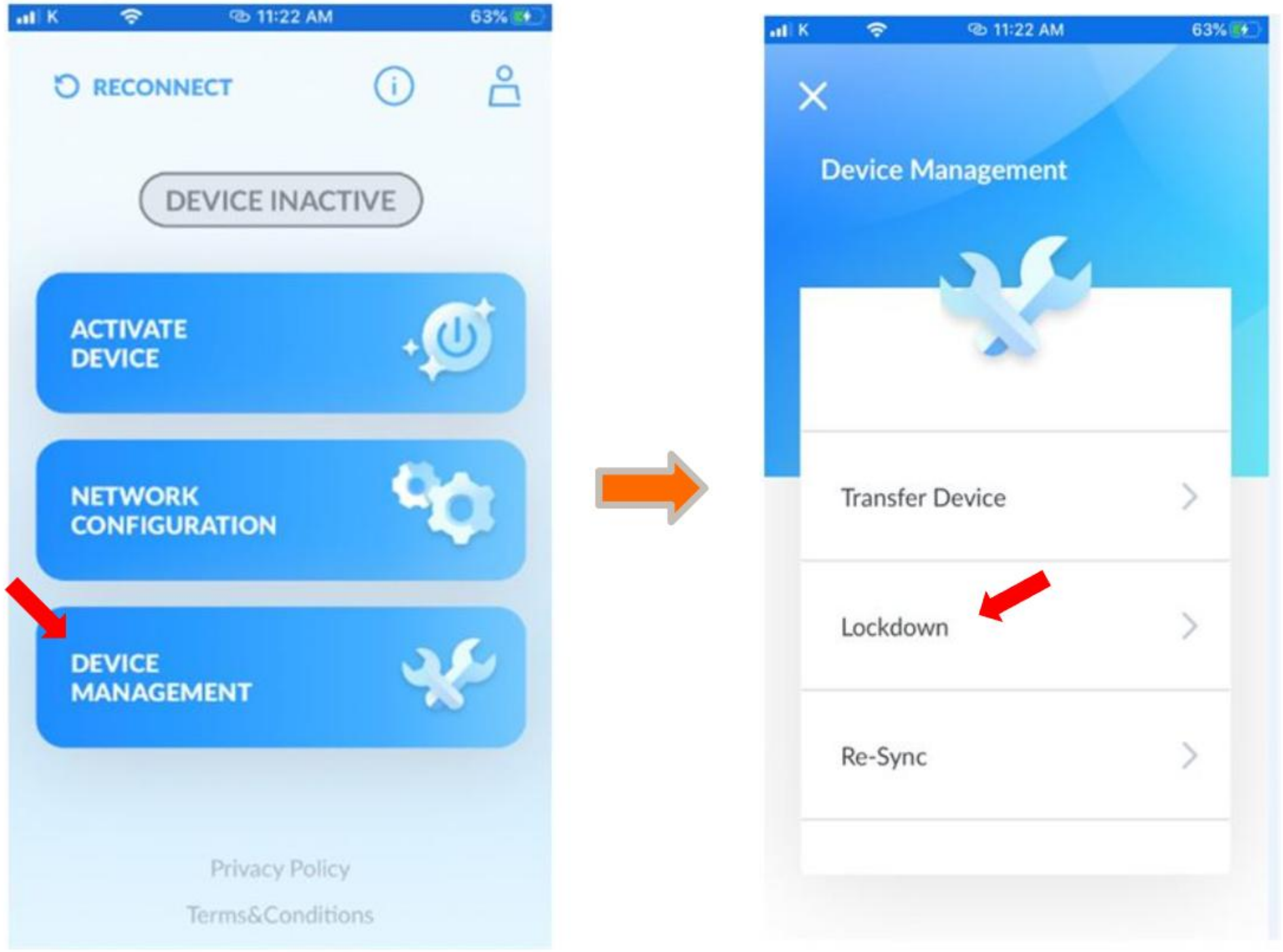
Click each number in turn to see the procedure.

Step 1 — 2

Activate system lockdown mode

- Make sure you have already read the **Connecting to a device** section of this course.
- Tap **DEVICE MANAGEMENT**.
- Tap **Lockdown**.

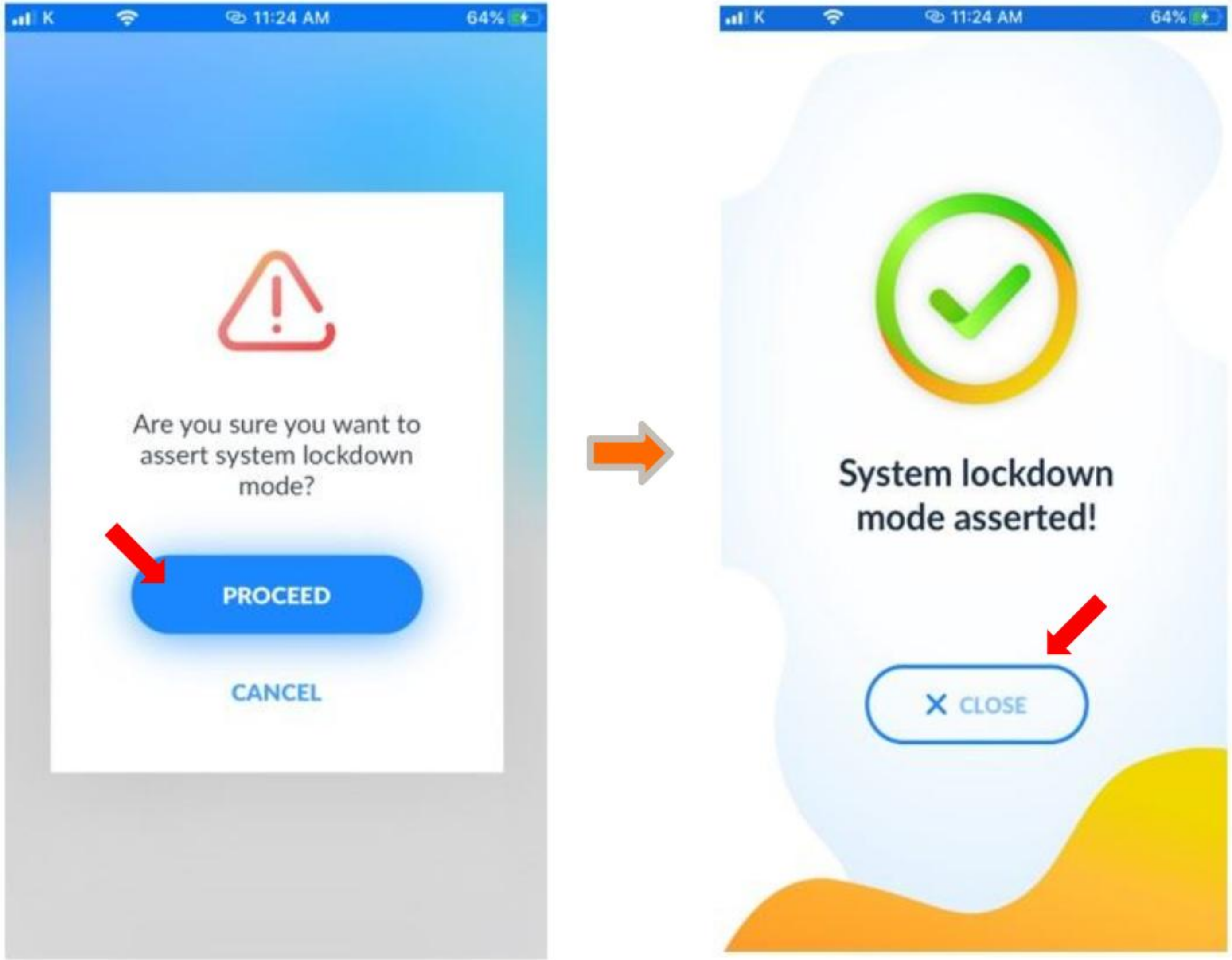
Step 1 2



Activate system lockdown mode

- Confirm the action by tapping **PROCEED** in the pop-up window.
- A **System lockdown mode asserted** message will be displayed. The status of the device will change to **Inactive**. Tap **Close** to return to the Menu screen.

Step 1 2



Are you sure you want to assert system lockdown mode?

System lockdown mode asserted!