KVL5000

QUICK REFERENCE GUIDE

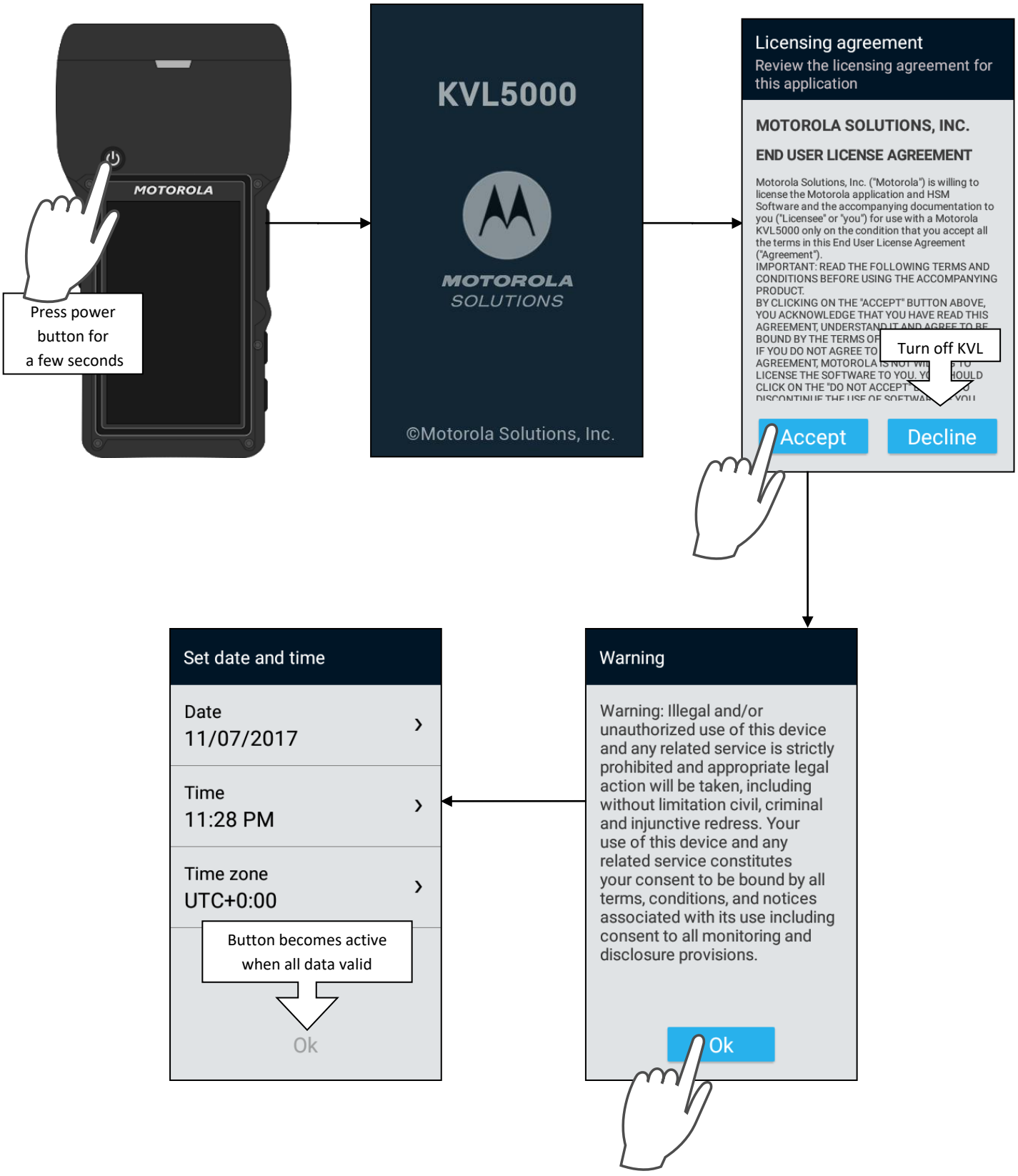
MARCH 2025

MN005847A01-G

Contents

First Launch

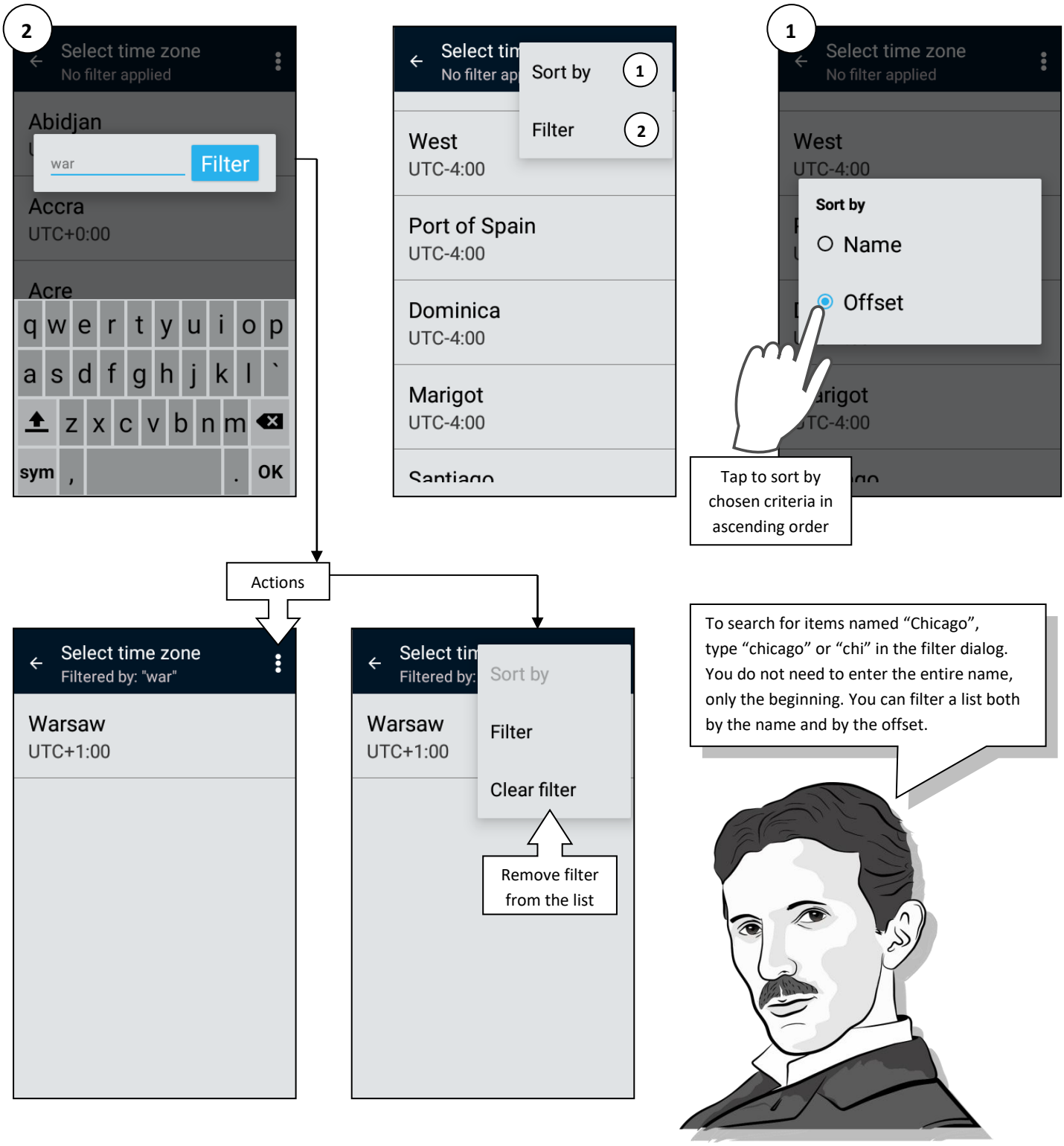
When you launch the Key Variable Loader (KVL) for the first time, you need to configure passwords and set time and date.



Date & Time

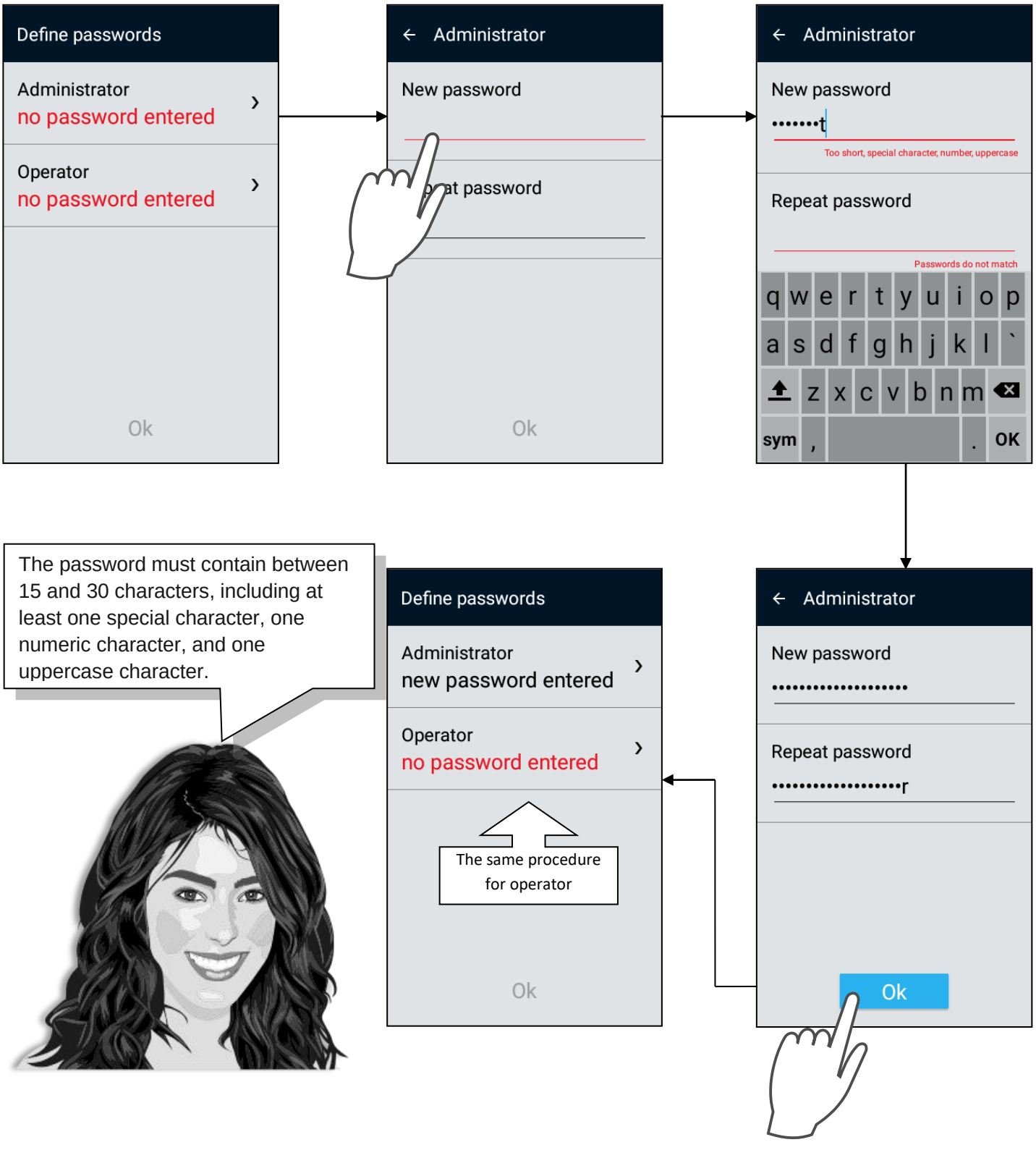
Choose date, time and time zone. You can change these settings later.

Time Zone filtering/sorting options



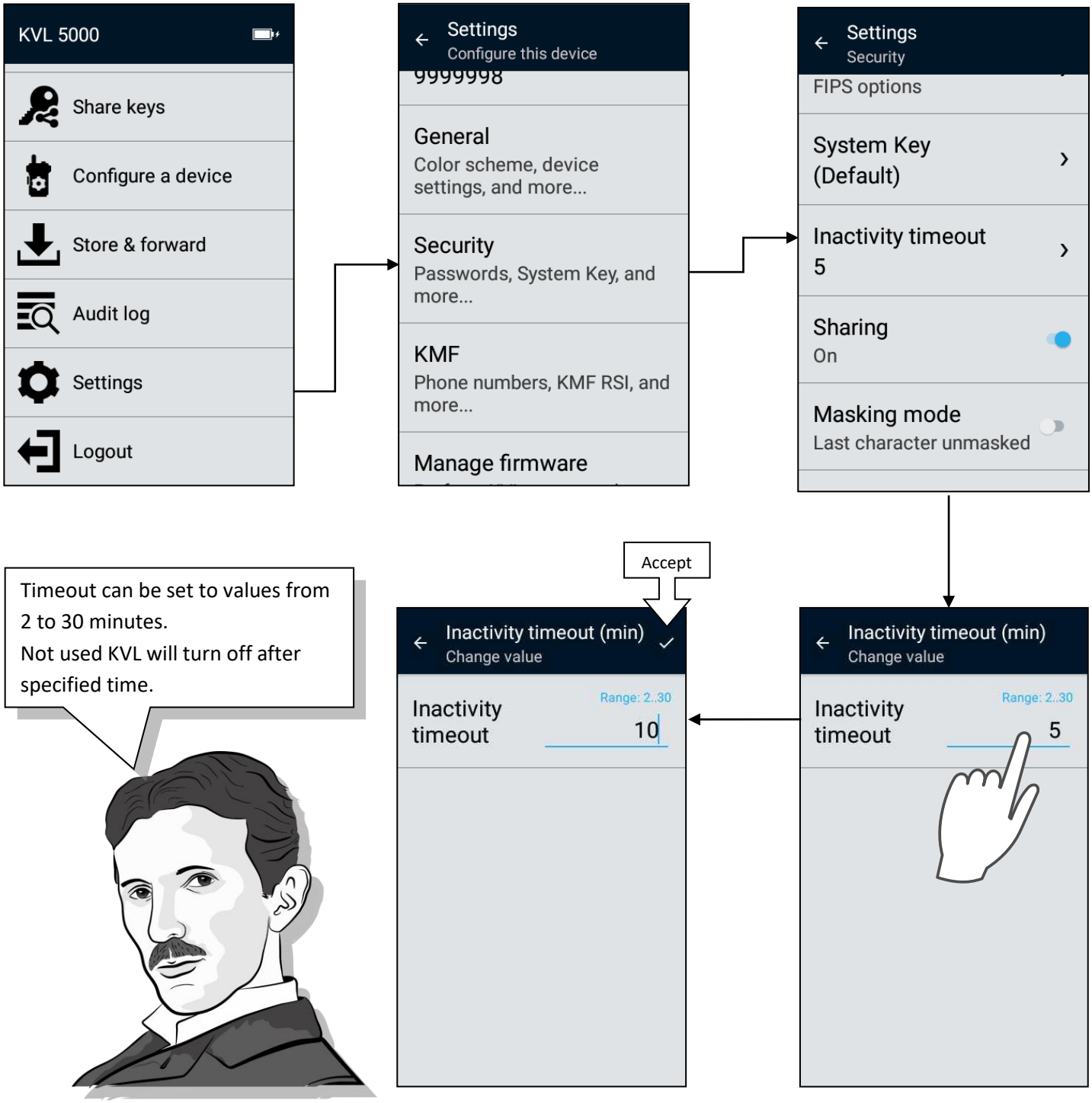
Define passwords

Setup passwords for both Operator and Administrator



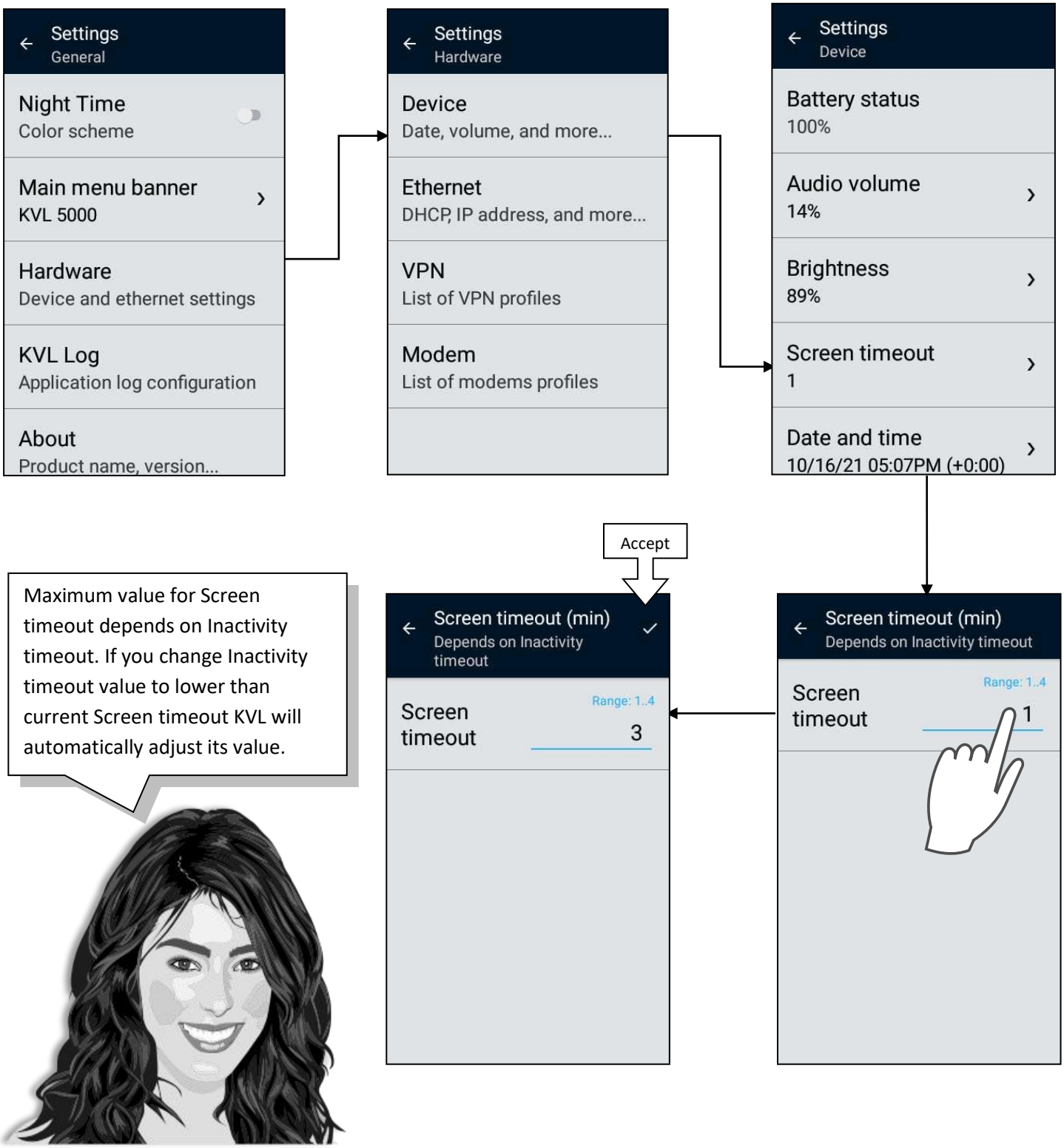
Inactivity timeout

Reduces unnecessary battery drain | Default set to 5 minutes | Only Administrator can change this



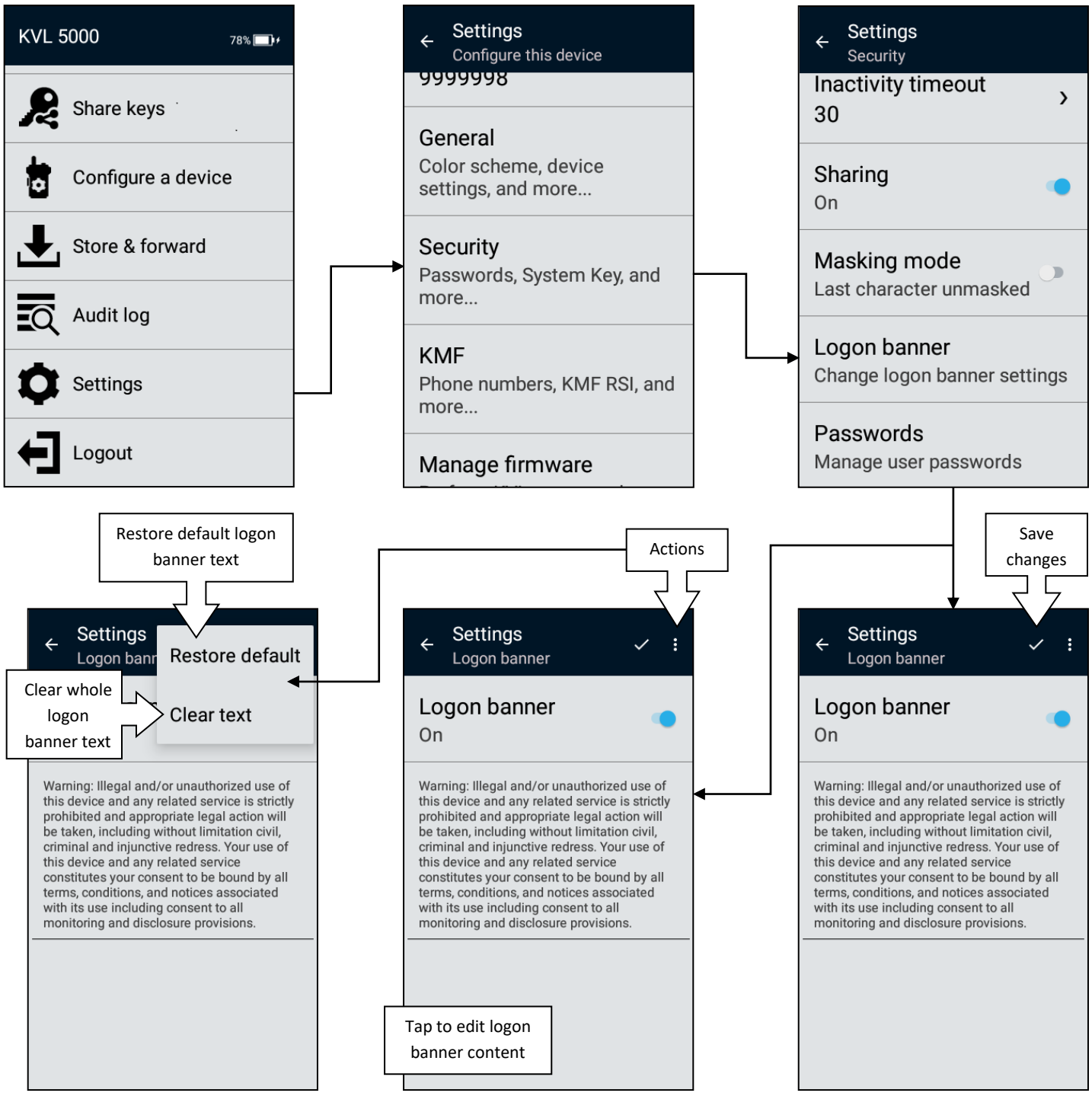
Screen timeout

Allows to set time before KVL's screen turns off | Default set to 1 minute | Depends on Inactivity timeout



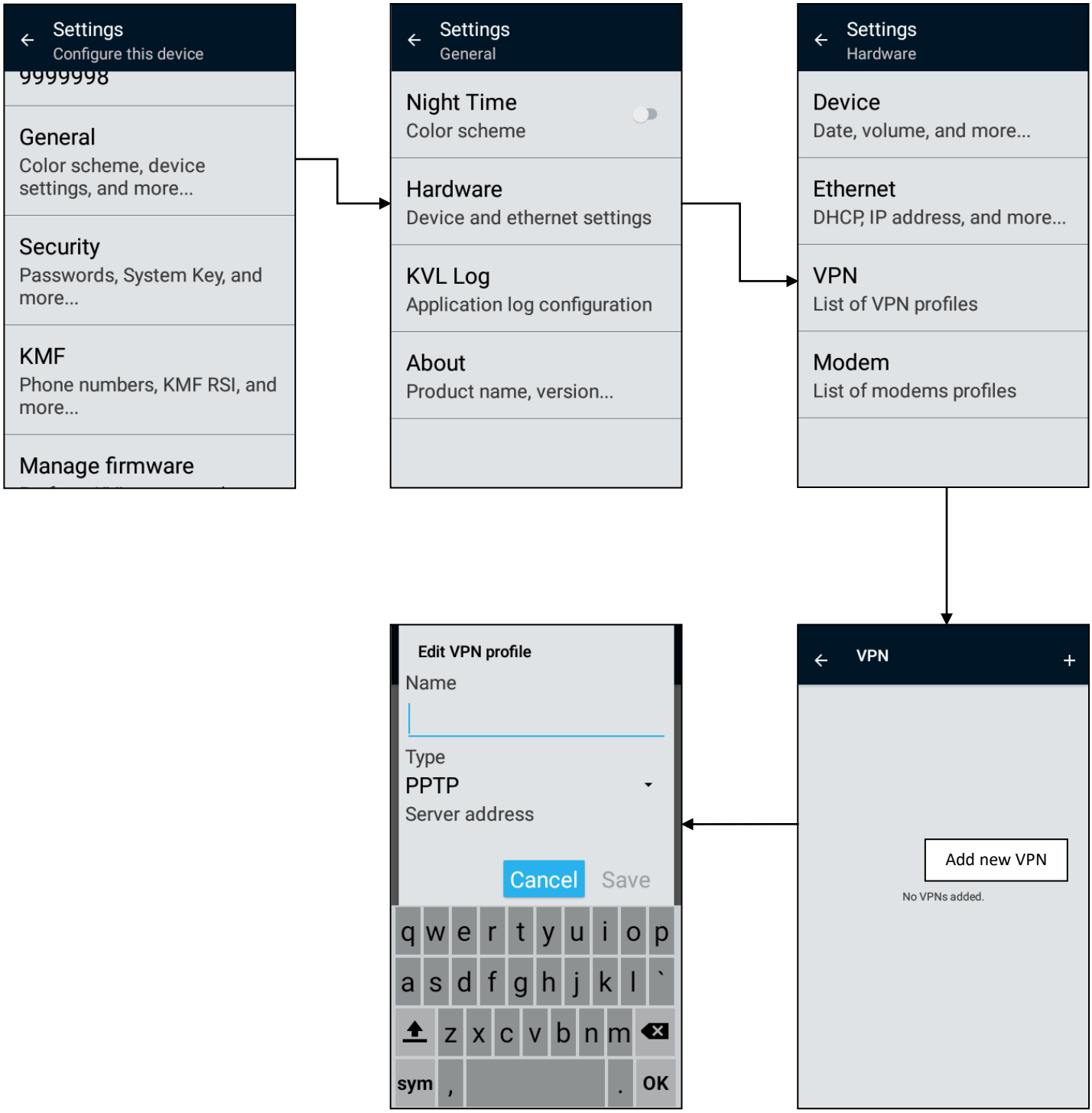
Logon banner

Information displayed when KVL starts | Only administrator can change this



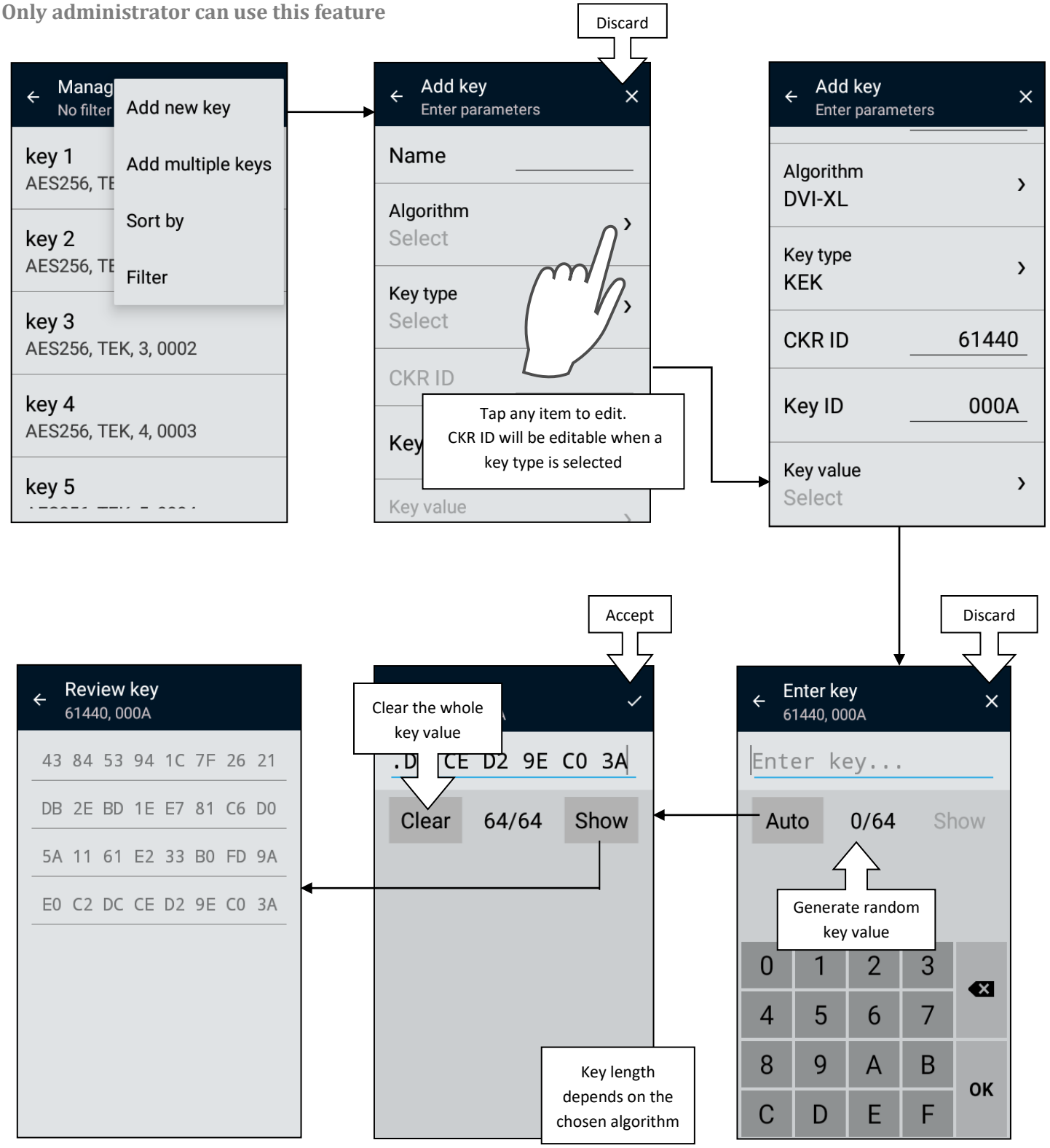
VPN

Setup Virtual Private Networks | Only Administrator can manage this



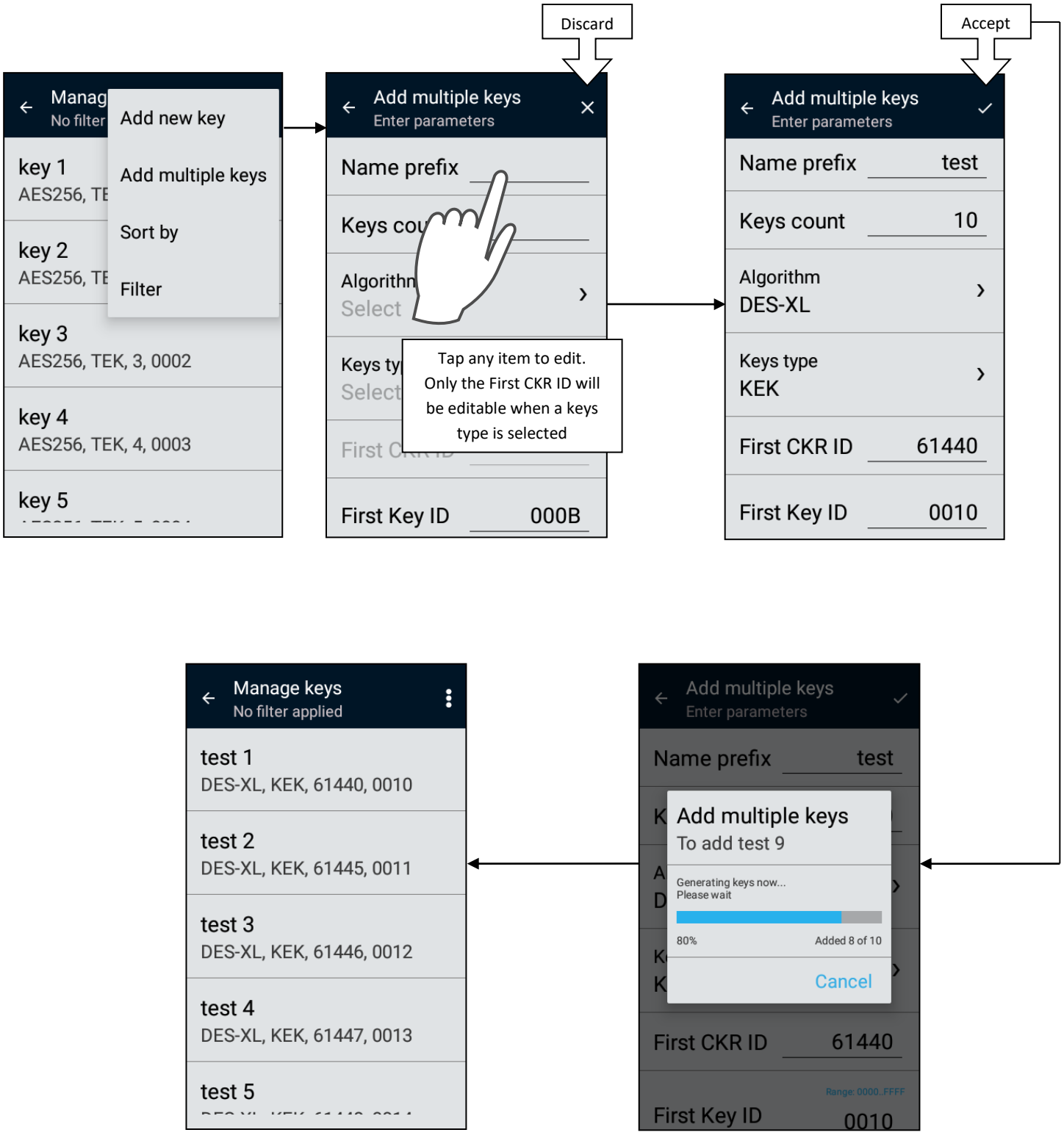
Add single key

Only administrator can use this feature



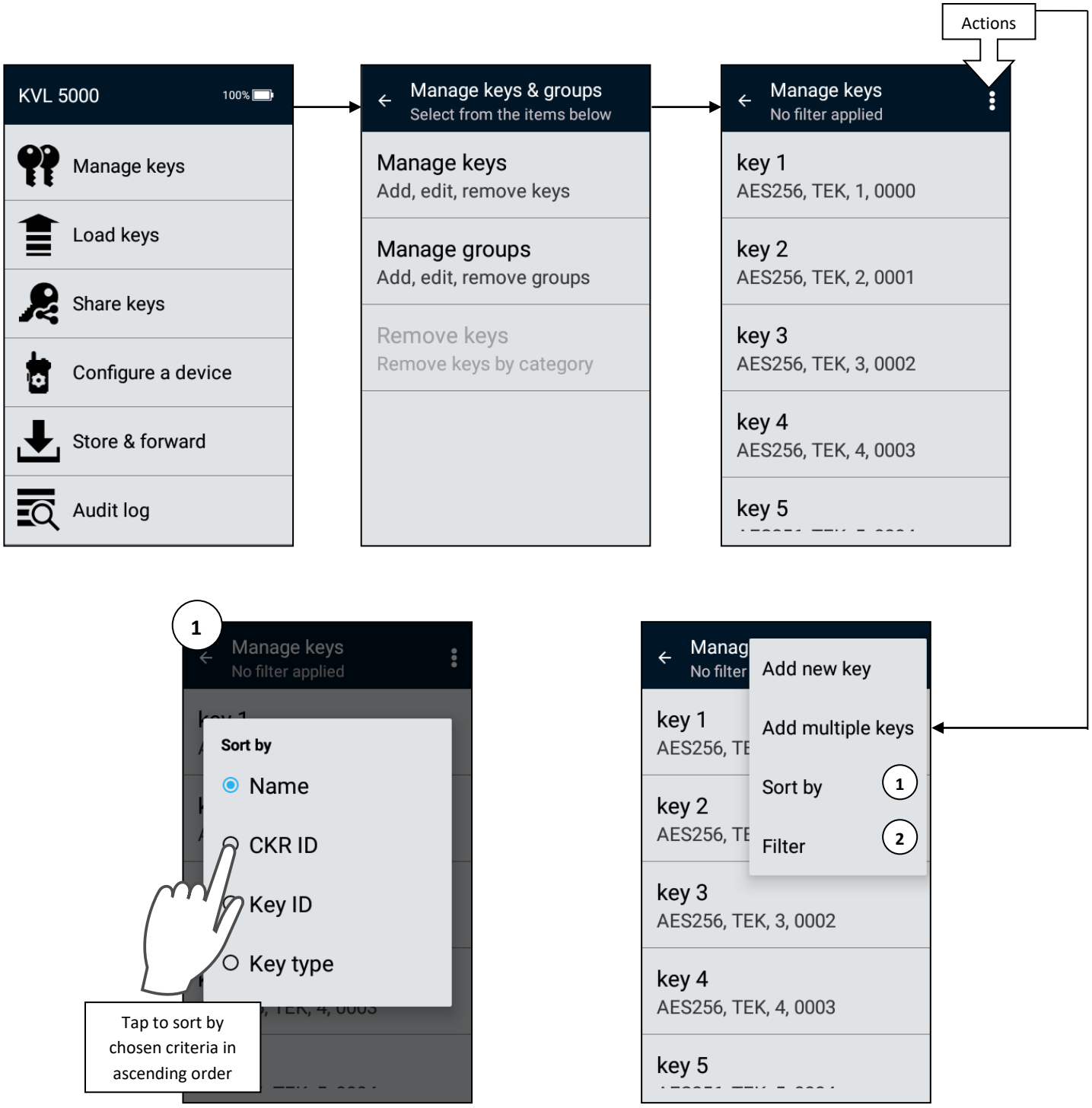
Add multiple keys

Add sequence of keys with autogenerated value | Only Administrator can manage this

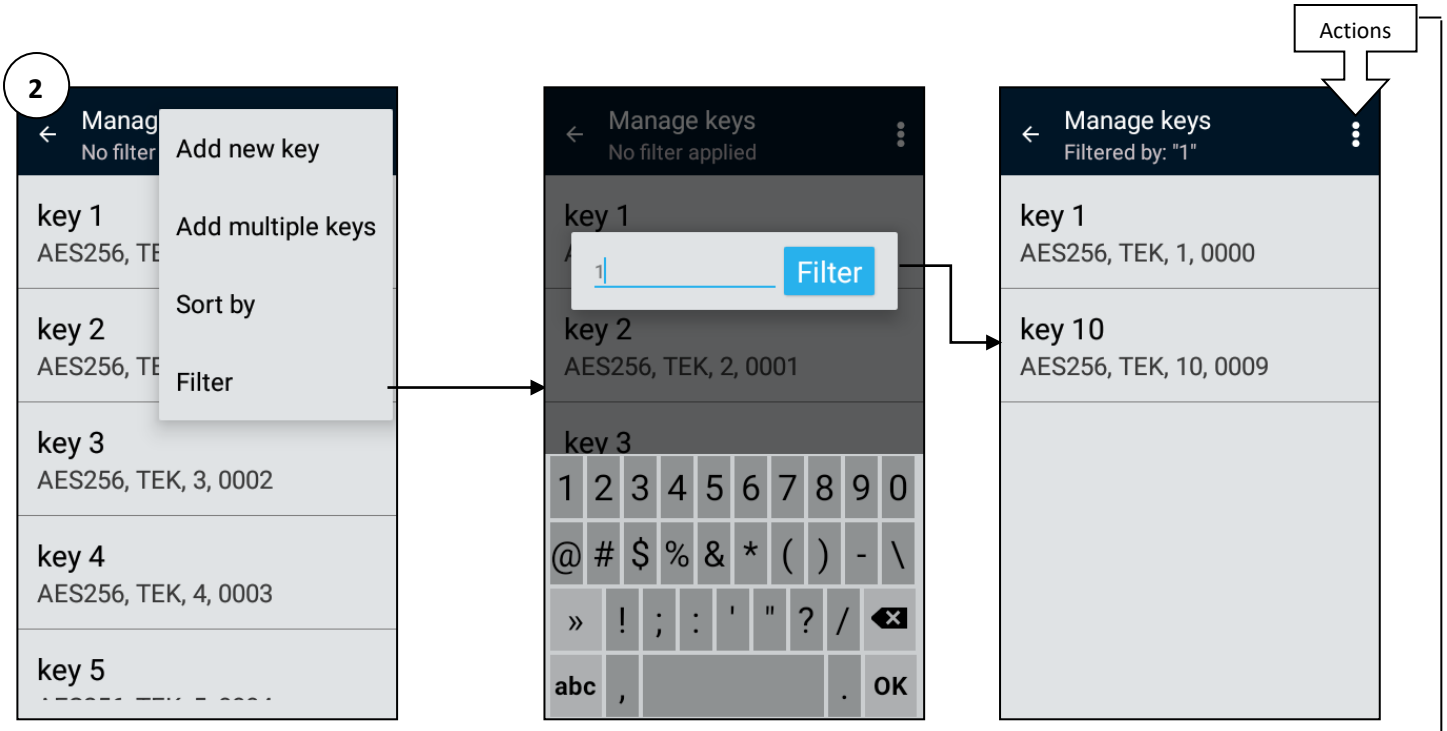


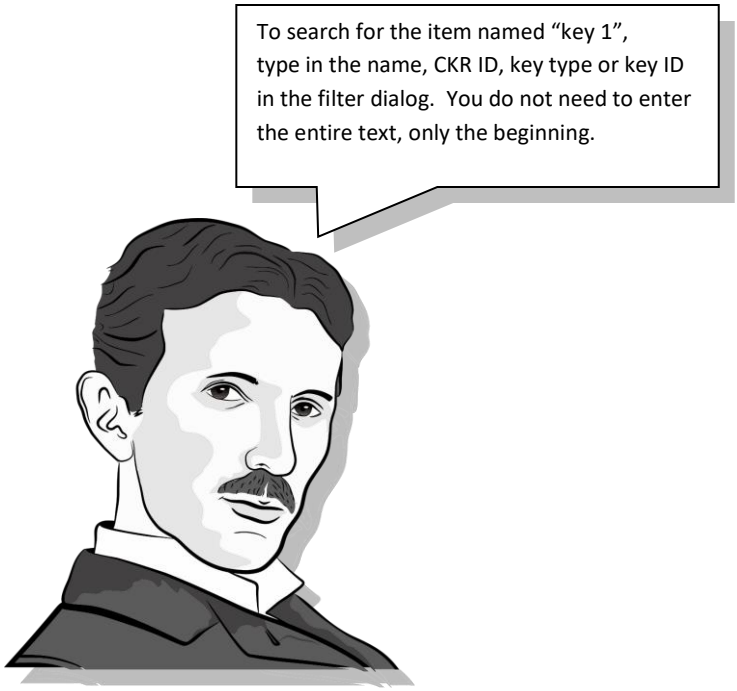
View and sort keys' list

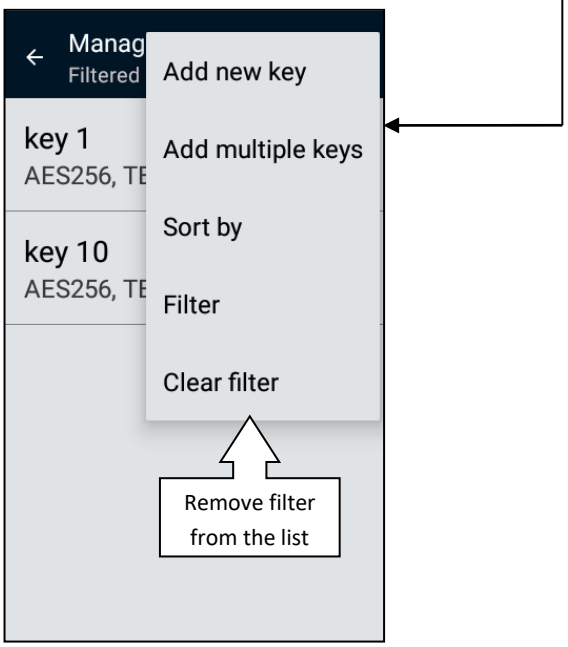
The KVL supports up to 1024 keys at a time



Filter keys' list

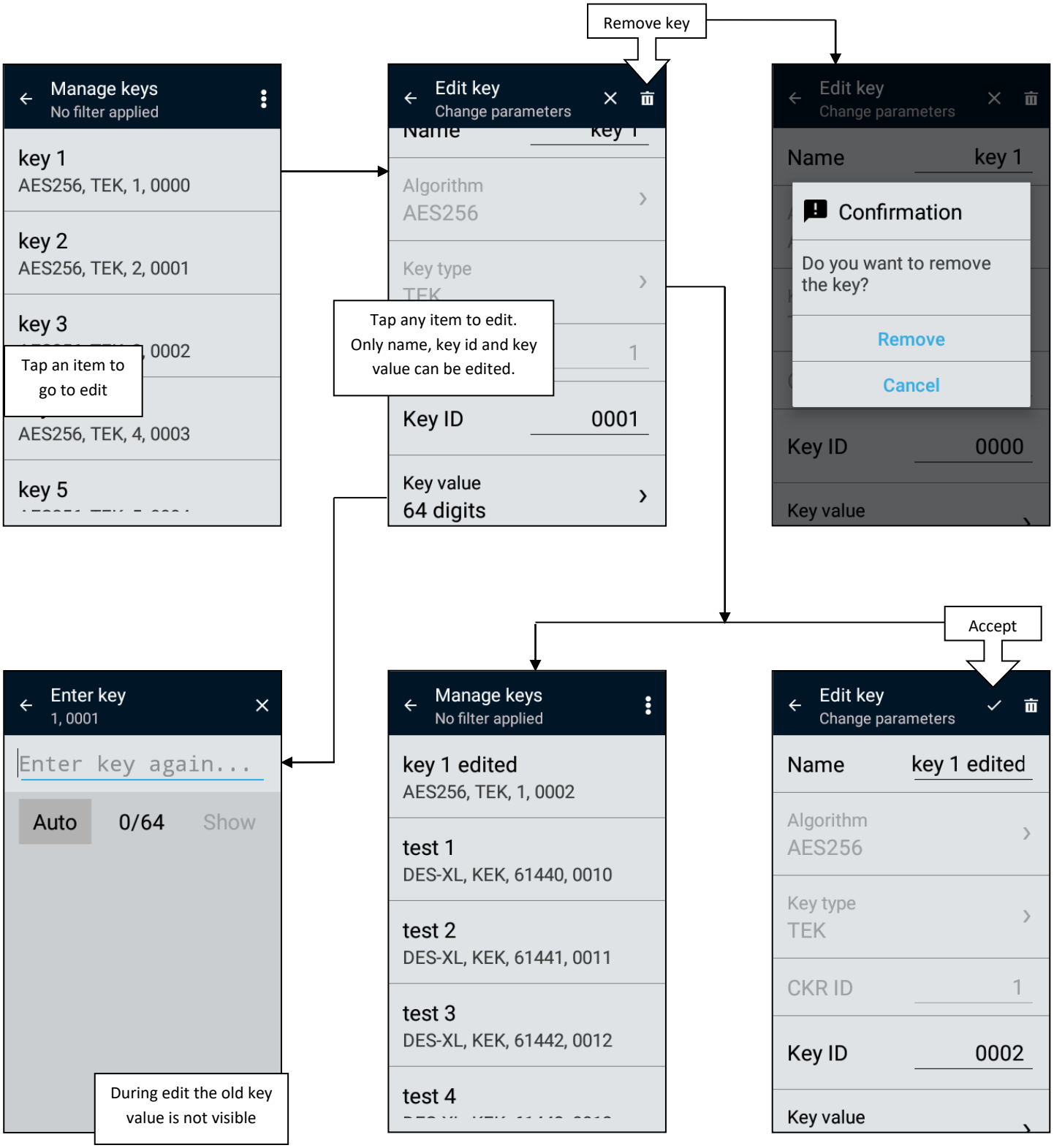






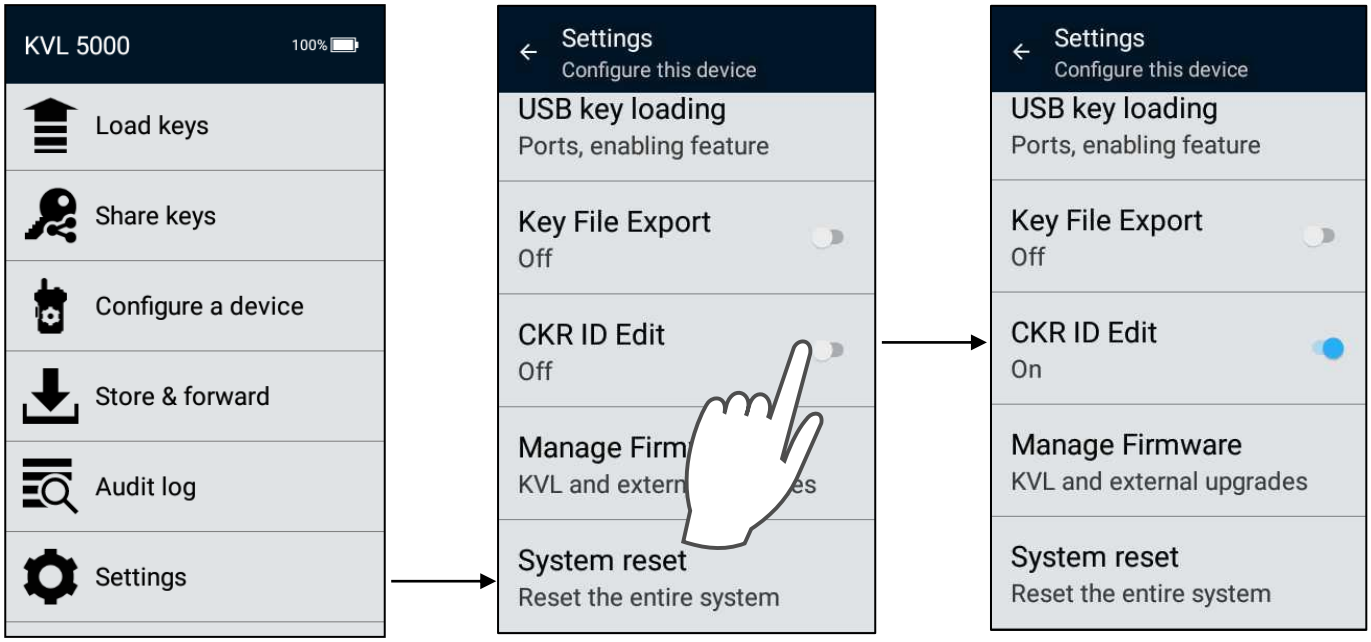
Edit key

Edit name, key ID or key value | Delete the key | Only Administrator can manage this



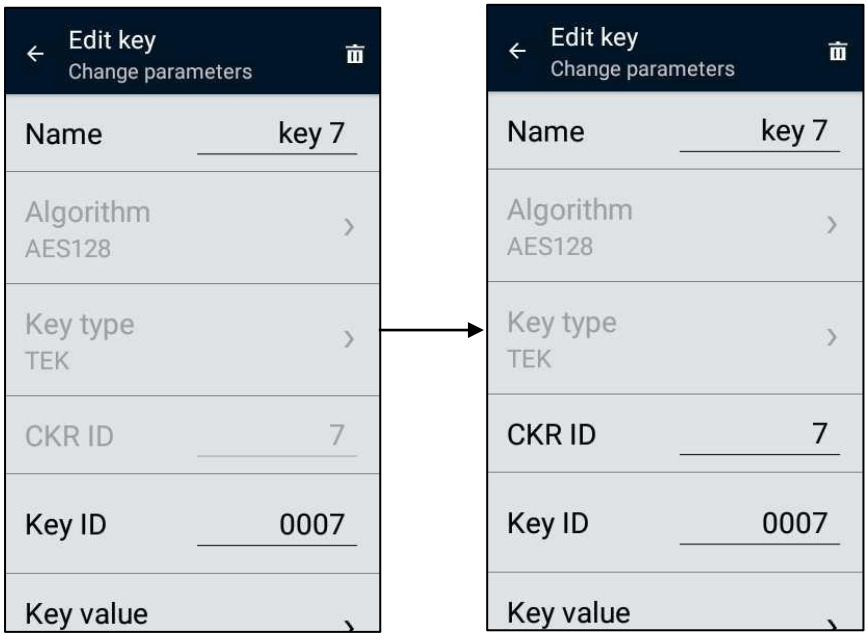
Edit key

Edit CKR ID | Only Administrator can manage this



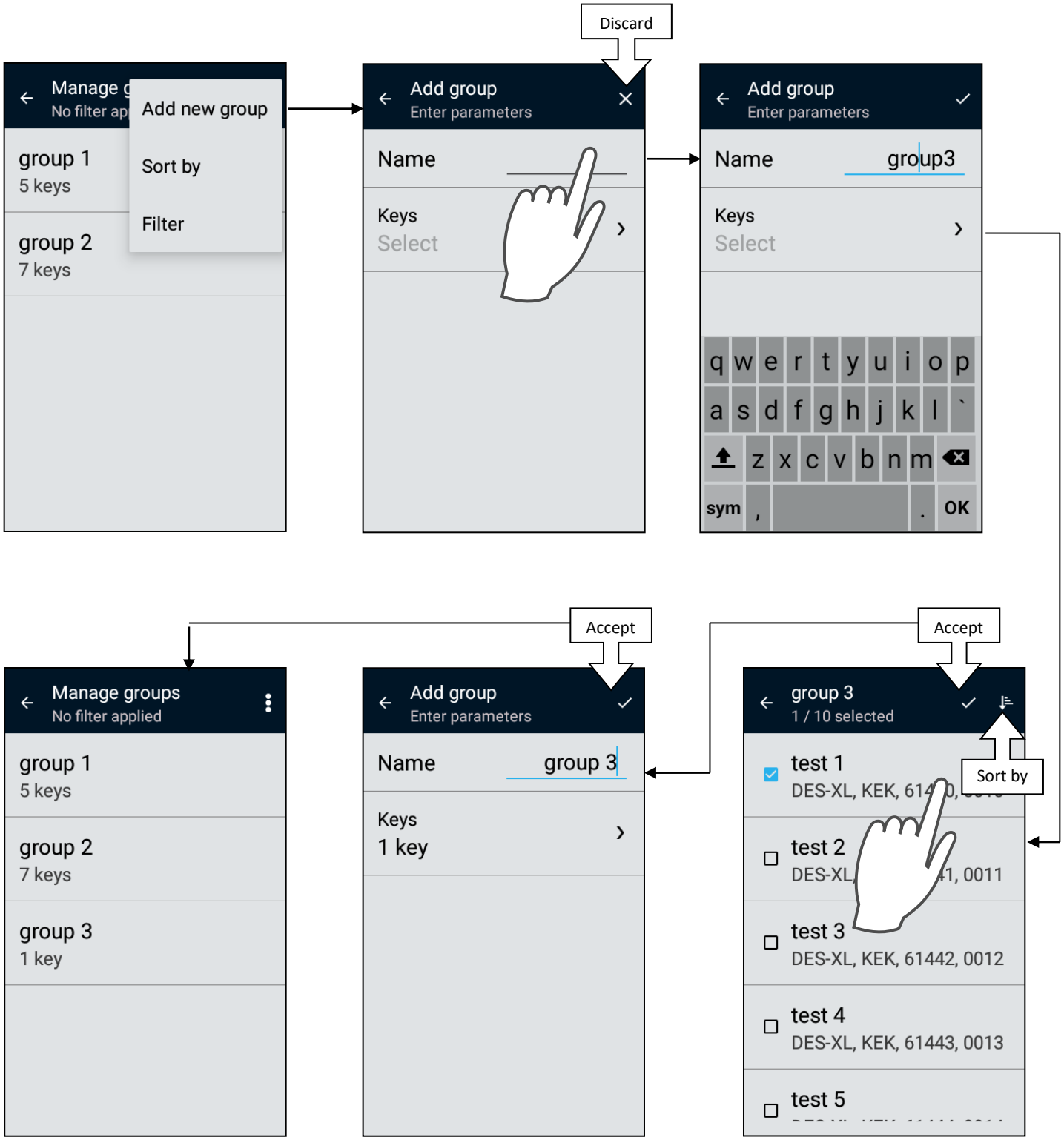
KVL Administrator can enable CKR ID Edit in KVL Settings.

KVL Operator with Manage Keys permission can edit CKR ID when the setting is switched on.



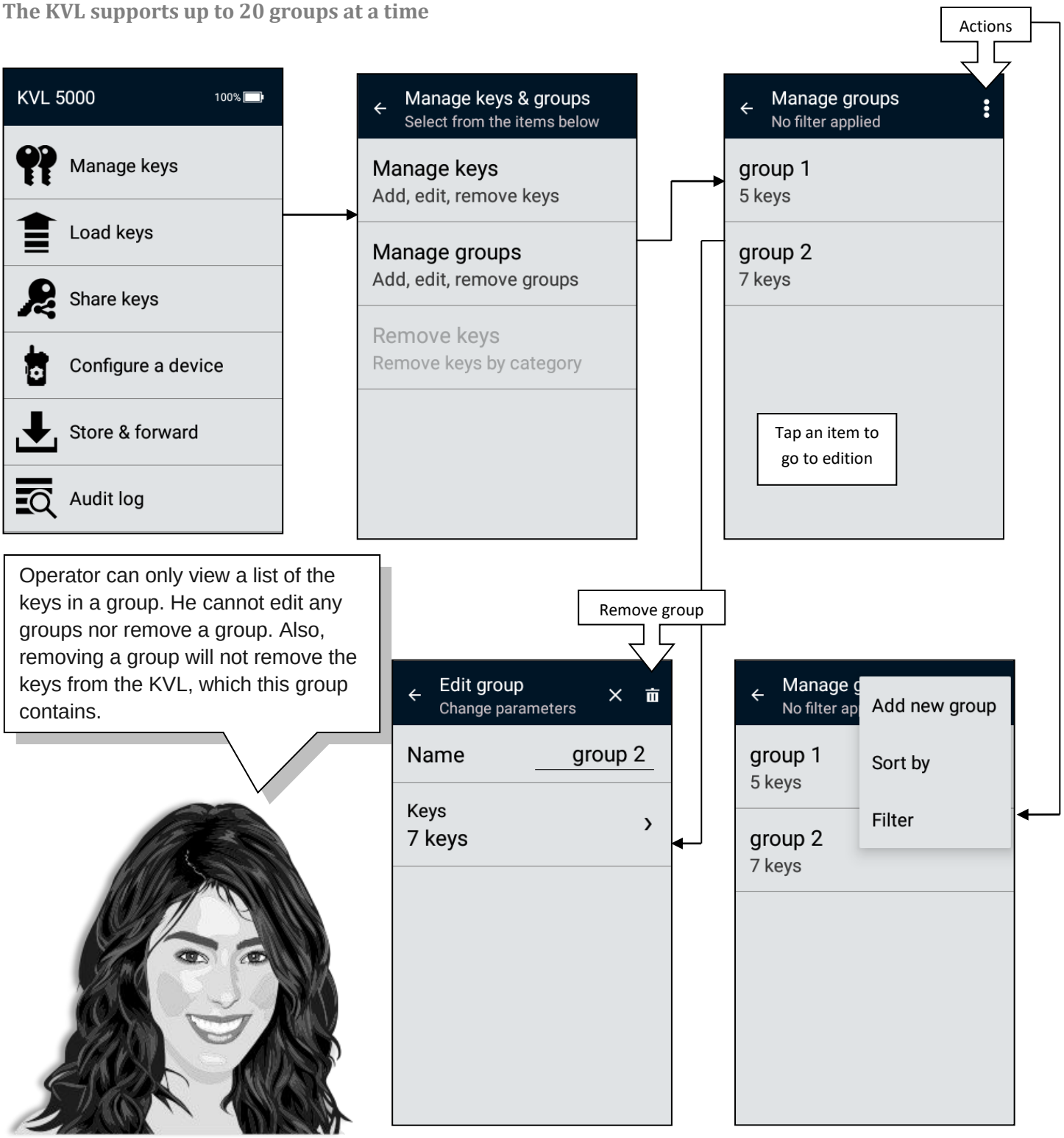
Add new group of keys

Only administrator can use this feature



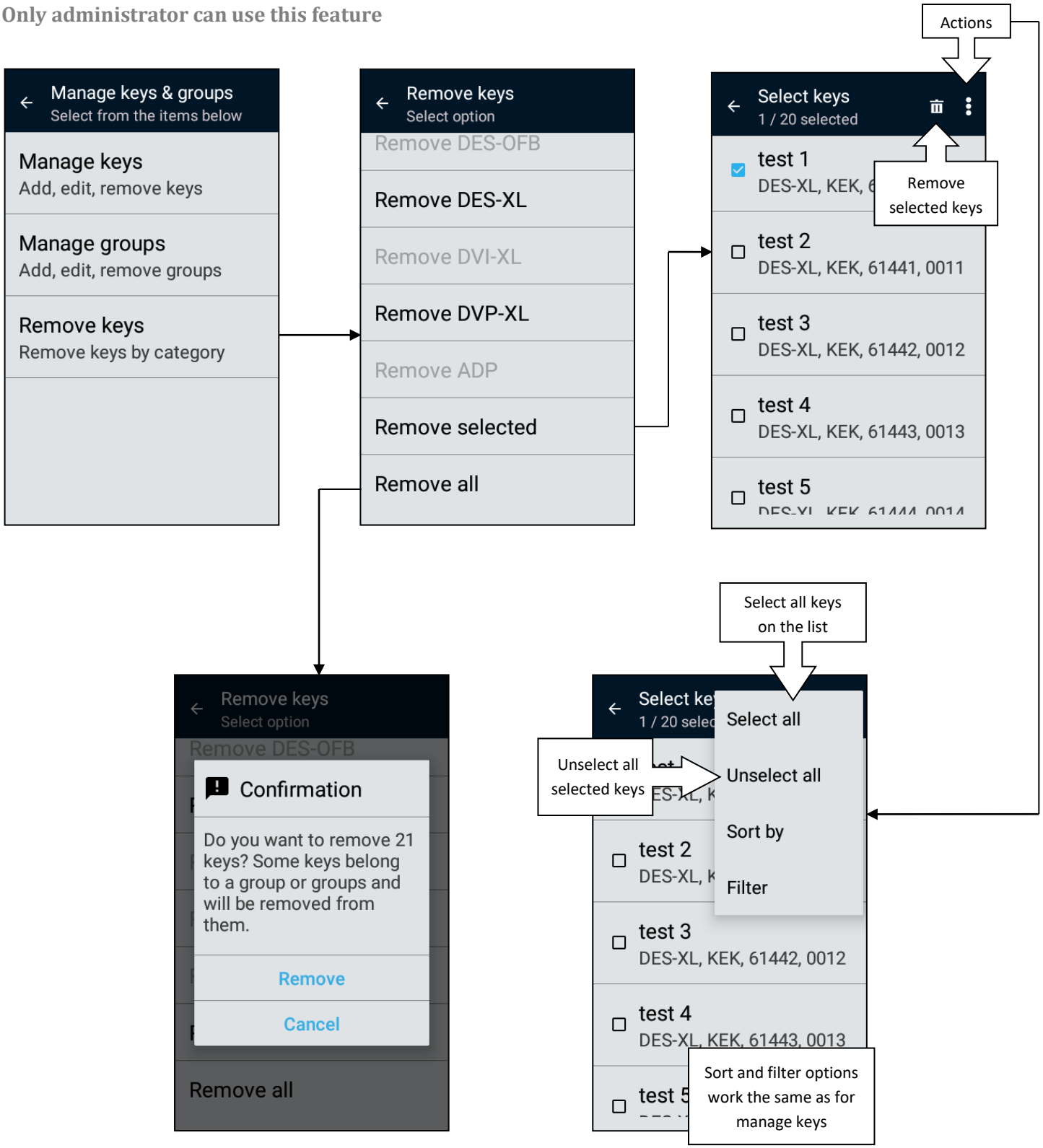
Manage group of keys

The KVL supports up to 20 groups at a time



Remove keys

Only administrator can use this feature



Key Profiles

Key profiles allow the user to manage keys, key groups and Tactical OTAR groups in separate logical storages. This allows much easier interoperability as you can store keys with the same CKR ID or the same key ID and algorithm combination on separate key profiles on one device.

Key Profile Configuration and Customization

The application includes one main Key Profile, which can support up to 1024 keys, and 50 secondary profiles, each capable of holding up to 100 keys. Additionally, each Key Profile has an independent limit for the number of groups and Tactical OTAR groups, with a maximum of 20 allowed for each.

To further aid in organization and identification, KVL Administrator can edit and personalize the name of each Key Profile, ensuring that each can be clearly labeled and easily recognized. The name of the active Key Profile is displayed on all screens that support Key Profile functions, keeping users informed. A quick tap on the hardware button allows users to swiftly navigate to the Key Profile management settings for easy adjustments.

Key Profile Clear

KVL Administrator can also clear given key profile when it is no longer needed or repurposed. Clearing key profile will remove all general keys, key groups and Tactical OTAR groups on given profile.

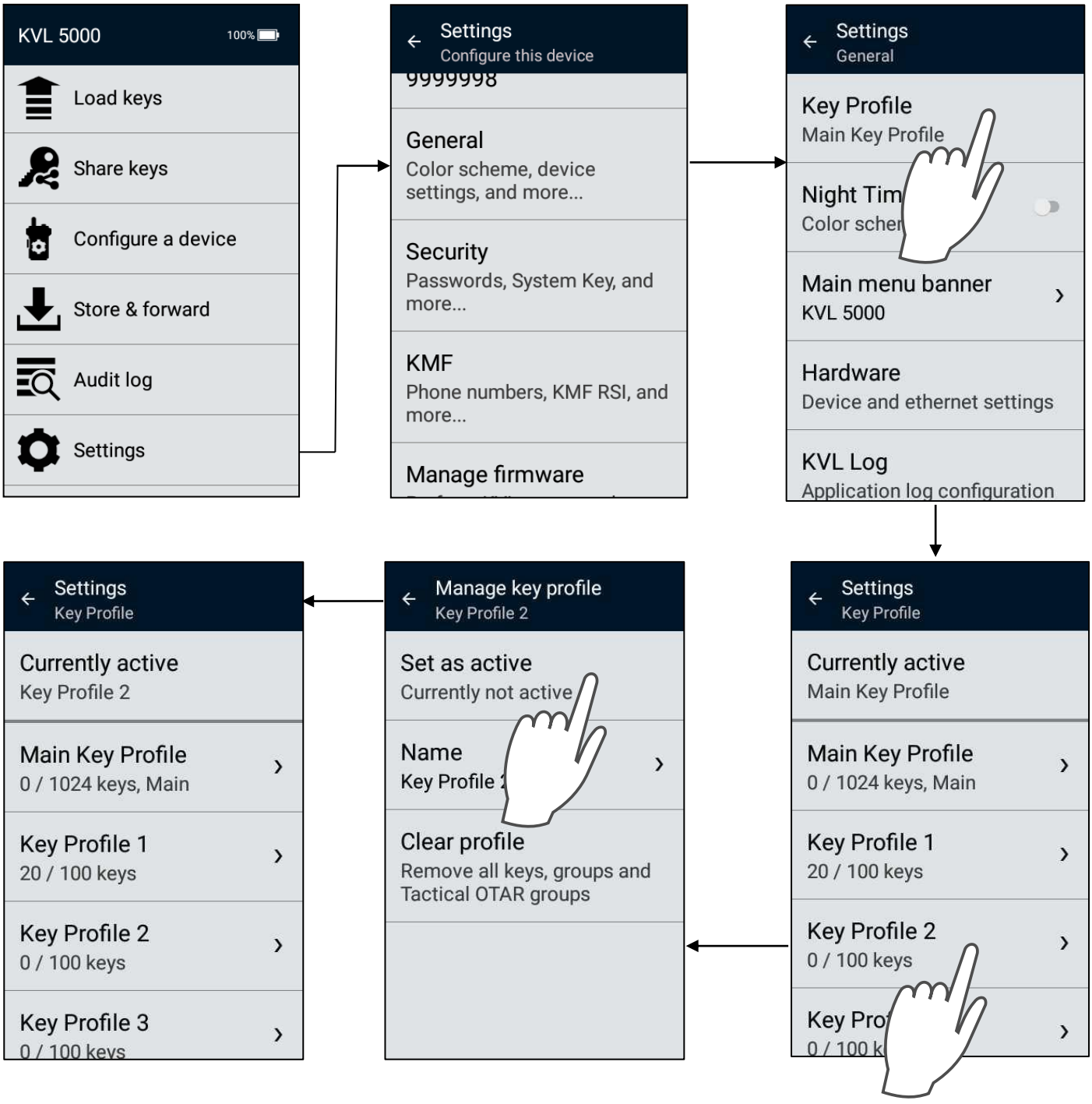
Store & Forward and Radio Authentication

Store & Forward, Radio Authentication and settings for mentioned operations are possible only within the Main Key Profile.

Transferring Keys Between Key Profiles

The application also offers the flexibility to move or copy multiple keys to another Key Profile, provided there are no conflicts, such as duplicate CKR IDs or algorithm and key ID pairs that already exist in the target profile. If any conflicts occur, users will be informed of them via a dedicated screen.

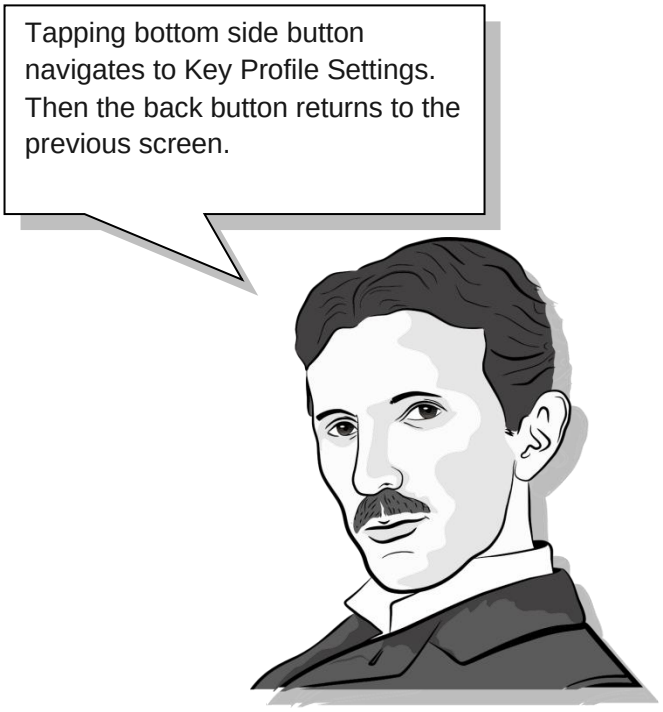
Setting active key profile



Setting active key profile

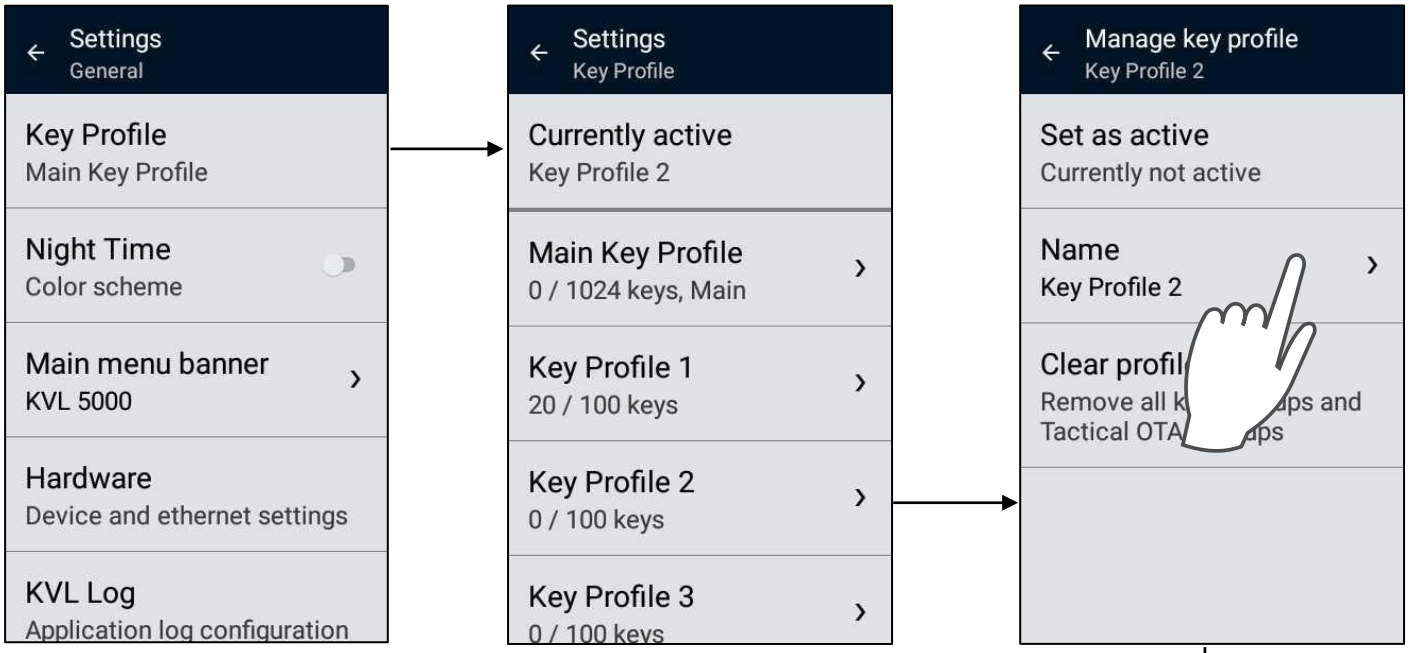
Setting active key profile may be quickly started by tapping the bottom button on the right KVL side. You can use this button to quickly change Key Profile when managing keys.

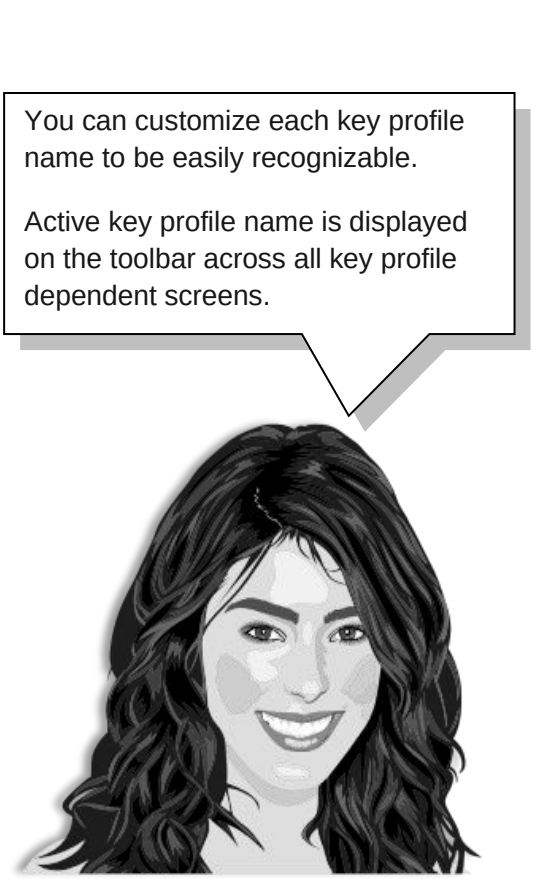
This button is disabled if any operation is in progress (for example share keys or upgrade).



Changing key profile name

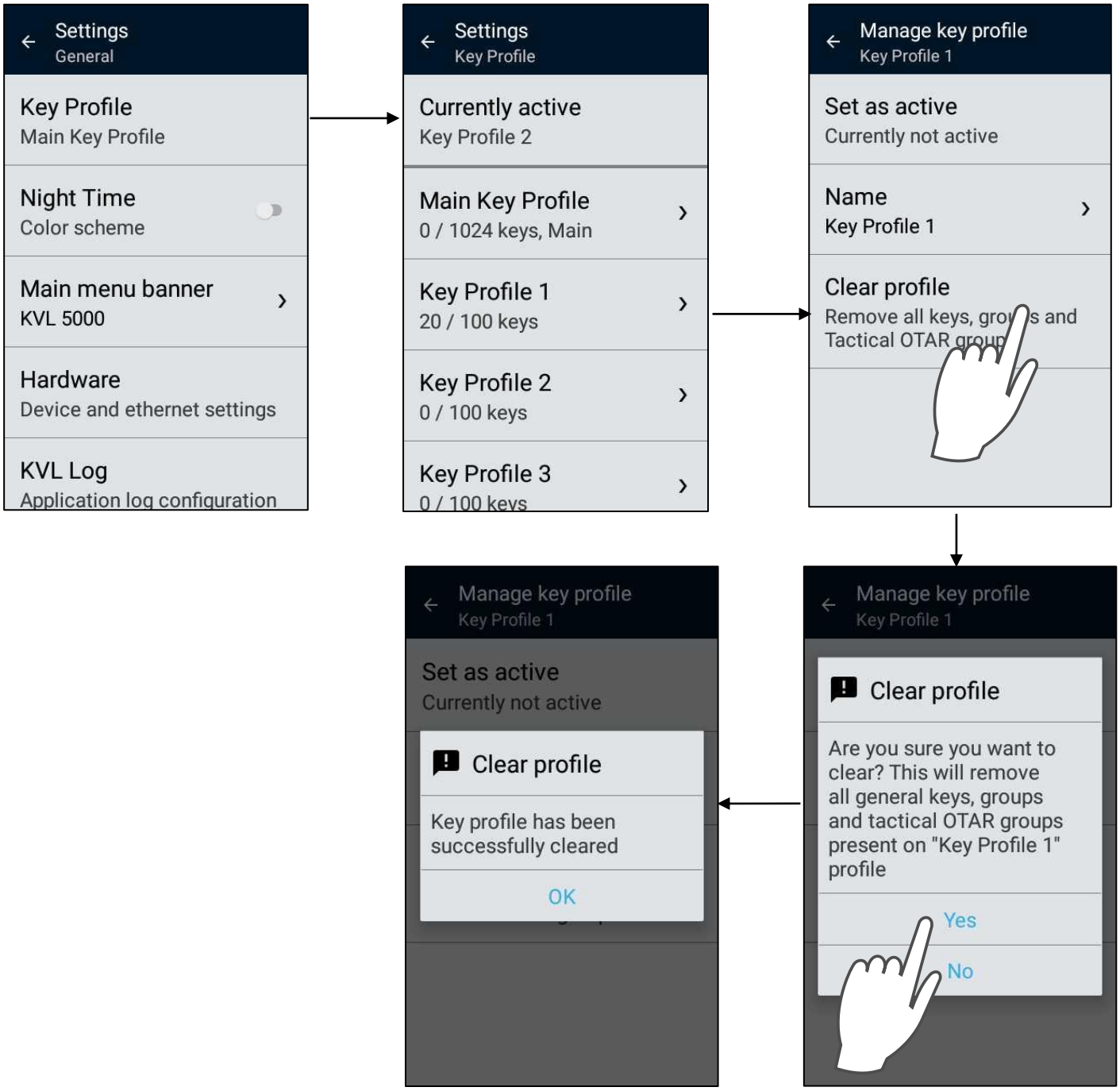
Only administrator can use this feature



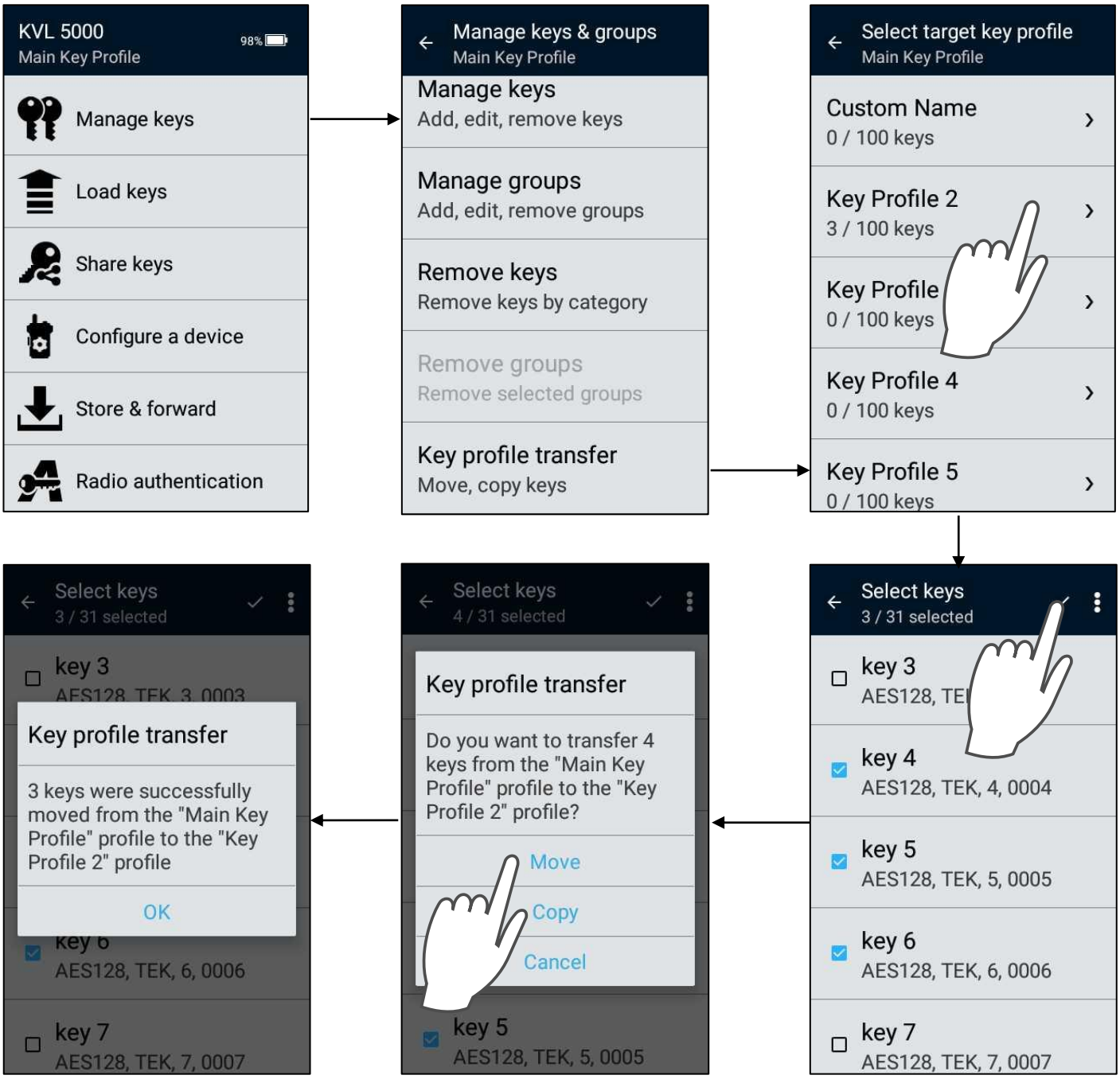


Clearing key profile

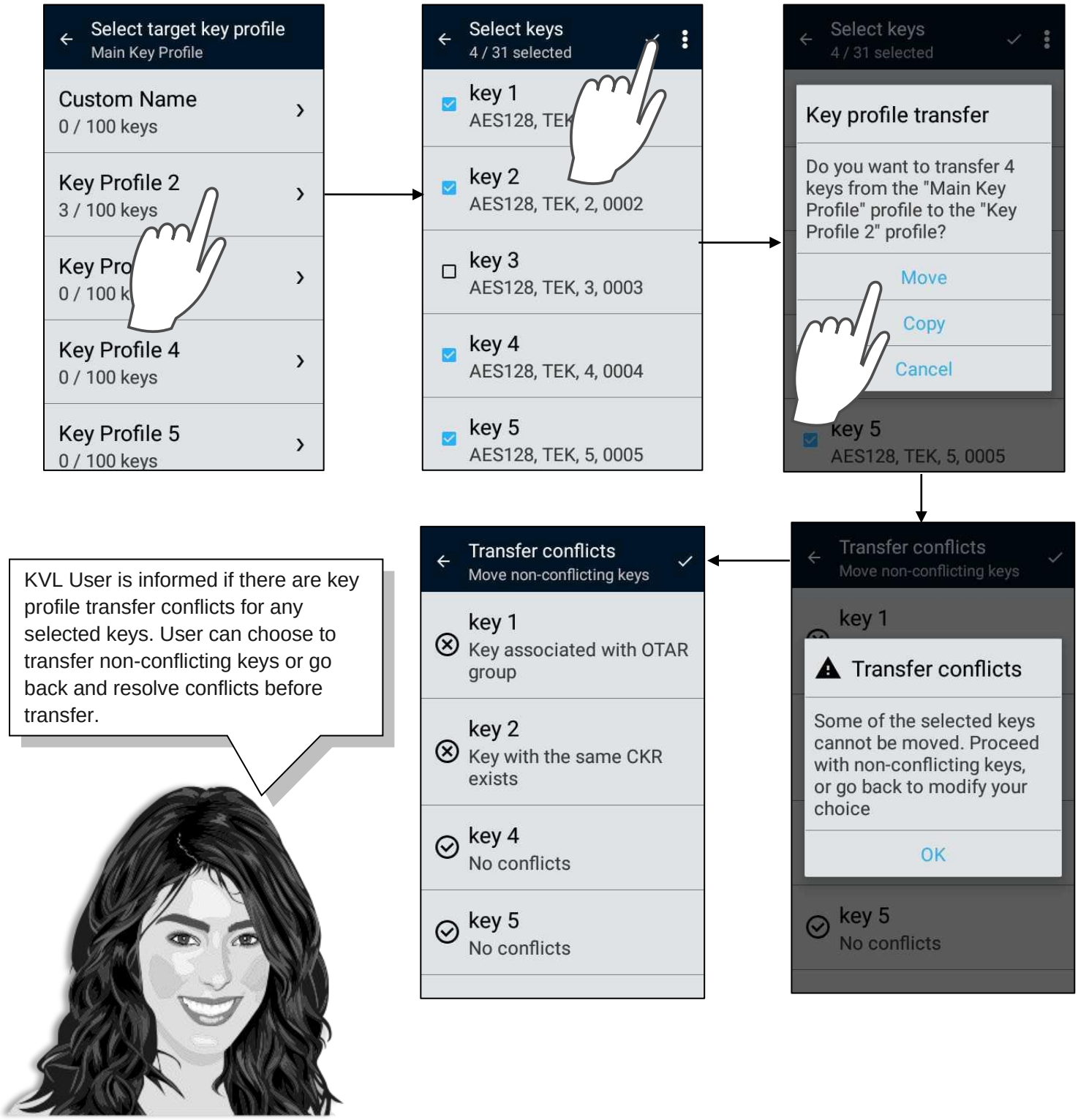
Only administrator can use this feature



Key profile transfer



Key profile transfer with conflicting keys



Connect target device to a KVL

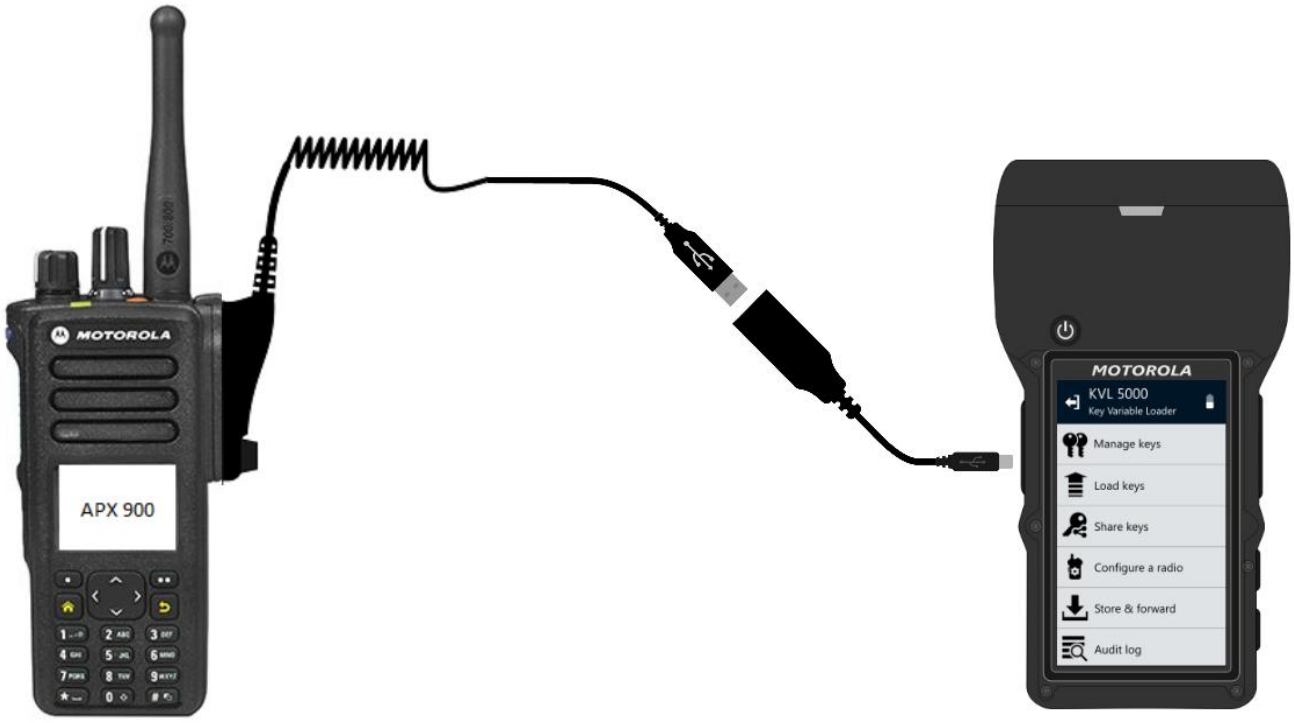
In ASTRO ® 25 systems, you can load encryption keys into the following devices:

- Secure ASTRO® 25 Single Key Target Radios
- Secure ASTRO® 25 Multiple Key Target Radios
- MCC 7500 VPM Dispatch Console
- PDEG Encryption Unit
- CAI Data Encryption Module (CDEM)
- KMF CryptR
- CRYPTR micro in User Equipment
- MCC7500E Console CRYPTR

In PS LTE systems, you can load encryption keys into the following devices:

- Secure ASTRO® 25 Single Key Target Radios
- Secure ASTRO^{yt}5 Multiple Key Target Radios
- KMF CryptR
- CRYPTR micro in User Equipment
- Broadband IPCRYPTR2

Load Keys

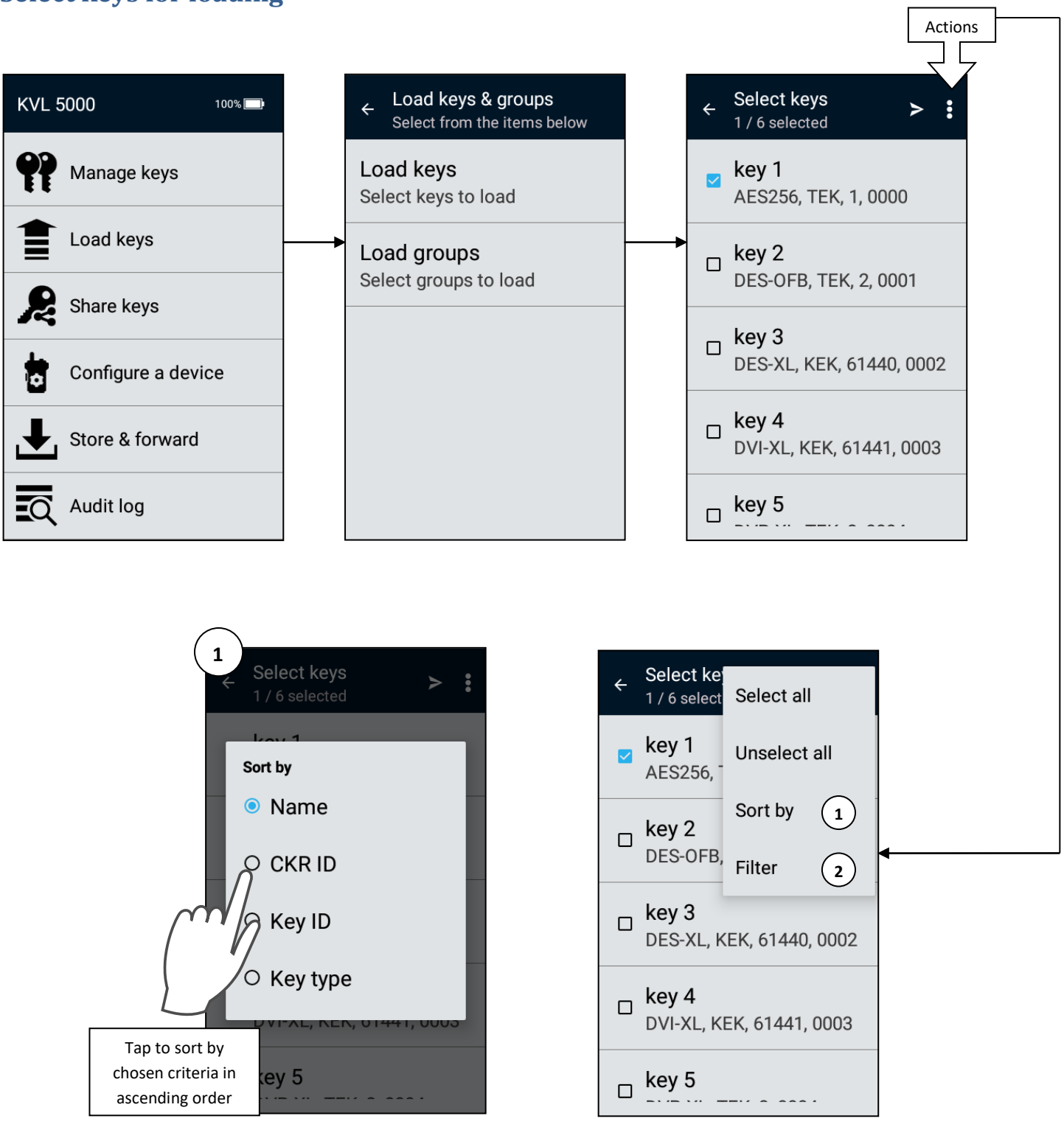


You can also connect devices over USB that support software encryption to perform key load operation when USB key loading feature is enabled.

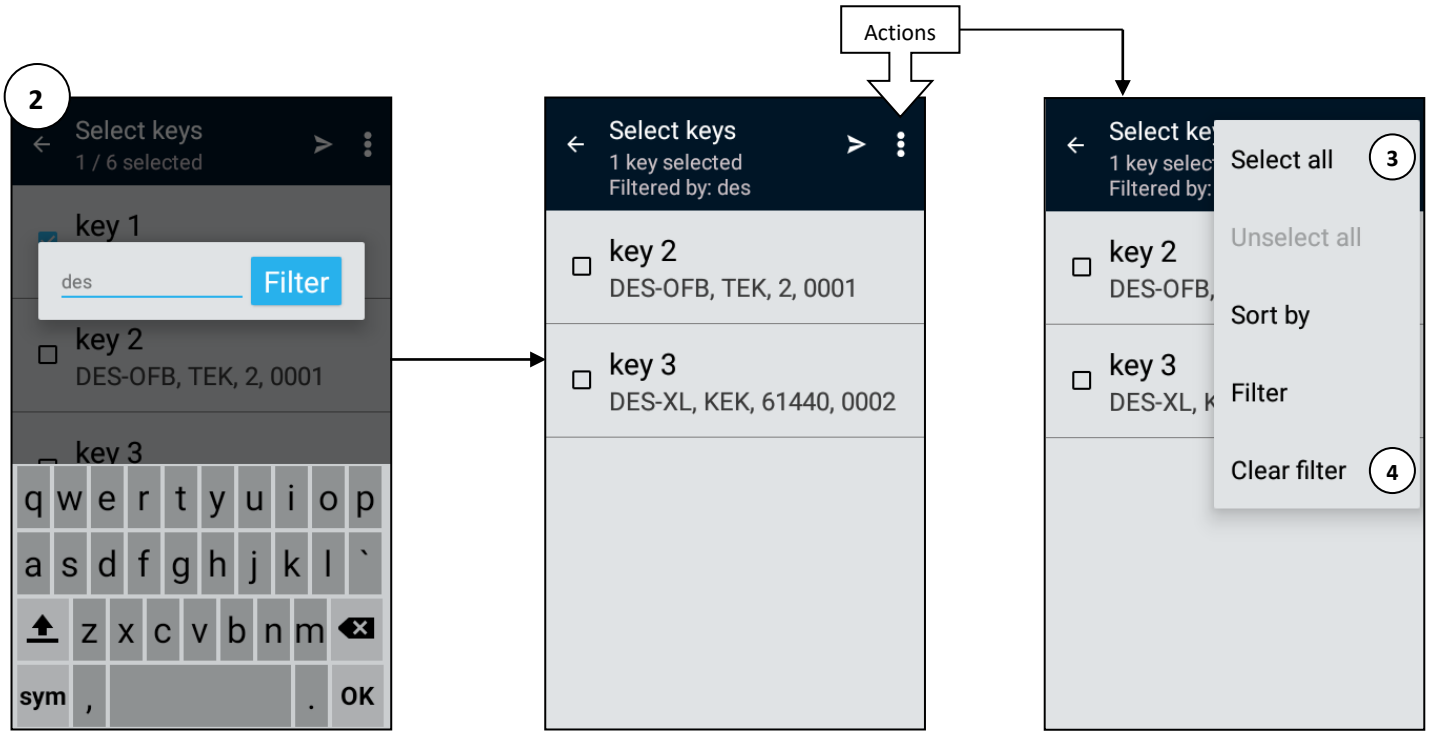
Load Keys

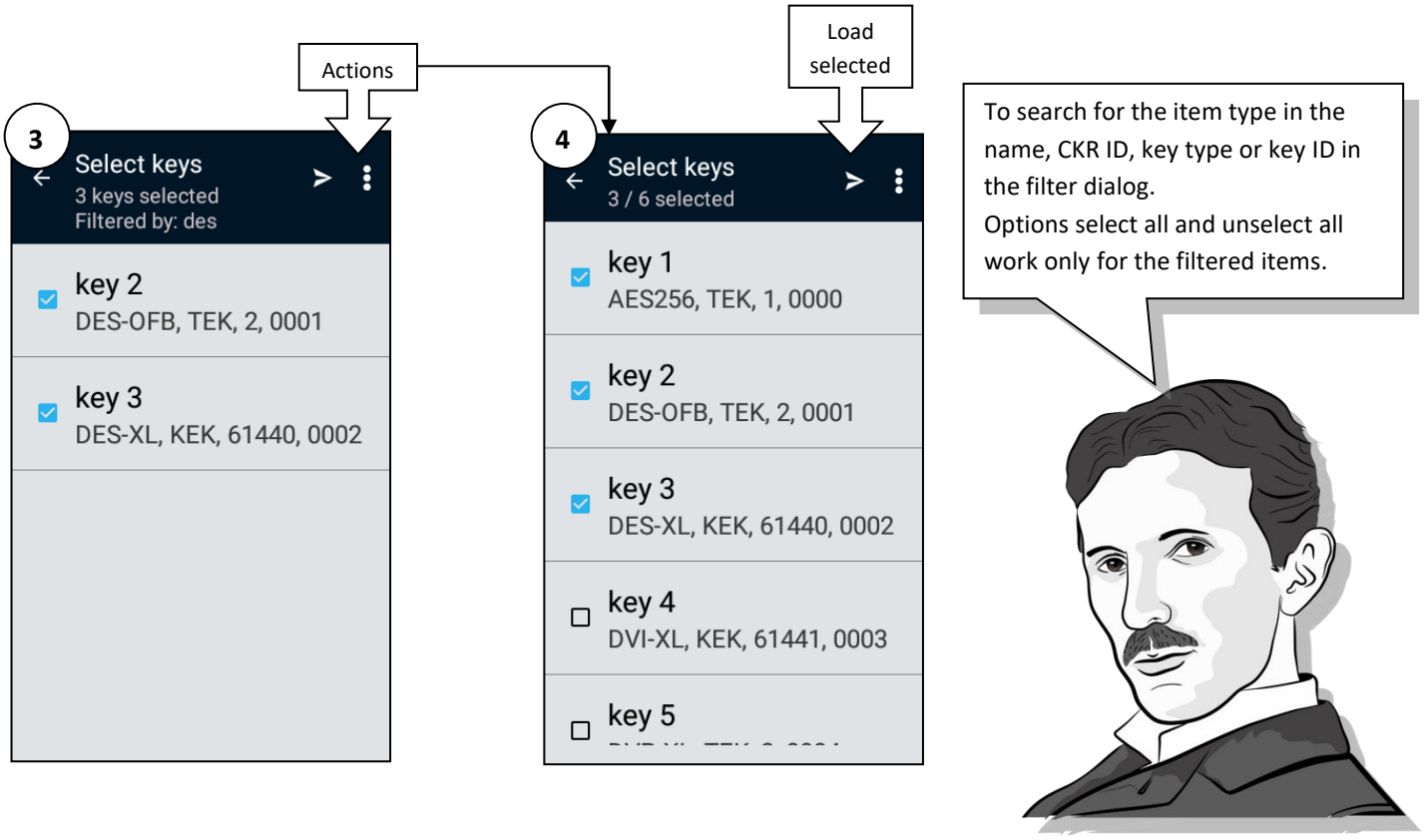
You can also load keys to mobile radios over control head using serial cable. To do that you must first Provision mobile radio with control head keys

Select keys for loading



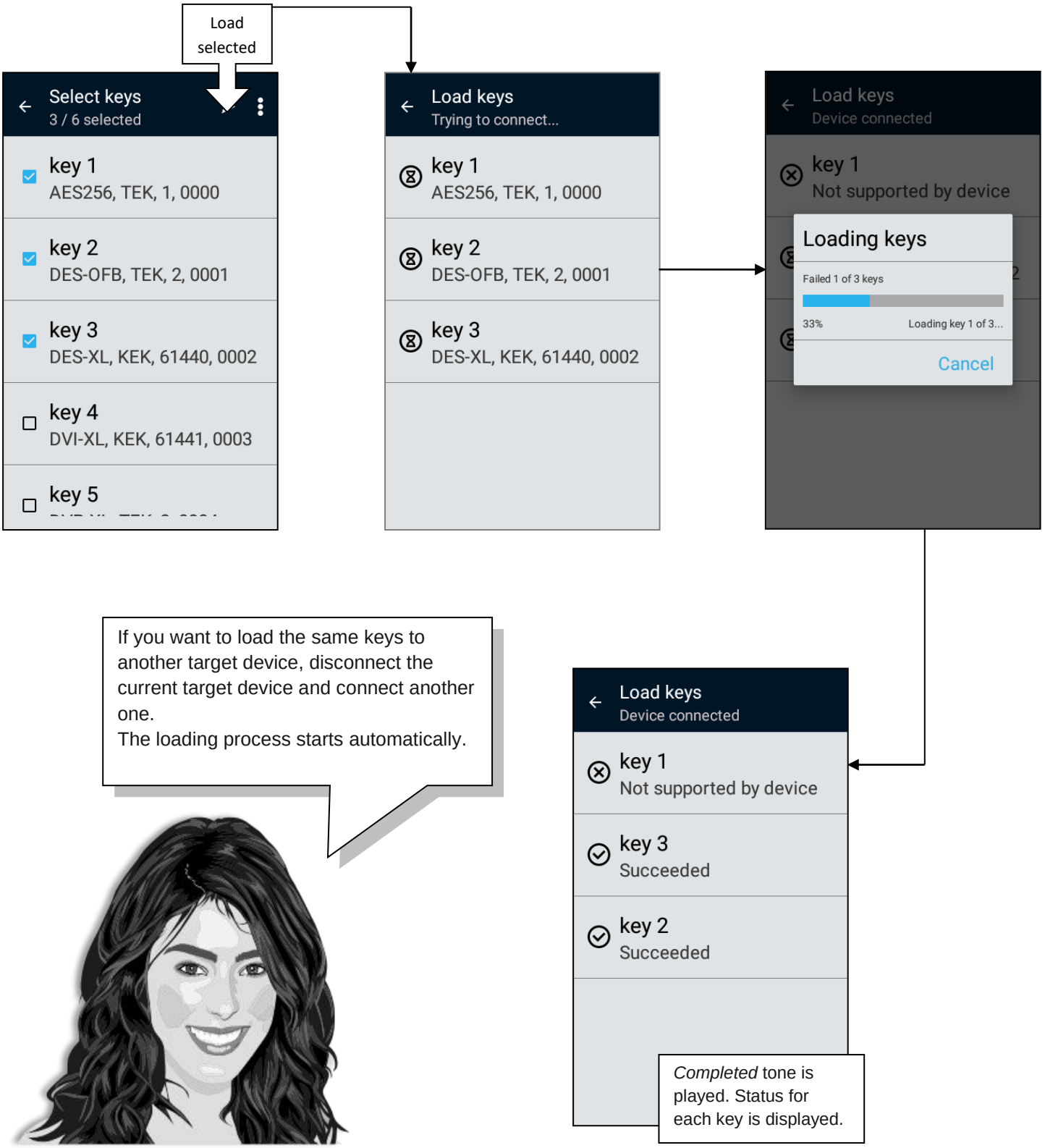
Select keys for loading with filter



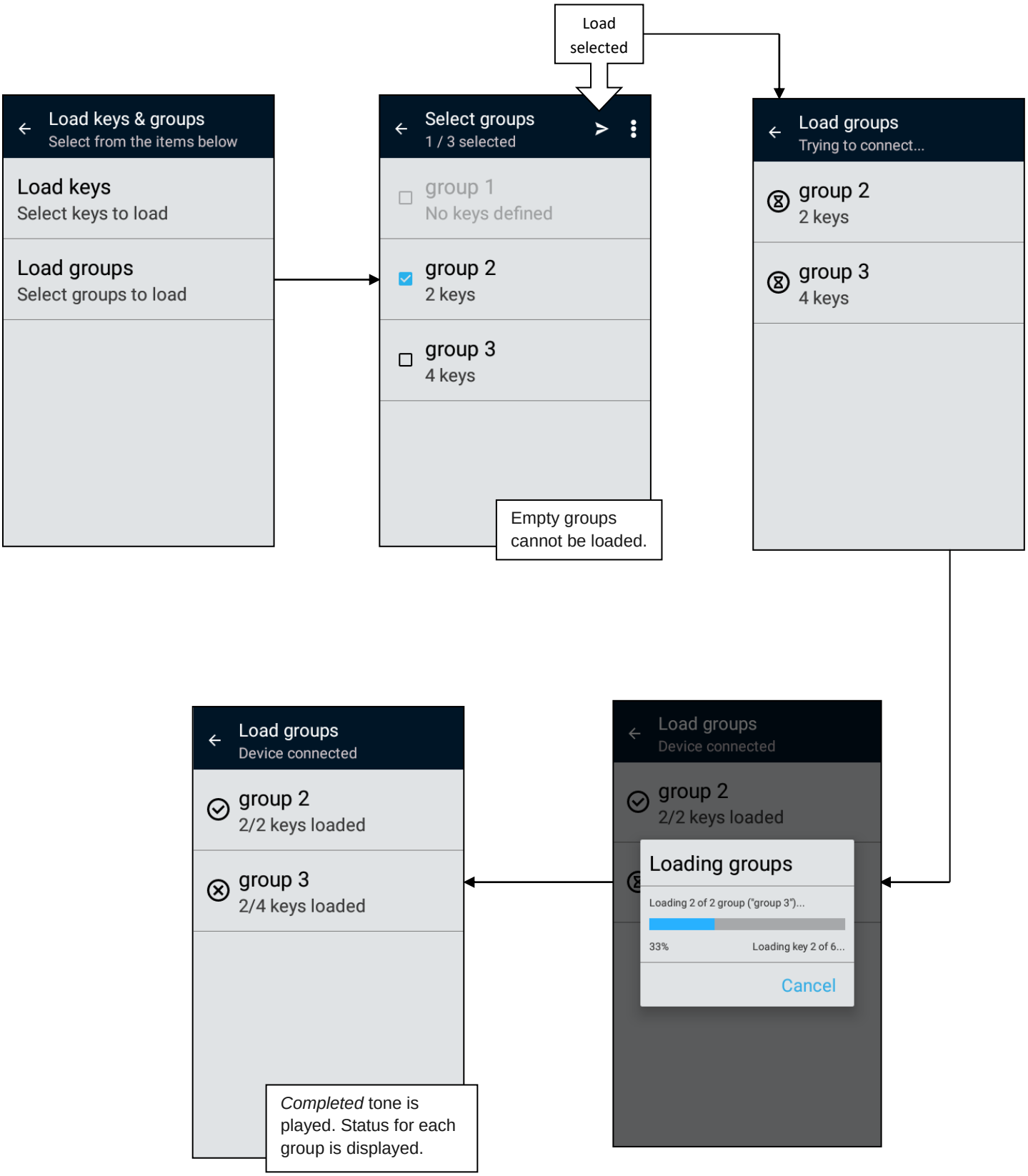


To search for the item type in the name, CKR ID, key type or key ID in the filter dialog.
Options select all and unselect all work only for the filtered items.

Load keys to a target device



Load groups of keys to a target device



Loading Keys Using Push to Load (PTL) Button

You can quickly repeat the last successful keys or key groups loading operation by using the PTL button. PTL button is disabled if any operation is in progress (for example share keys or upgrade).

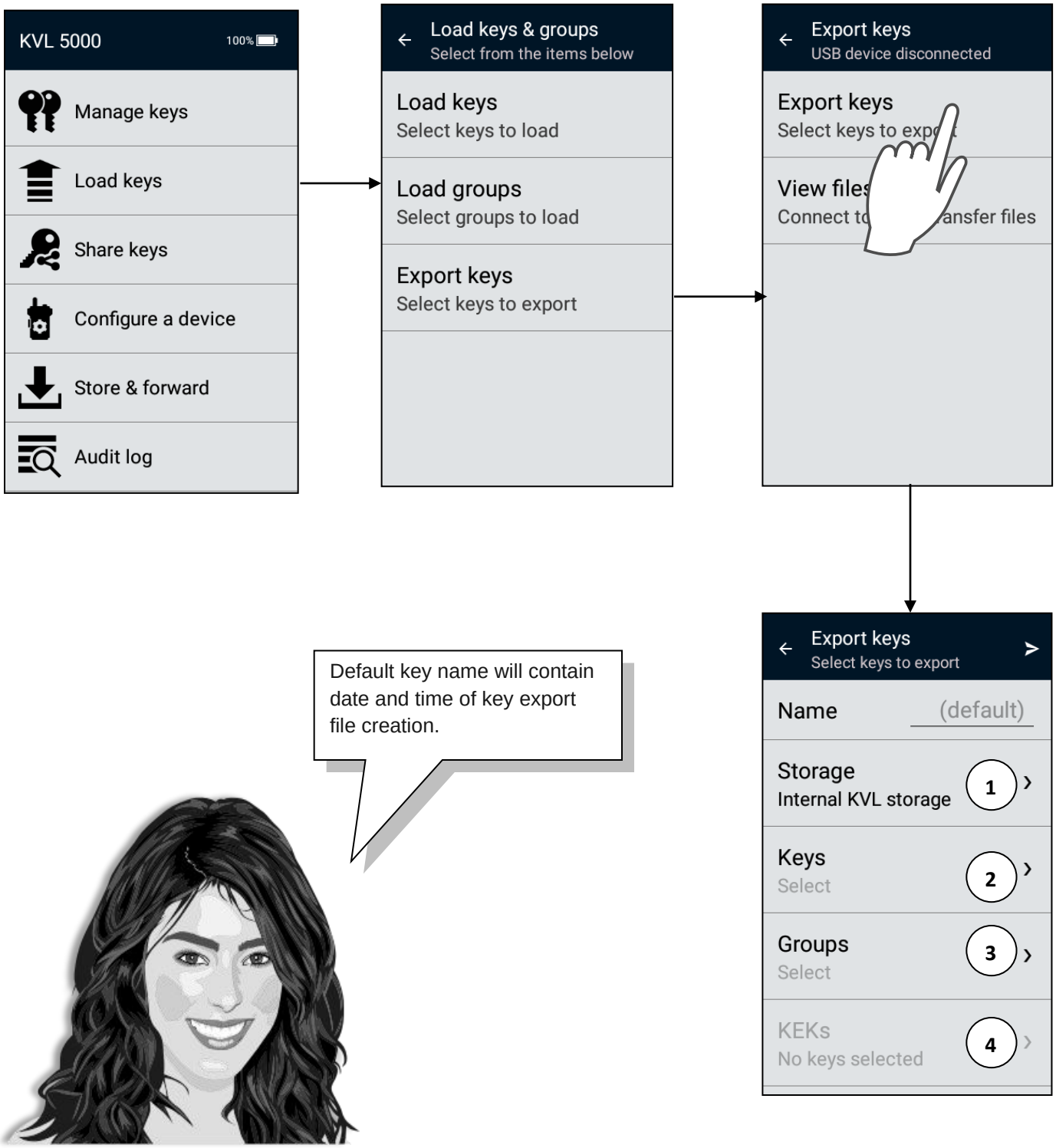
Press Push to Load button

If this is the first time you are loading keys (or previously loaded keys were removed from KVL), push the PTL button and you will be moved to Select keys menu. You can go back to your previous screen by pressing back button.

If you previously loaded keys to a target device, push the PTL button and keys or groups that you loaded previously are immediately loaded into the target device.

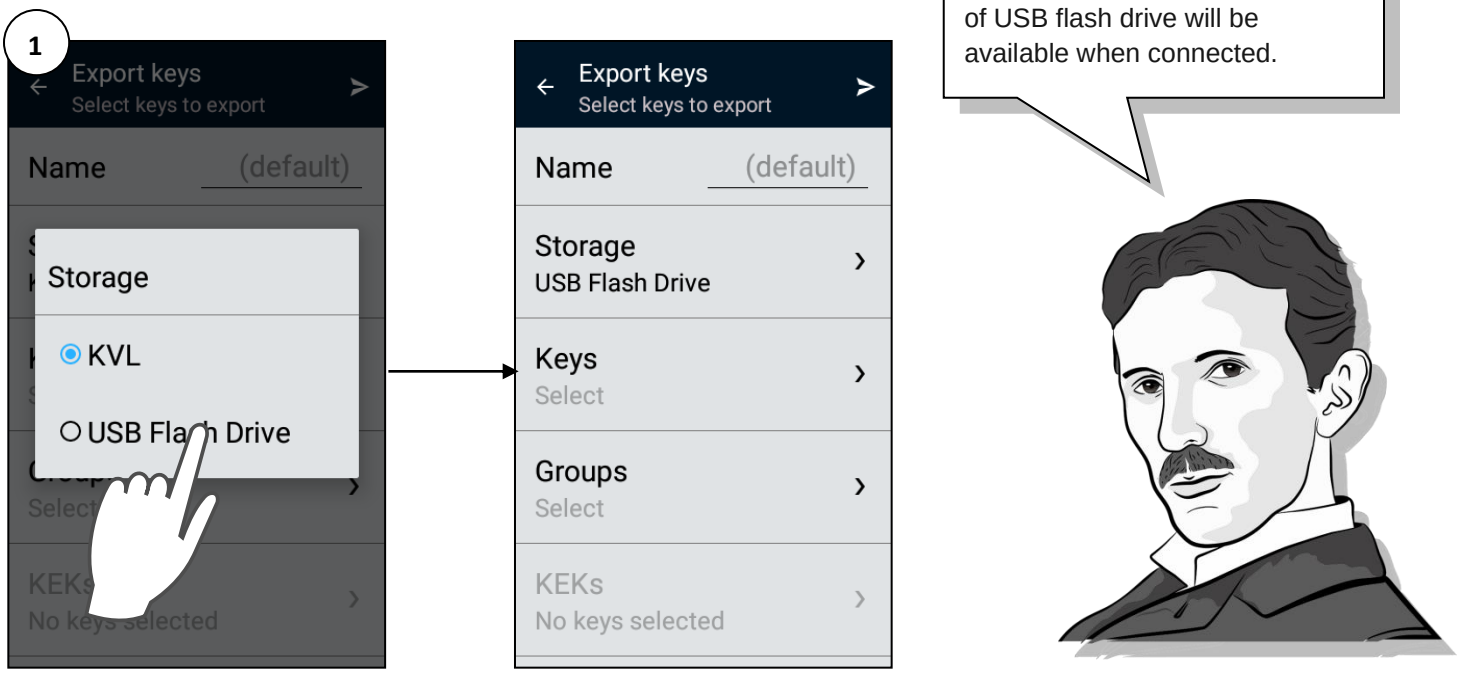
You can load auto generated Radio Authentication key to the same radio using PTL button. See Provisioning Radios with Authentication Keys using PTL Button

Exporting new file

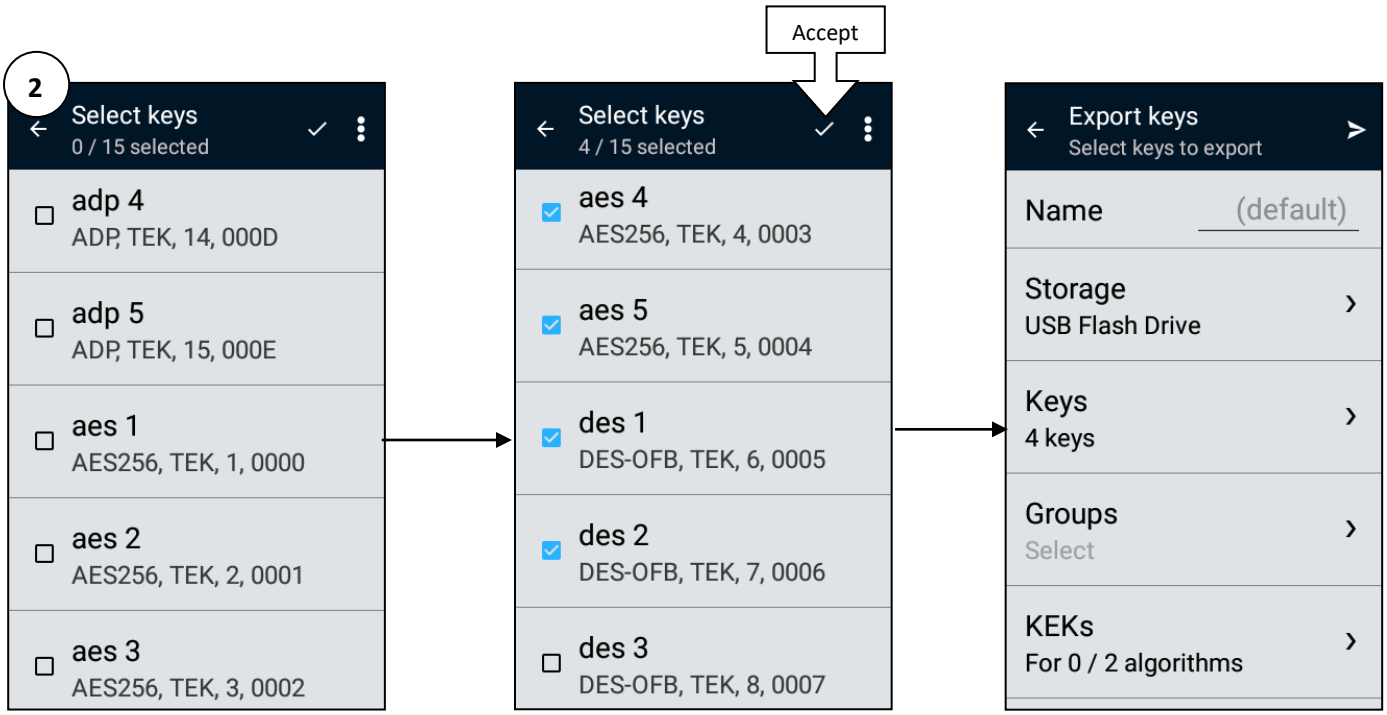


Preparing export file

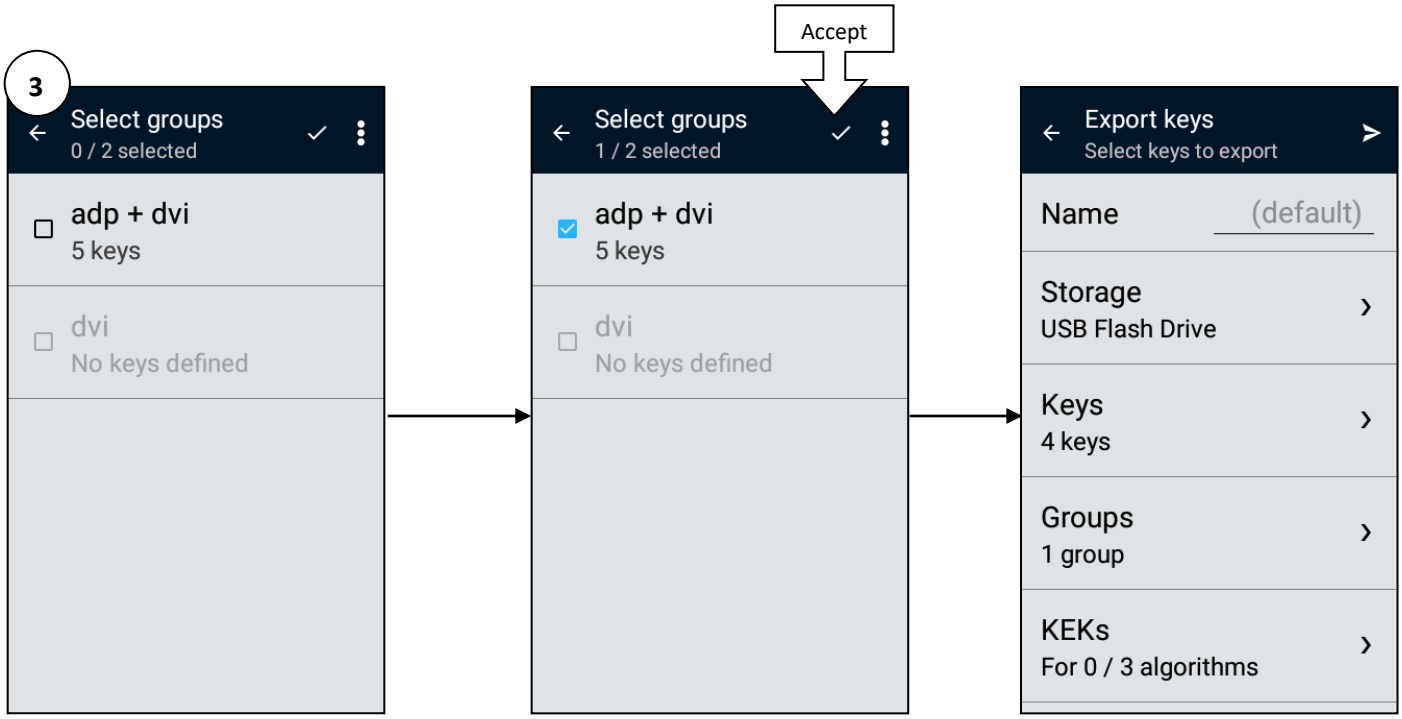
Select export destination



Select keys and groups for export



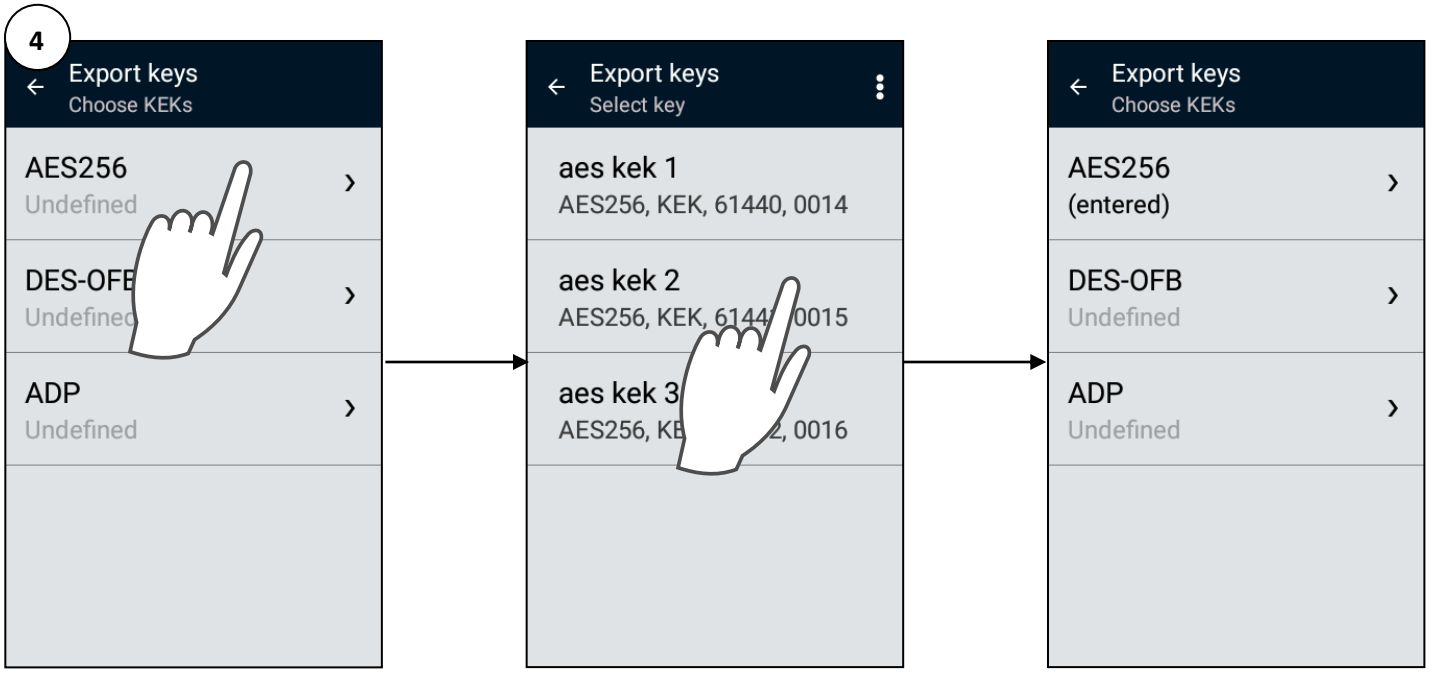
Key File Export

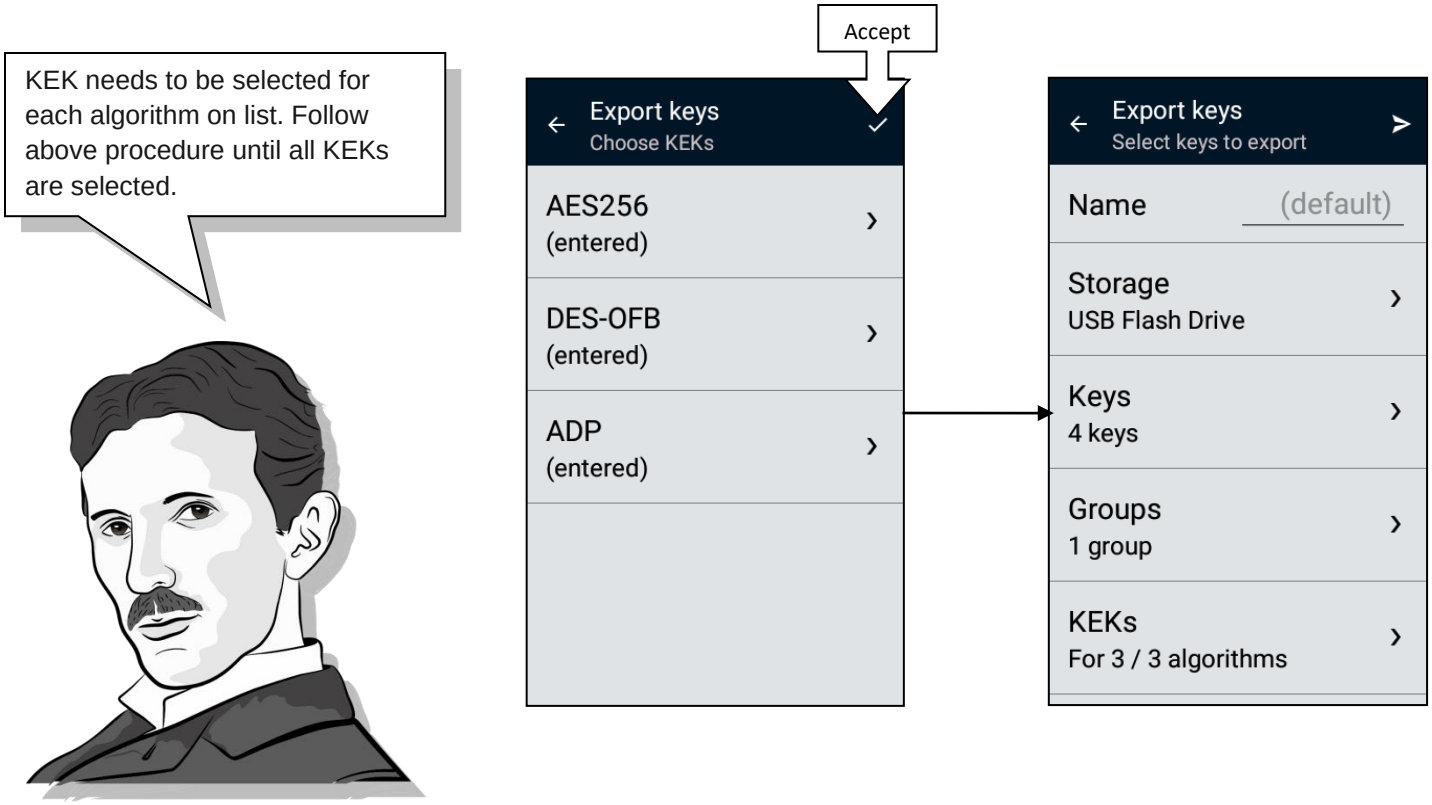


Only keys of algorithms that support key file export (AES256, DES-OFB, ADP) can be selected. Key groups that contain keys of other algorithms can be selected, but only keys of supported algorithms will be exported.

When selecting keys and groups you can use sort and filter options in same way like in Load Keys.

Select KEKs for key export algorithms





Key File Export

Administrator can create new KEK that will be used for selected algorithm.

When no KEK exists for selected algorithm Operator needs to contact Administrator.

Actions

Export keys
Select key

aes kek 1
AES256, KEK, 61440, 0014

aes kek 2
AES256, KEK, 61441, 0015

aes kek 3
AES256, KEK, 61442, 0016

Export ke
Select key

Add new key

Sort b

Filter

aes kek 1
AES256, KE

aes kek 2
AES256, KEK, 61441, 0015

aes kek 3
AES256, KEK, 61442, 0016

Create key

Add key
Enter parameters

Name new kek

Algorithm
AES256

Key type
KEK

CKR ID 65535

Key ID FFFF

Key value

Add key
Enter parameters

Name

Algorithm
AES256

Key type
KEK

CKR ID 61449

Key ID 001D

Key value

Fill key parameters

Export keys
Choose KEKs

AES256
(entered)

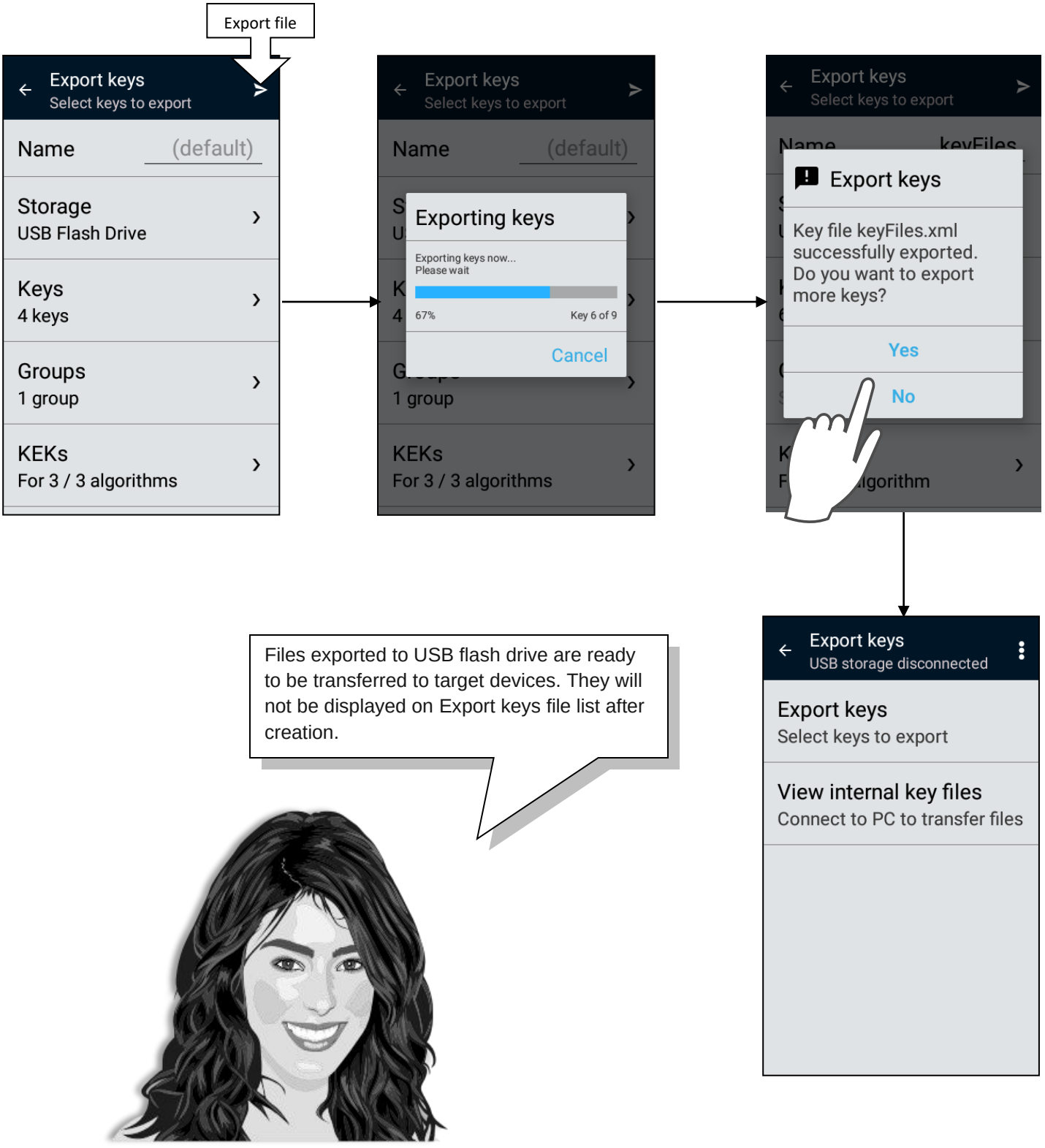
DES-OFB
Undefined

ADP
Undefined

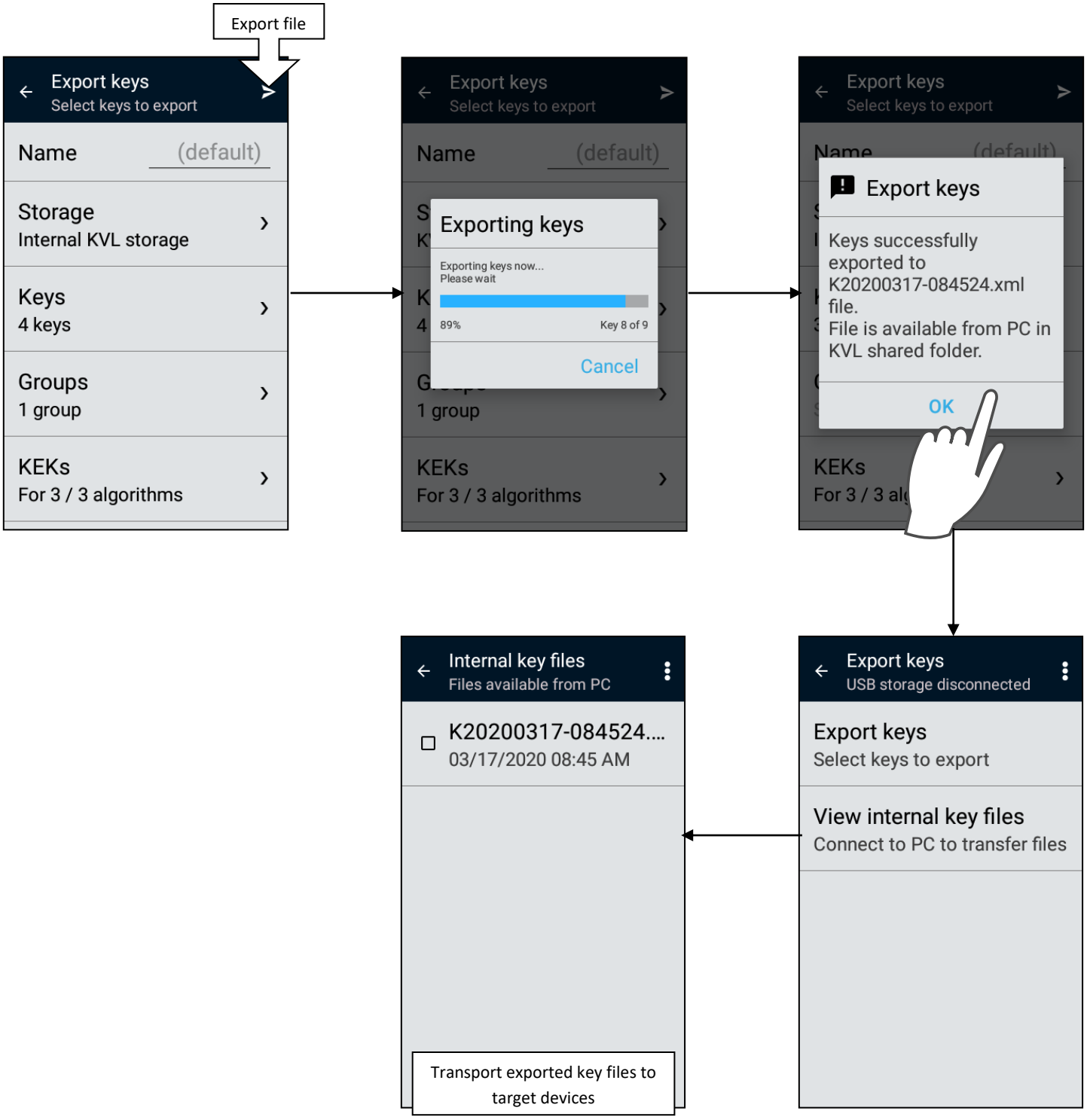
Created key will be entered as KEK for selected algorithm

Key File Export

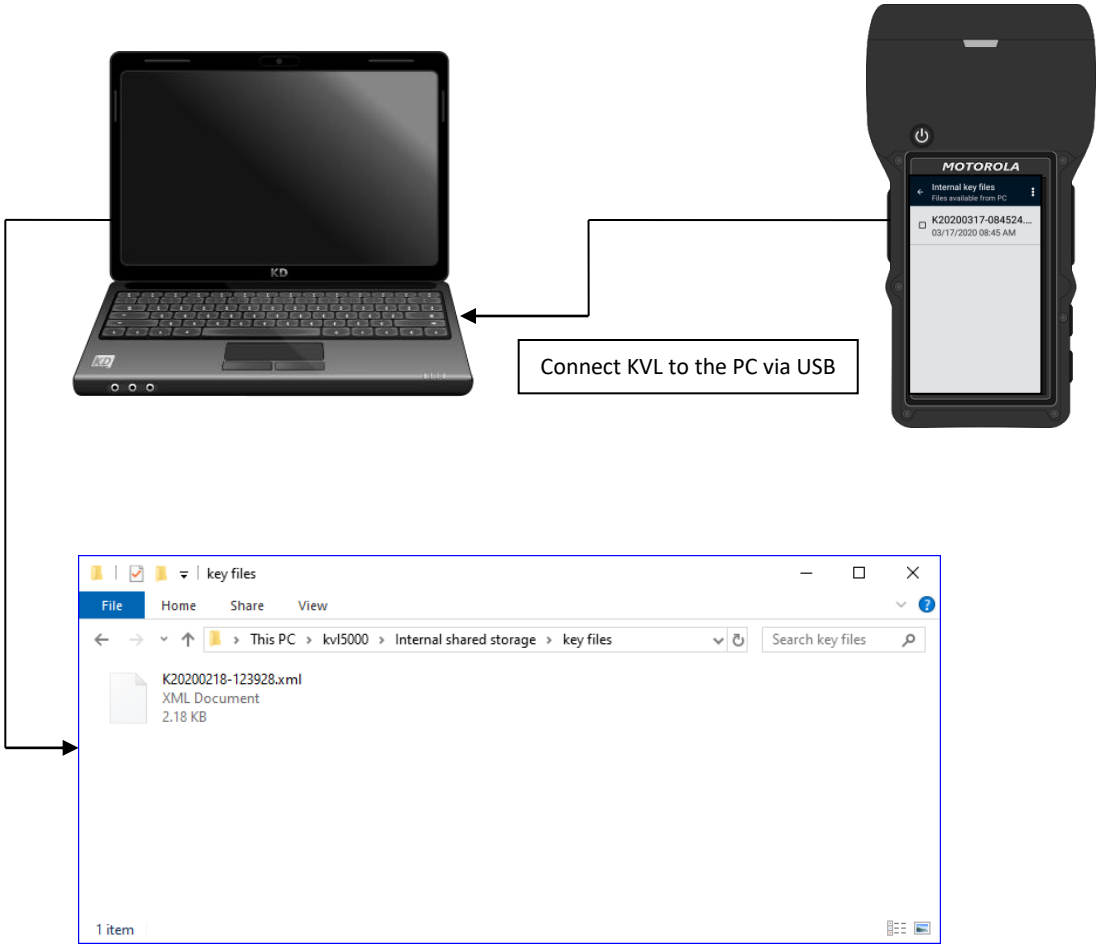
Generating export file to USB flash drive



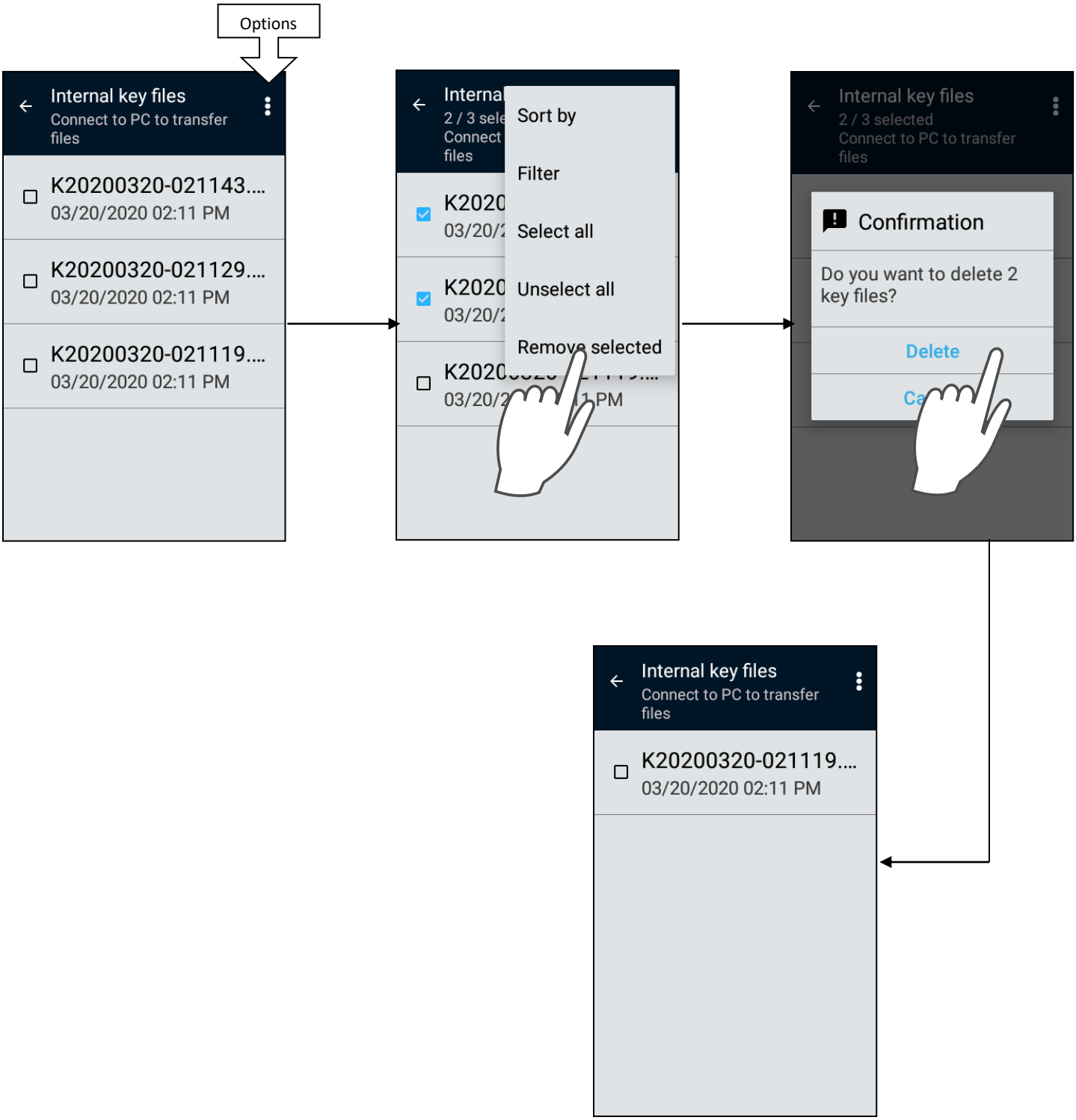
Generating export file to KVL internal storage



Connecting KVL to PC to transfer key export files



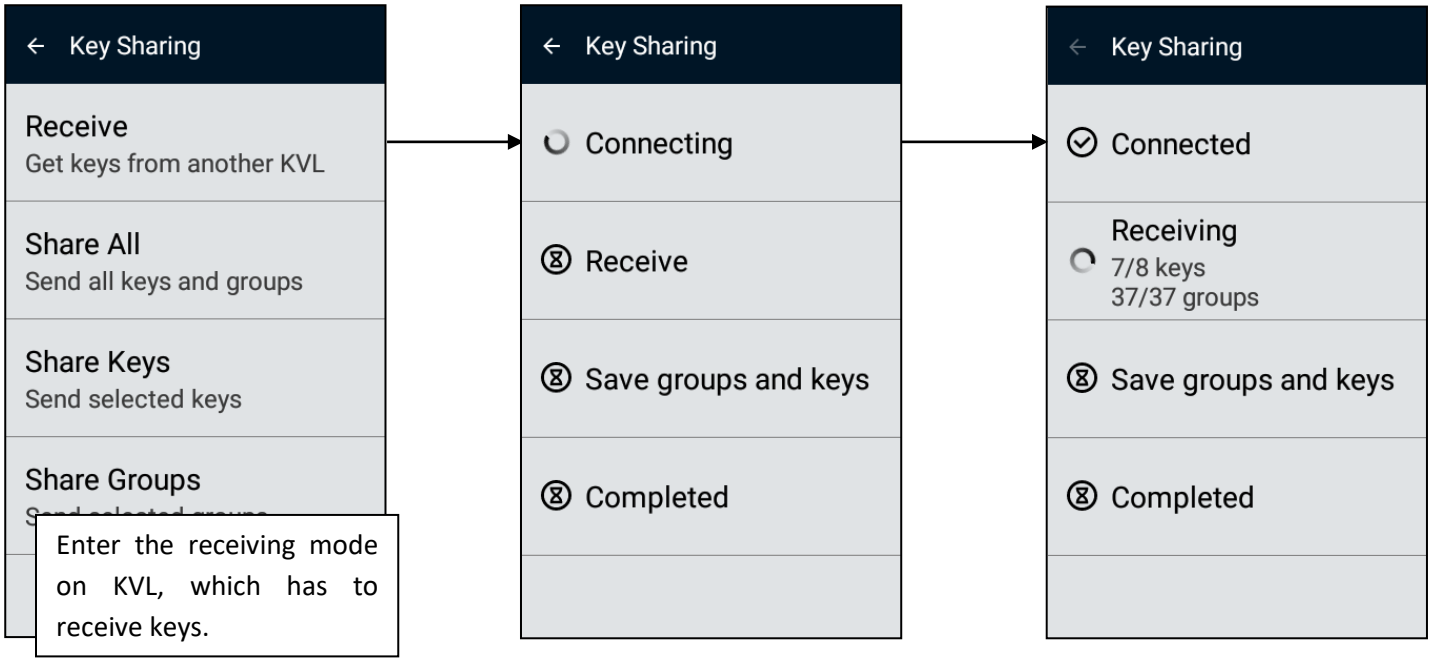
Removing export files from KVL internal storage

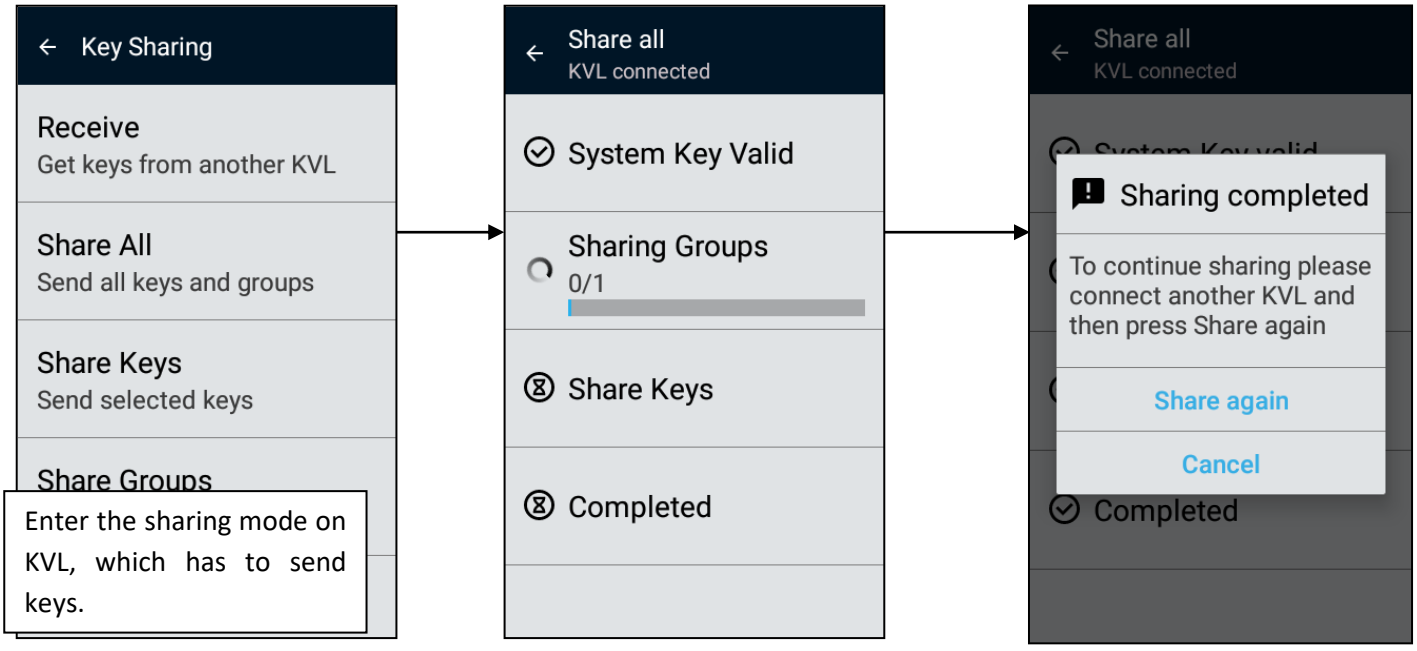


Connecting devices

Sharing operation is done between two KVLs connected via MX Port.

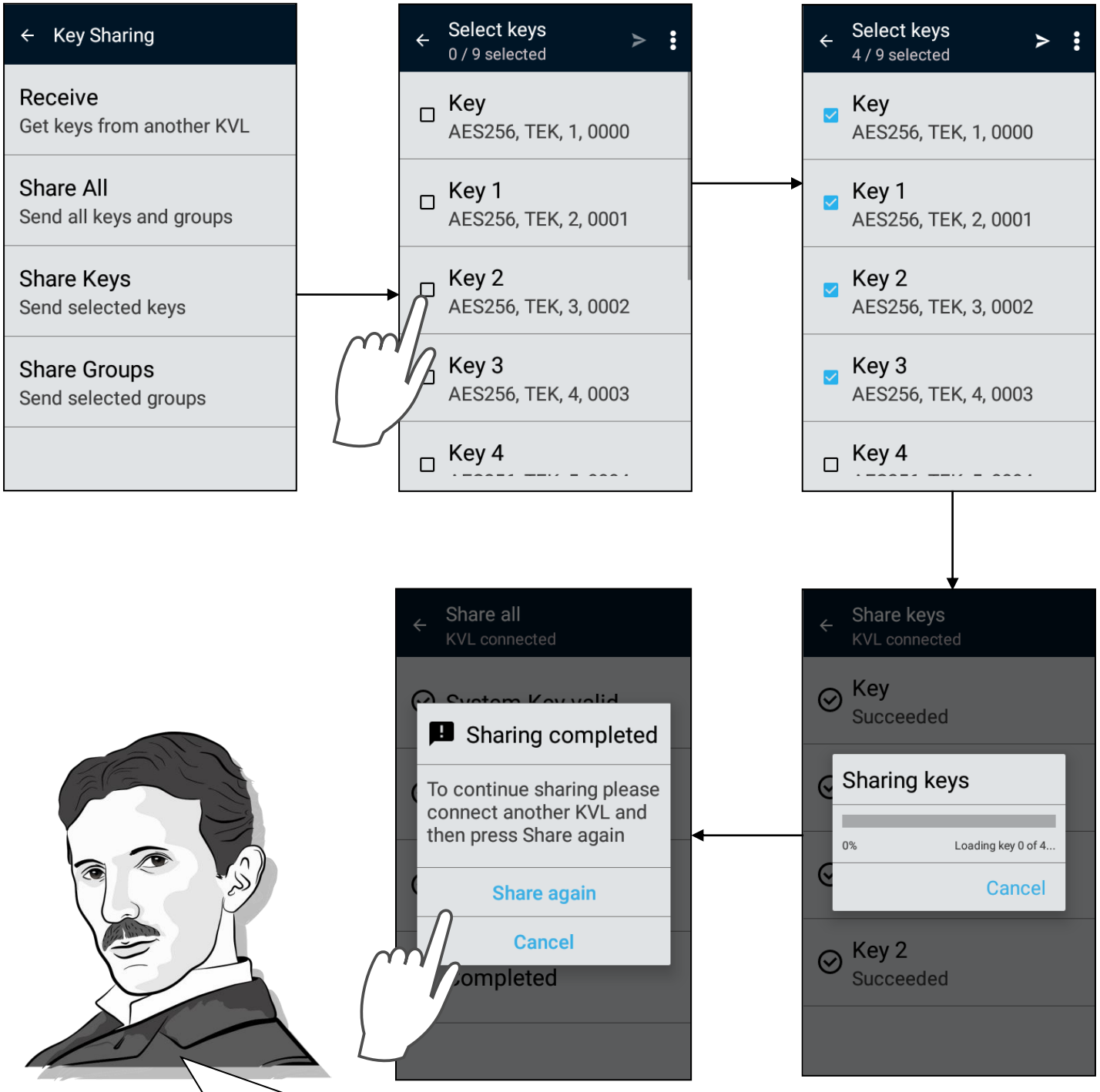
Sharing between two KVL5000s





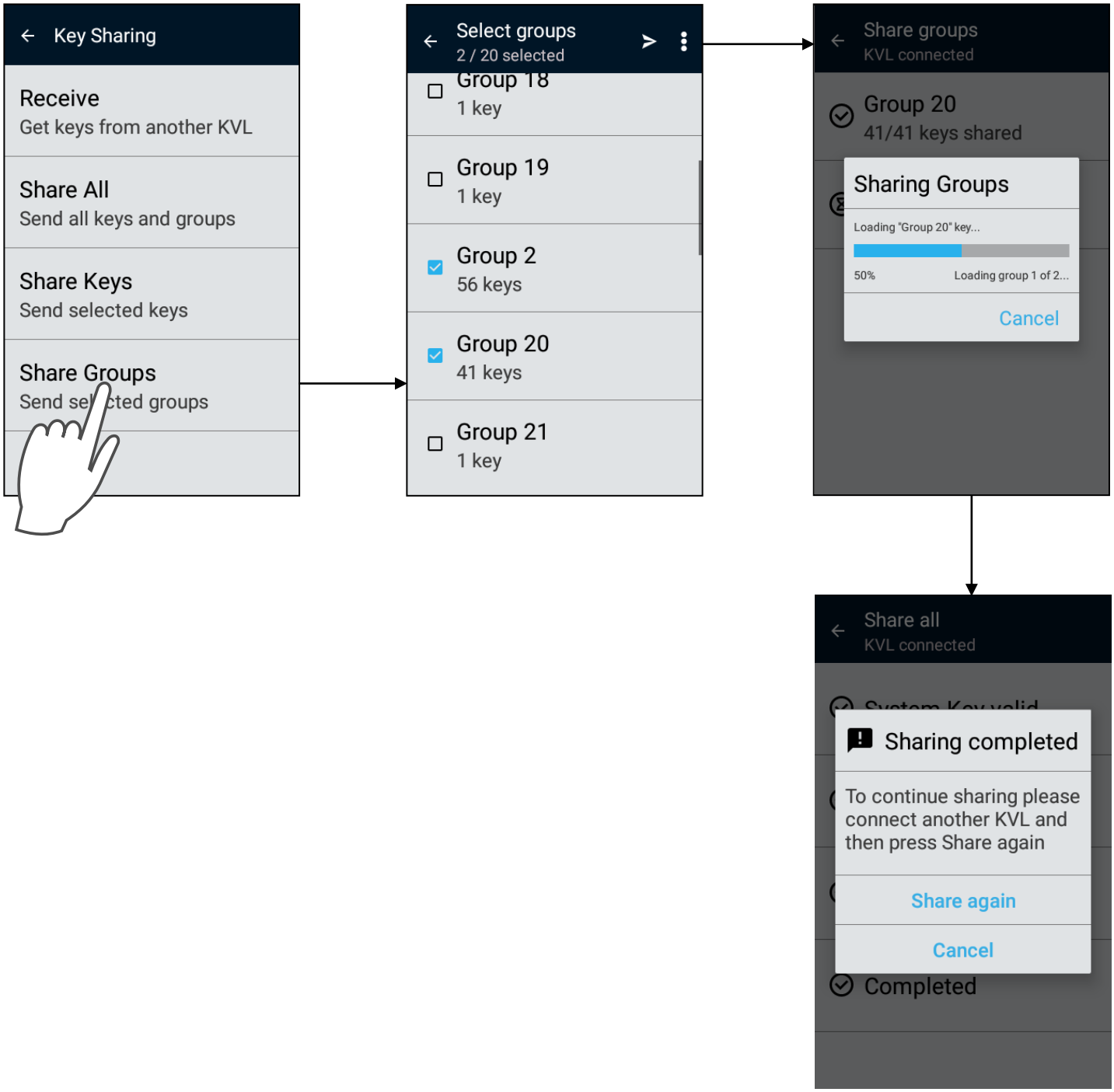
When sharing is completed, you can connect another KVL and continue sharing by pressing Share again or you can finish by pressing Cancel

Sharing selected keys

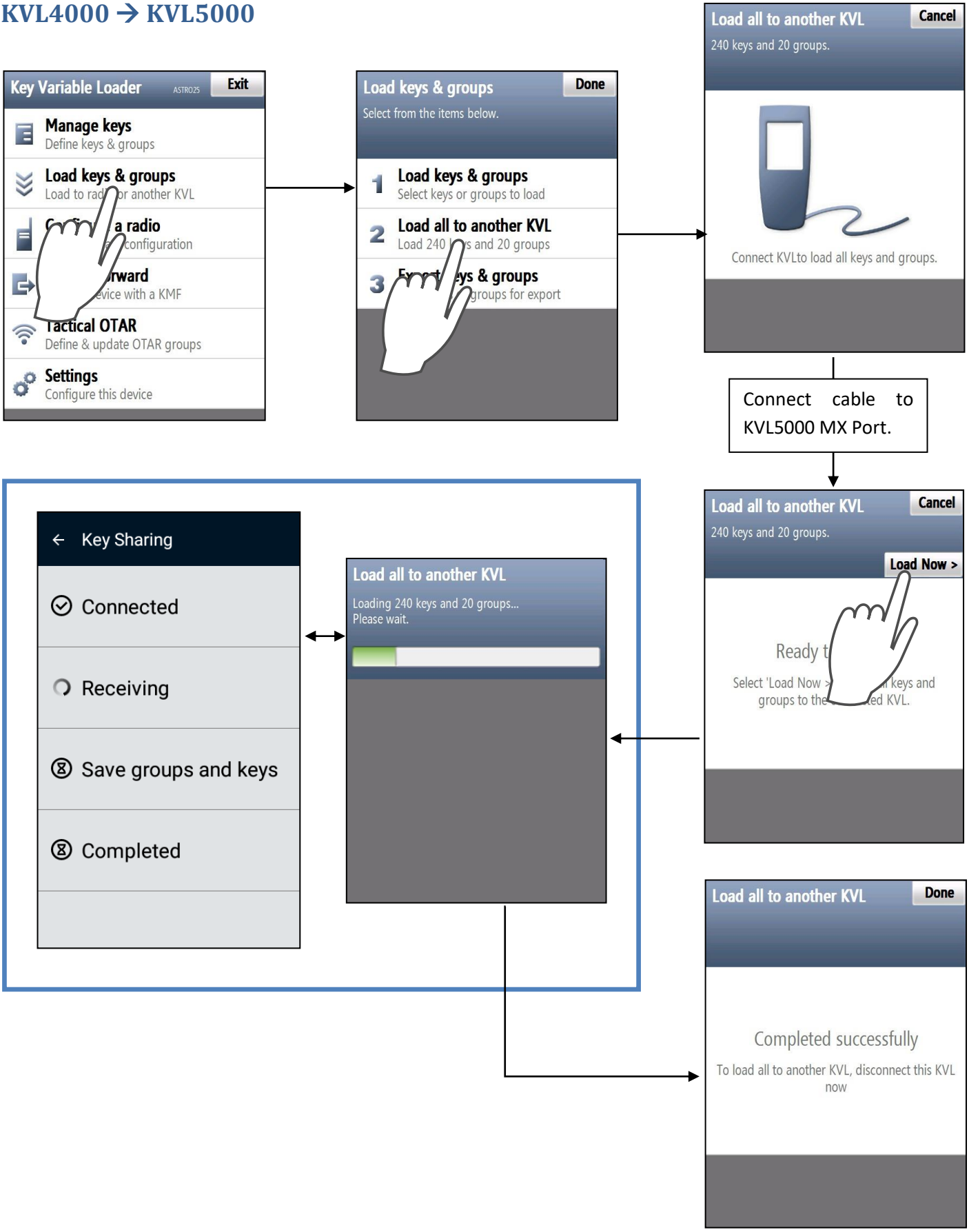


Sharing selected groups

Sharing selected groups share those groups as well as all keys which belong to them.

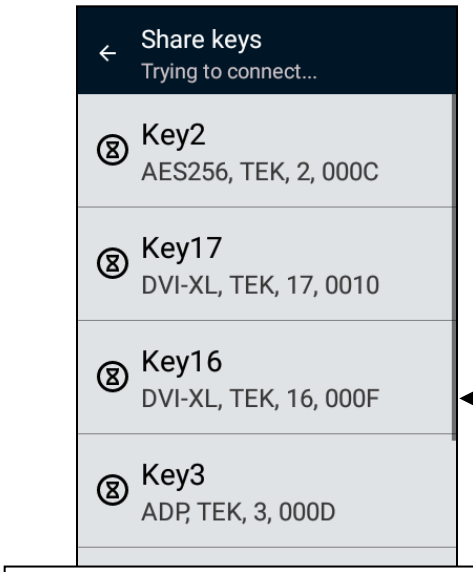


KVL4000 → KVL5000



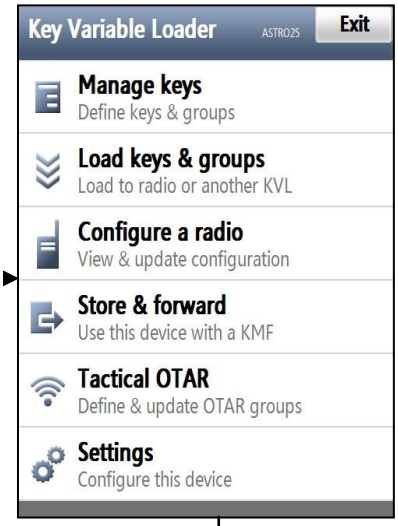
KVL5000 → KVL4000

KVL4000 should stay in Main Menu while connecting another KVL.

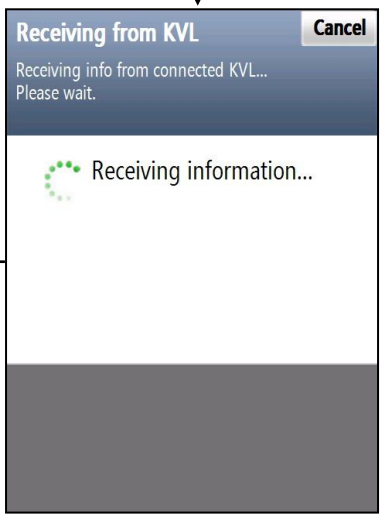


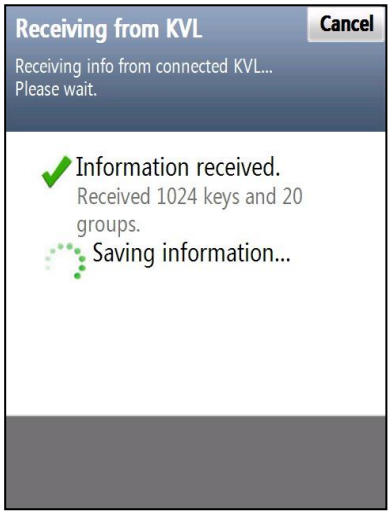
On KVL5000 enter sharing mode:
Share All / Share Keys / Share Groups

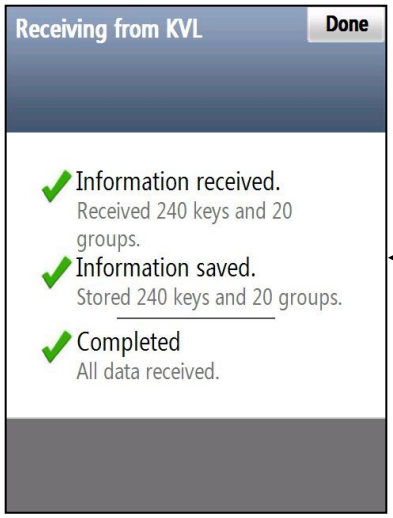
Connect KVL4000 with MX cable.



After connection is detected KVL5000 starts sharing and KVL4000 starts receiving.



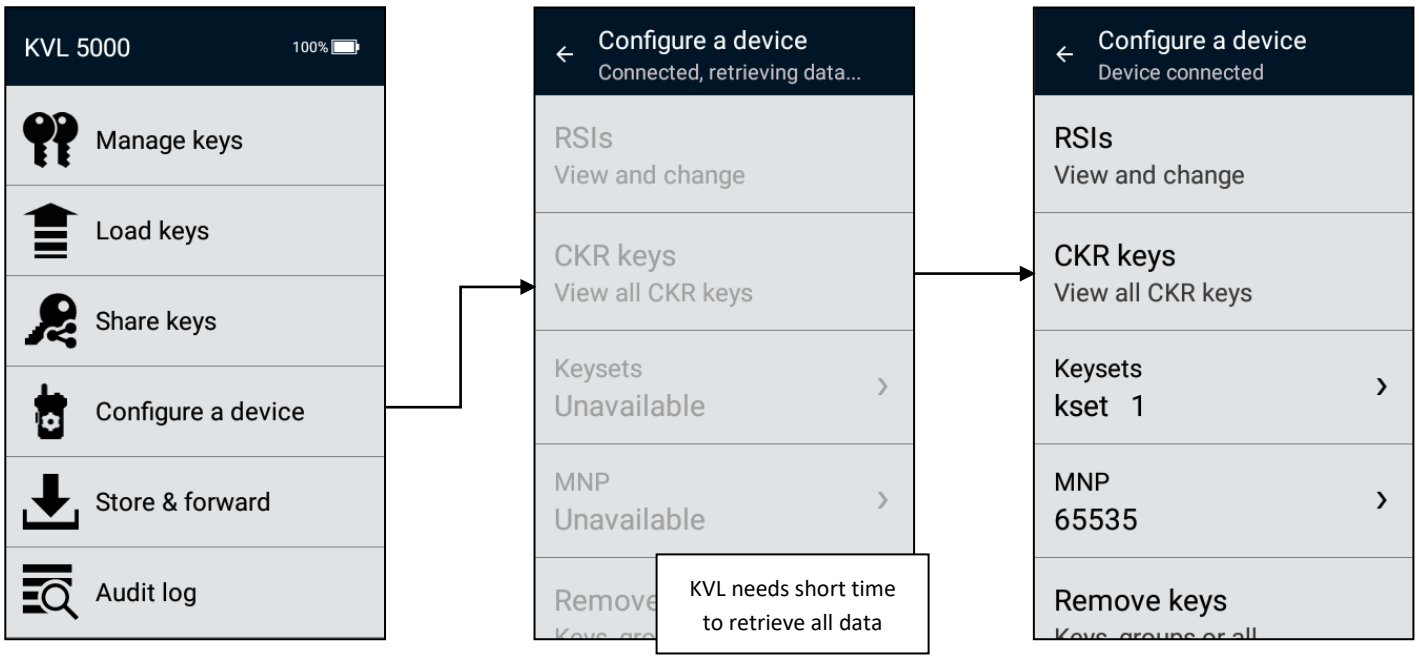




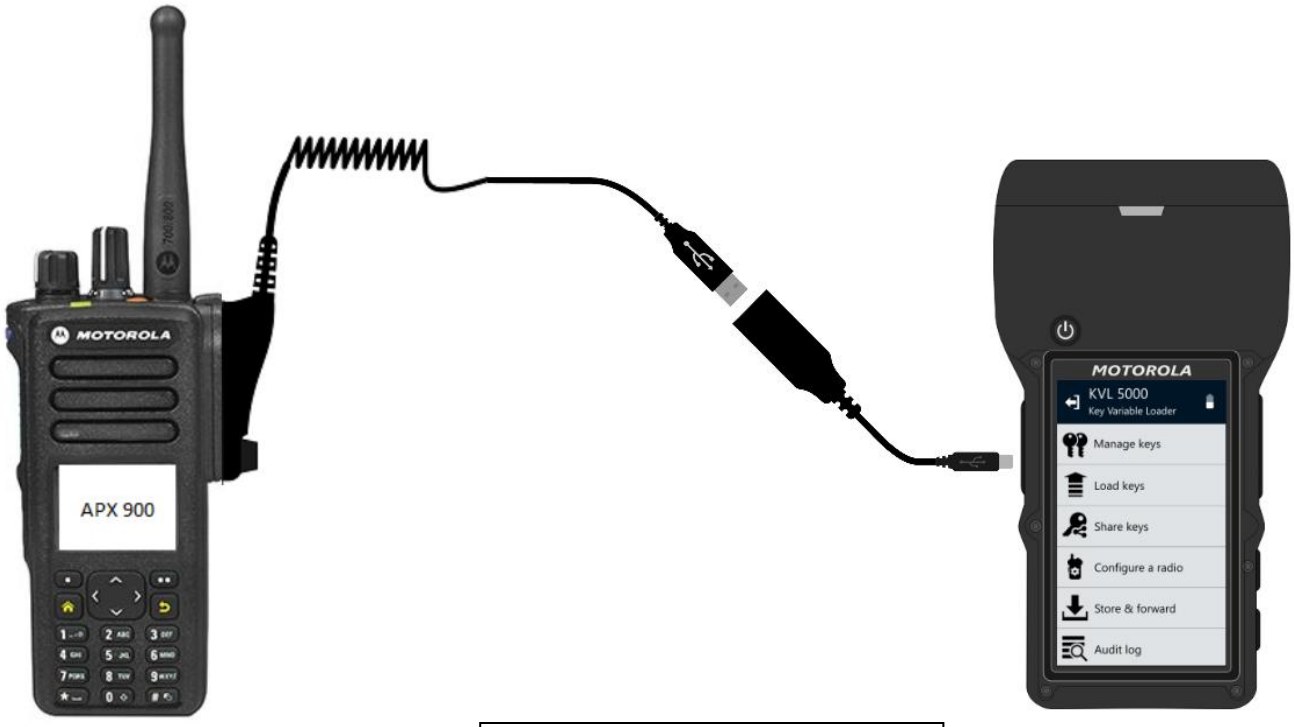
After sharing is done, disconnect MX cable.

You may connect another KVL to receive the same set of keys and/or groups.

Connect a device to KVL



Configure a device

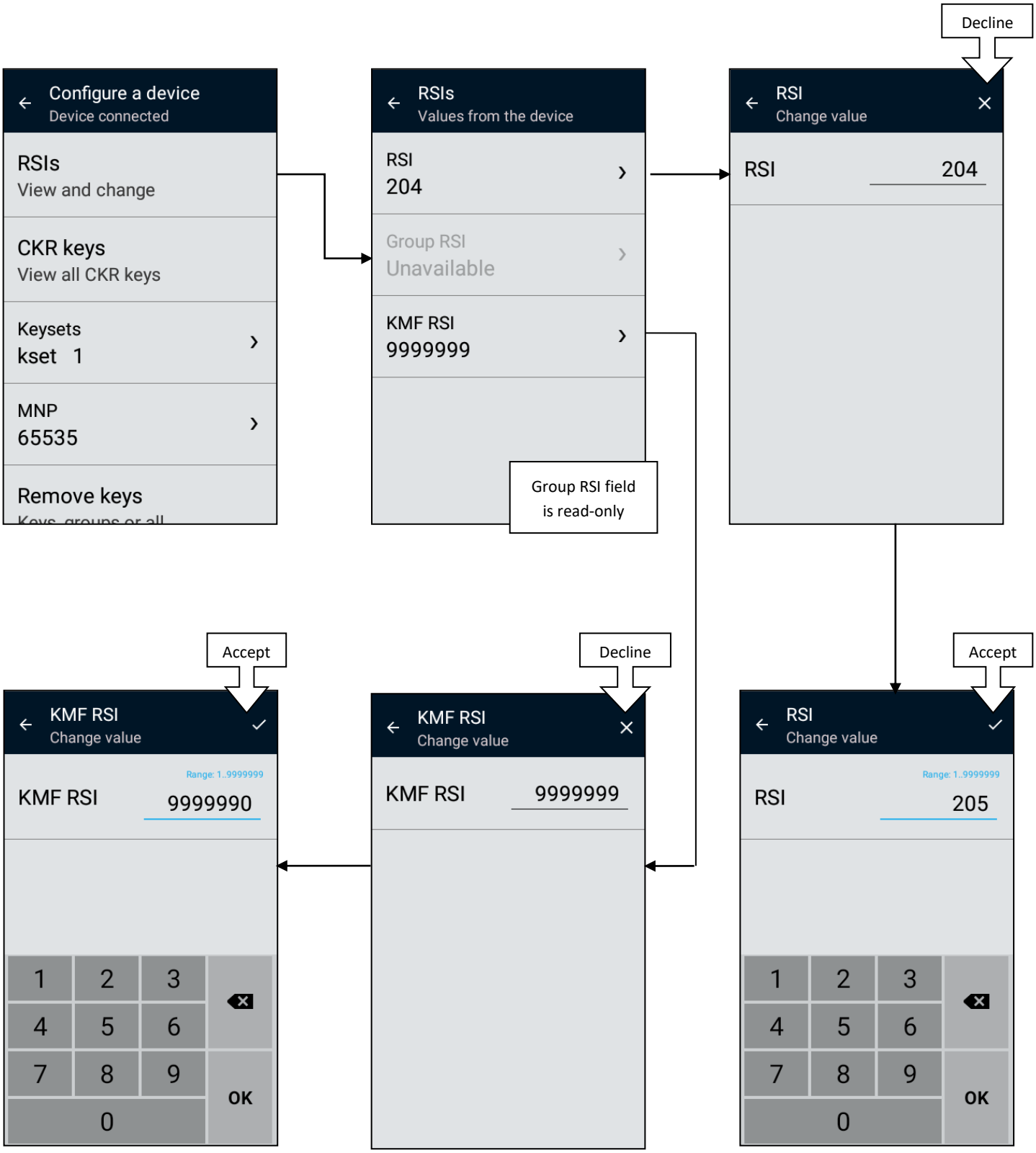


You can also connect devices over USB that support software encryption to perform key load operation when USB key loading feature is enabled.

Configure a device

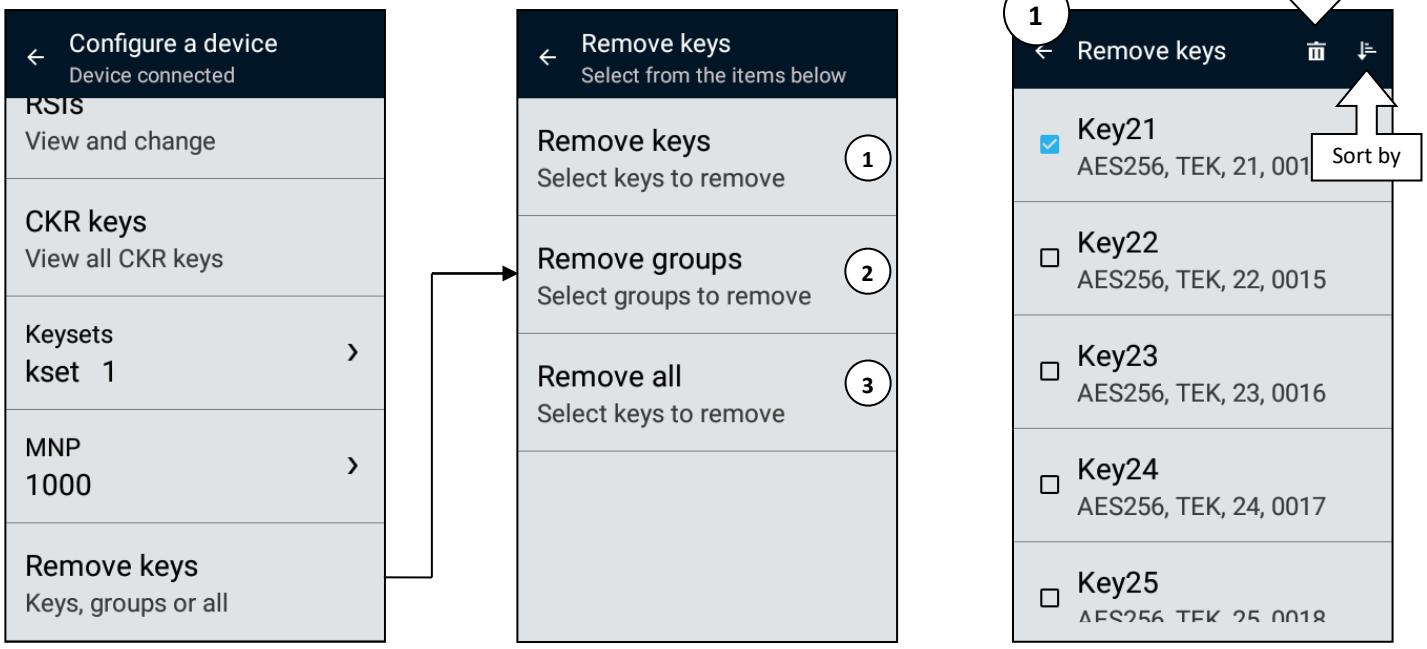
You can also configure mobile radio over control head using serial cable. To do that you must first Provision mobile radio with control head keys

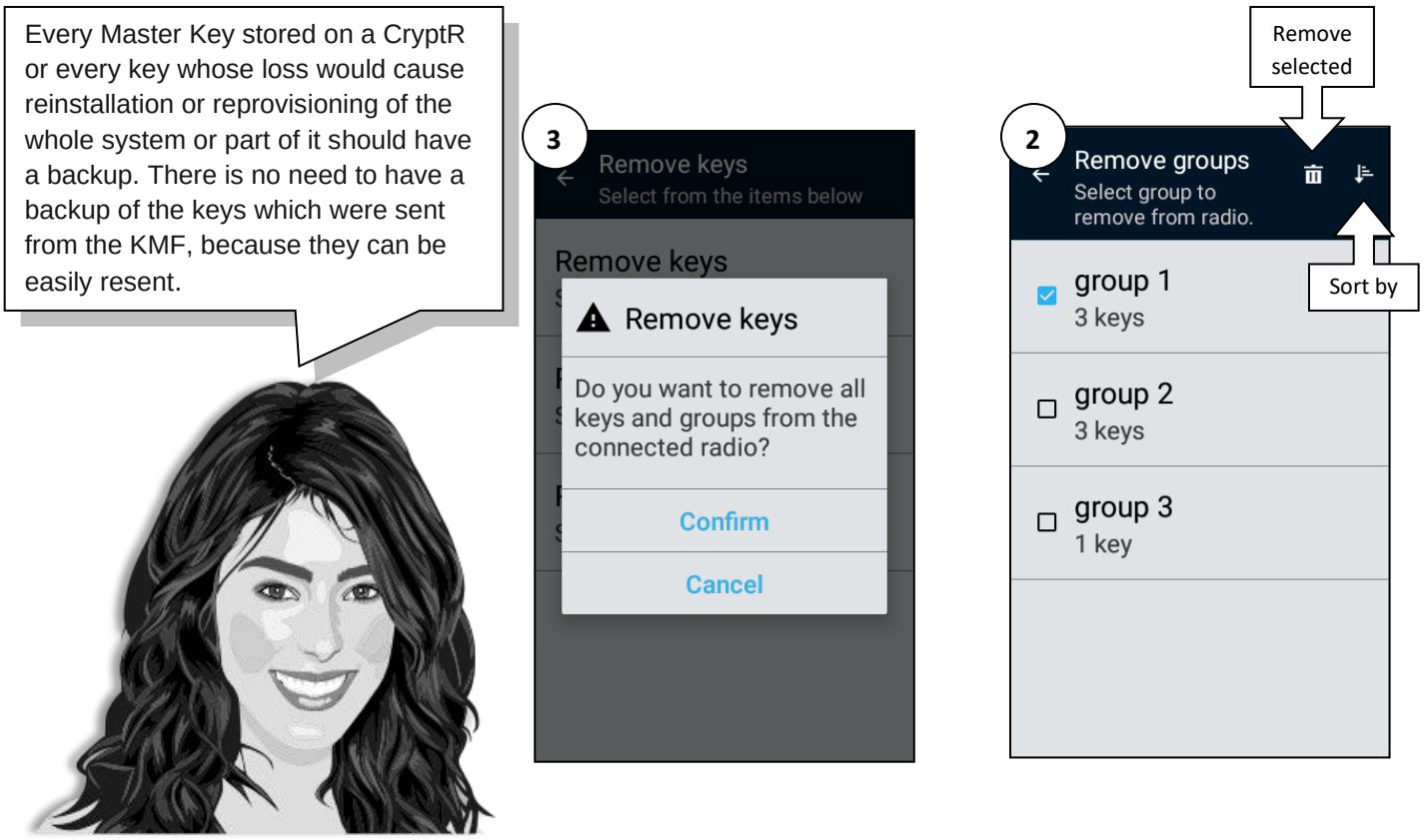
Change RSIs


Decline
Configure a device
Device connected
RSIs
View and change
CKR keys
View all CKR keys
Keysets
kset 1
MNP
65535
Remove keys
RSIs
Values from the device
RSI
204
Group RSI
Unavailable
KMF RSI
9999999
Group RSI field is read-only
RSI
Change value
RSI
204
Accept
KMF RSI
Change value
Range: 1..9999999
KMF RSI
9999990
1 2 3
4 5 6
7 8 9
0
OK
Decline
KMF RSI
Change value
KMF RSI
9999999
Accept
RSI
Change value
Range: 1..9999999
RSI
205
1 2 3
4 5 6
7 8 9
0
OK

Other settings

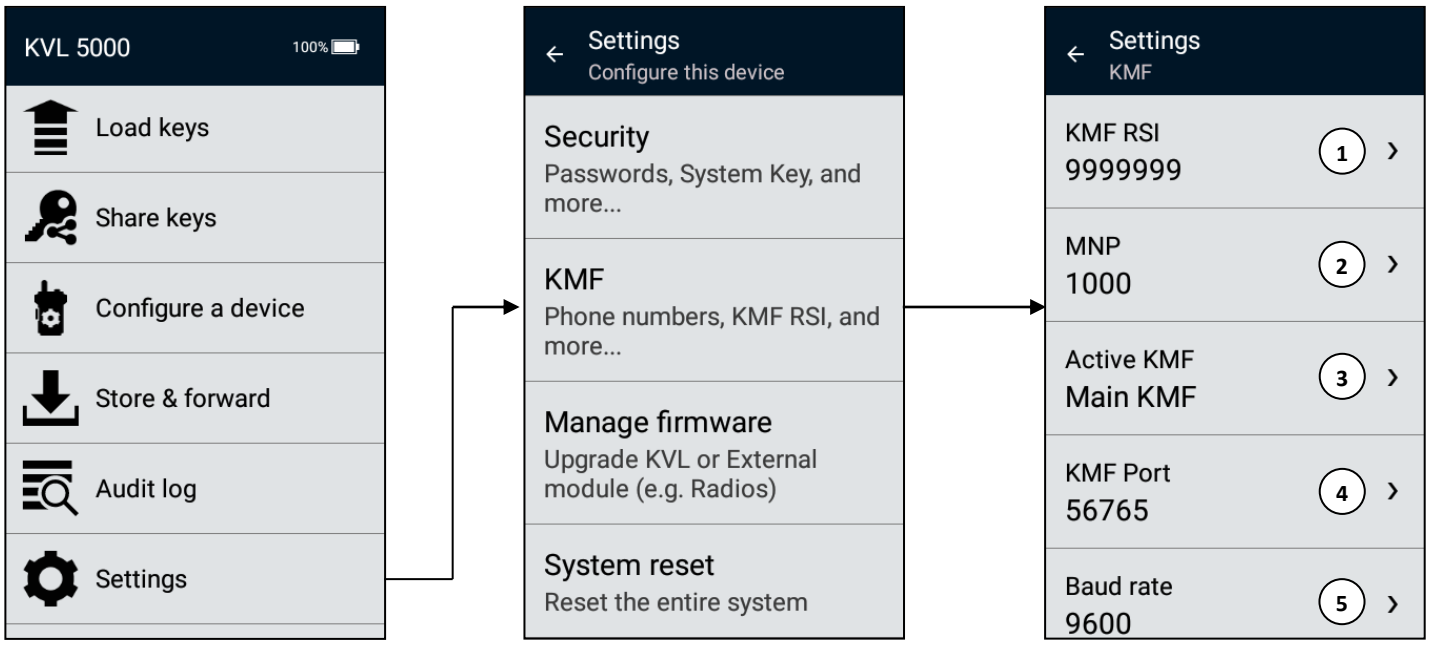
Remove keys from a device

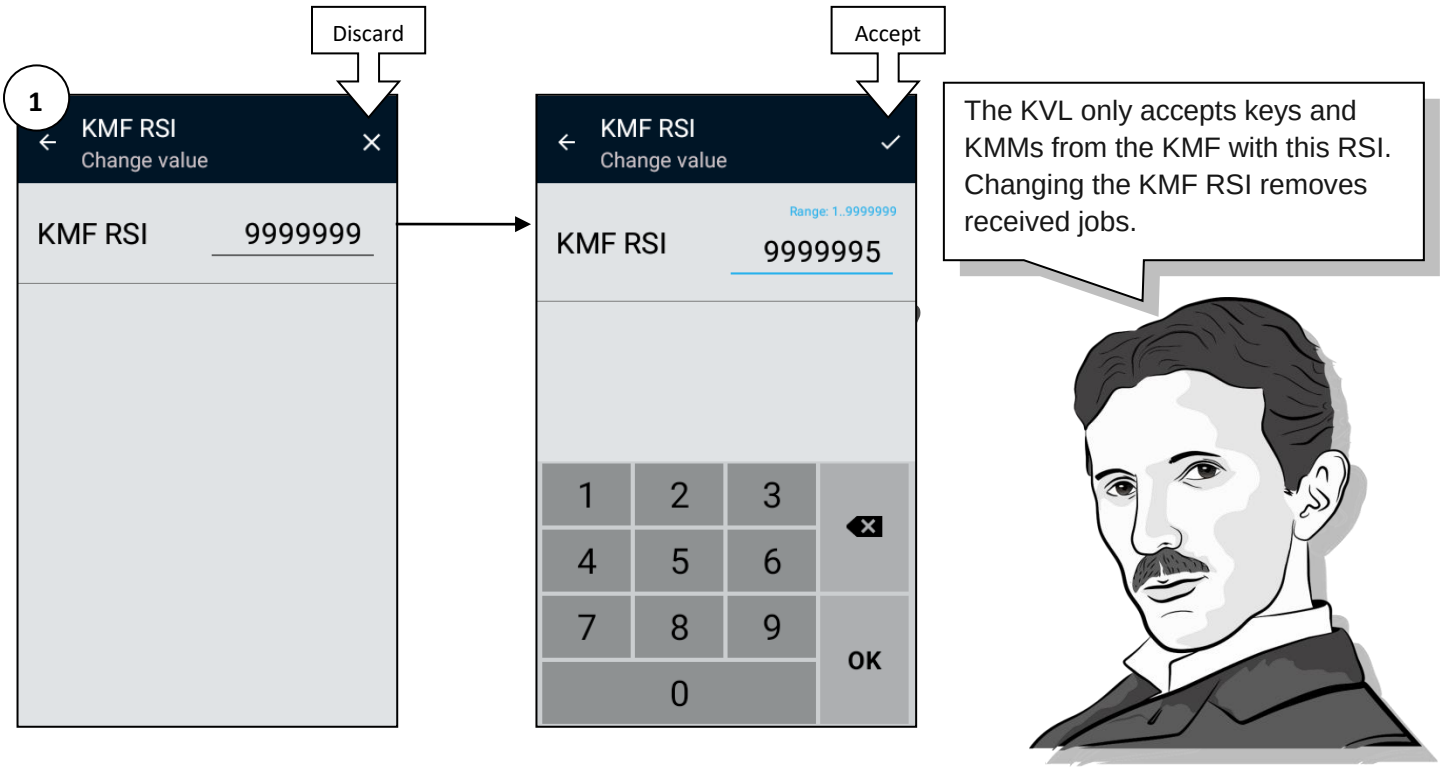




KMF Settings (1)

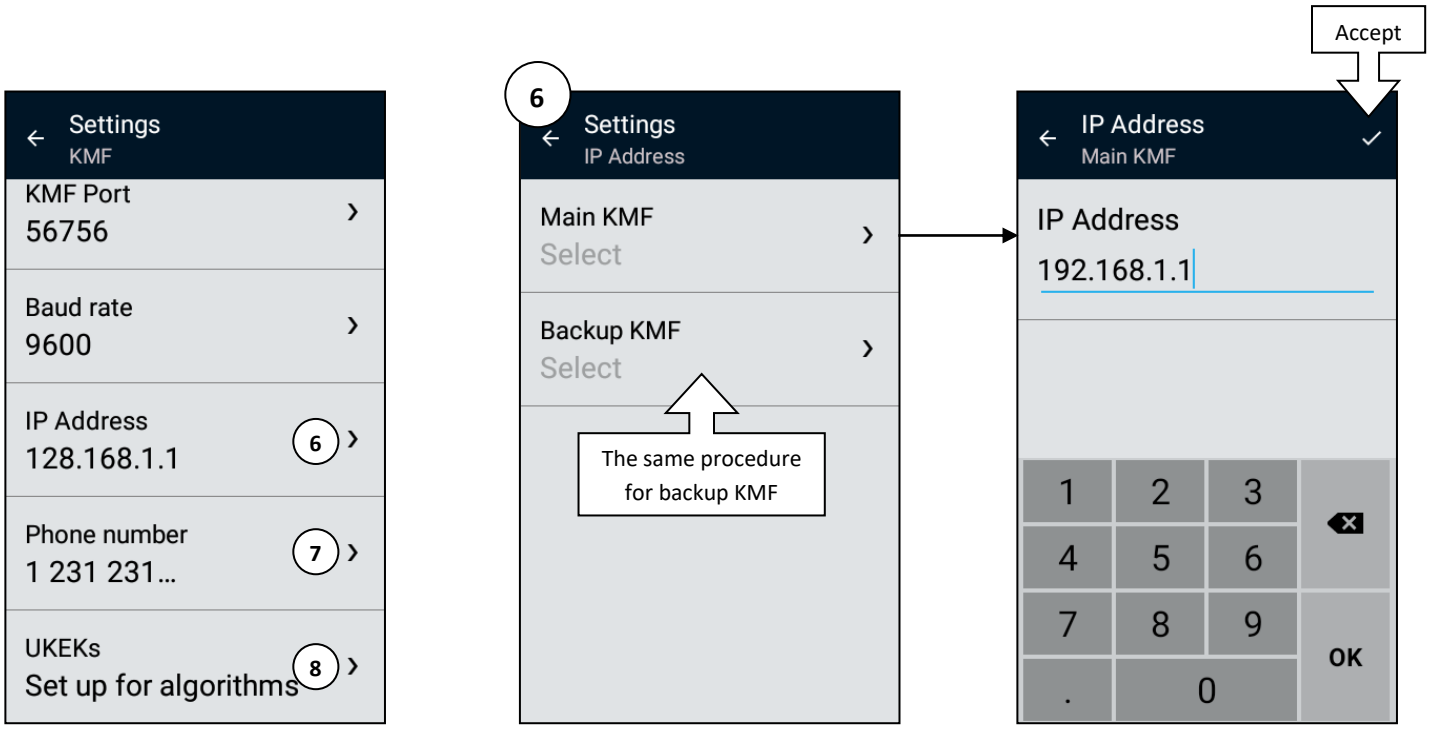
Before using your KVL to work with a KMF, you need to program several KMF related parameters.

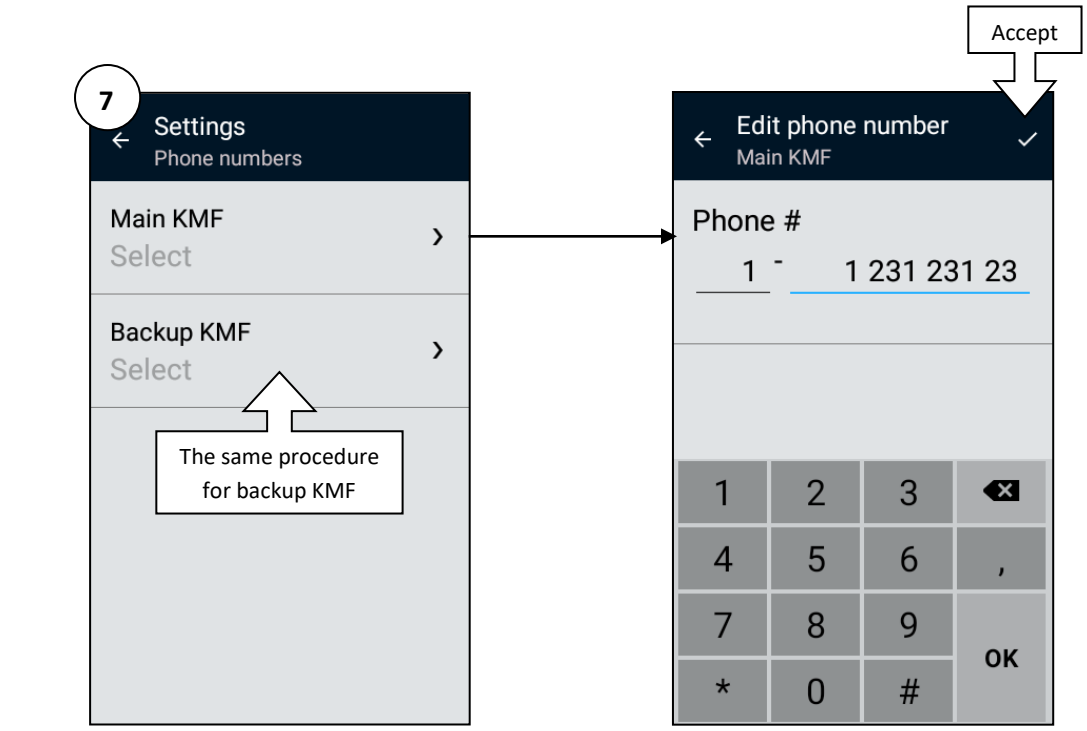




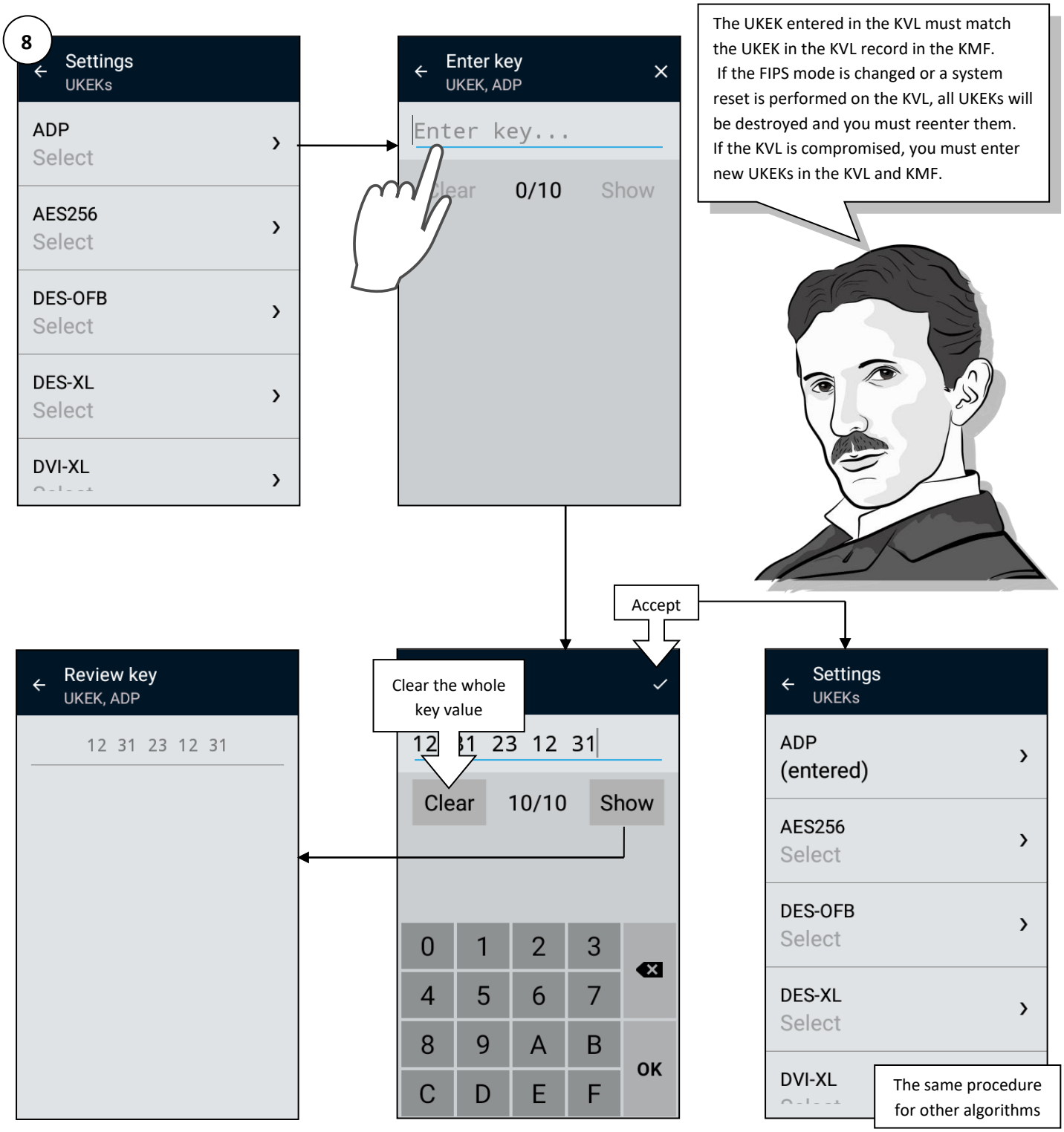
KMF Settings (2)

KMF Settings (3)

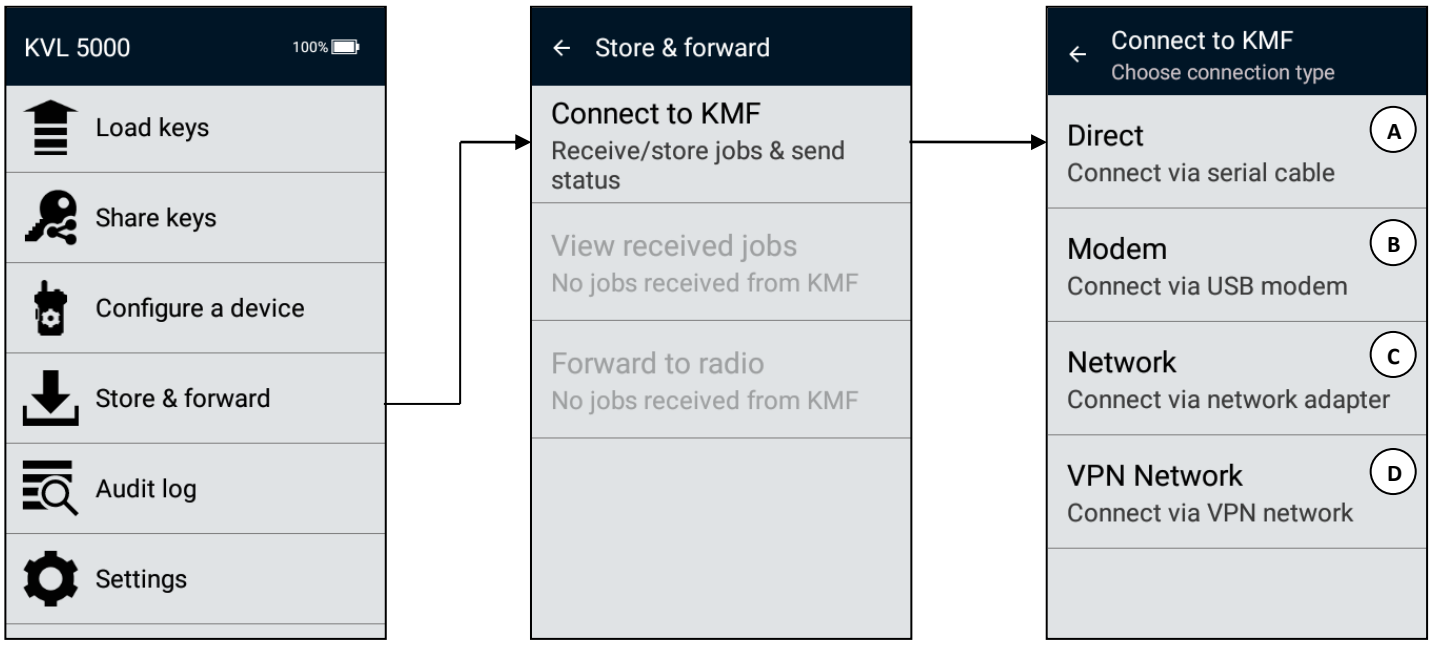




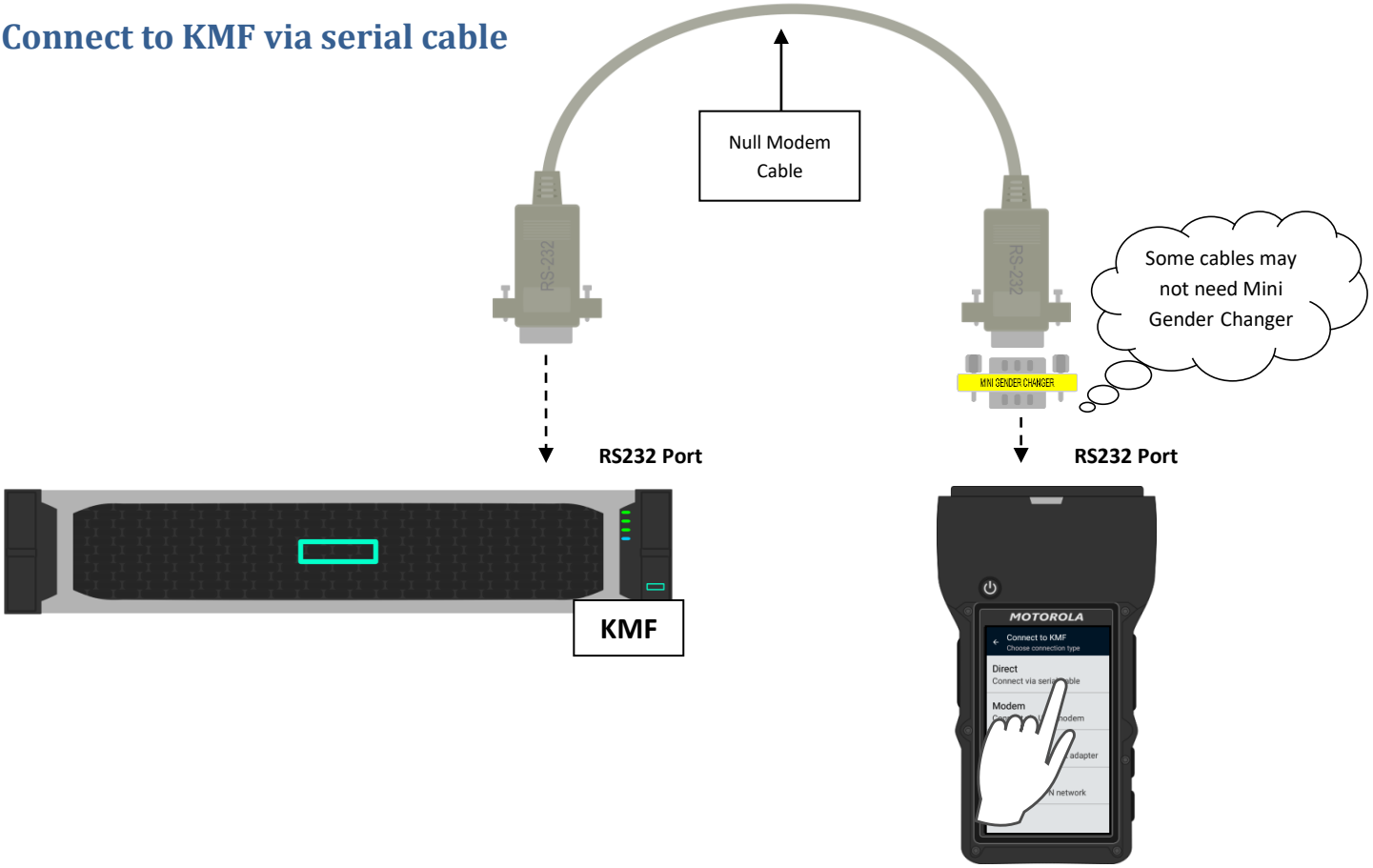
Entering the UKEK



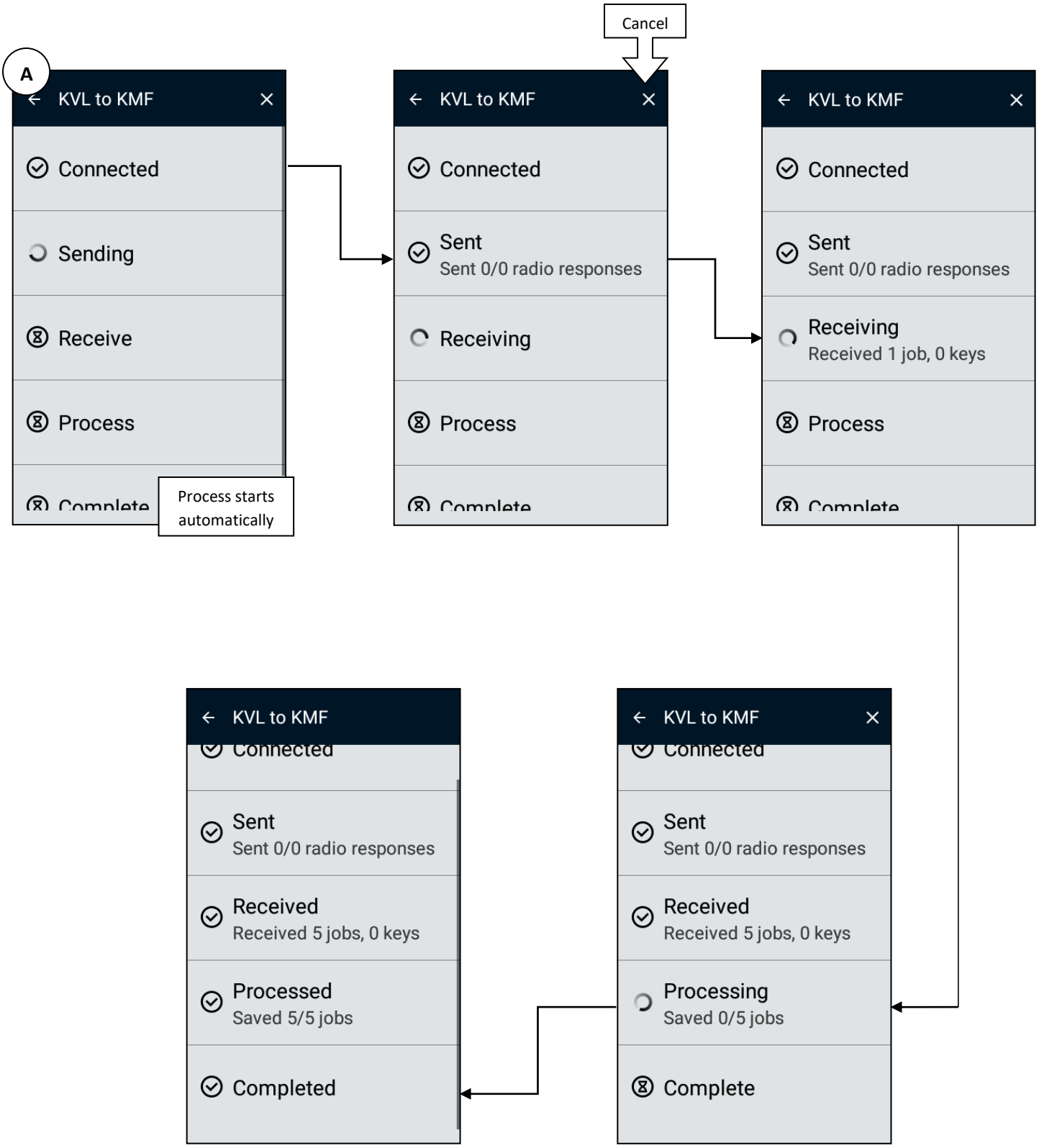
Make sure that the KVL battery is charged.



Connect to KMF via serial cable

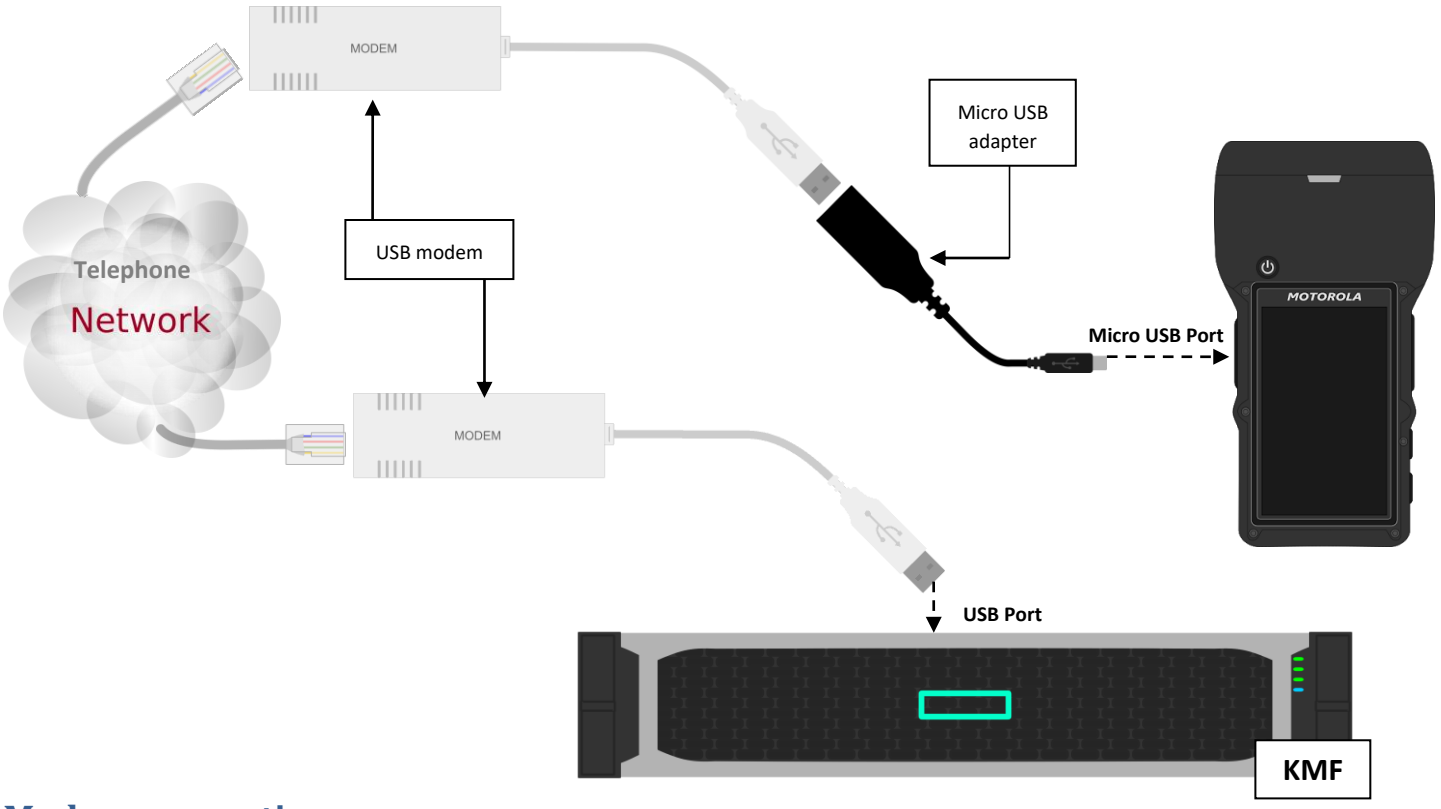


Direct Connection

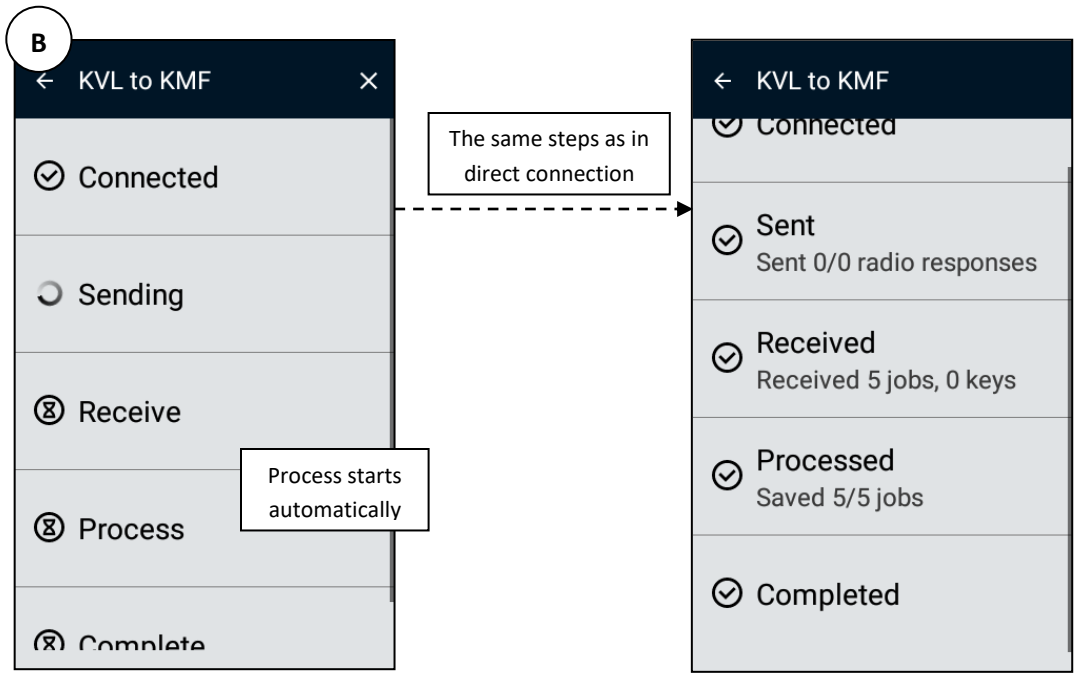


Connect to KMF via USB Modem

Phone number in KMF settings must be set

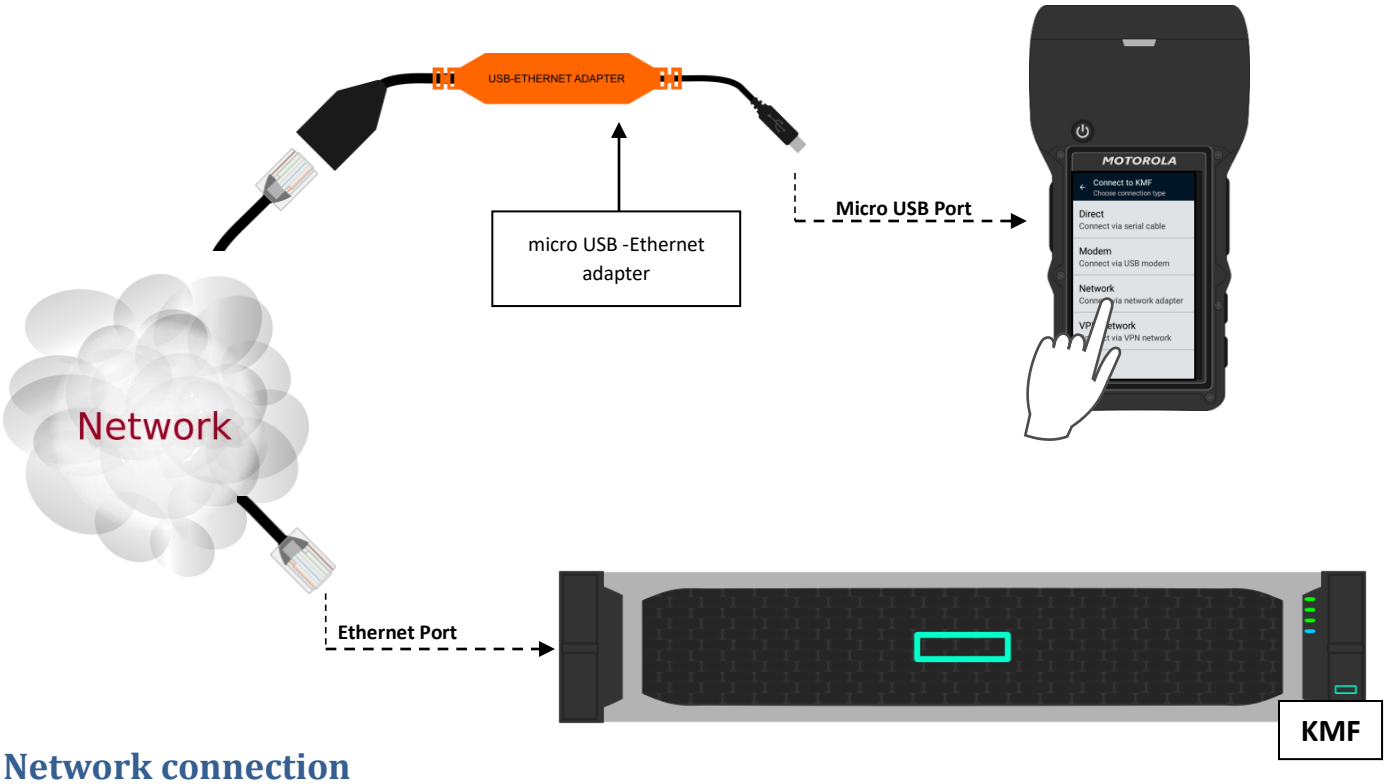


Modem connection

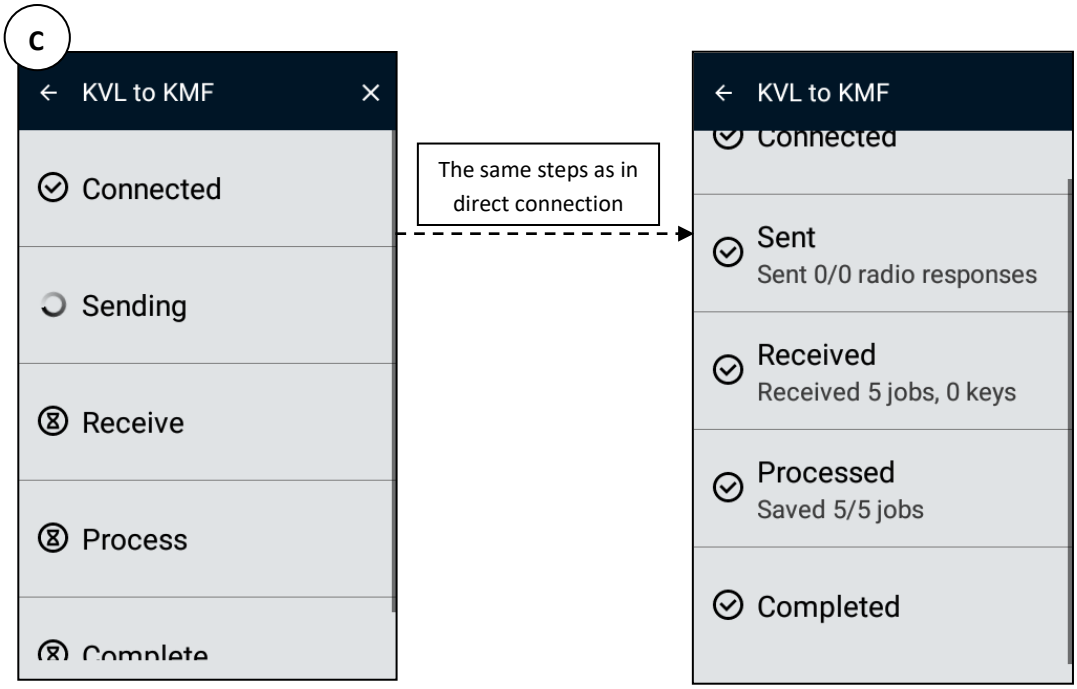


Connect to KMF via Network / VPN Network

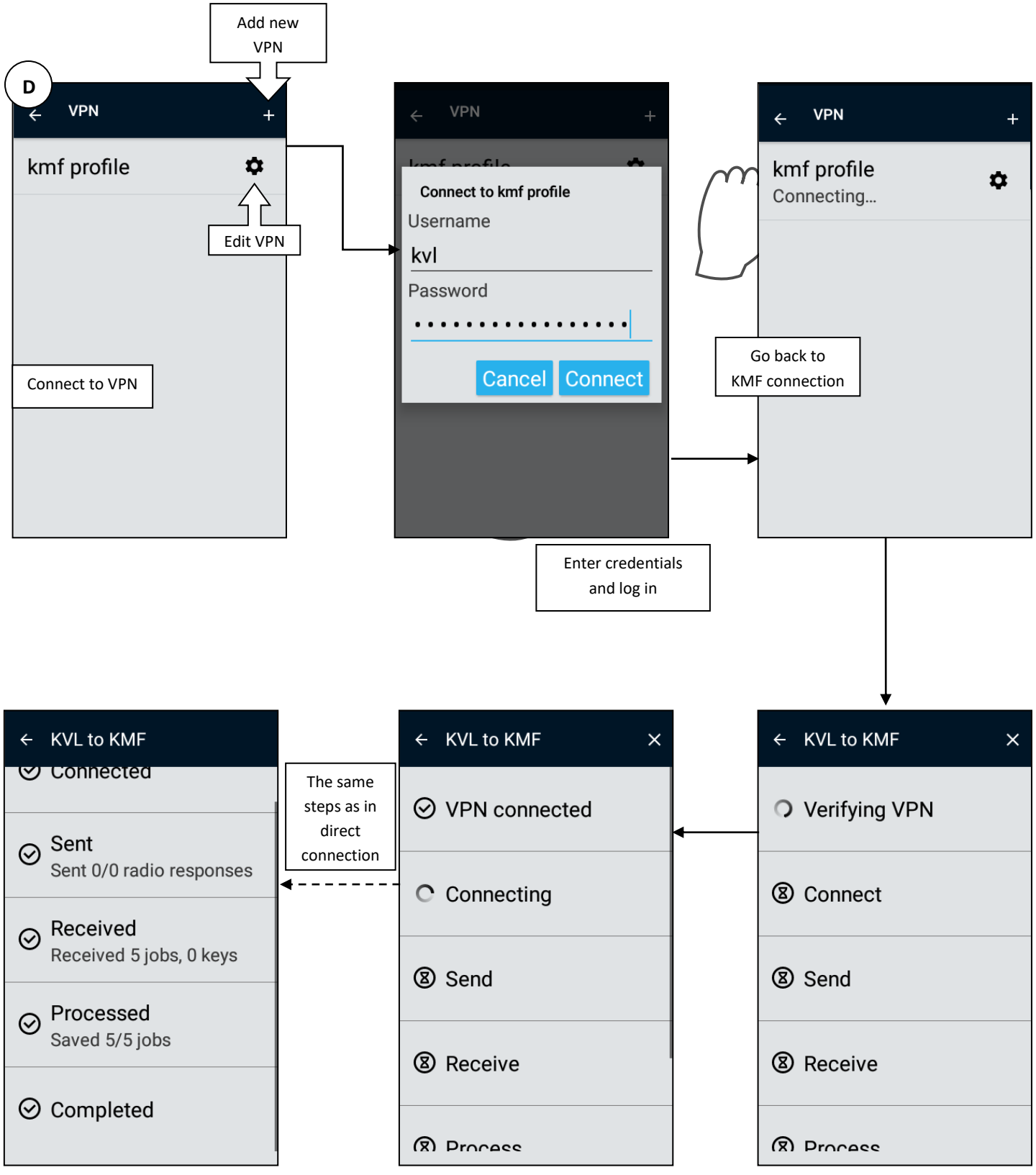
IP address in KMF settings must be set



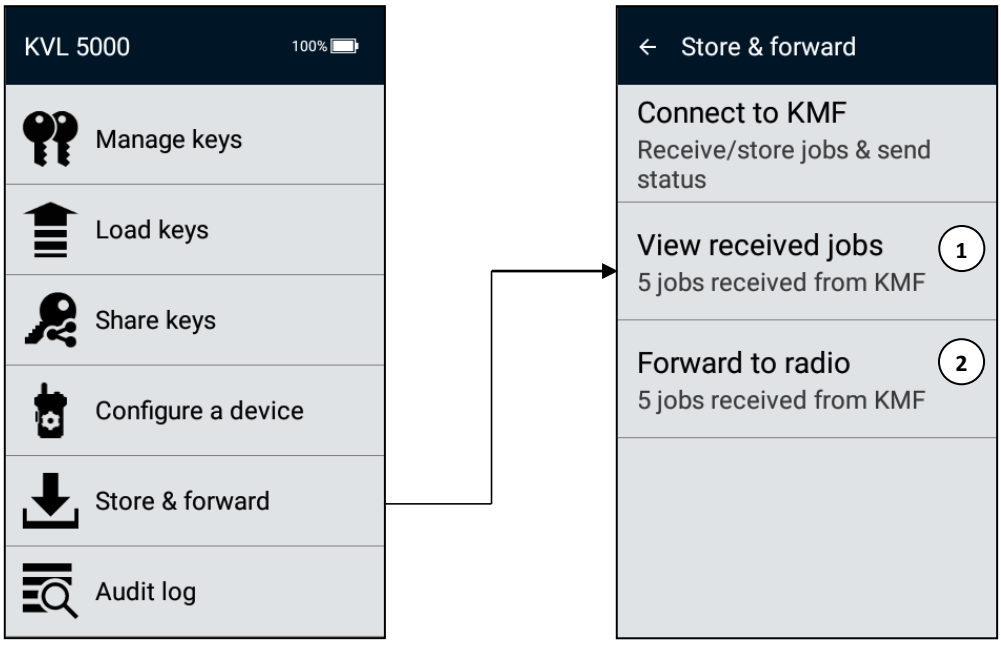
Network connection



VPN Connection

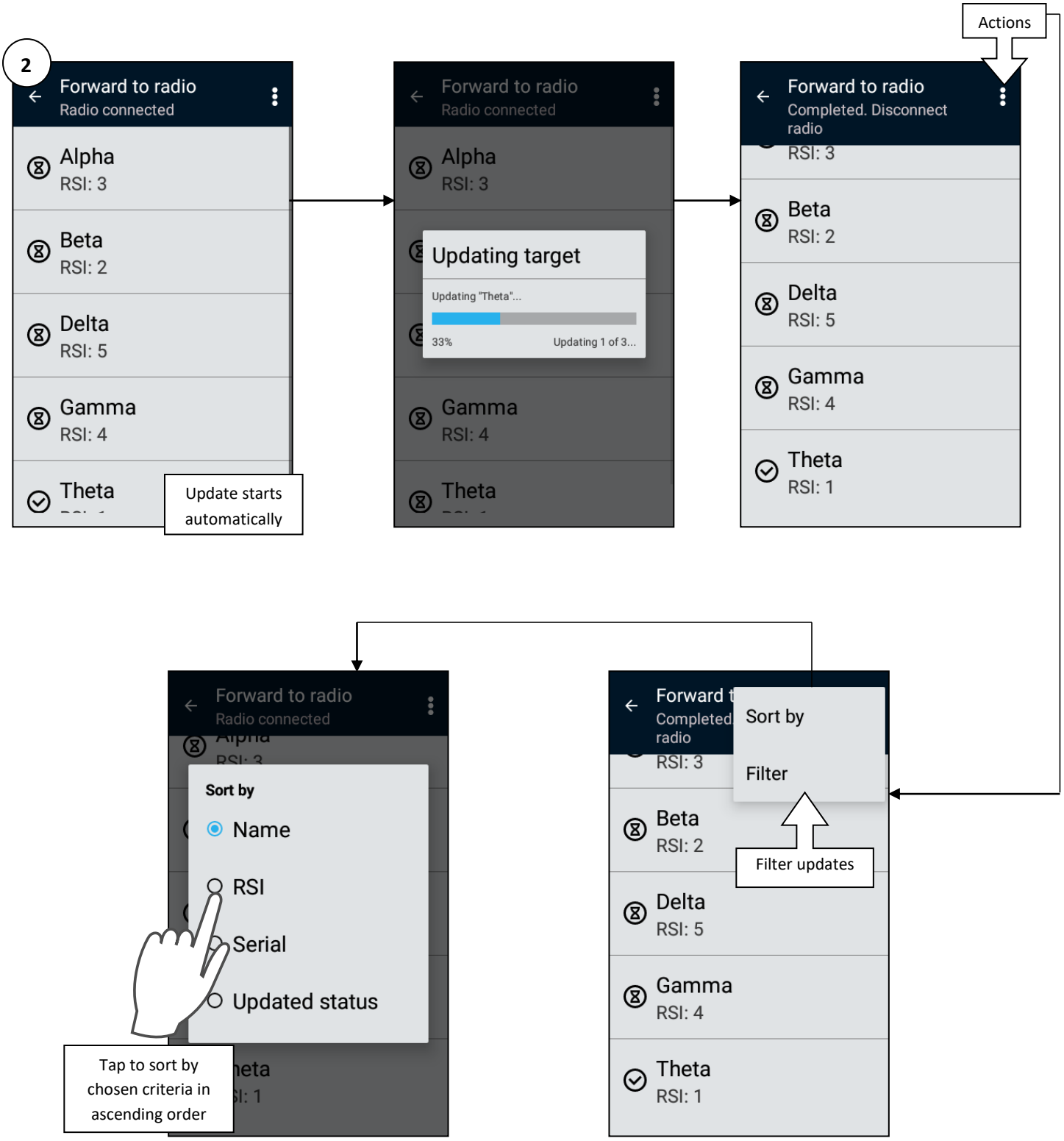


Connect target device to a KVL

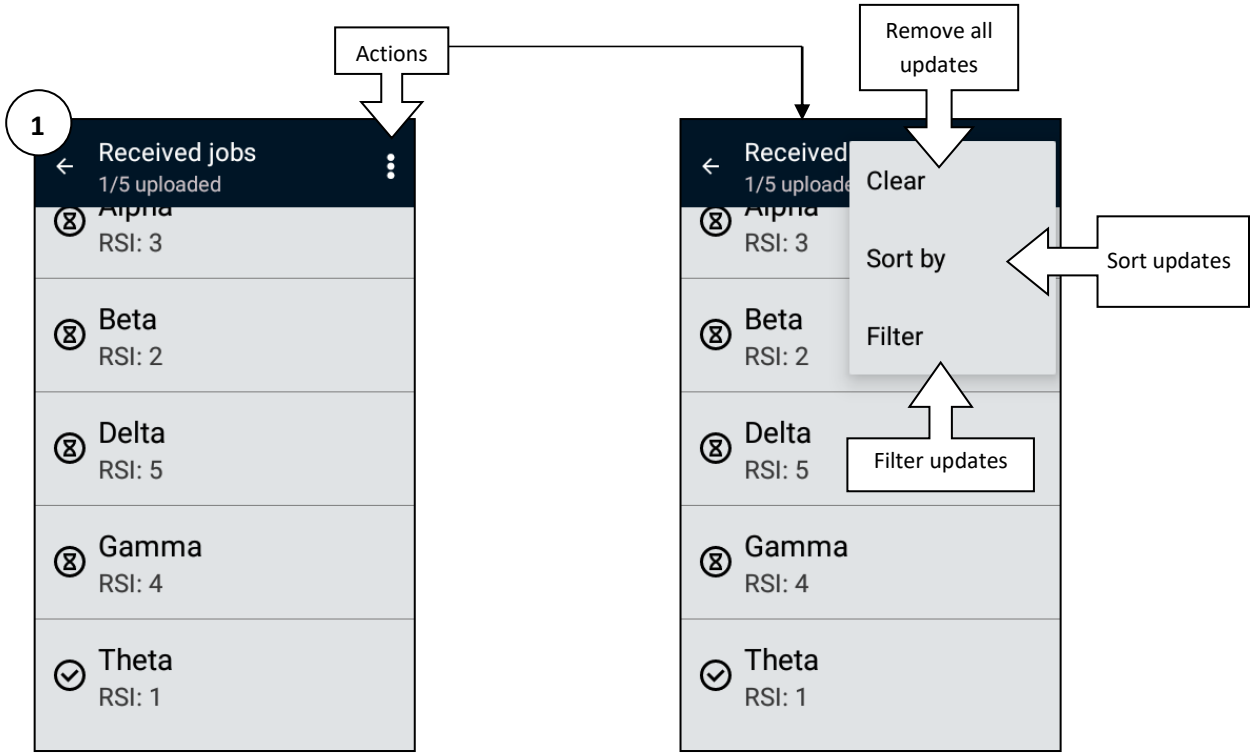


You can also perform forward to mobile radio over control head using serial cable. To do that you must first Provision mobile radio with control head keys

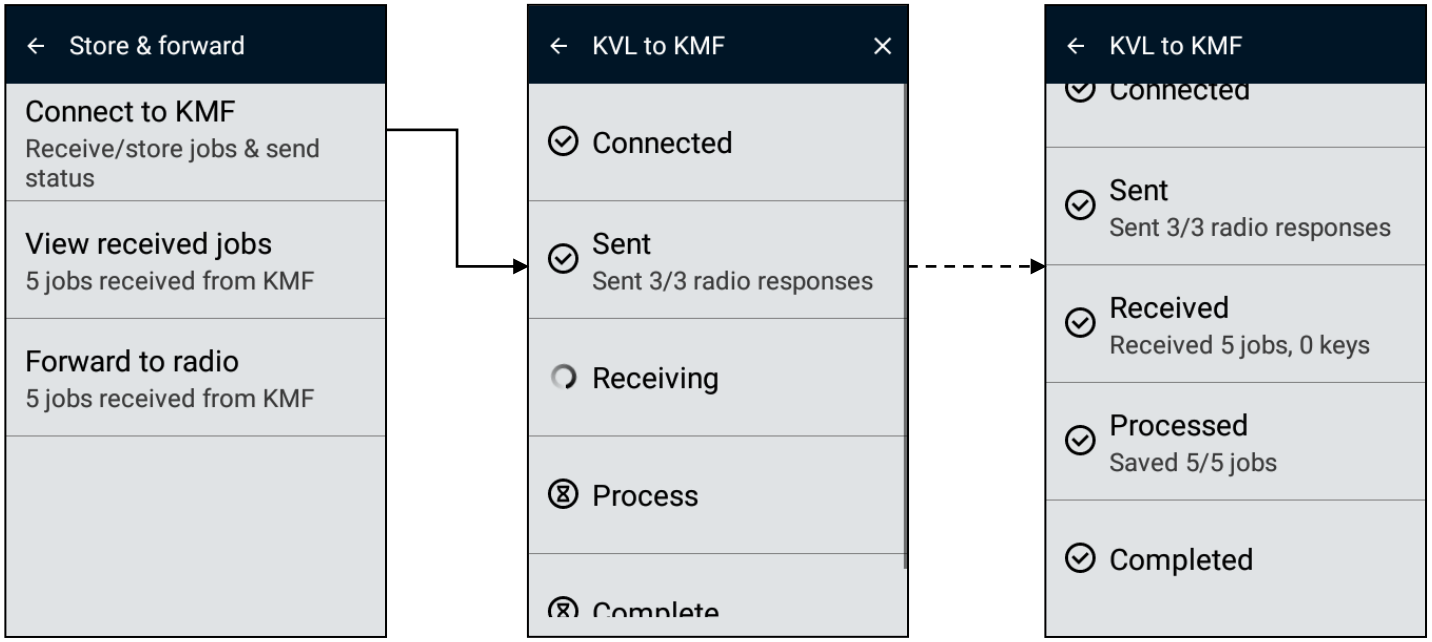
Forward jobs to a target device

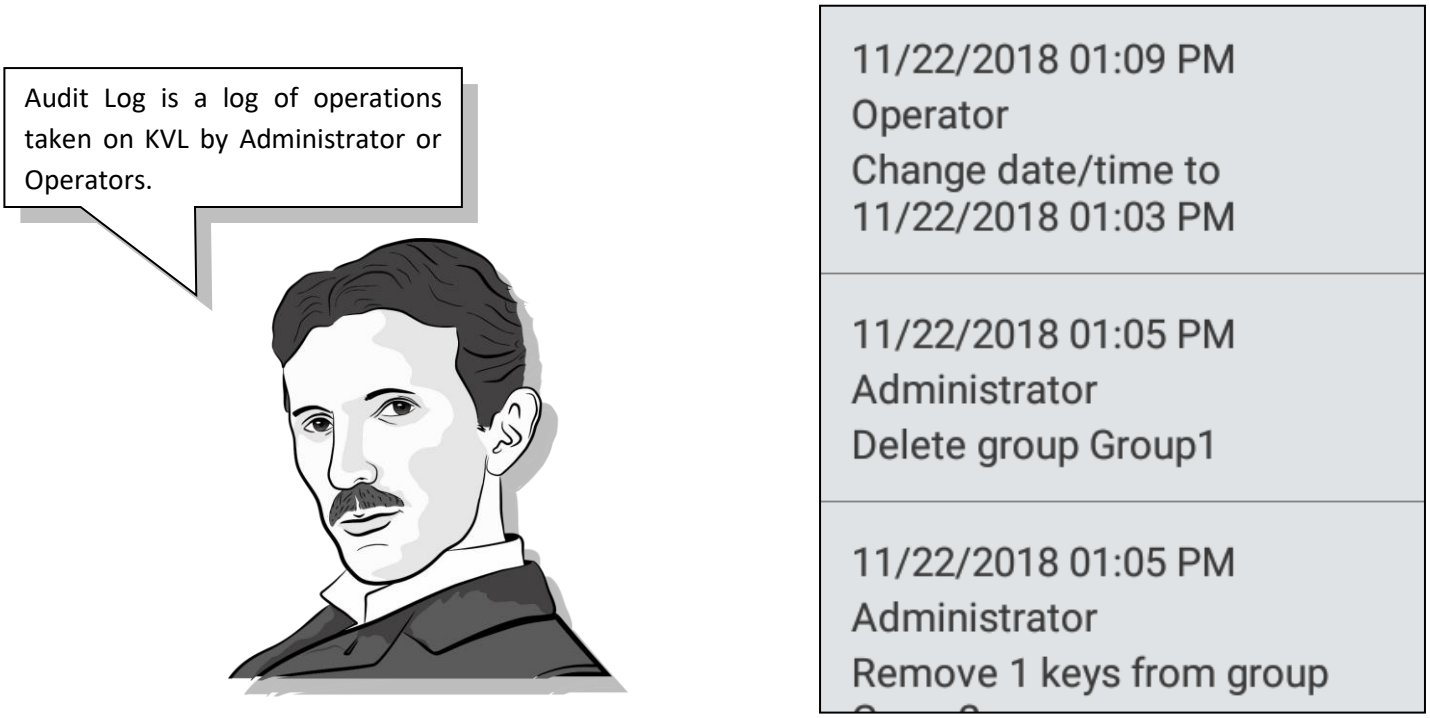


Viewing and clearing received jobs



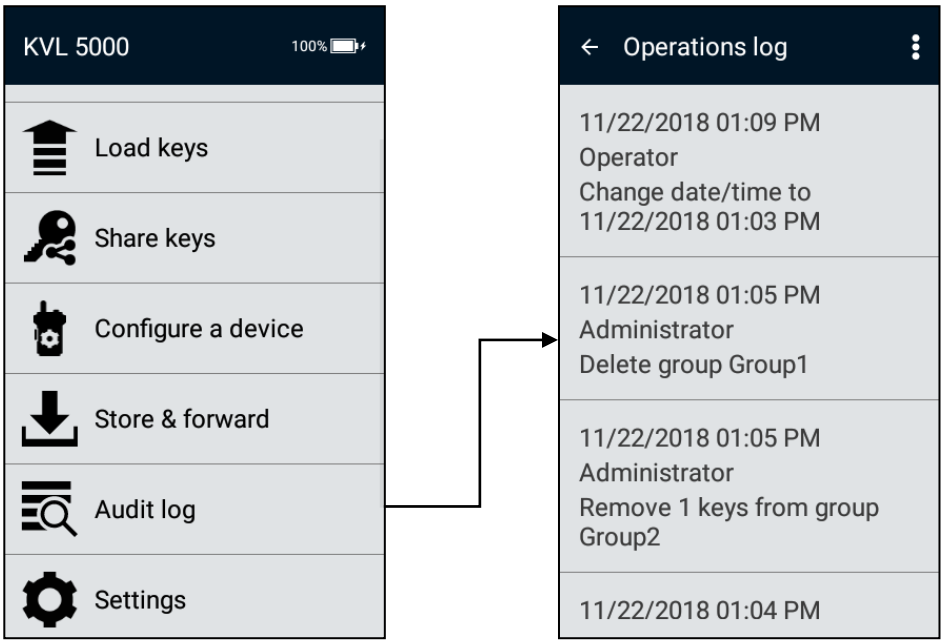
Upload the unit response messages to KMF



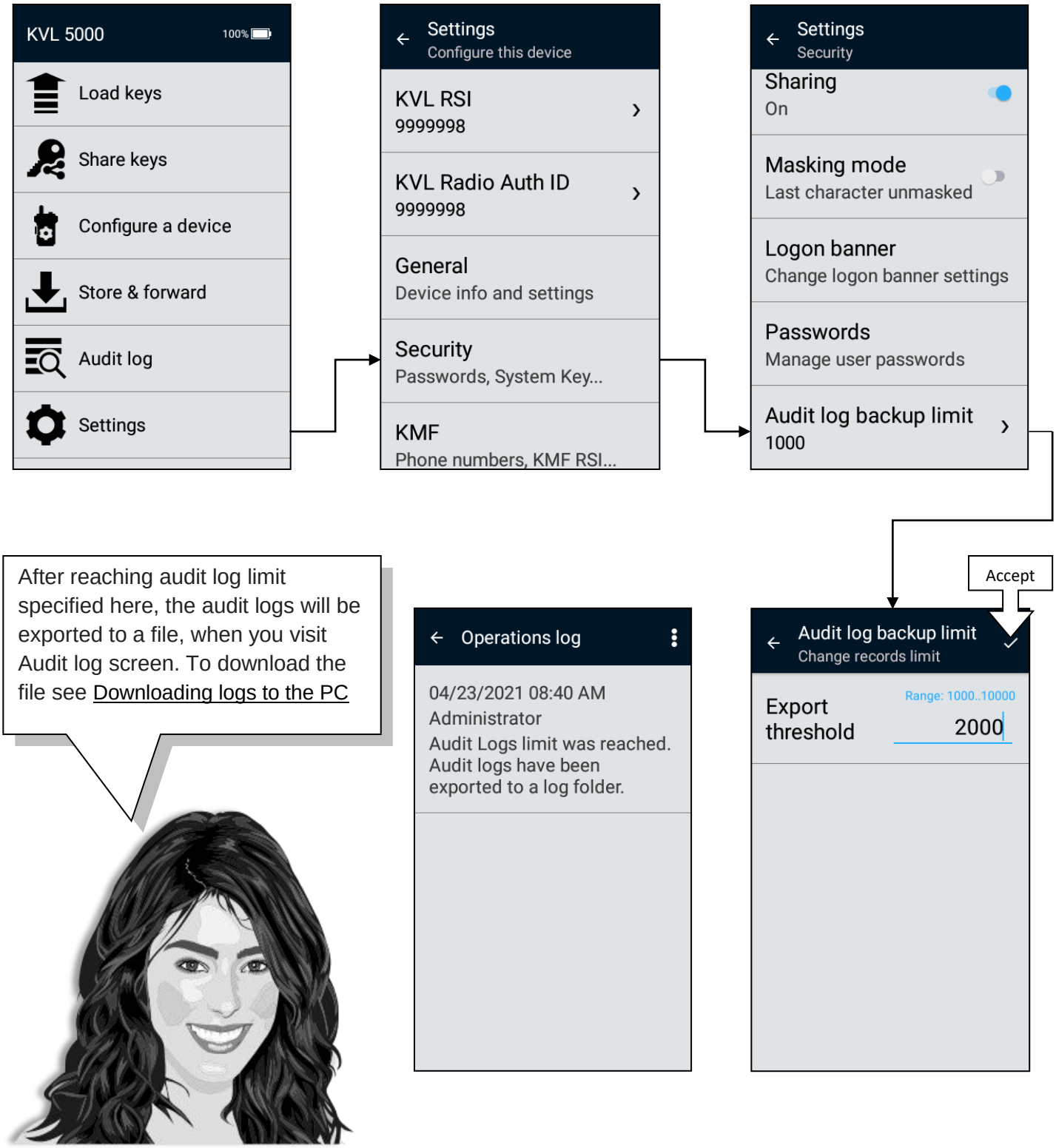


Reading the logs

Every user can read operation logs accessing it via Audit Log icon.

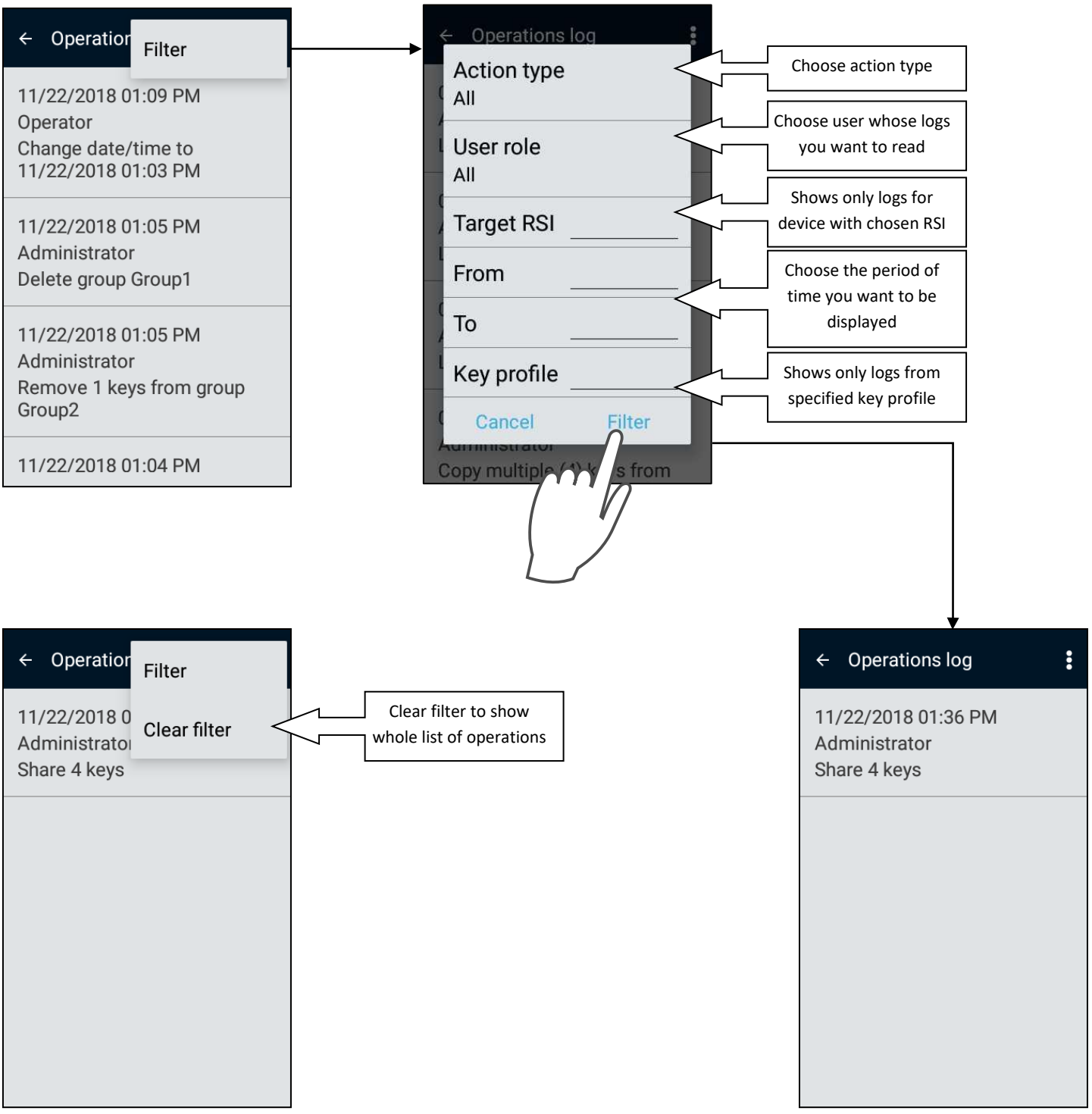


Audit log backup limit

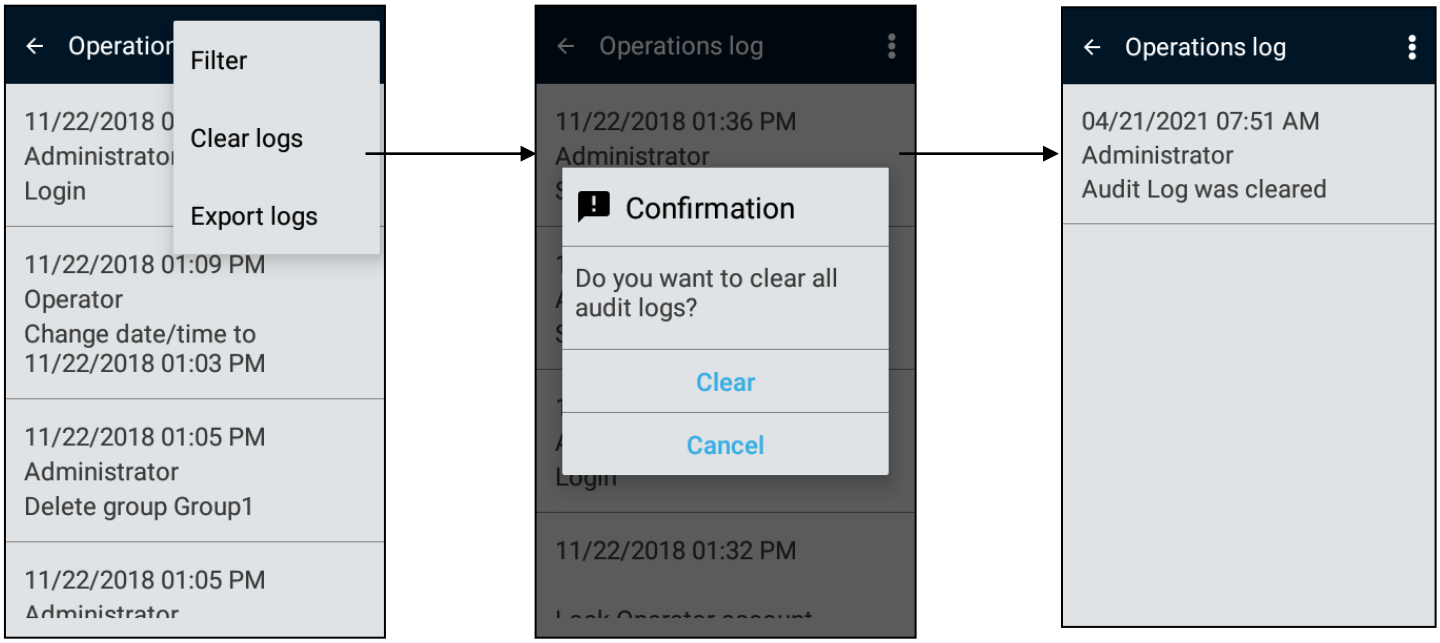


Filtering logs

User can filter logs to narrow the list of logs.

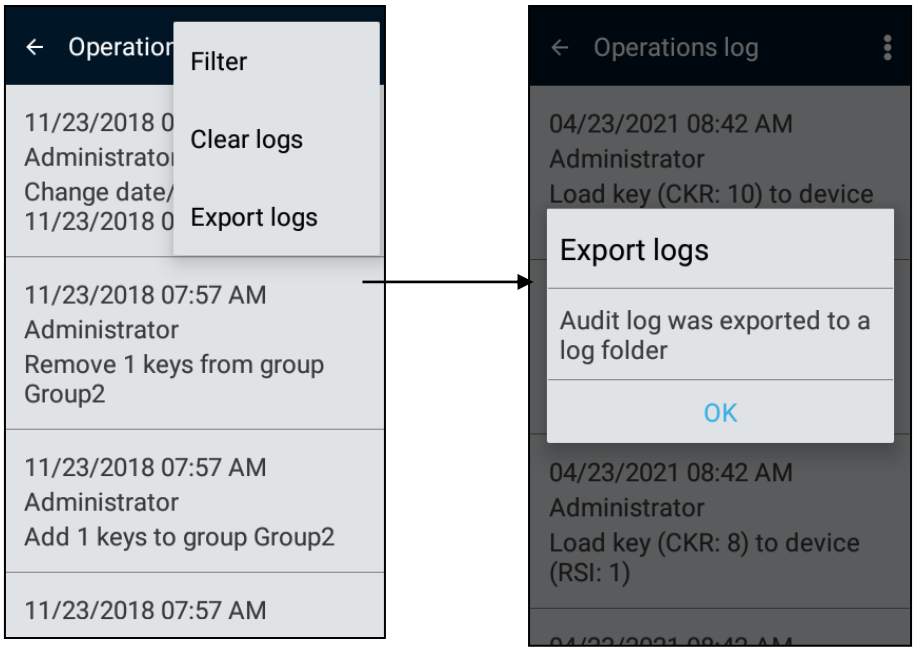


Administrator can clear operations log.



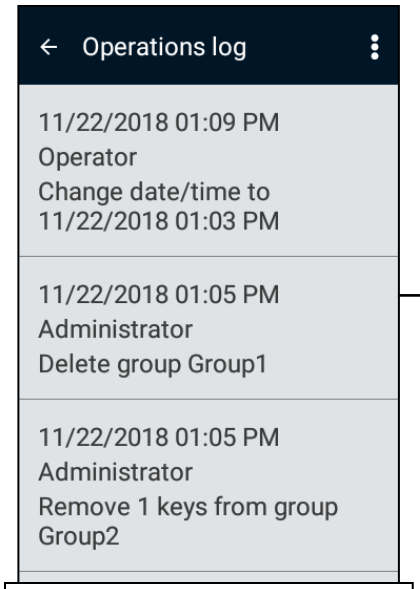
Exporting logs

Administrator can export logs to HTML file for detailed operations log.



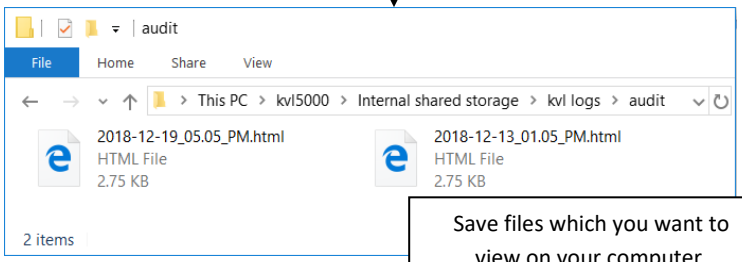
Downloading logs to the PC

After exporting logs, Administrator can download exported logs into PC

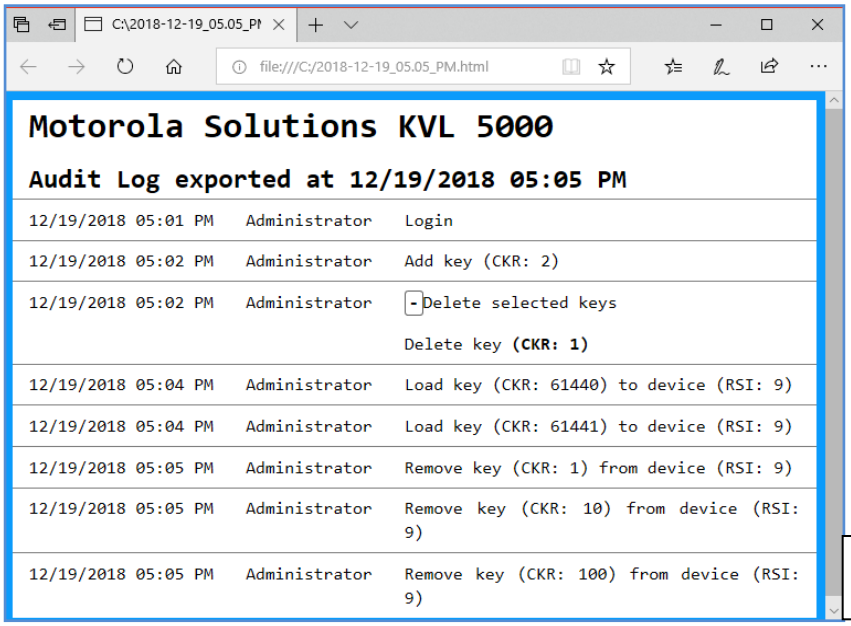


Go to Operations log screen

Connect KVL via USB to the PC



Save files which you want to view on your computer.



Motorola Solutions KVL 5000

Audit Log exported at 12/19/2018 05:05 PM

12/19/2018 05:01 PM	Administrator	Login
12/19/2018 05:02 PM	Administrator	Add key (CKR: 2)
12/19/2018 05:02 PM	Administrator	-Delete selected keys Delete key **(CKR: 1)**
12/19/2018 05:04 PM	Administrator	Load key (CKR: 61440) to device (RSI: 9)
12/19/2018 05:04 PM	Administrator	Load key (CKR: 61441) to device (RSI: 9)
12/19/2018 05:05 PM	Administrator	Remove key (CKR: 1) from device (RSI: 9)
12/19/2018 05:05 PM	Administrator	Remove key (CKR: 10) from device (RSI: 9)
12/19/2018 05:05 PM	Administrator	Remove key (CKR: 100) from device (RSI: 9)

.html file provides more details about operations.

Operator permissions

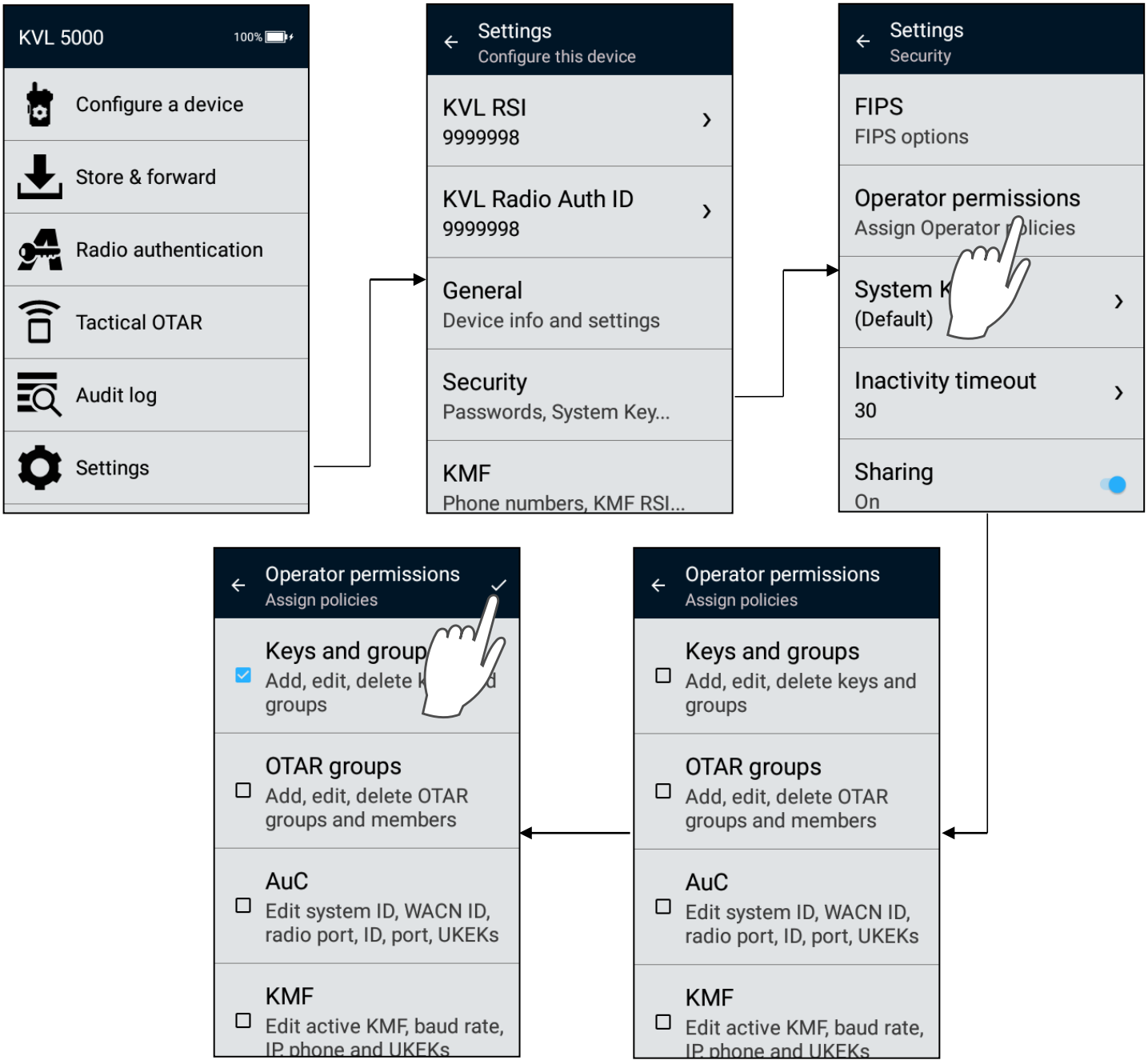
The Administrator has access to all functions and features. The Operator does **not** have access to the following functions and features:

- Upgrading Crypto Module of the KVL and radio
- Upgrading KVL software
- Adding, deleting, and editing keys and groups of keys
- Entering and changing KVL Radio Set Identifier (RSI)
- Entering and changing KVL Radio Authentication ID
- Entering and changing KMF RSI
- Setting and changing the KVL inactivity timeout
- Changing Federal Information Processing Standard (FIPS) mode
- Changing the System Key
- Changing the Sharing mode
- Changing the USB key load mode and port
- Changing the Key File Export mode
- Changing the Administrator password
- Changing the certain KMF parameters: port value, IP address, phone number
- Changing the certain AuC parameters: System ID, WACN ID, port value, IP address
- Adding, deleting, and editing OTAR groups
- Updating OTAR groups
- Entering and changing KMF RSI
- Entering and changing KMF Message Number Period (MNP)
- Changing UKEK for KMF or AuC operation

- Clearing the list of received jobs
- Clearing the list of KSuId
- Clearing audit log records
- Setting password security options
- Renaming and clearing key profiles

Full Role based Action List available on KVL

Assigning additional operator permissions

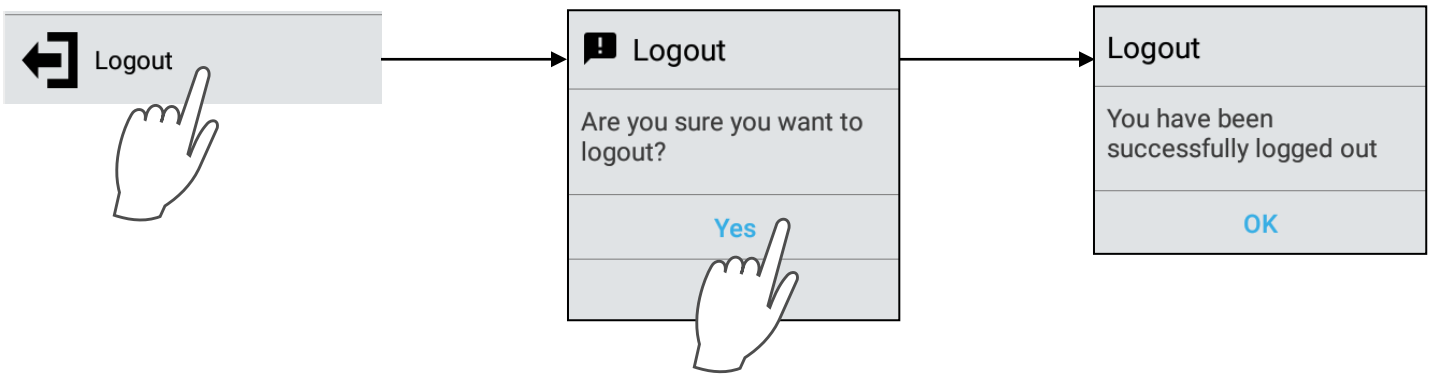


Operator permissions

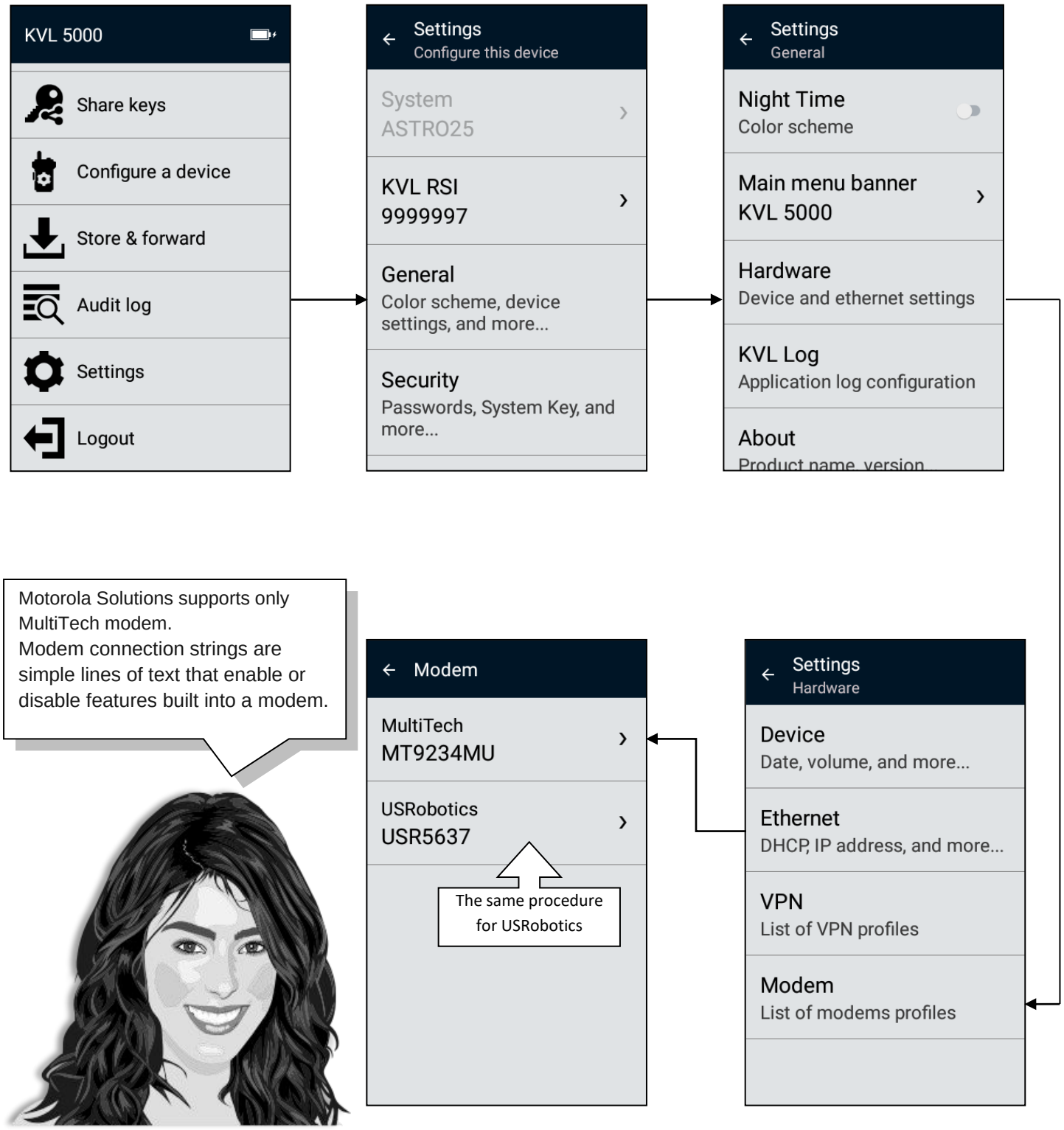
The Administrator can assign additional permissions for the Operator by selecting policies on Operator permissions menu. Policies give following functions and features for the Operator:

- Keys and groups
  - ✓ Adding, deleting, and editing keys and groups of key
- OTAR groups
  - ✓ Adding, deleting, and editing OTAR groups
- AuC
  - ✓ Changing the certain AuC parameters: System ID, WACN ID, port value, IP address
  - ✓ Changing UKEK for AuC operation
- KMF
  - ✓ Changing the certain KMF parameters: port value, IP address, phone number
  - ✓ Changing UKEK for KMF operation

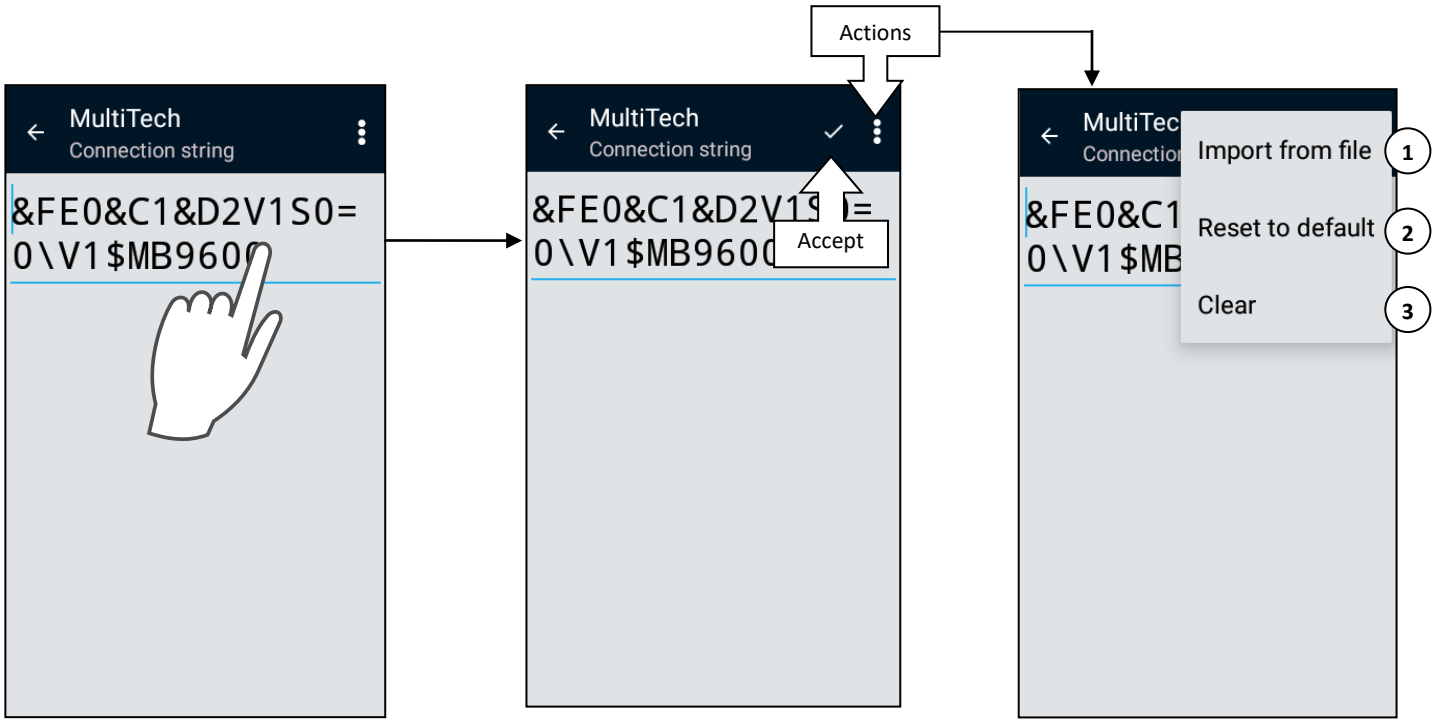
You can quickly switch between account types (Administrator or Operator) by logging off the current account.

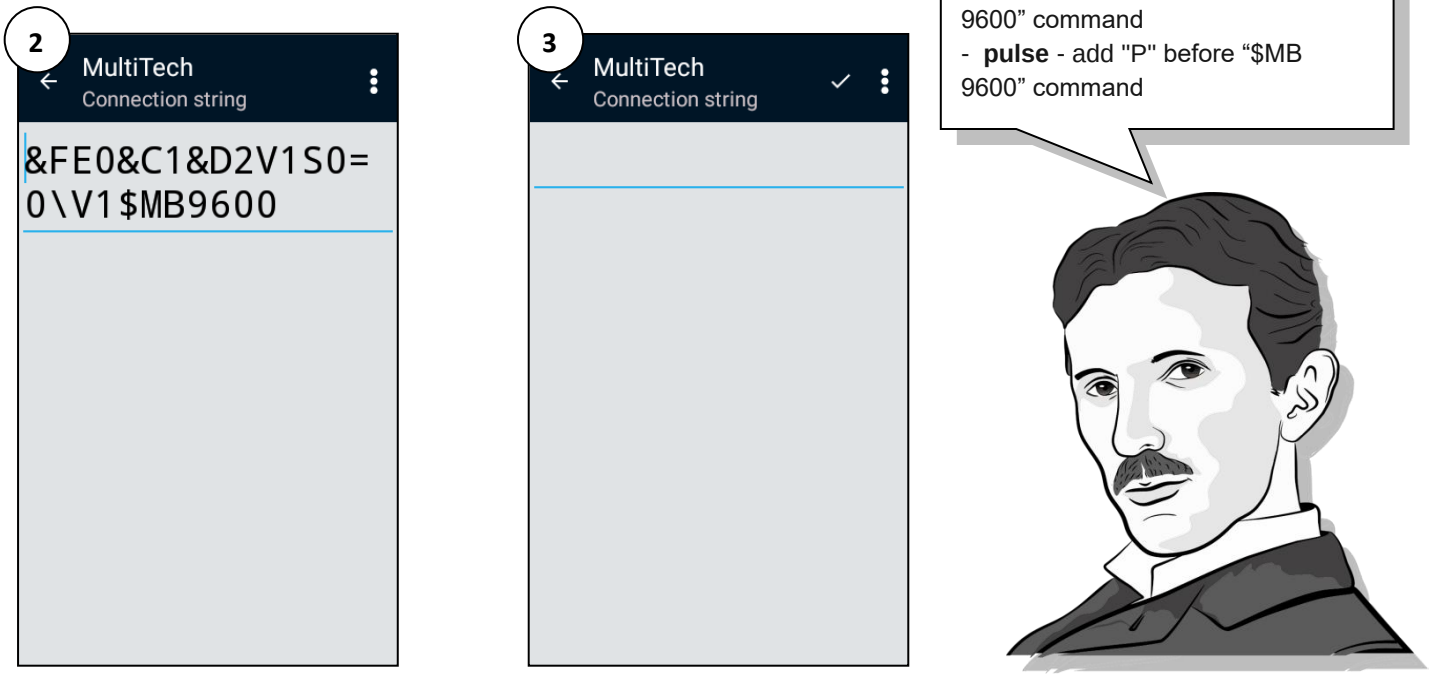


Edit Modem Connection String (1)

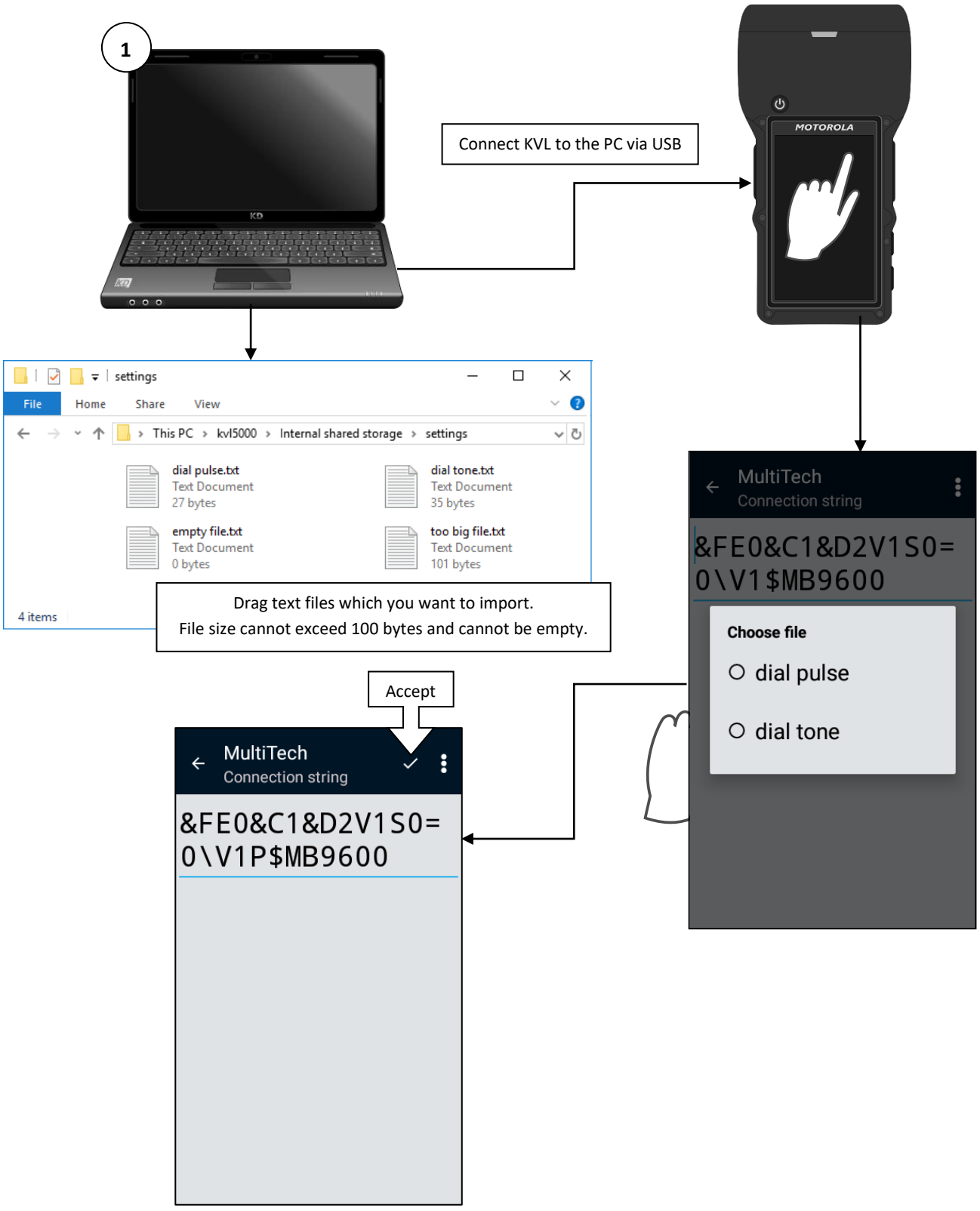


Edit Modem Connection String (2)



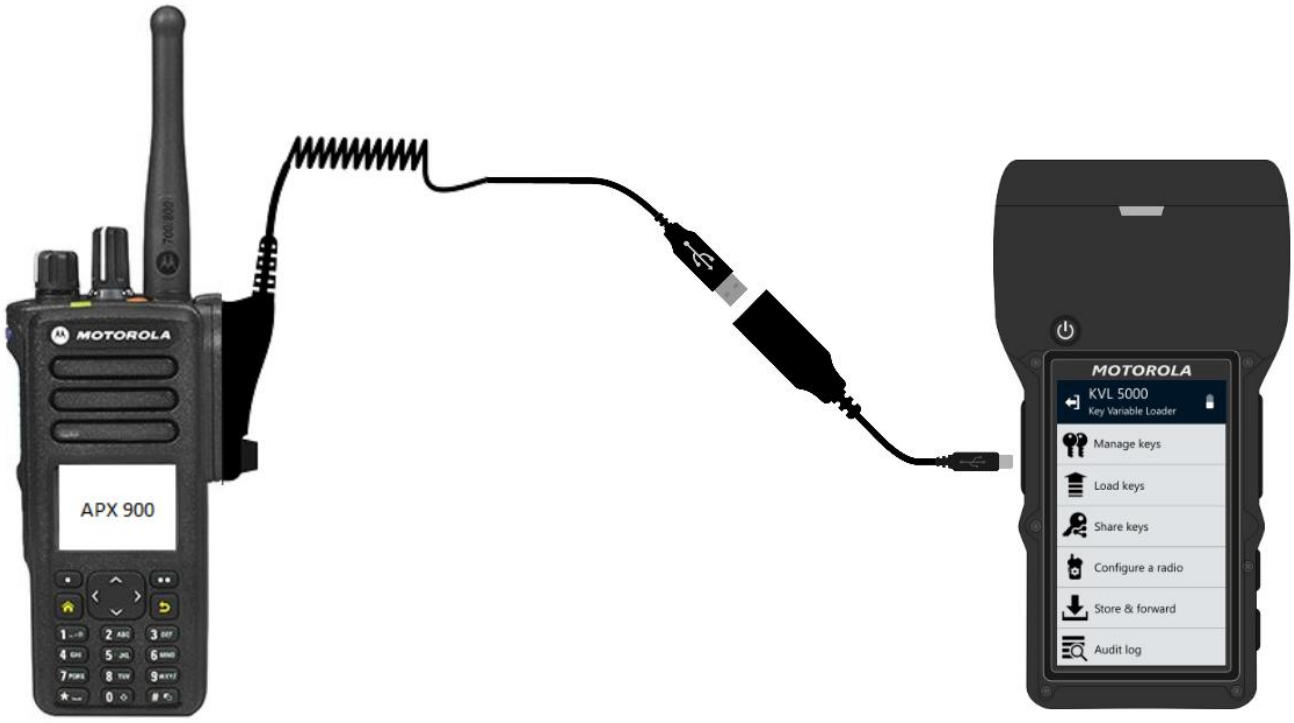


Import Modem Connection String



Provision radio

Radio provisioning is an operation of loading authentication key to a device. All Motorola radios configured for the radio authentication feature are supported. The radio provisioning is executed using RS-232 cable.

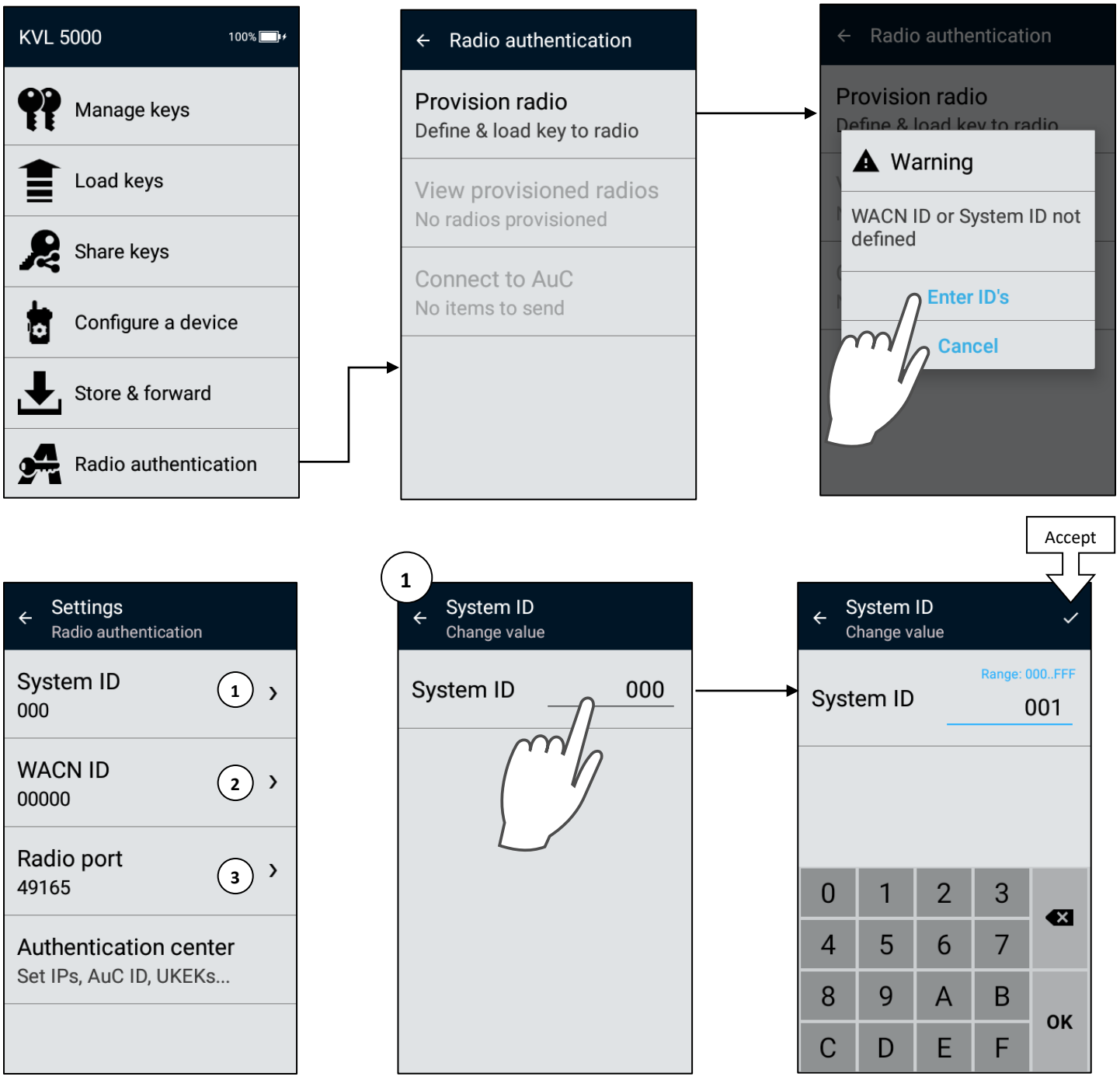


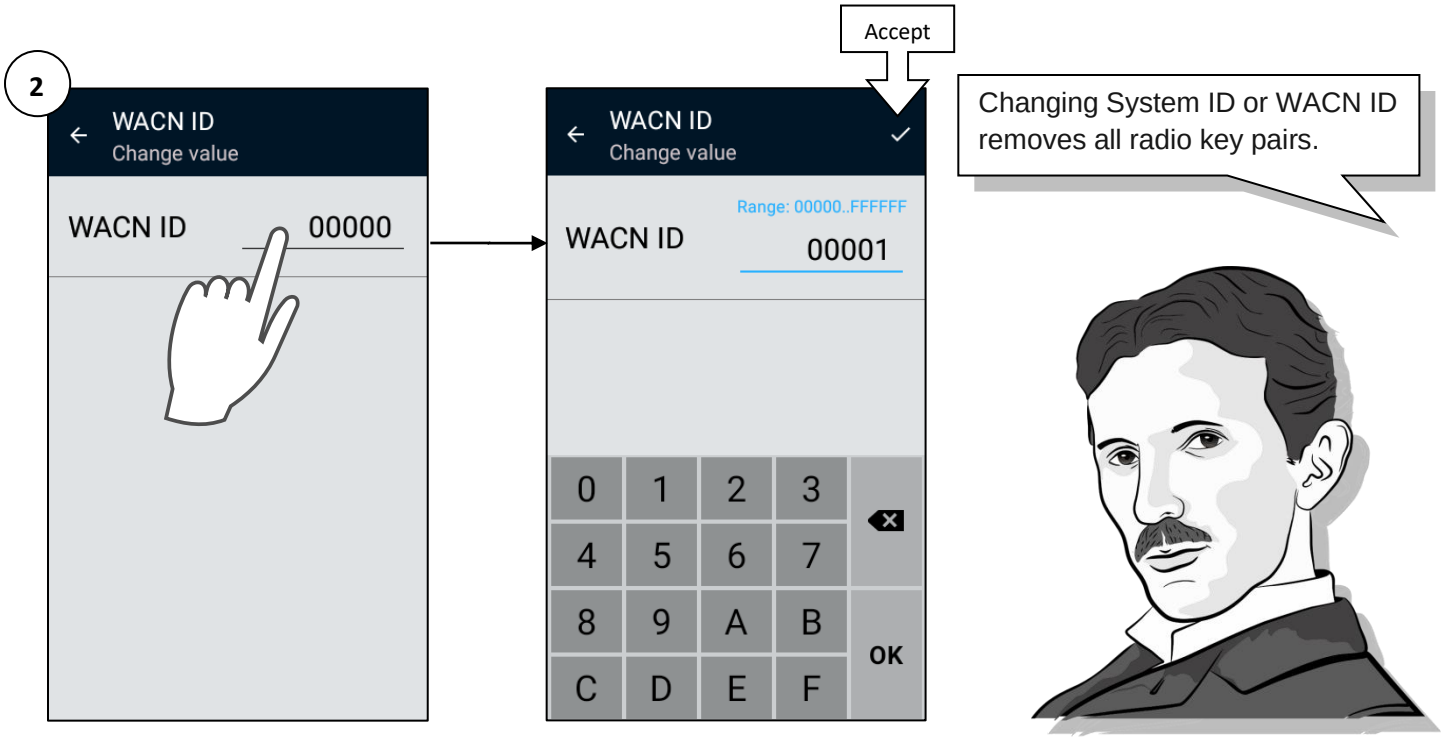
You can also connect devices over USB that support software encryption to perform key load operation when USB key loading feature is enabled.

You can also load authentication keys to mobile radios over control head using serial cable.

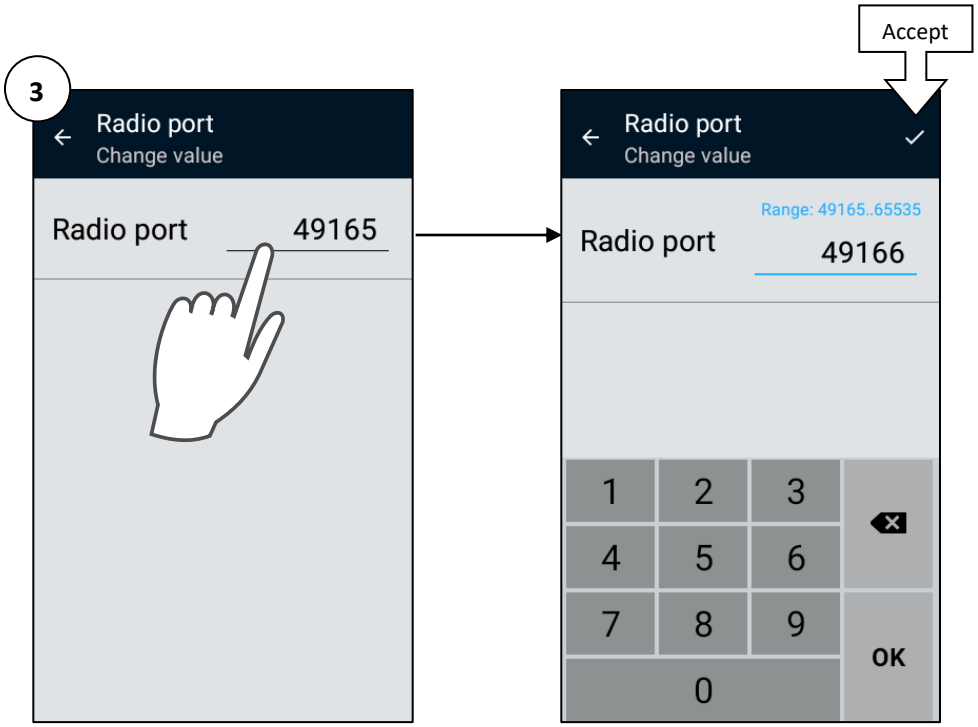
Radio provision settings

Before provisioning a radio there is a need to define System ID and WACN ID.

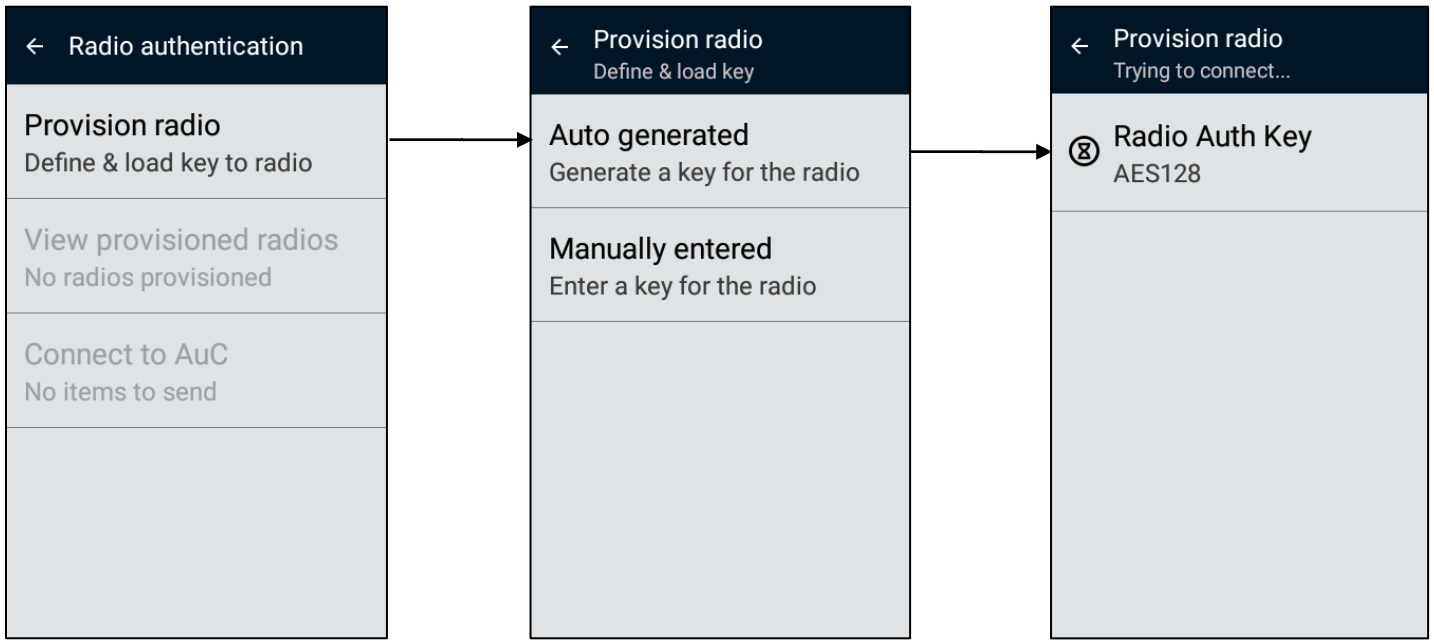


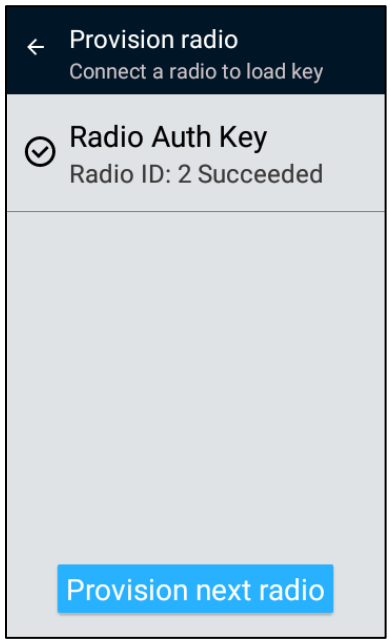


Additionally a radio port for radio authentication can be modified.



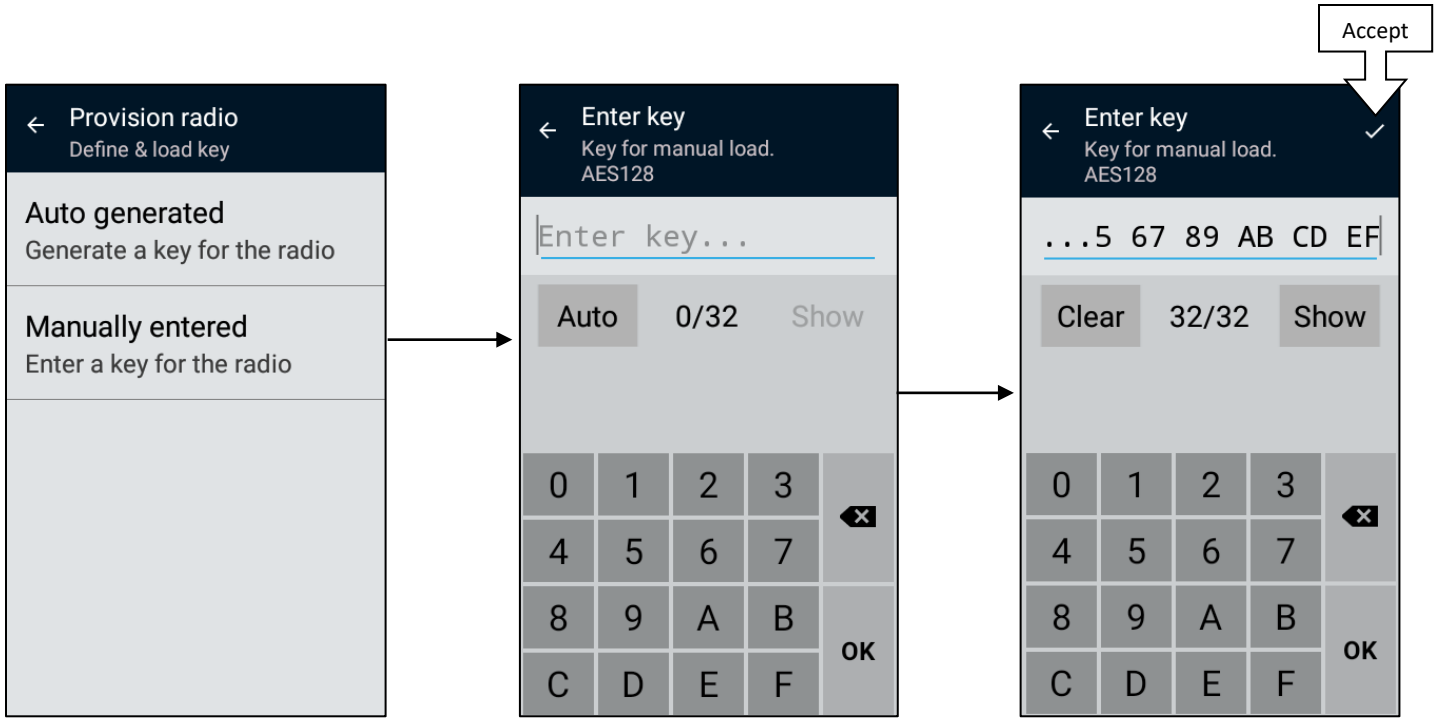
Provision radio with auto generated authentication key.

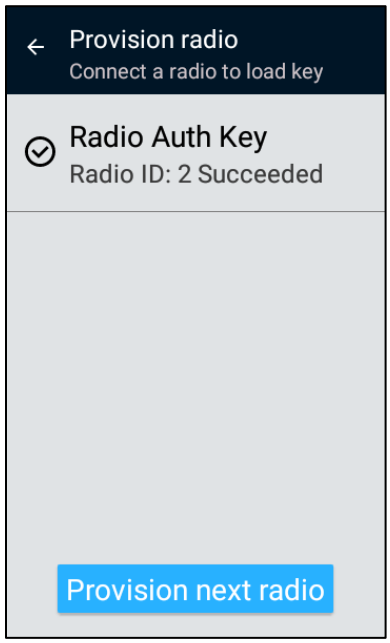




Next radio may be connected to the KVL and after pressing 'Provision next radio' button a new radio authentication key will be generated and loaded to the radio.

Provision radio with manually entered authentication key.





Next radio may be connected to the KVL and after pressing 'Provision next radio' button KVL application goes to the next screen where a user can enter a key value again.

Loading authentication keys using long press Push to Load (PTL) button

The authentication key loading operation may be quickly started by long press of the PTL button (hold for 3 seconds).

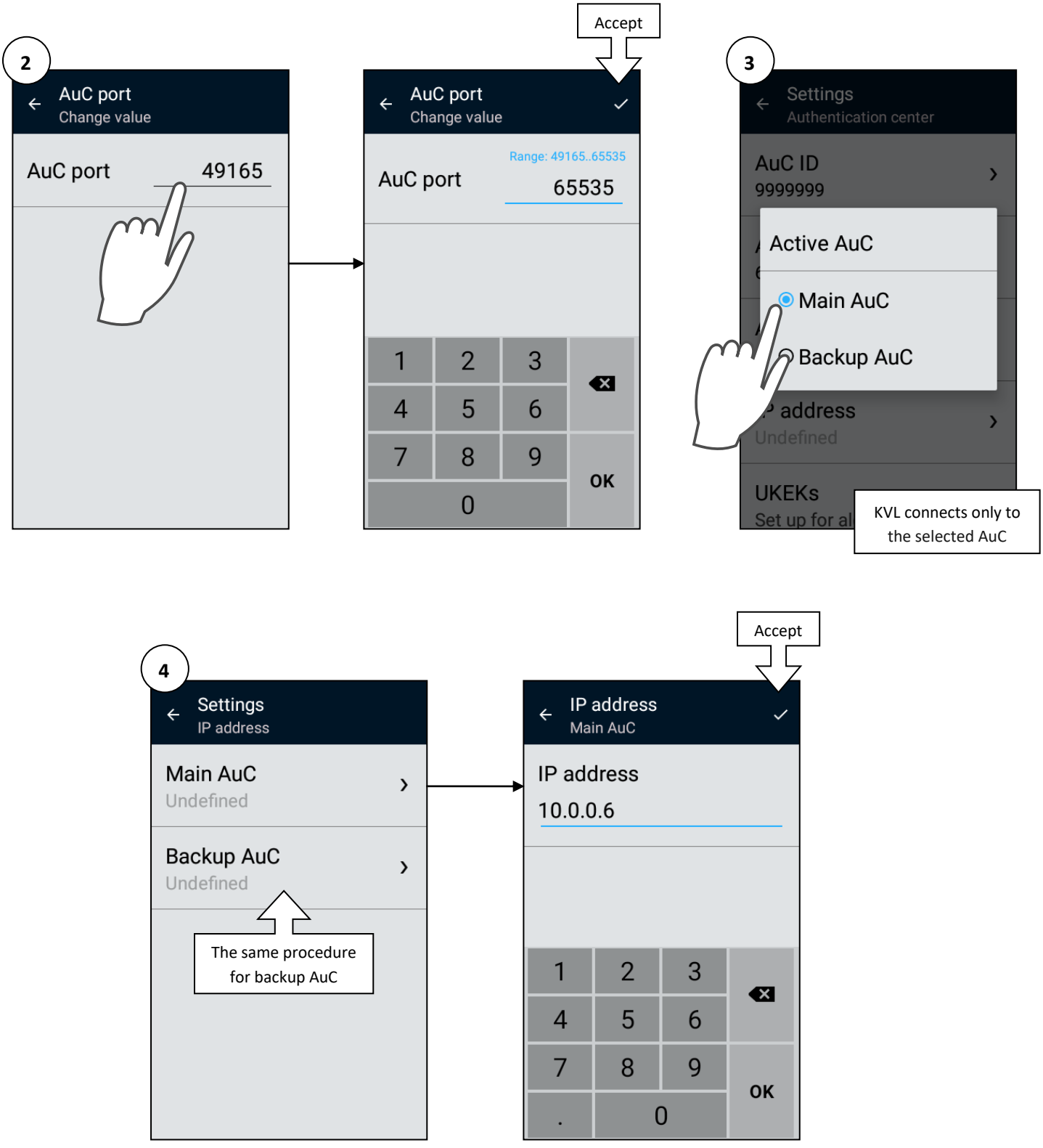
PTL button is disabled if any operation is in progress (for example share keys or upgrade).

Connect to AuC

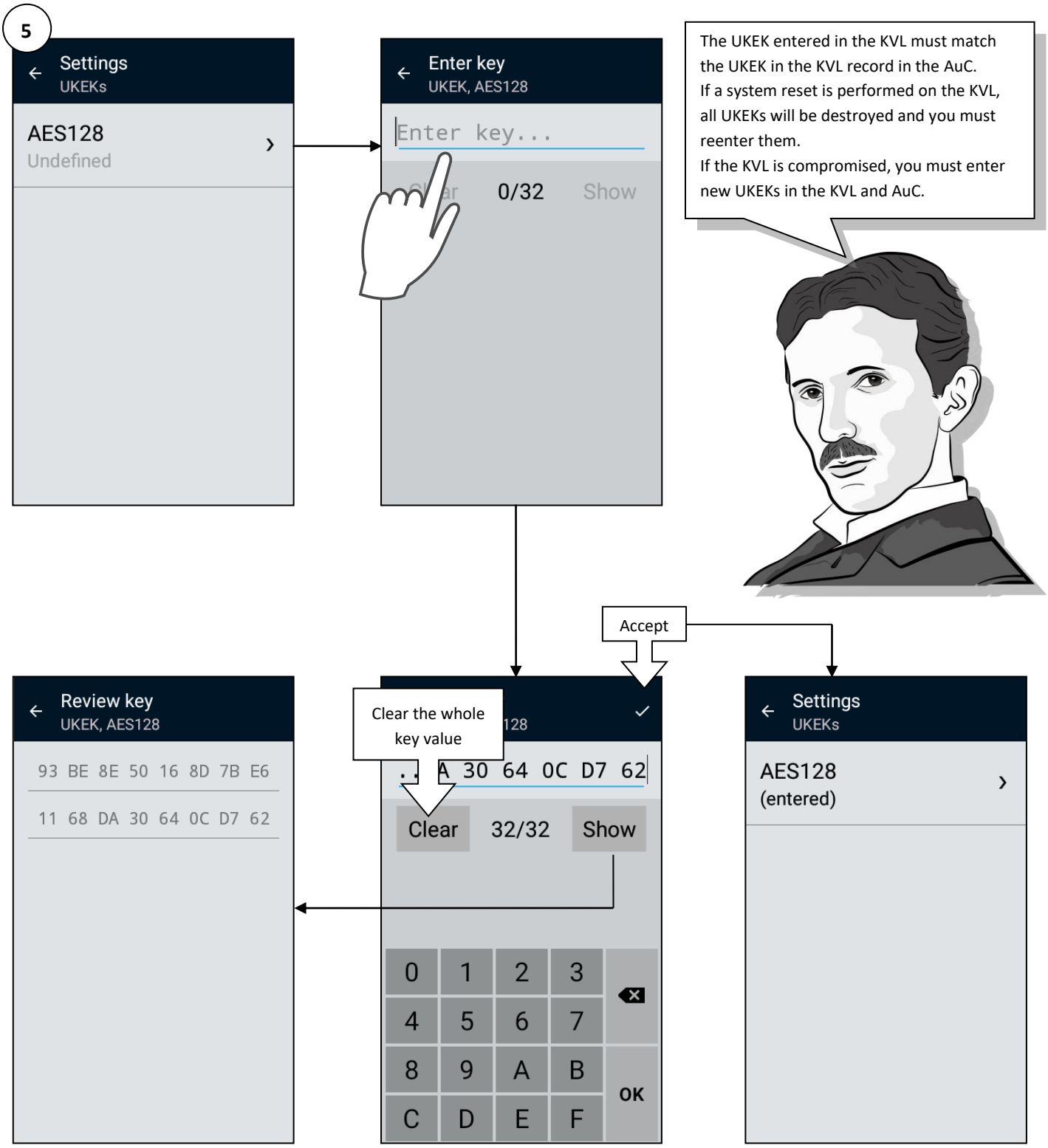
AuC Settings (1)

Before using your KVL to work with AuC, you need to program several AuC related parameters.

AuC Settings (2)

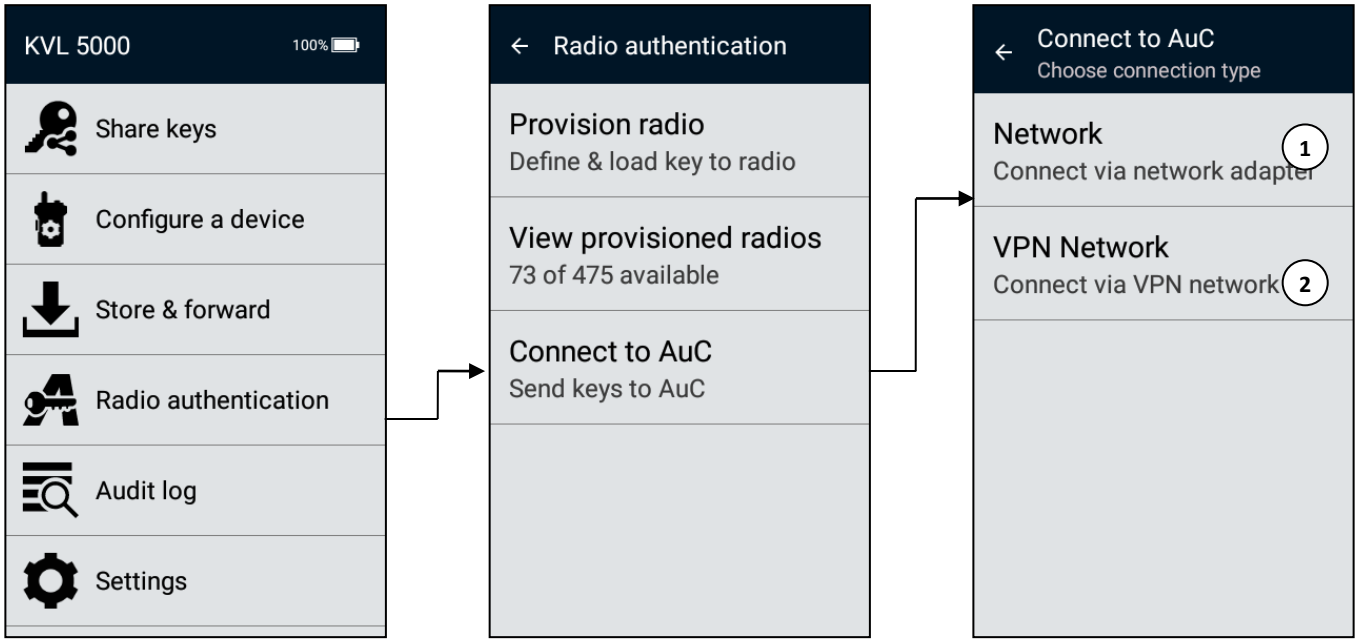


Entering the UKEK

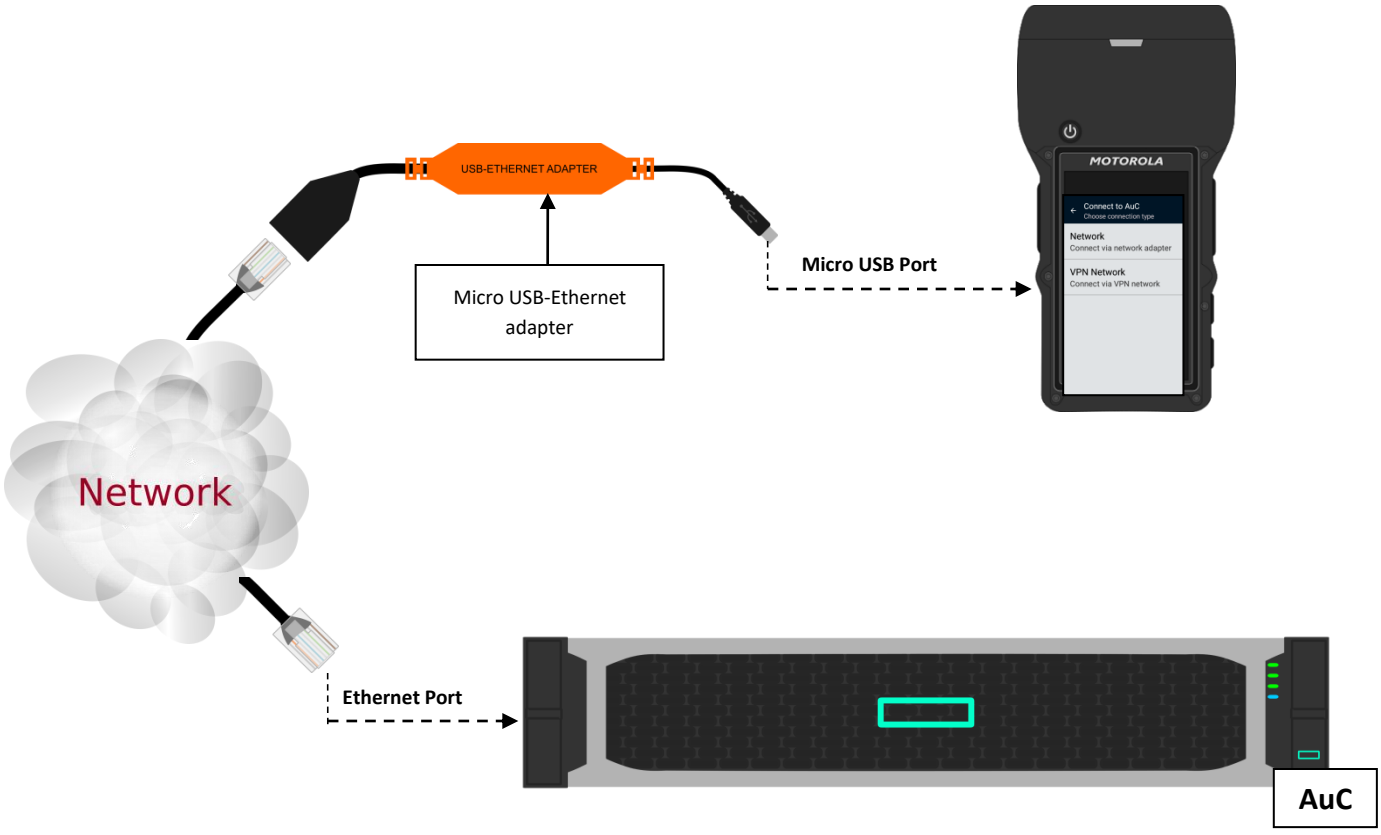


Connect to AuC via Network / VPN Network

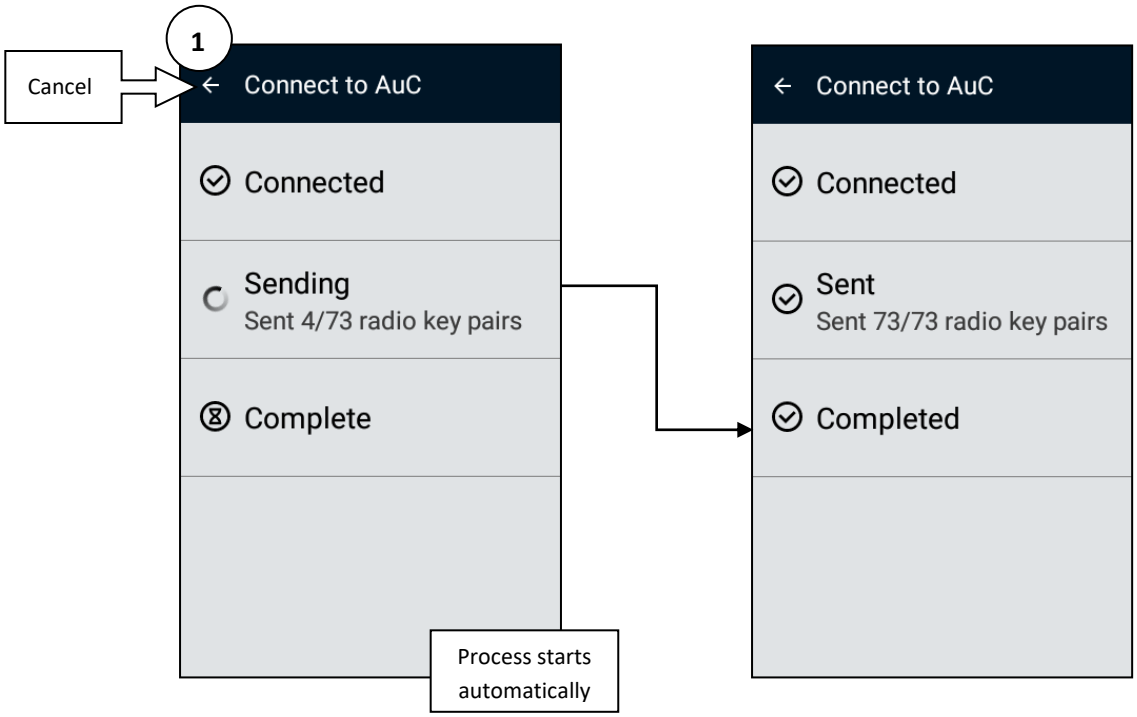
Make sure that the KVL battery is charged.



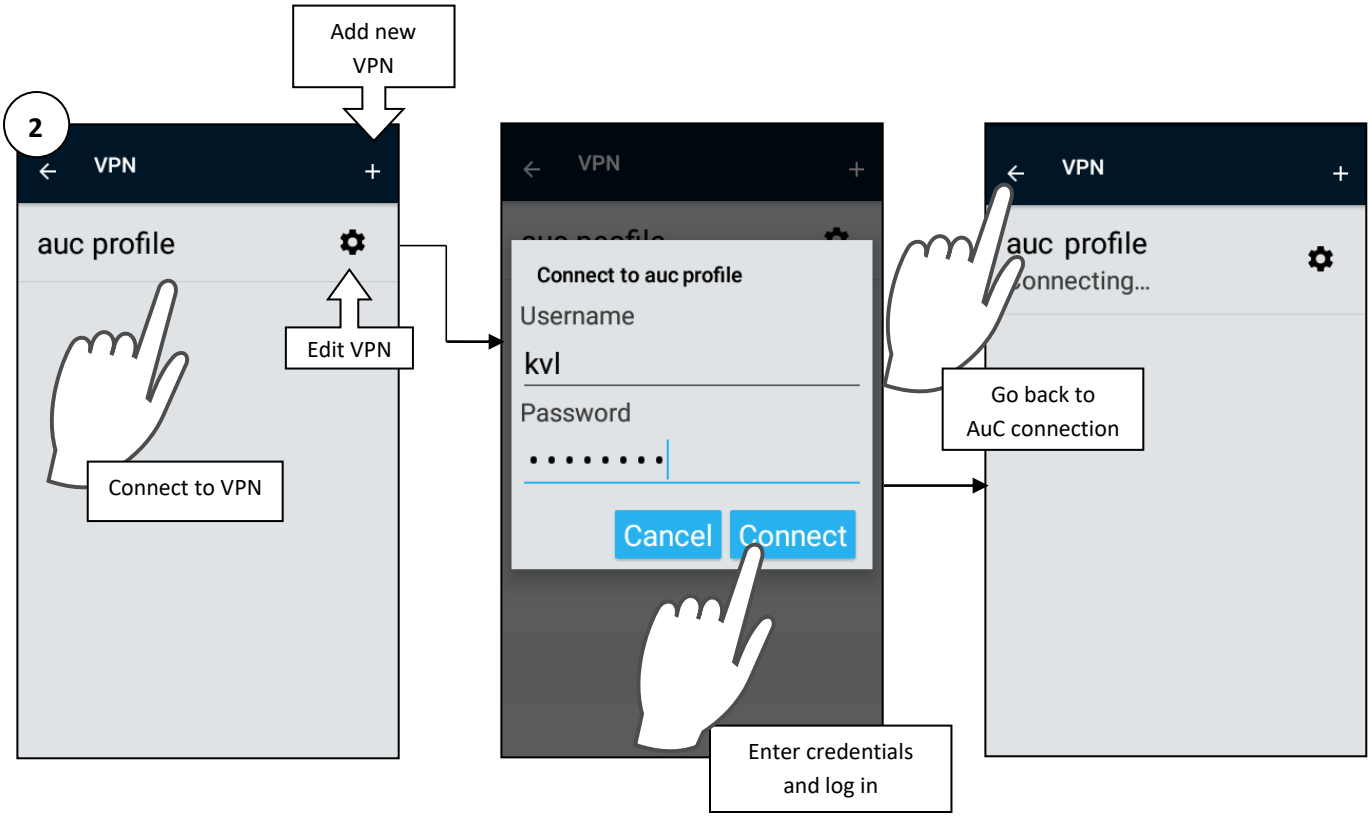
IP address in AuC settings must be set.



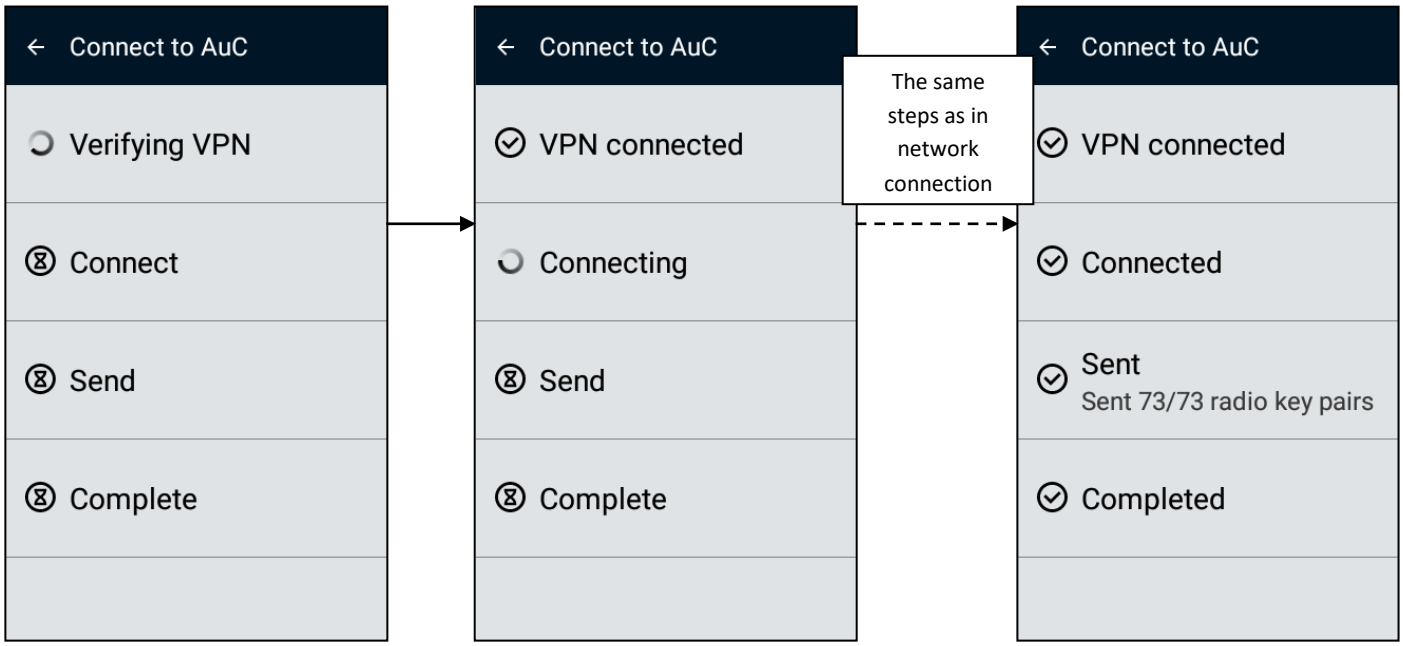
Network connection



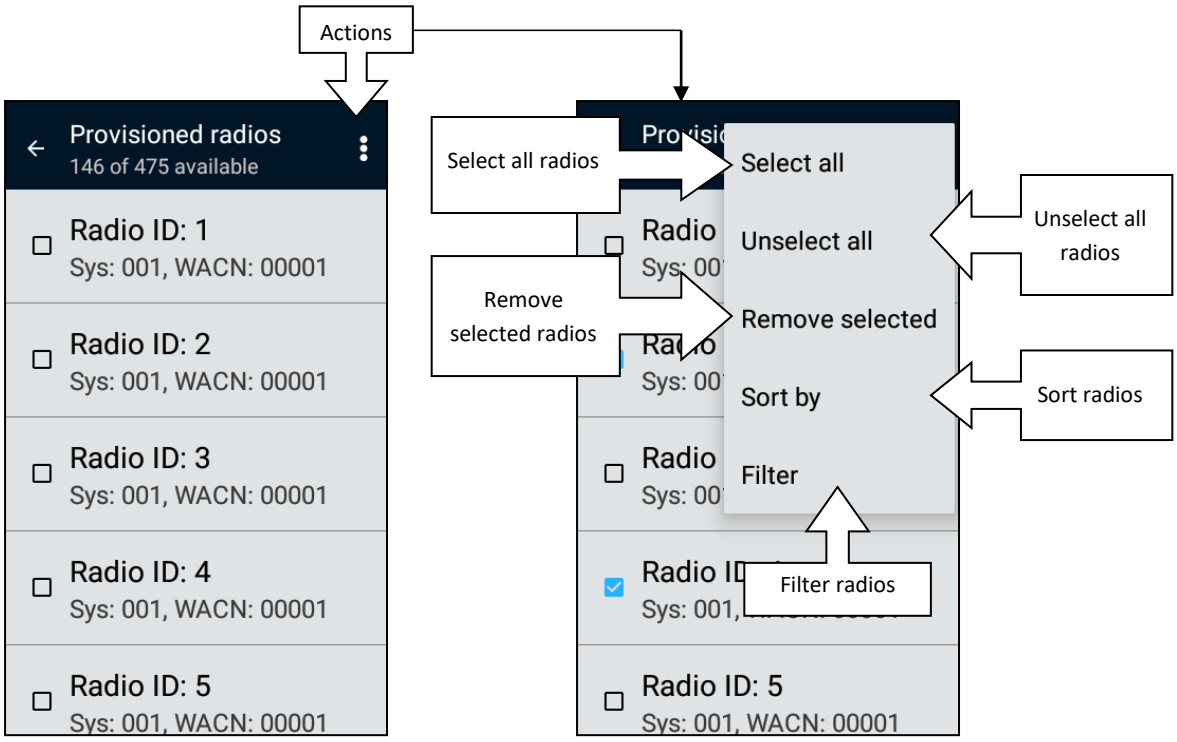
VPN connection (1)



VPN connection (2)

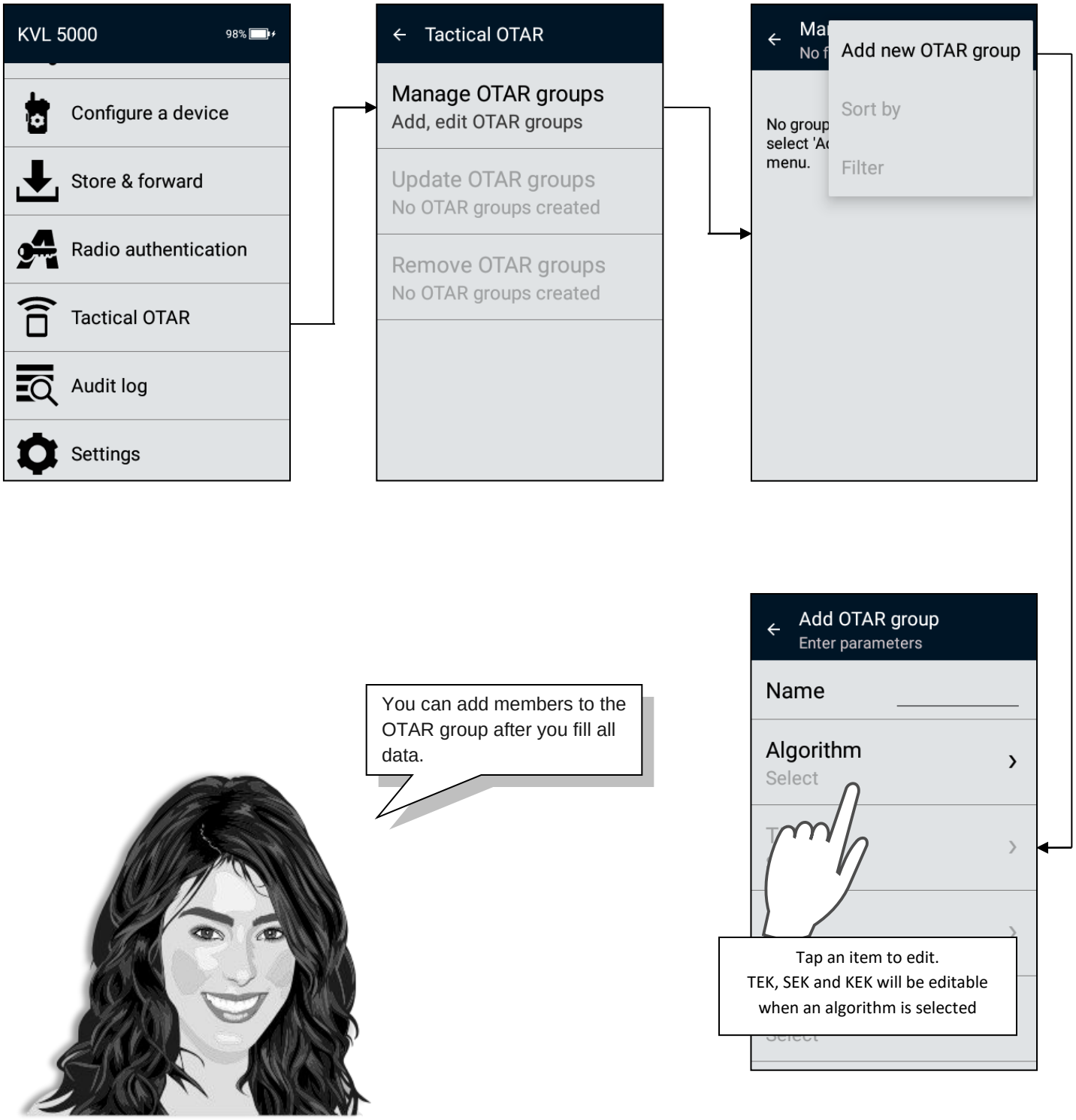


Viewing and removing provisioned radios

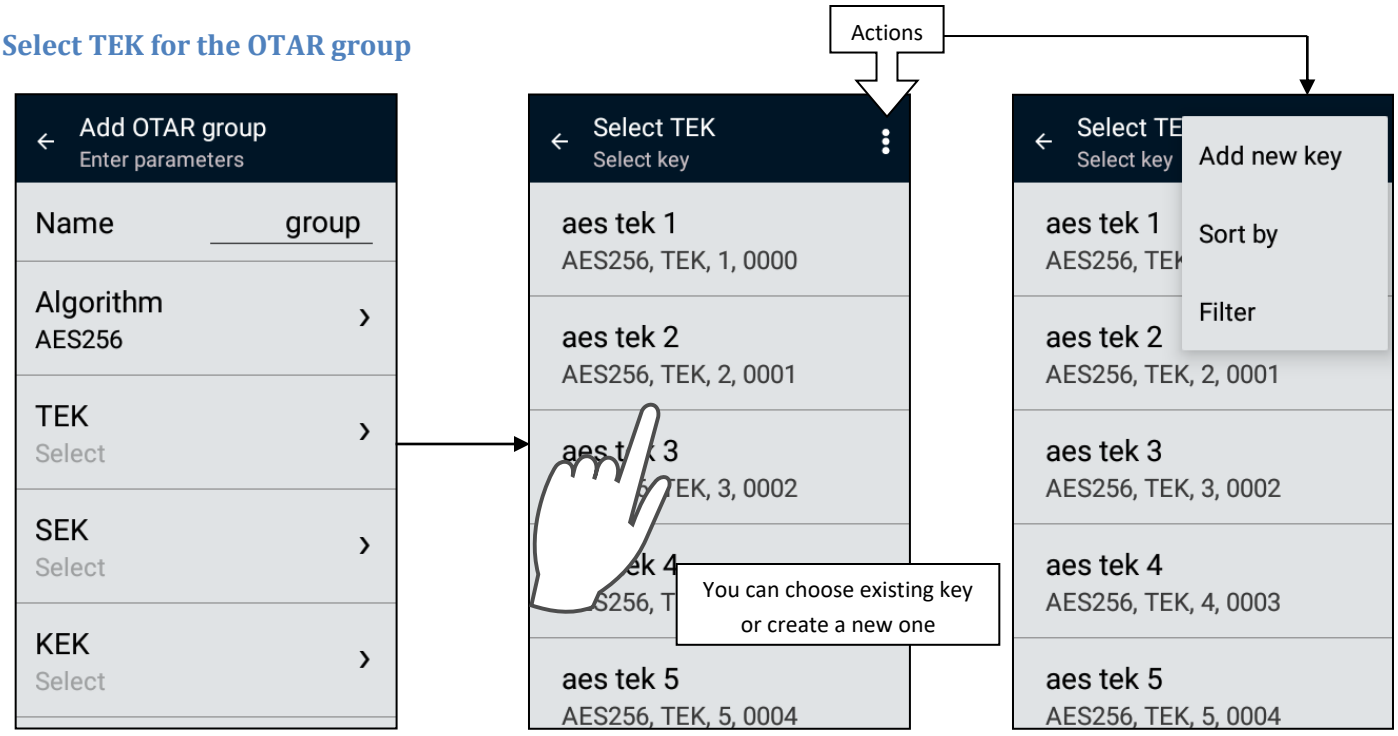


Add new tactical OTAR group

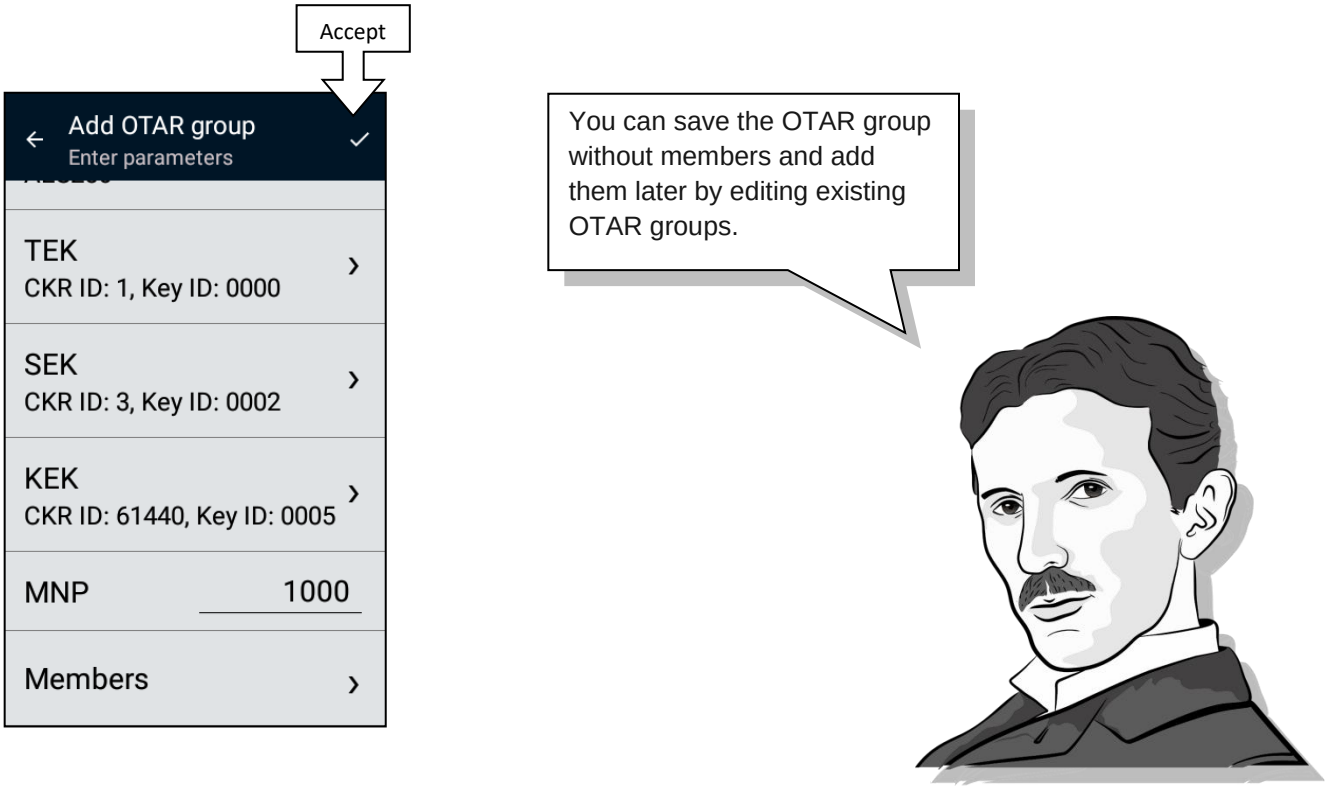
Only administrator can use this feature.



Select TEK for the OTAR group



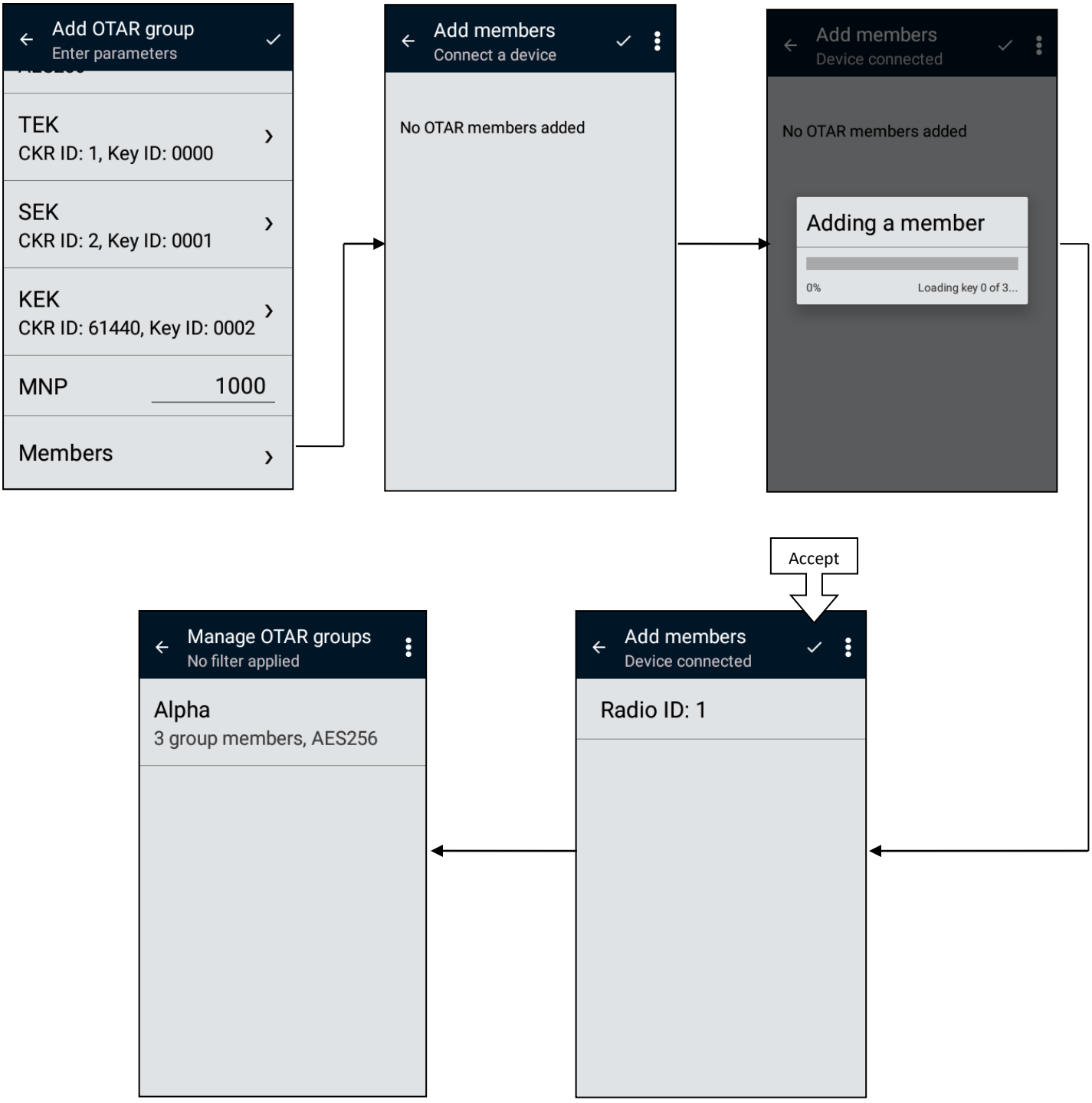
The same procedure is for selecting SEK and KEK.



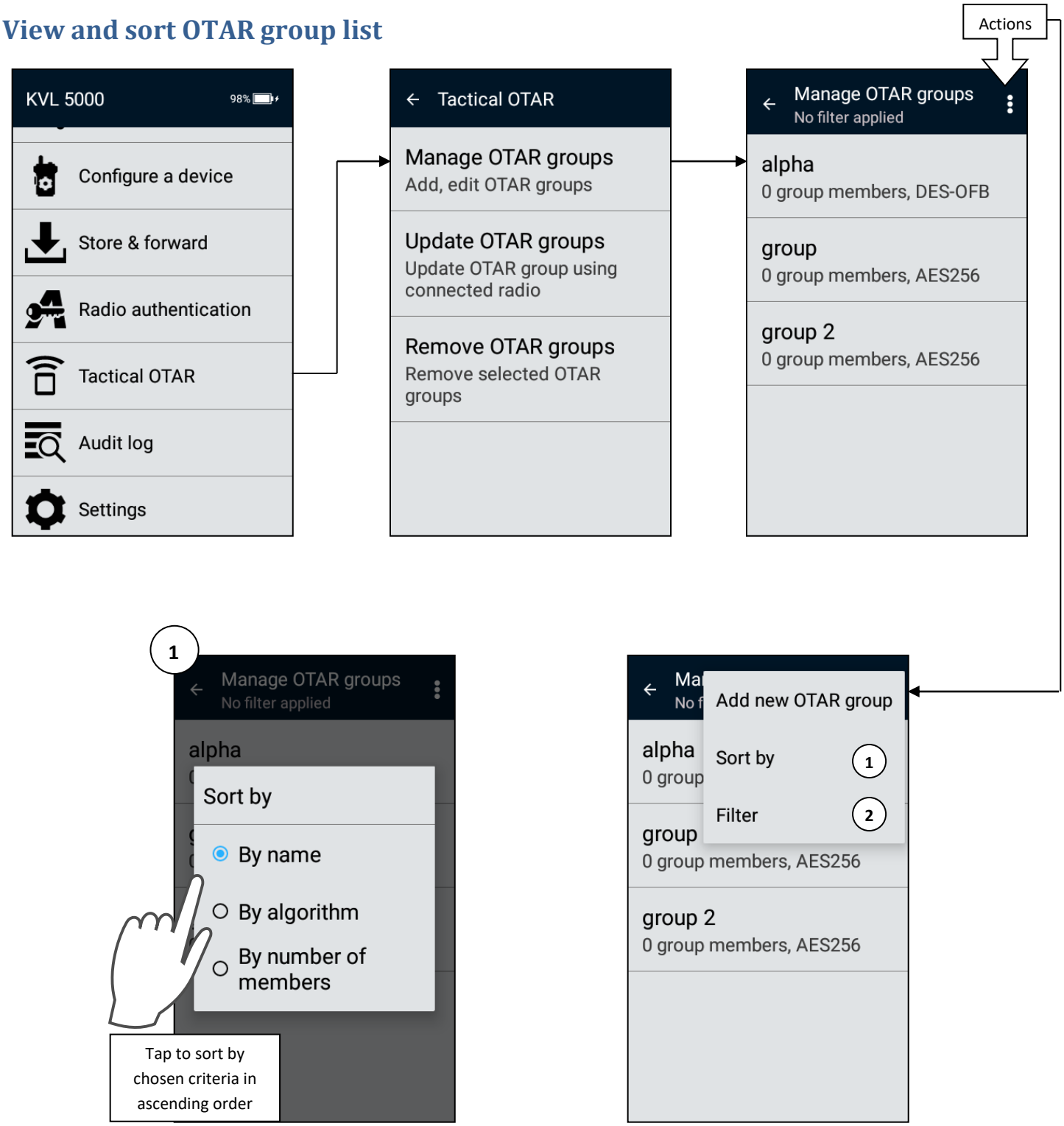
Adding new members to OTAR group (1)

To add radios to OTAR group connect each one to provision them with TEK, KEK and SEK. Single group can contain up to 50 members.

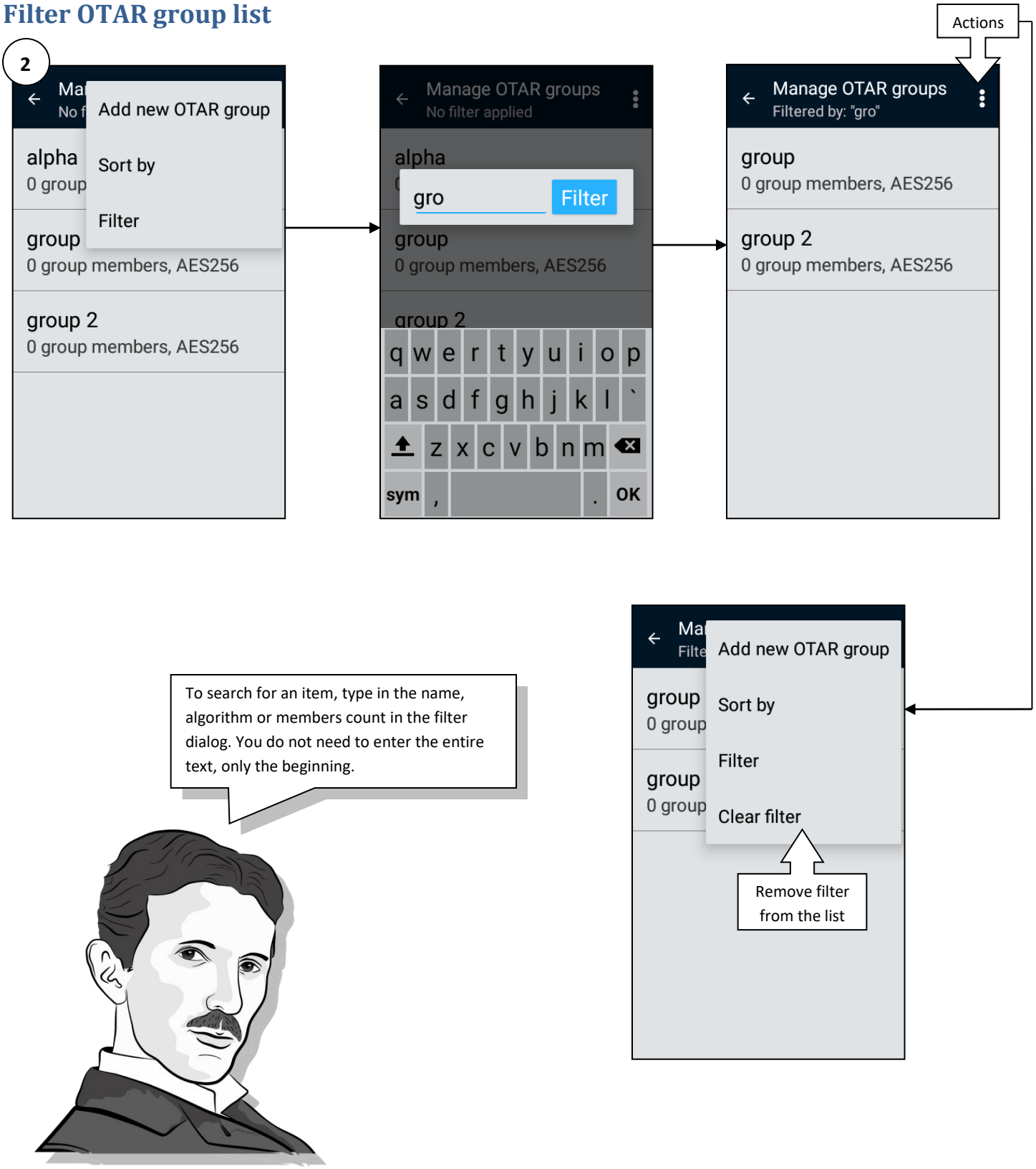
Adding new members to OTAR group (2)



View and sort OTAR group list



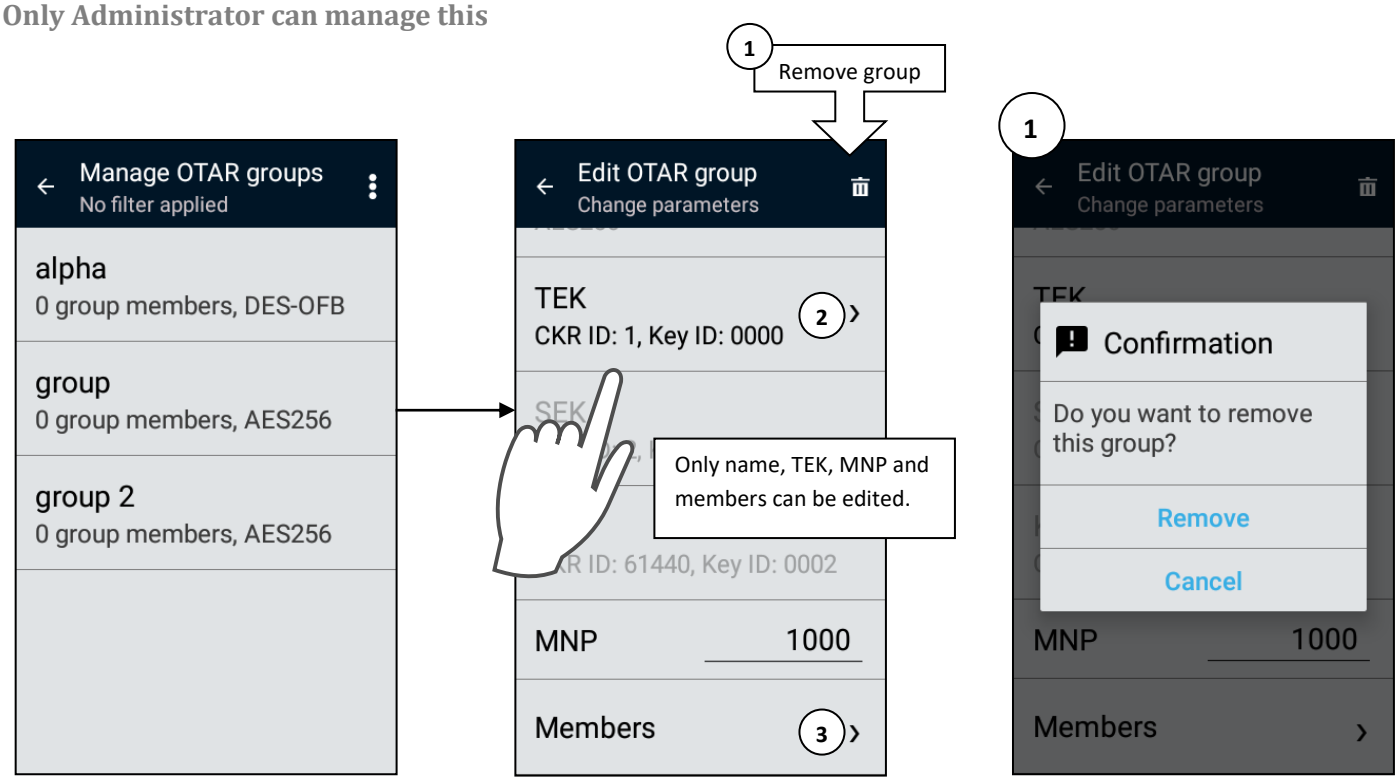
Filter OTAR group list



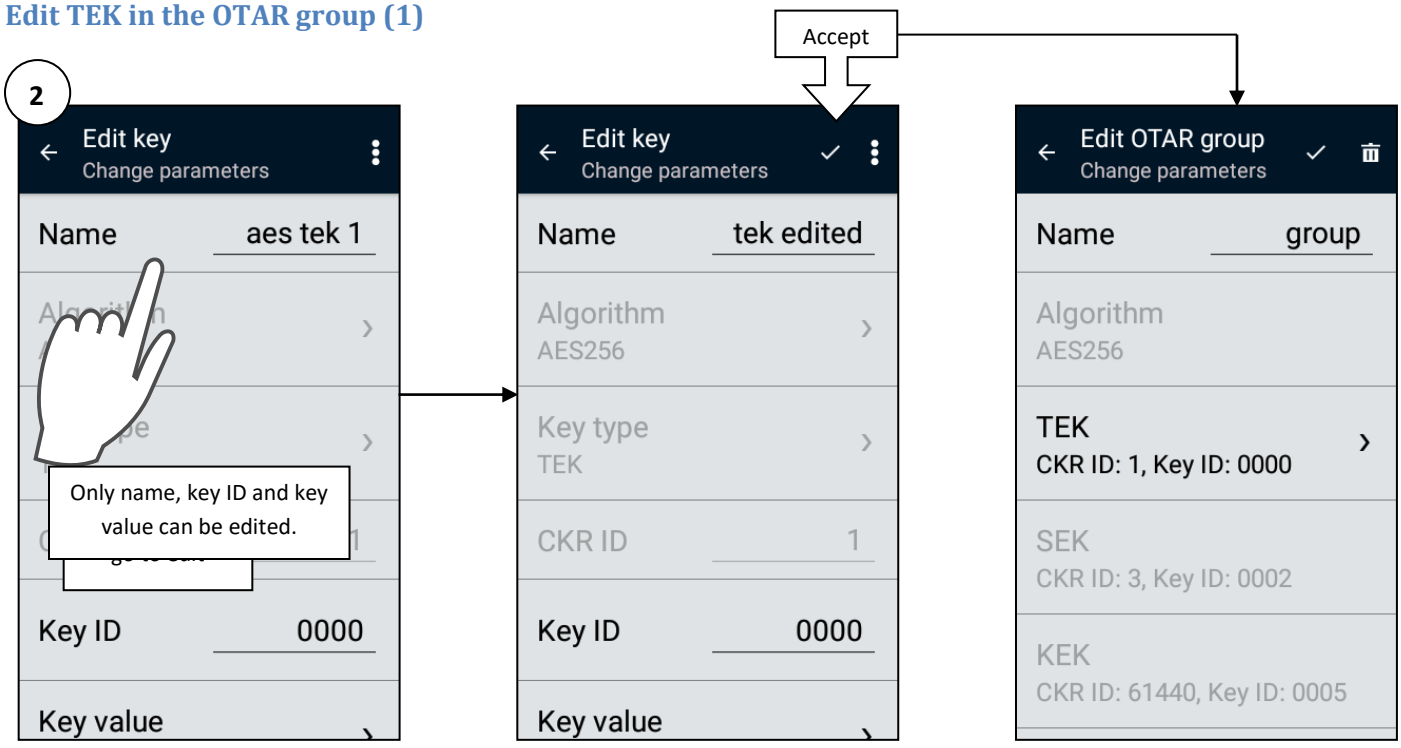
Edit OTAR group

Edit OTAR group name, TEK, MNP and members | Delete the group |

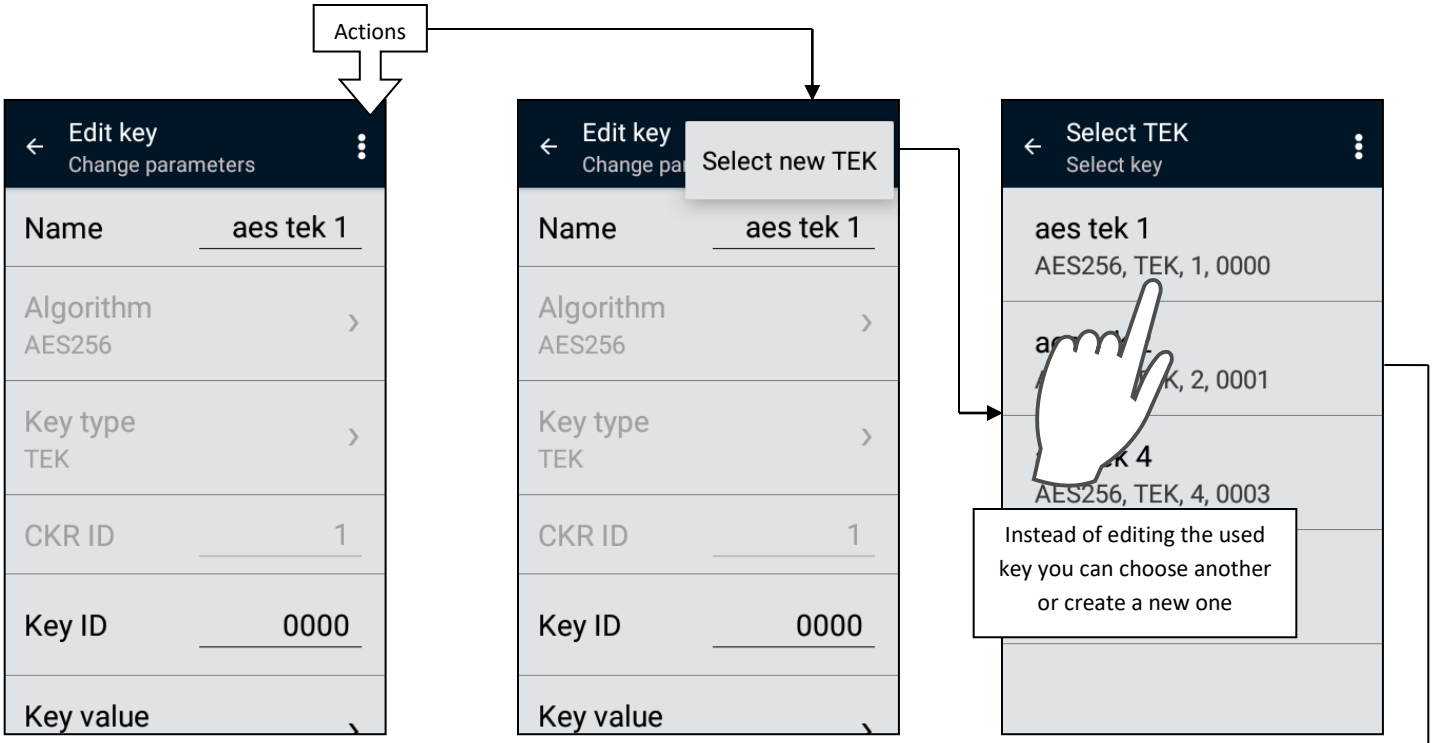
Only Administrator can manage this

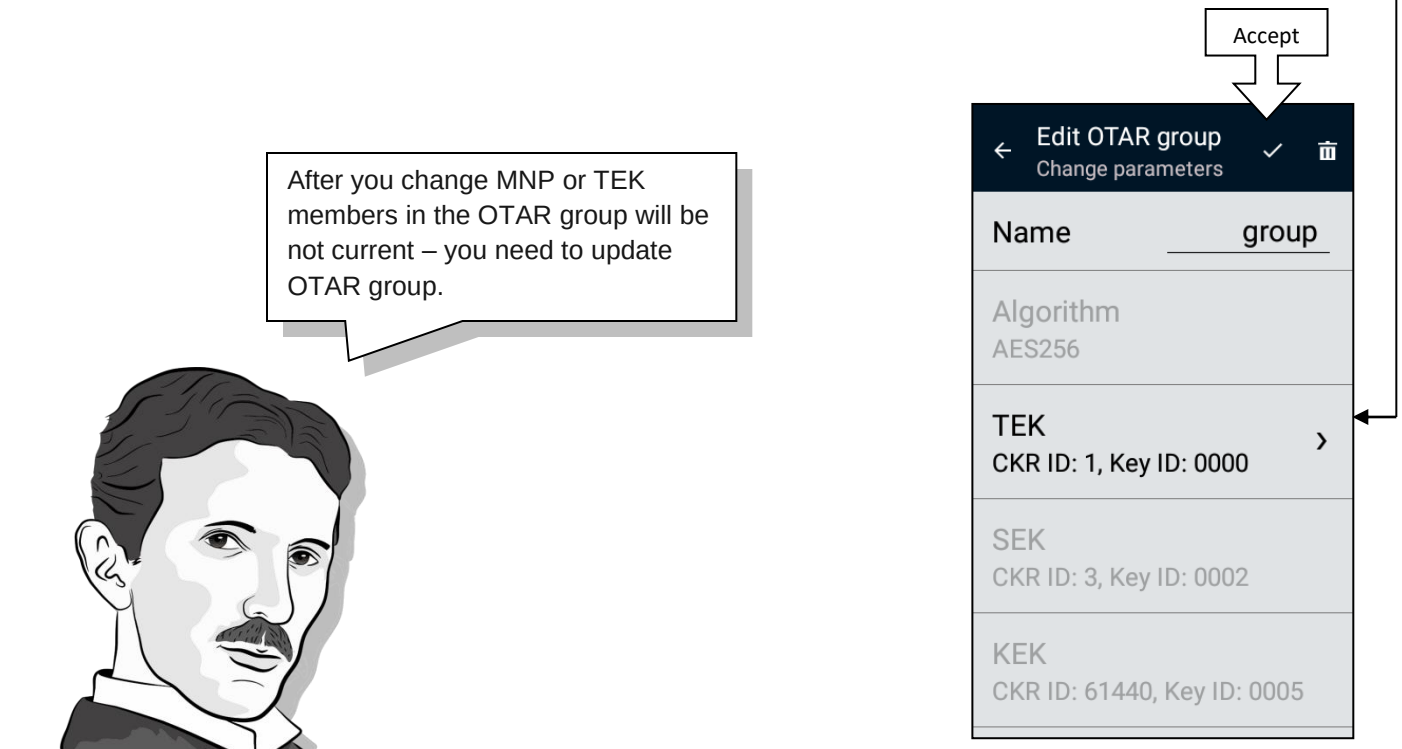


Edit TEK in the OTAR group (1)

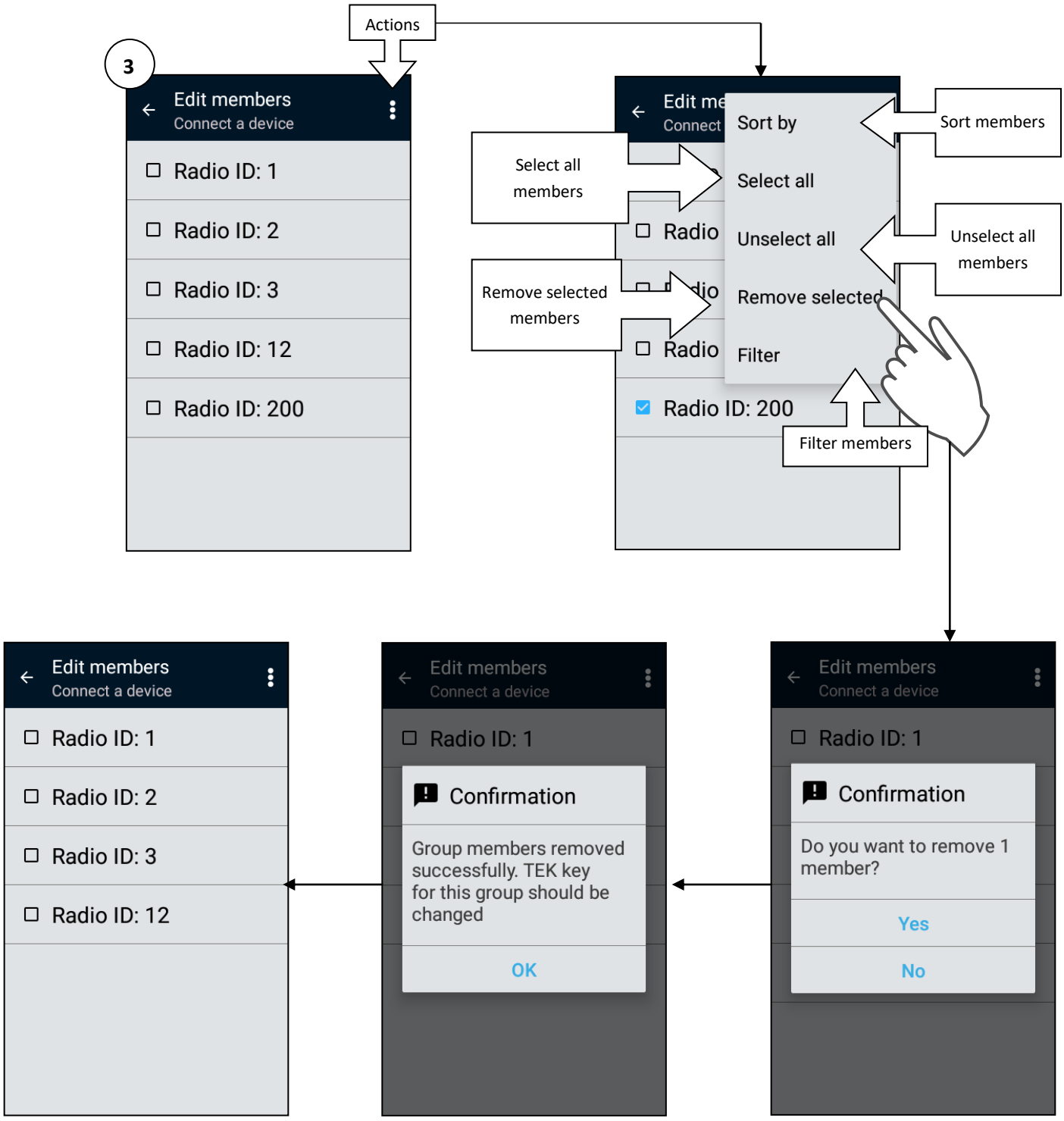


Edit TEK in the OTAR group (2)

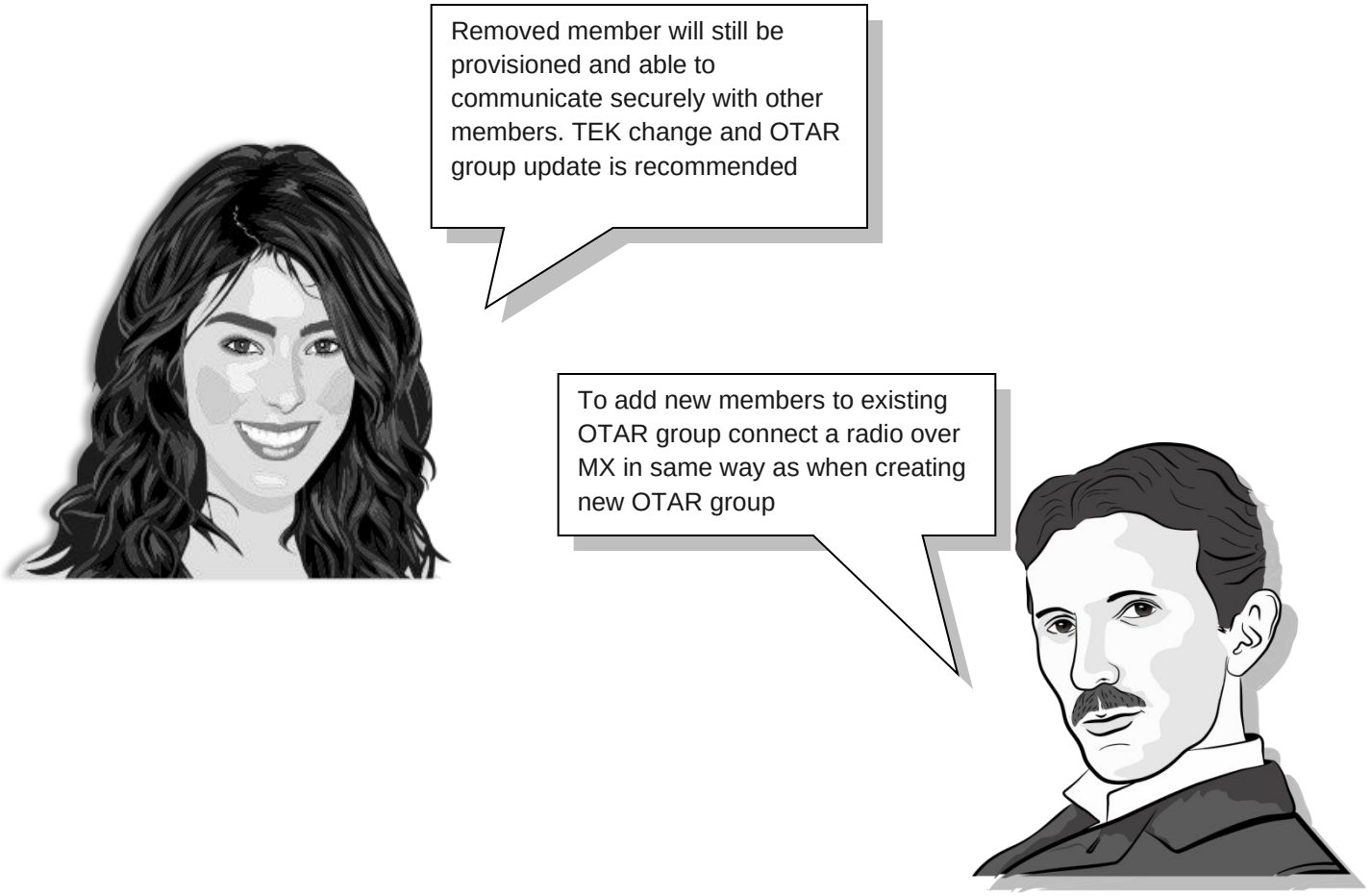




Edit members in the OTAR group (1)



Edit members in the OTAR group (2)



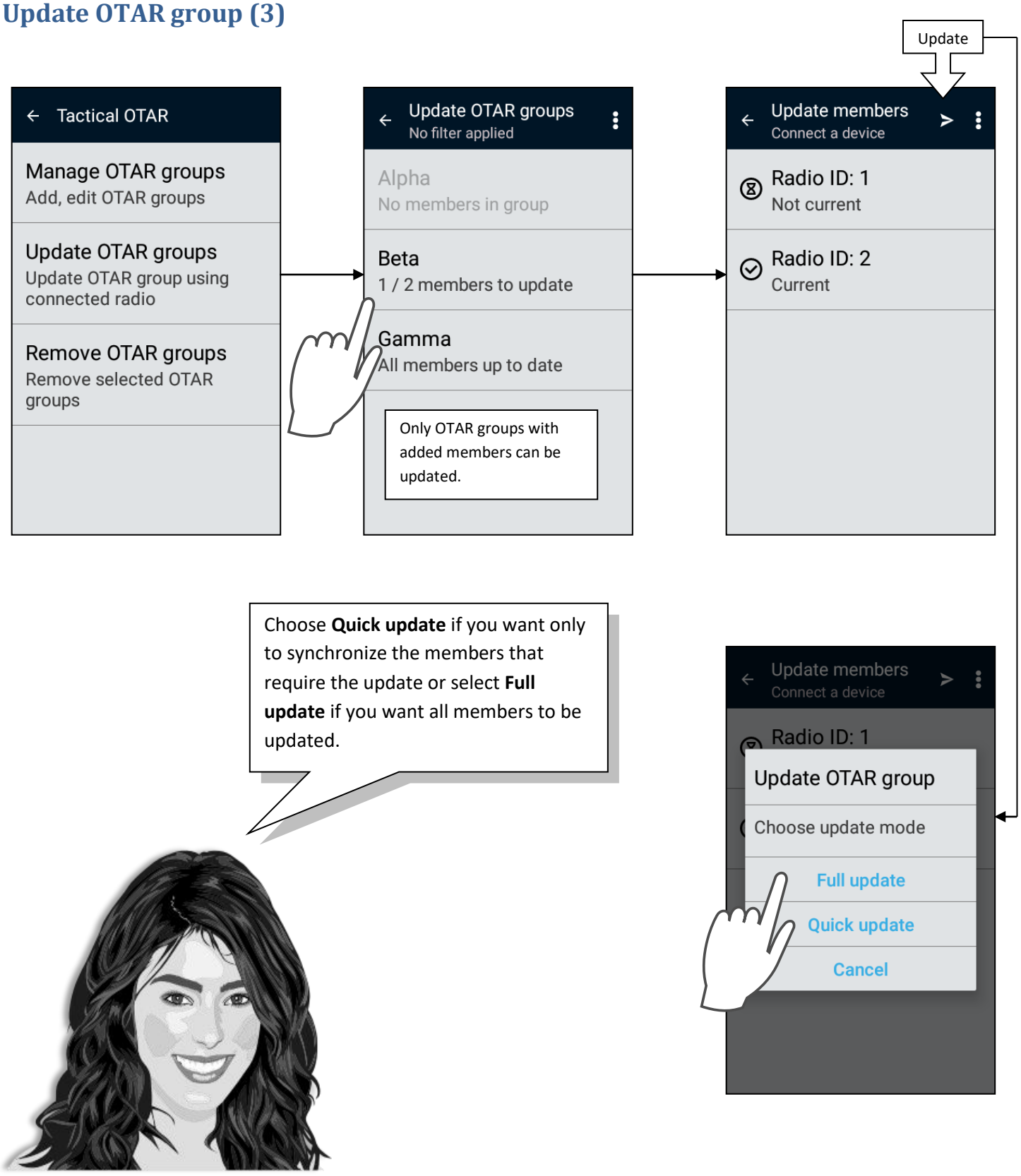
Update OTAR group (1)

Tactical OTAR is a Motorola feature that allows a KVL to wirelessly manage a key (TEK only) for a small group of radios, with one radio serving as an RF modem. The radio serving as an RF modem must be equipped with the Tactical Rekey/OTAR feature. The OTAR group update is executed using RS-232 or USB cable.

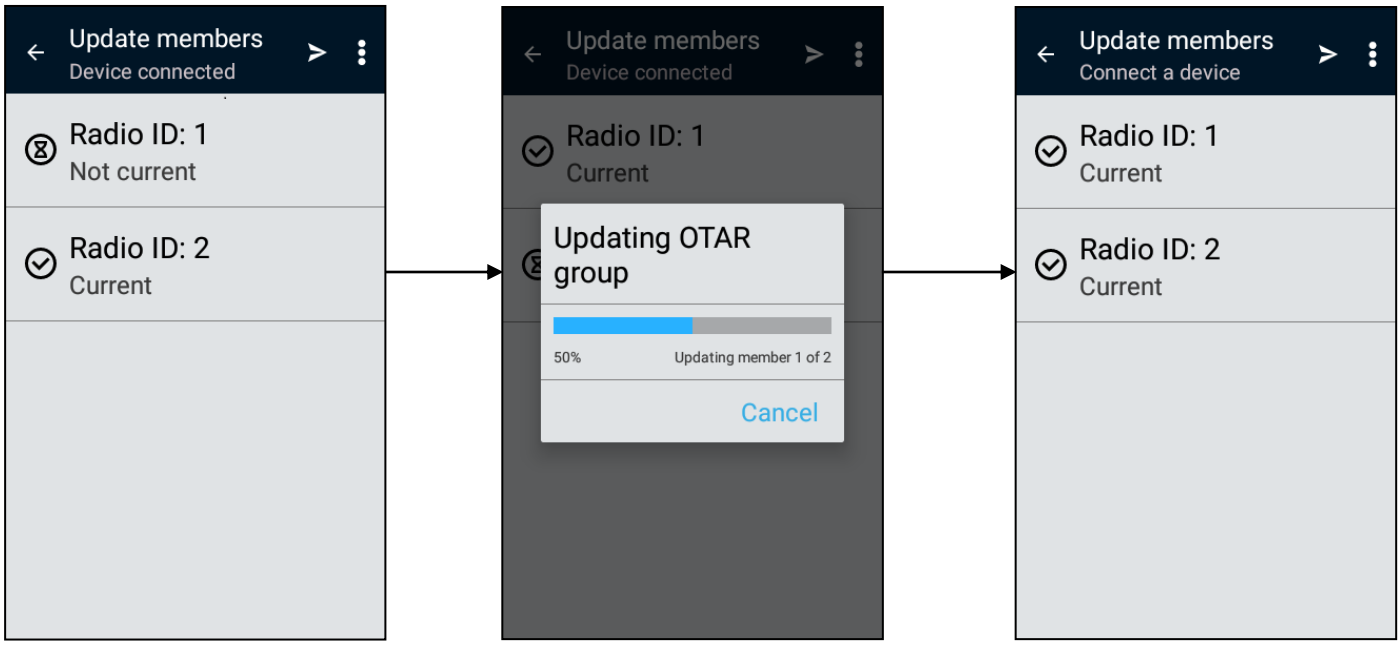
Update OTAR group (2)

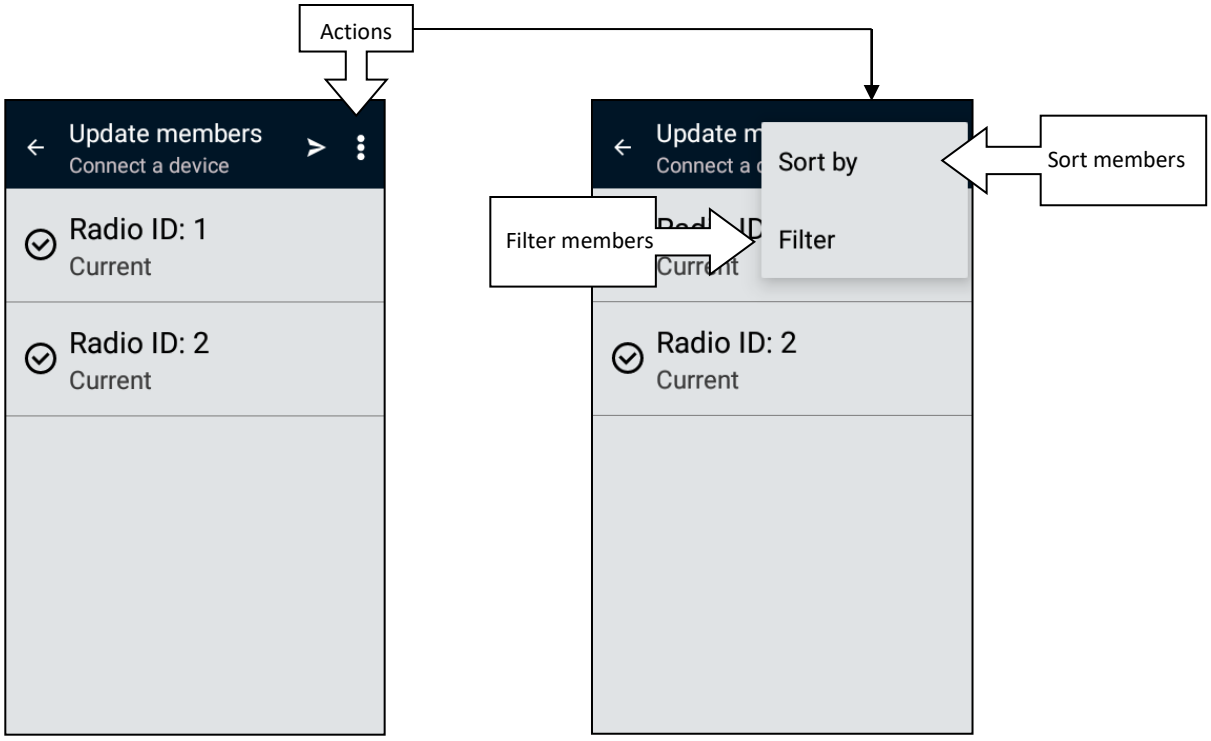
You can also connect devices over USB to update OTAR group when USB key loading feature is enabled.

Update OTAR group (3)



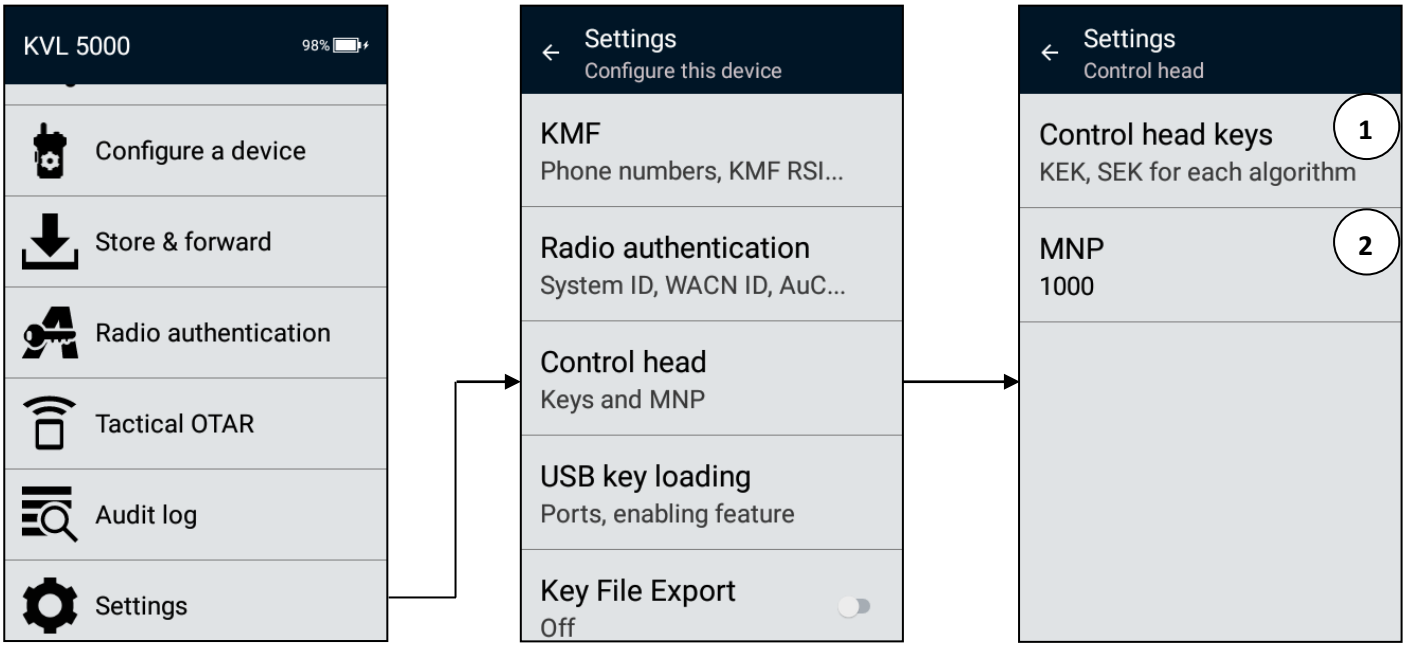
Update OTAR group (4)

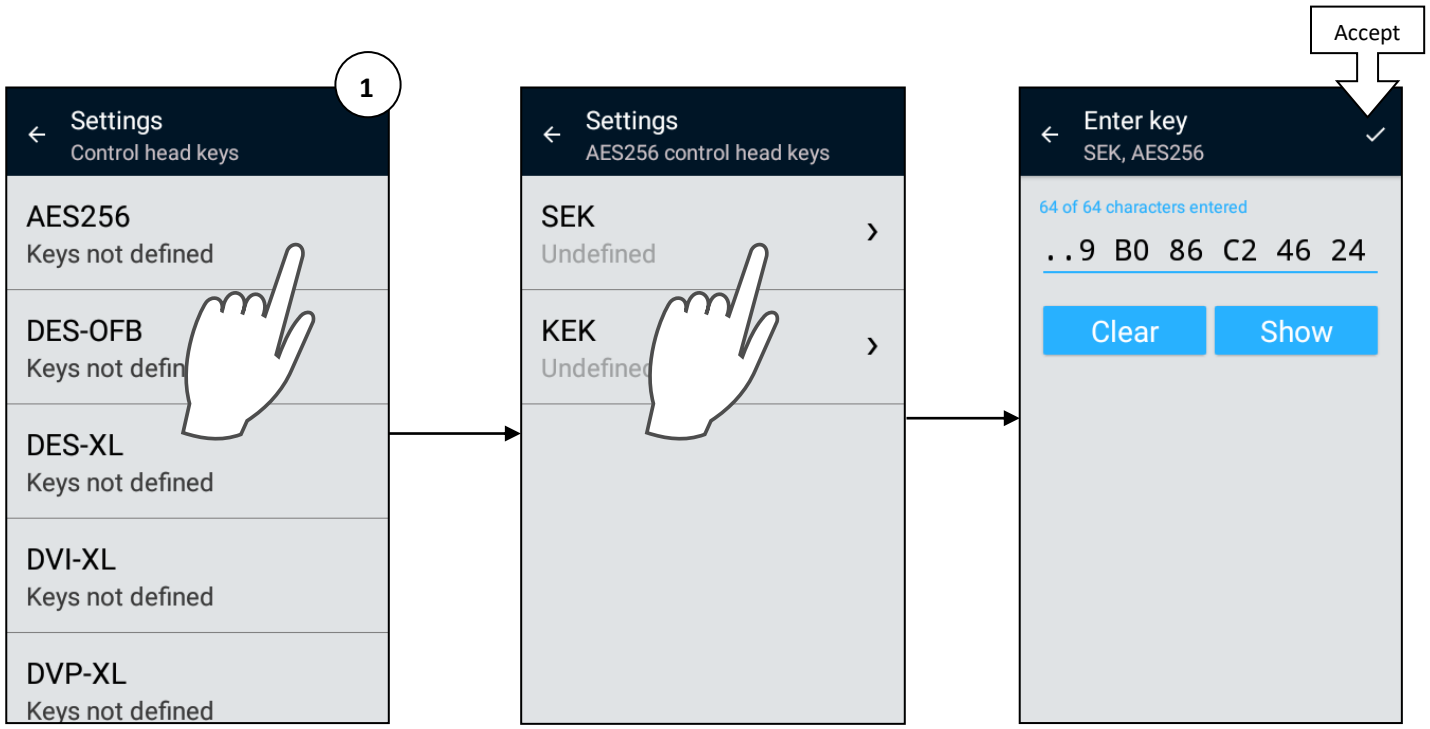




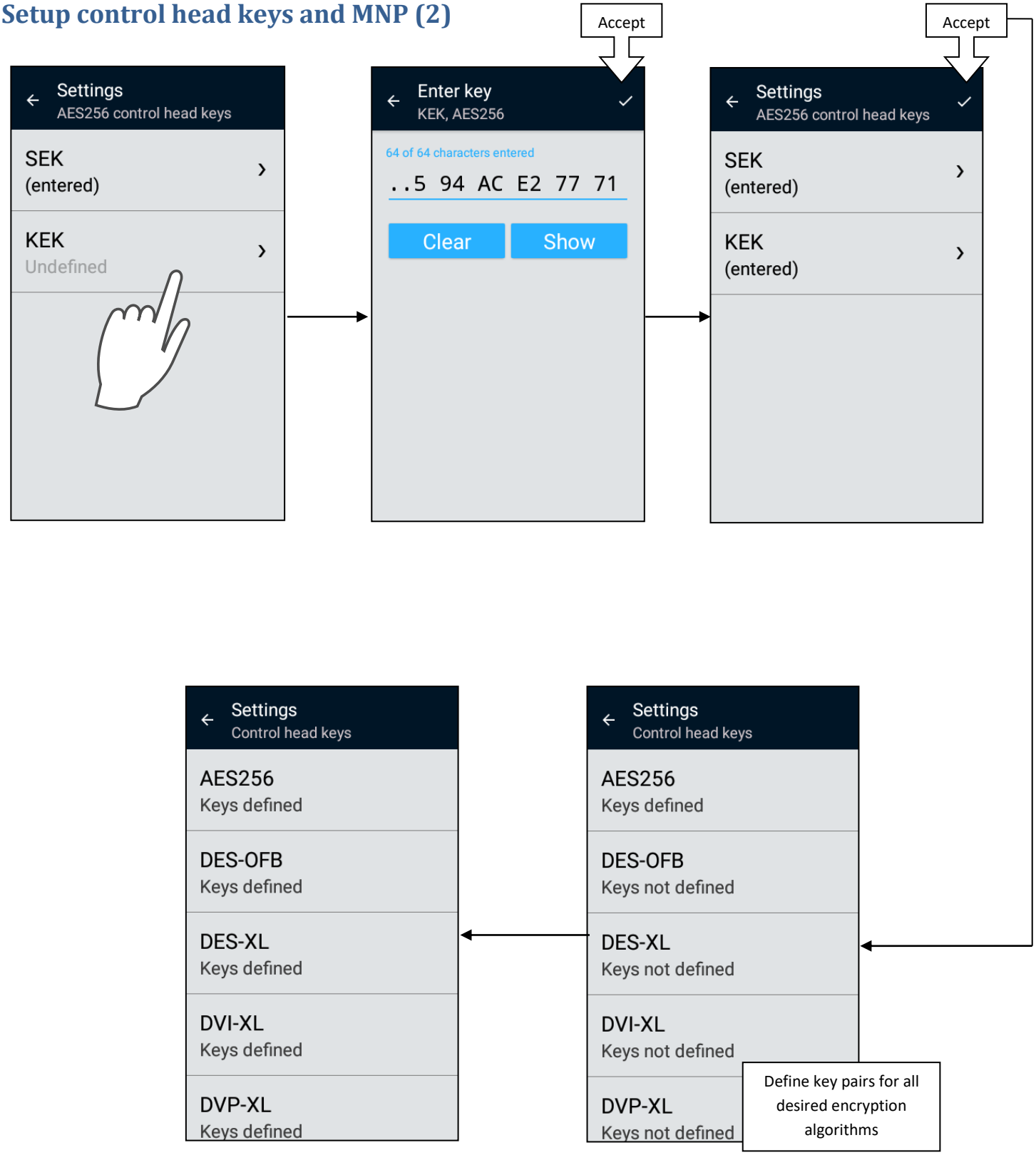
Setup control head keys and MNP (1)

Sometimes the radio may be mounted in a vehicle's trunk and is difficult to access. Remote control head feature allows you to load and manage keys on a radio through a remote control head that can be mounted in vehicle's cabin.

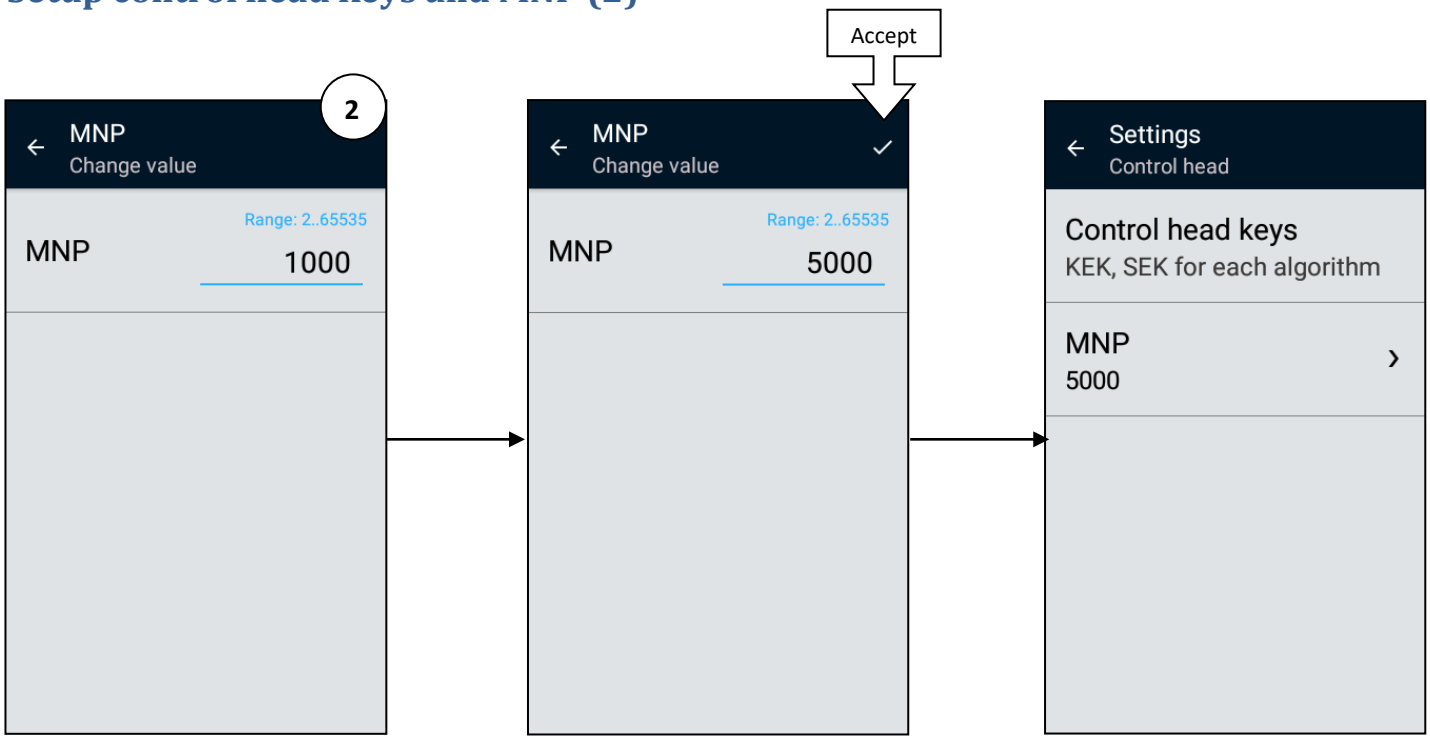




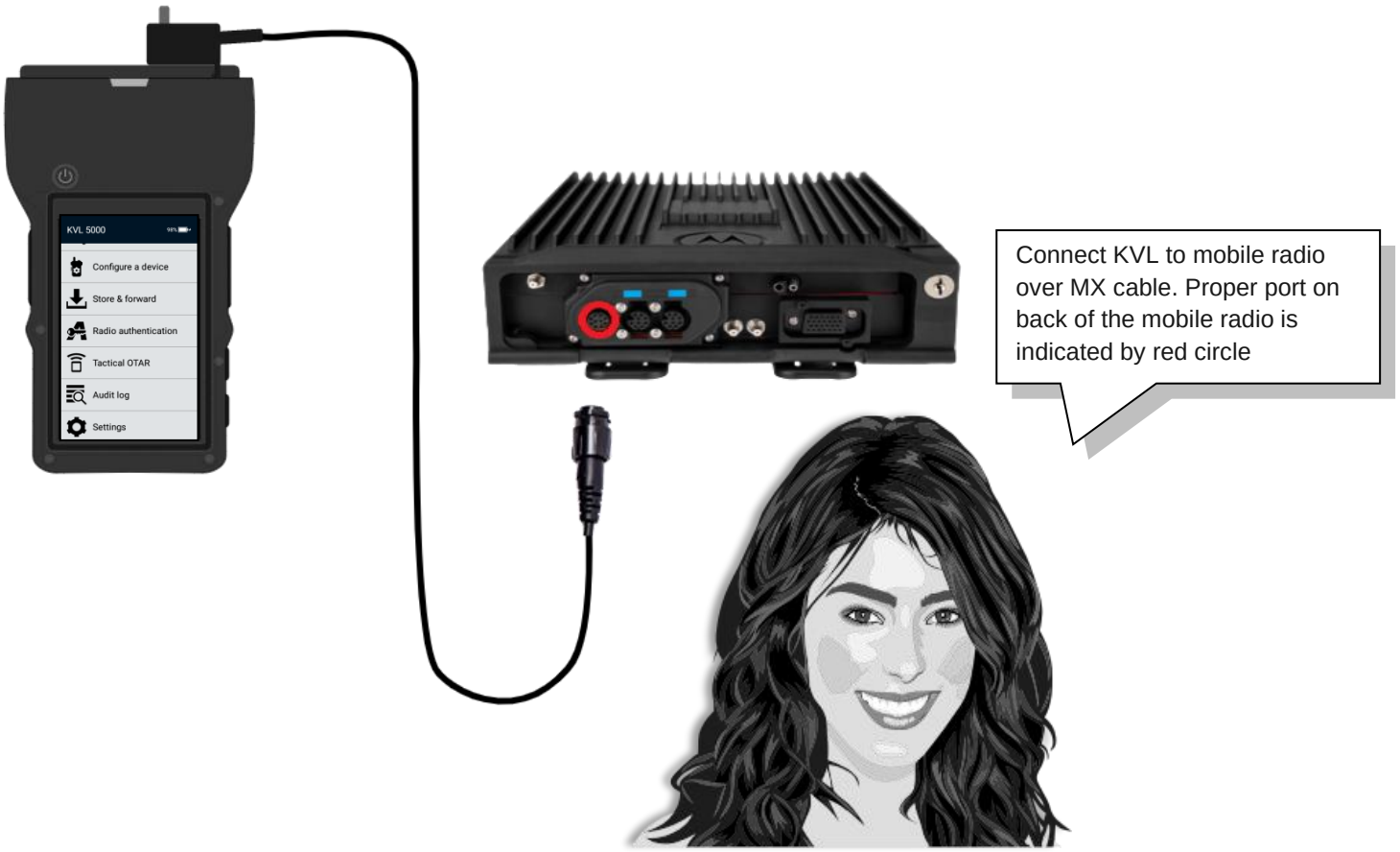
Setup control head keys and MNP (2)



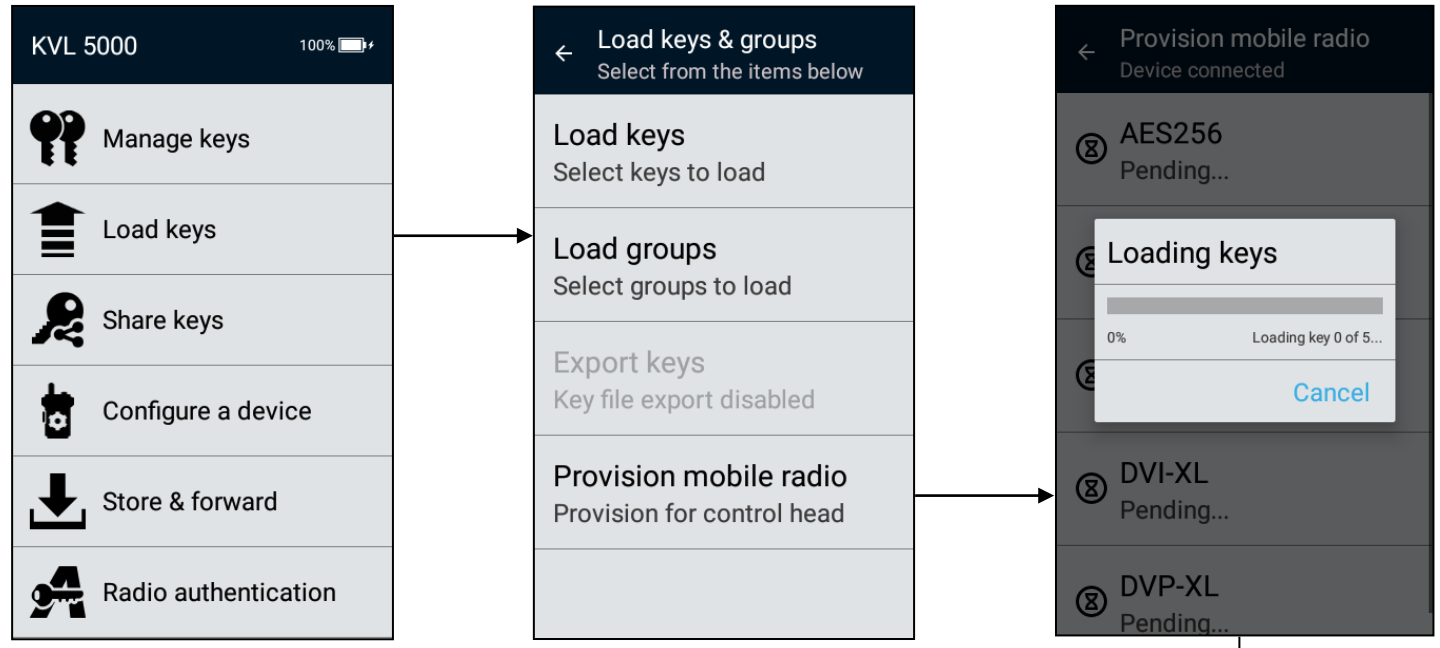
Setup control head keys and MNP (2)

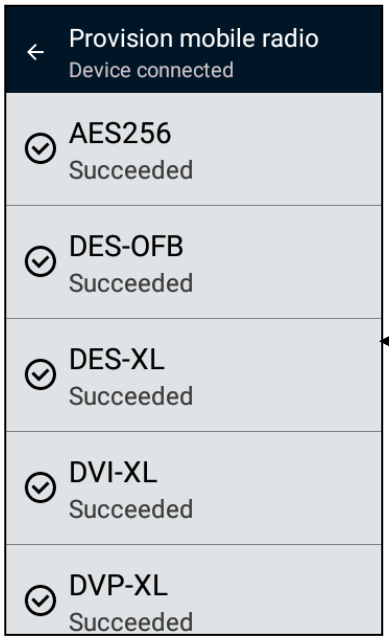


Provision mobile radio (1)

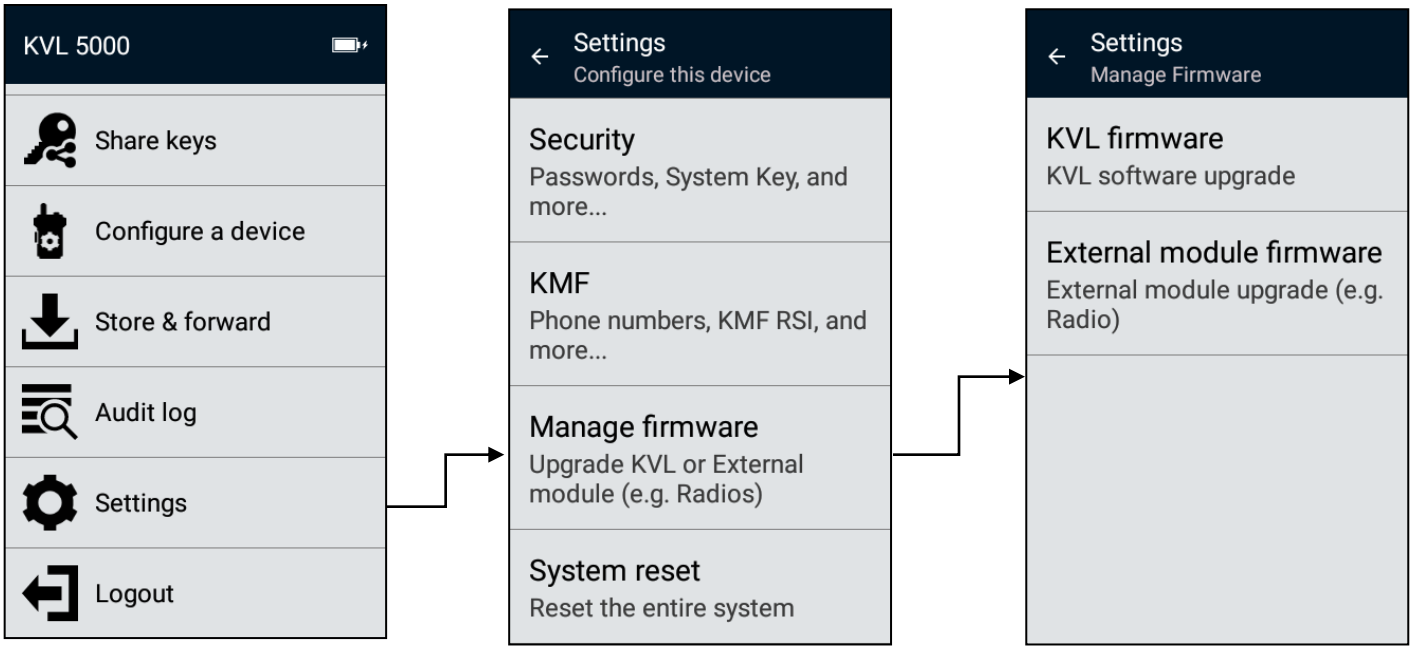


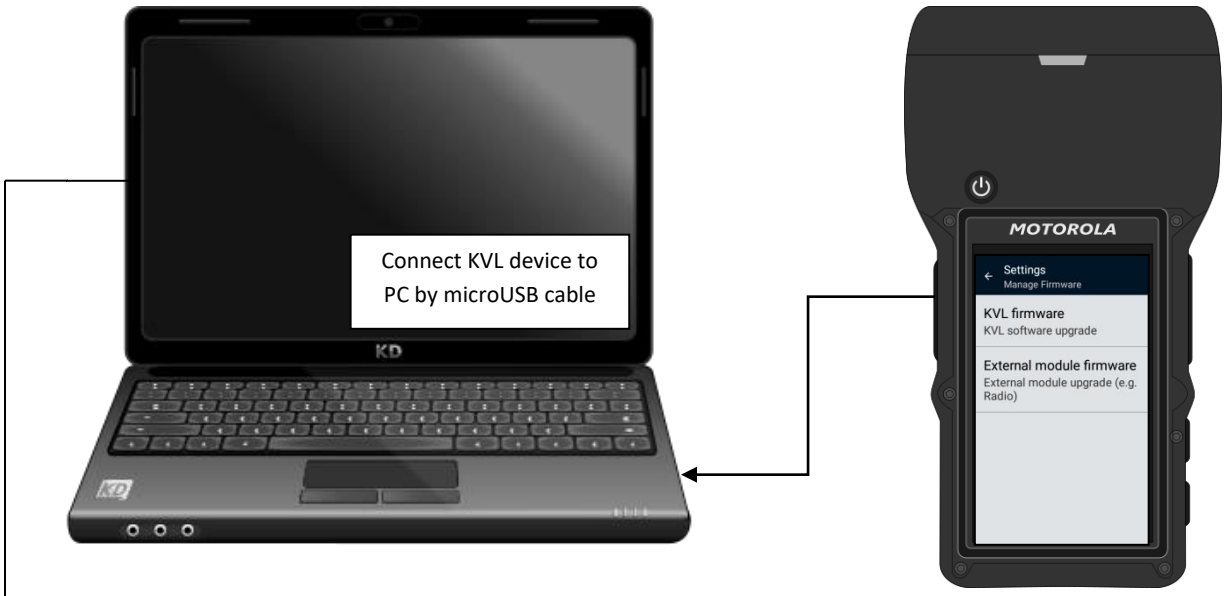
Provision mobile radio (2)





Importing upgrade images





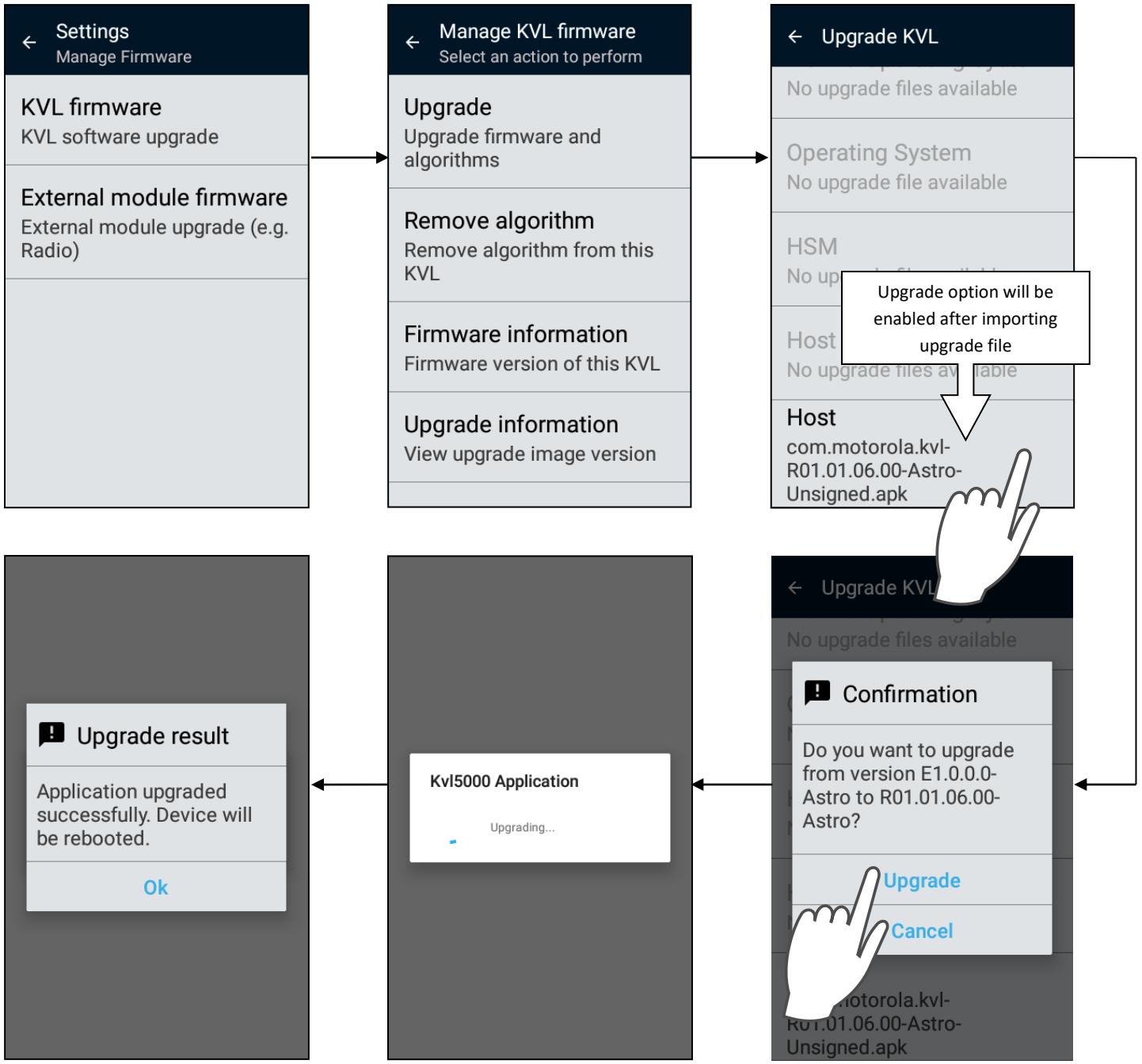
Copy any upgrade files to *This PC\kvl5000\Internal shared storage\fwupdate* directory. KVL needs to be in any Manage Firmware screen to have access to that directory

There are four types of upgrade files that can be imported into KVL:

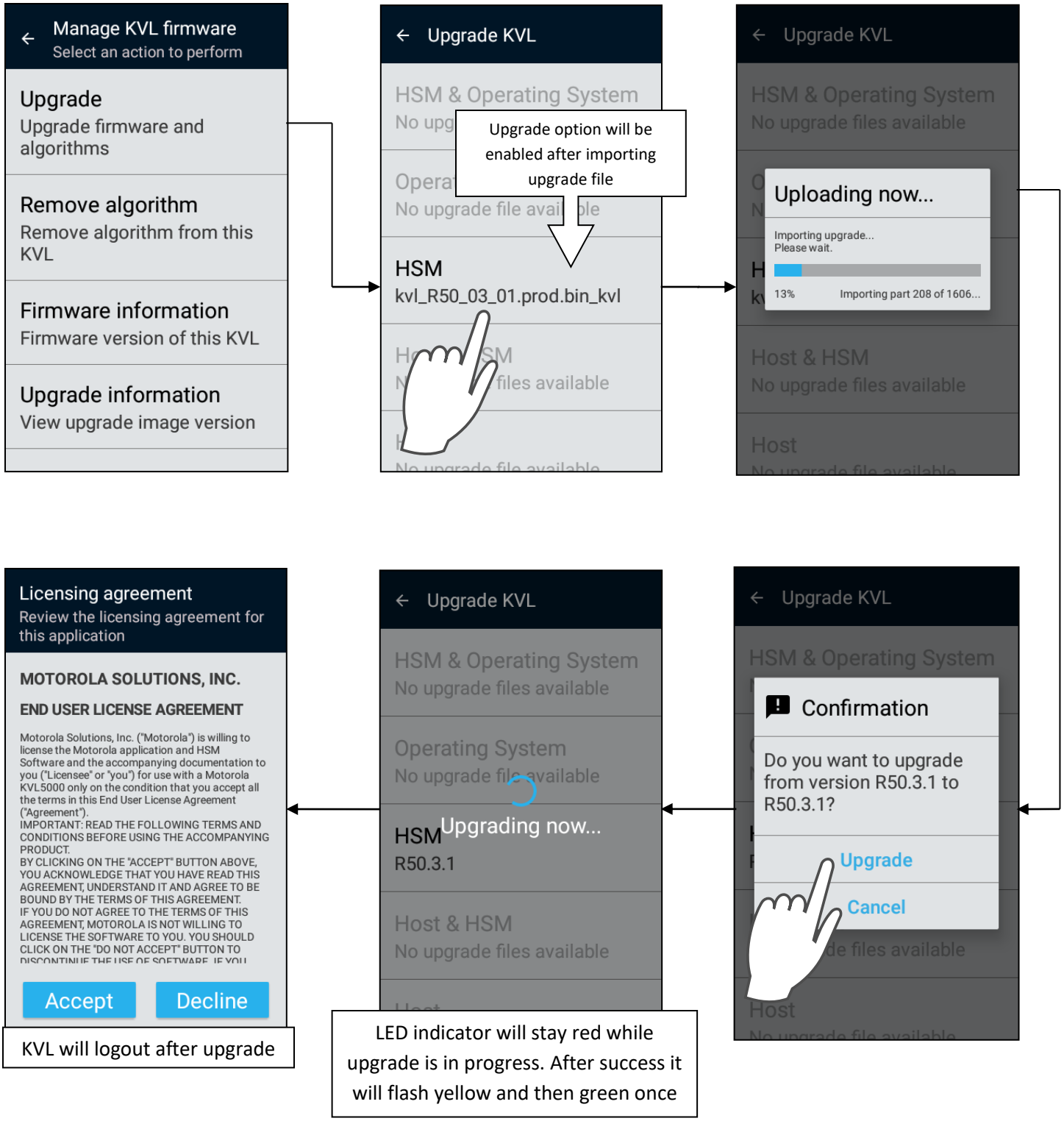
- KVL application (Host) upgrade files with .apk extension
- HSM upgrade files with .bin_kvl extension
- OS upgrade packages with .zip extension
- External device upgrade files with .bin_module extension

KVL will automatically recognize latest upgrade file for each upgrade type. Downgrades are not possible.

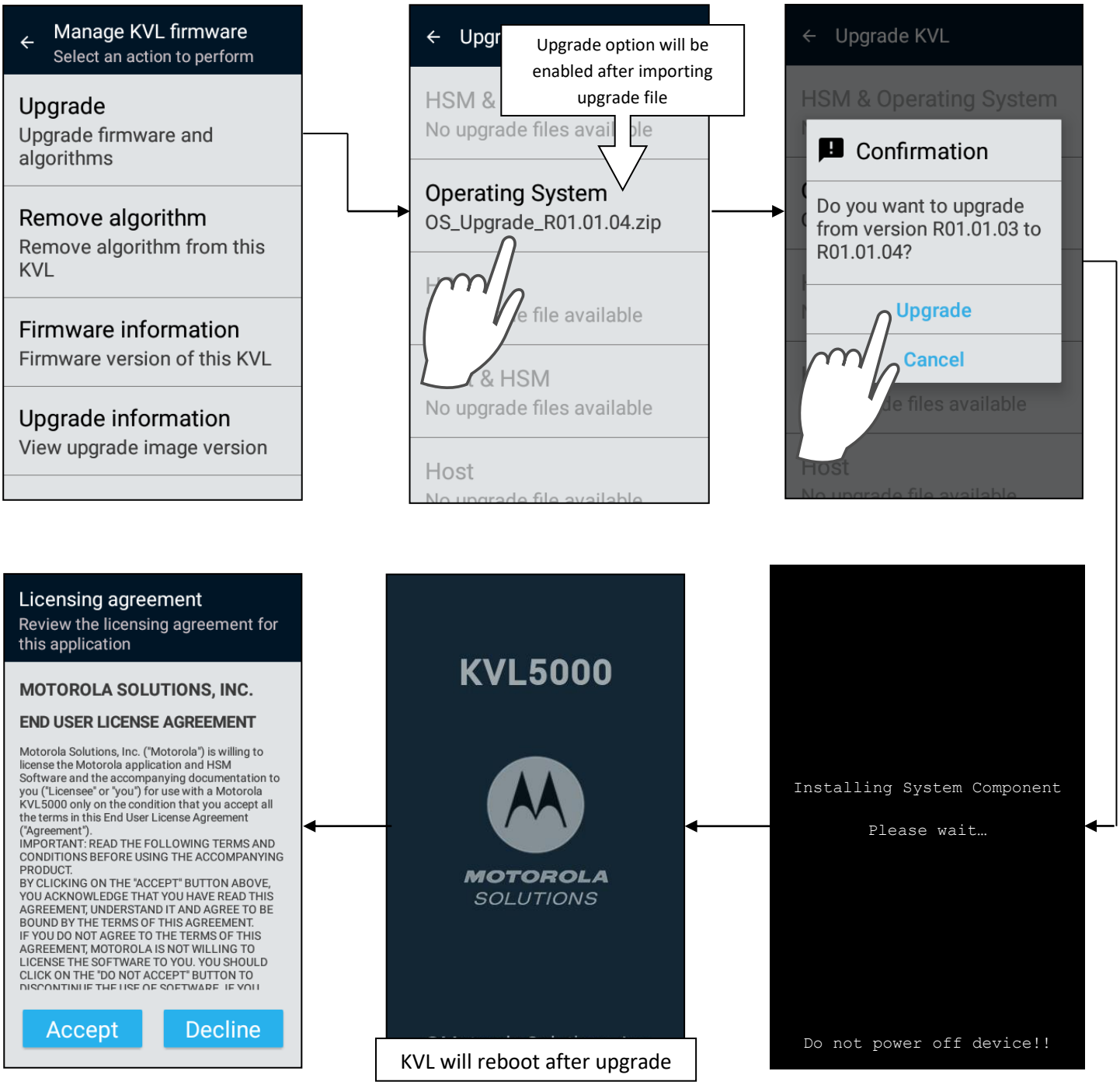
KVL application upgrade



HSM upgrade


Manage KVL firmware
Select an action to perform
Upgrade
Upgrade firmware and algorithms
Remove algorithm
Remove algorithm from this KVL
Firmware information
Firmware version of this KVL
Upgrade information
View upgrade image version
Upgrade KVL
HSM & Operating System
Upgrade option will be enabled after importing upgrade file
HSM
kvl_R50_03_01.prod.bin_kvl
Host & HSM
No upgrade files available
Host
Uploading now...
Importing upgrade...
Please wait.
13%
Importing part 208 of 1606...
Licensing agreement
Review the licensing agreement for this application
MOTOROLA SOLUTIONS, INC.
END USER LICENSE AGREEMENT
Motorola Solutions, Inc. ("Motorola") is willing to license the Motorola application and HSM Software and the accompanying documentation to you ("Licensee" or "you") for use with a Motorola KVL5000 only on the condition that you accept all the terms in this End User License Agreement ("Agreement").
IMPORTANT: READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING PRODUCT.
BY CLICKING ON THE "ACCEPT" BUTTON ABOVE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT.
IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, MOTOROLA IS NOT WILLING TO LICENSE THE SOFTWARE TO YOU. YOU SHOULD CLICK ON THE "DO NOT ACCEPT" BUTTON TO
Accept
Decline
KVL will logout after upgrade
Operating System
No upgrade files available
Upgrading now...
R50.3.1
LED indicator will stay red while upgrade is in progress. After success it will flash yellow and then green once
Confirmation
Do you want to upgrade from version R50.3.1 to R50.3.1?
Upgrade
Cancel

Operating system upgrade

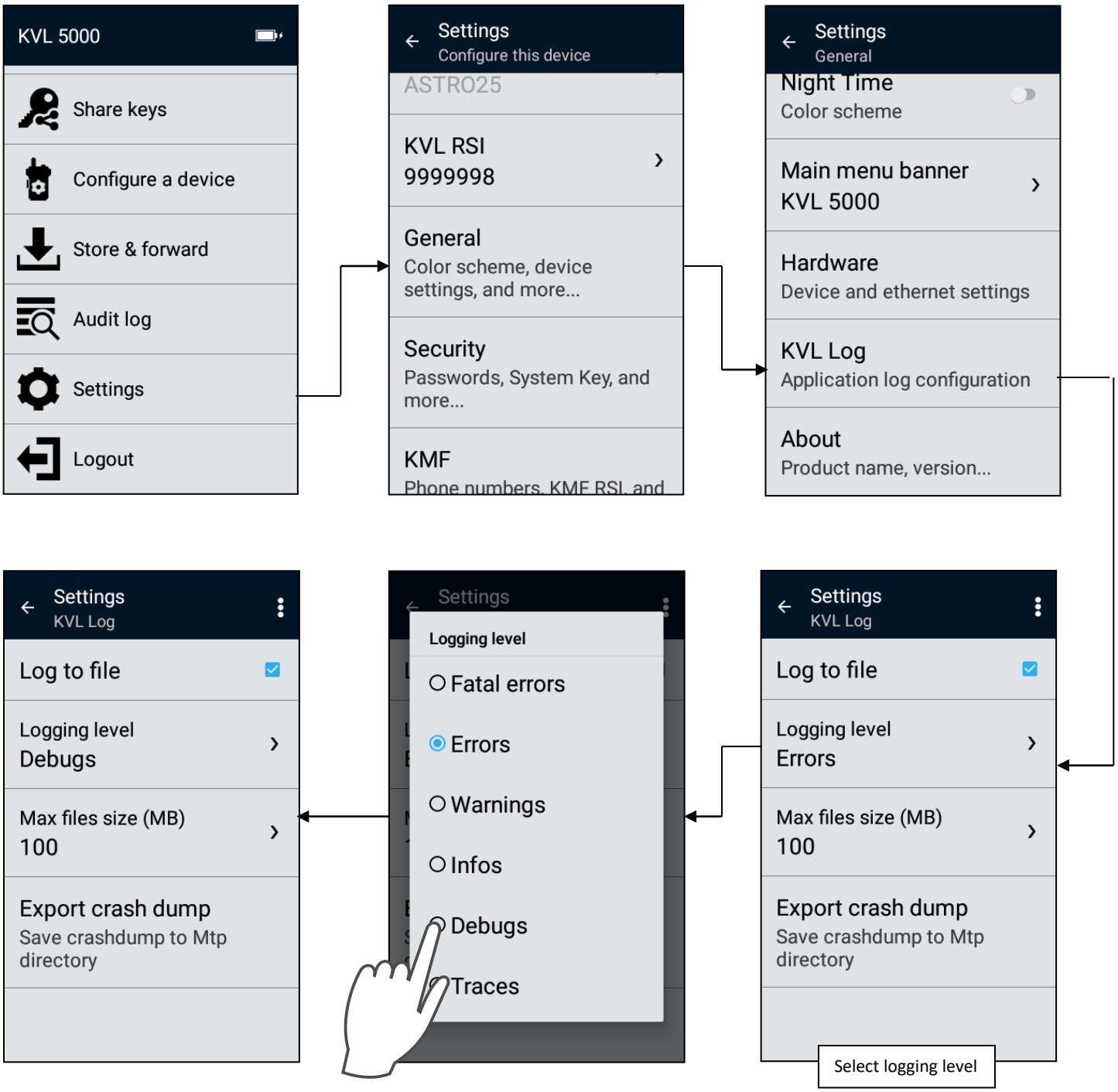


External device upgrade (1)

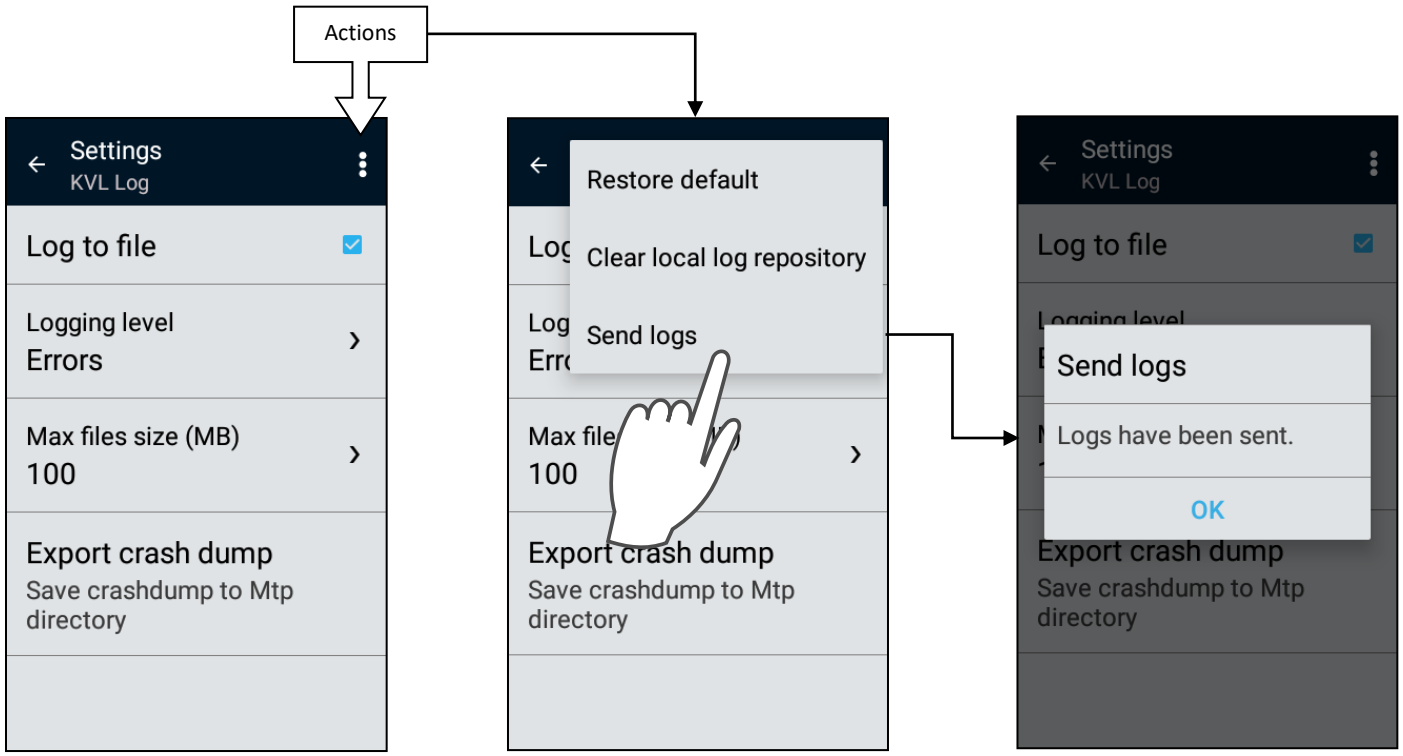
External device upgrade (2)

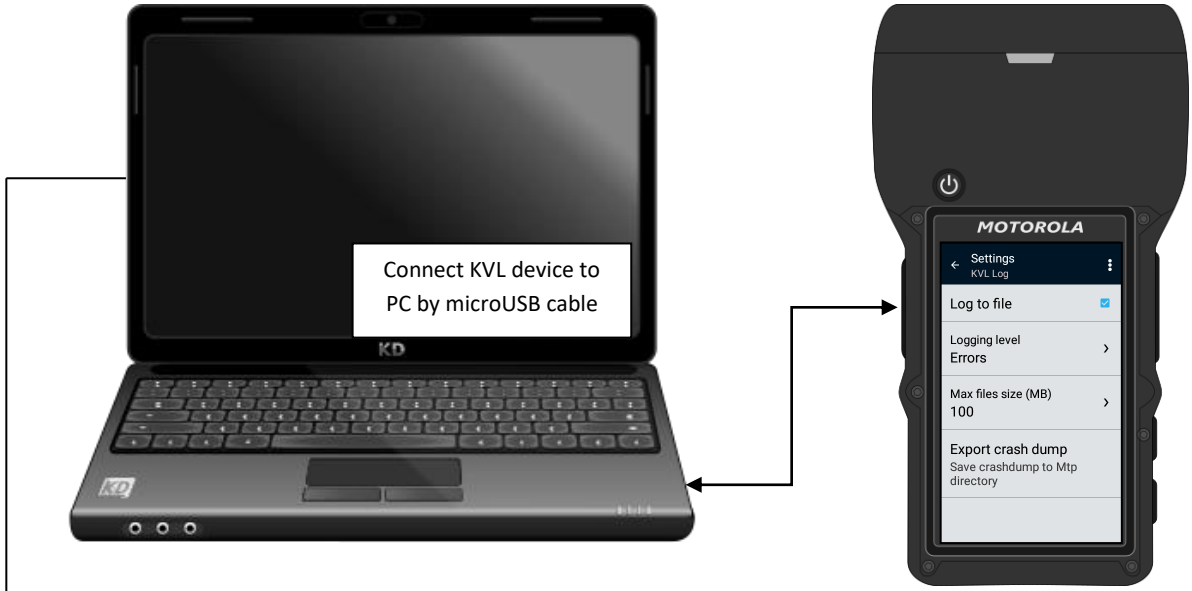
Debug logs

Configuring logging level



Downloading KVL logs to PC





Logs are stored in *This PC\kvl5000\Internal shared storage\kvl logs* directory. KVL needs to be in KVL Log menu to have access to log files

Log event description

The events on the list are sorted from the most severe to the least severe. When you choose a type of event, all more severe events will be logged as well.

For example, if you choose **Warnings**, then **Fatal errors**, **Errors**, and **Warnings** will be logged.

See the following table for more information on the event types:

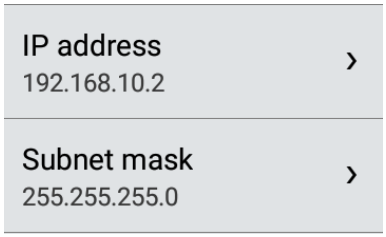
Event Type	Description
Fatal errors	Errors that cause the KVL to stop working correctly
Errors	Errors that do not stop the KVL from running
Warnings	Potentially harmful events
Infos	General informational messages about KVL operation
Debugs	Detailed information about events that are helpful while debugging the KVL
Traces	The lowest severity level of events. All events are logged

Potential IP Connection Issue (1)

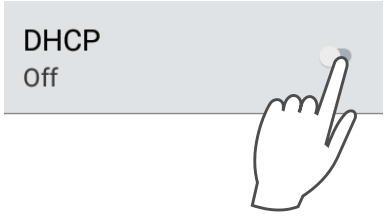
When you connect the KVL to a network and DHCP on KVL is **ON**, in some networks it is possible that the default gateway is not set properly. This may result in connection failure.

IP Connection Troubleshooting Procedure

1. Connect KVL to the network. See S&F with KMF via Ethernet.
2. Go to **Settings →General→Hardware→Ethernet**

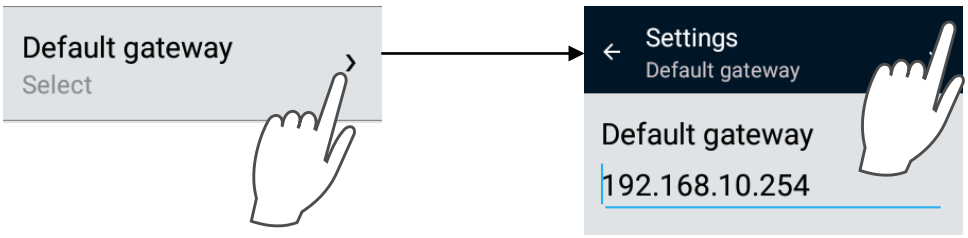


3. Note down values from **IP address** and **Subnet mask** fields.
4. Set **DHCP** to **Off**.

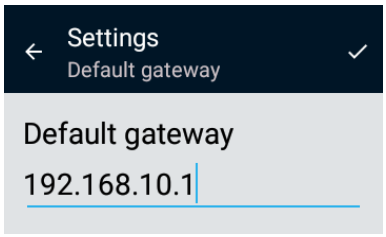


Potential IP Connection Issue (2)

5. In **IP address** and **Subnet mask** fields, manually enter the values that you noted down.
6. Tap **Default gateway**. The maximum value is entered automatically.



7. If the problem is not solved, in the **Default gateway** field enter the minimum allowed value.

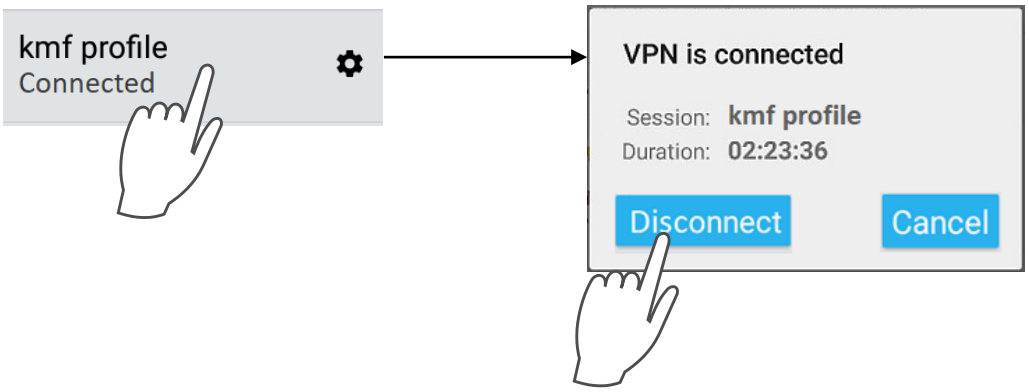


8. If the problem is still not solved, contact your system administrator.

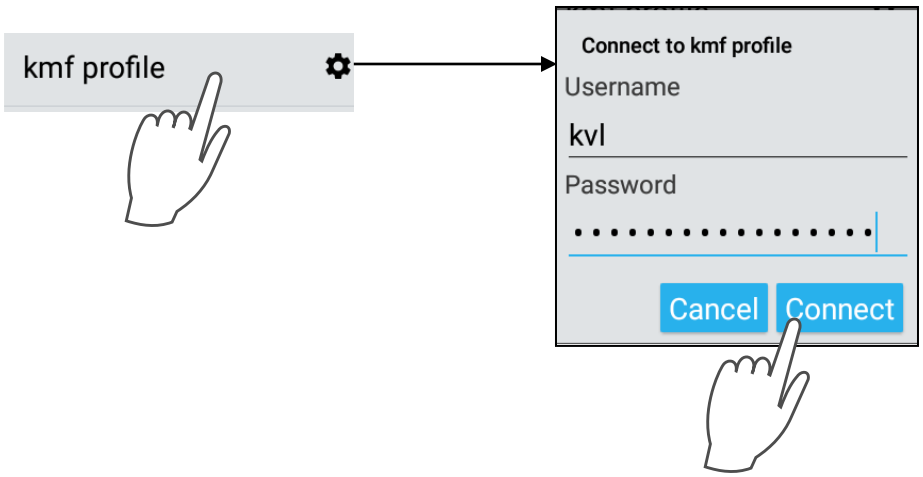
Potential VPN Connection Issue

Most of the VPN connection issues may be resolved in the following way:

- Check the cable connection between KVL and KMF.
- Make sure that the VPN is configured correctly. See Settings VPN section.
- Disconnect and connect to a VPN again by performing the following actions:
  1. From the KVL main menu, go to **Settings → General → Hardware → VPN**.
  2. Tap on a selected VPN to disconnect.



3. Connect to a VPN by tapping its name on the list. When prompted, enter the credentials for your VPN.



KVL Led Indicators

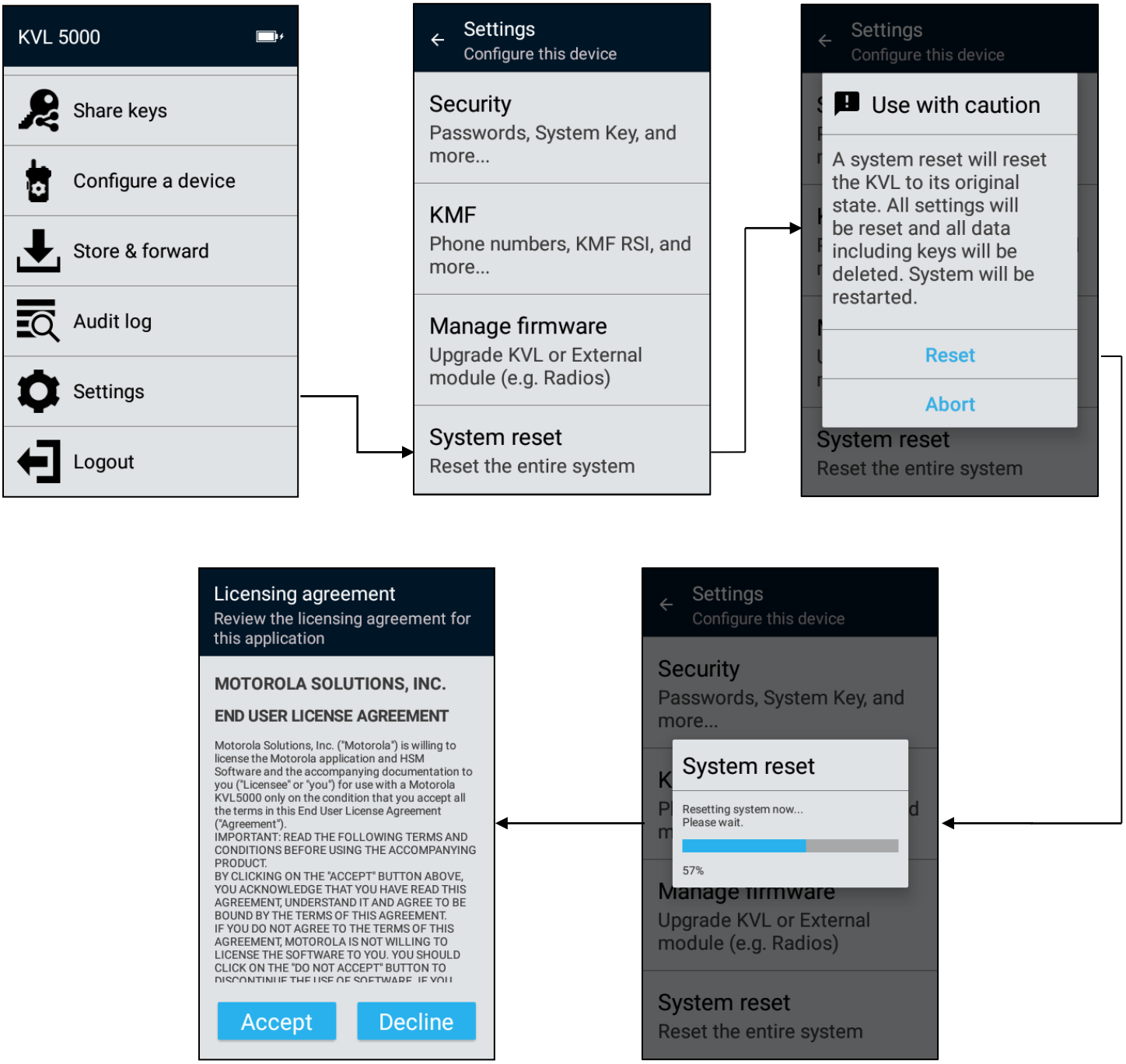
Led color on the KVL provides on current KVL status.

KVL 5000 LED Indicators

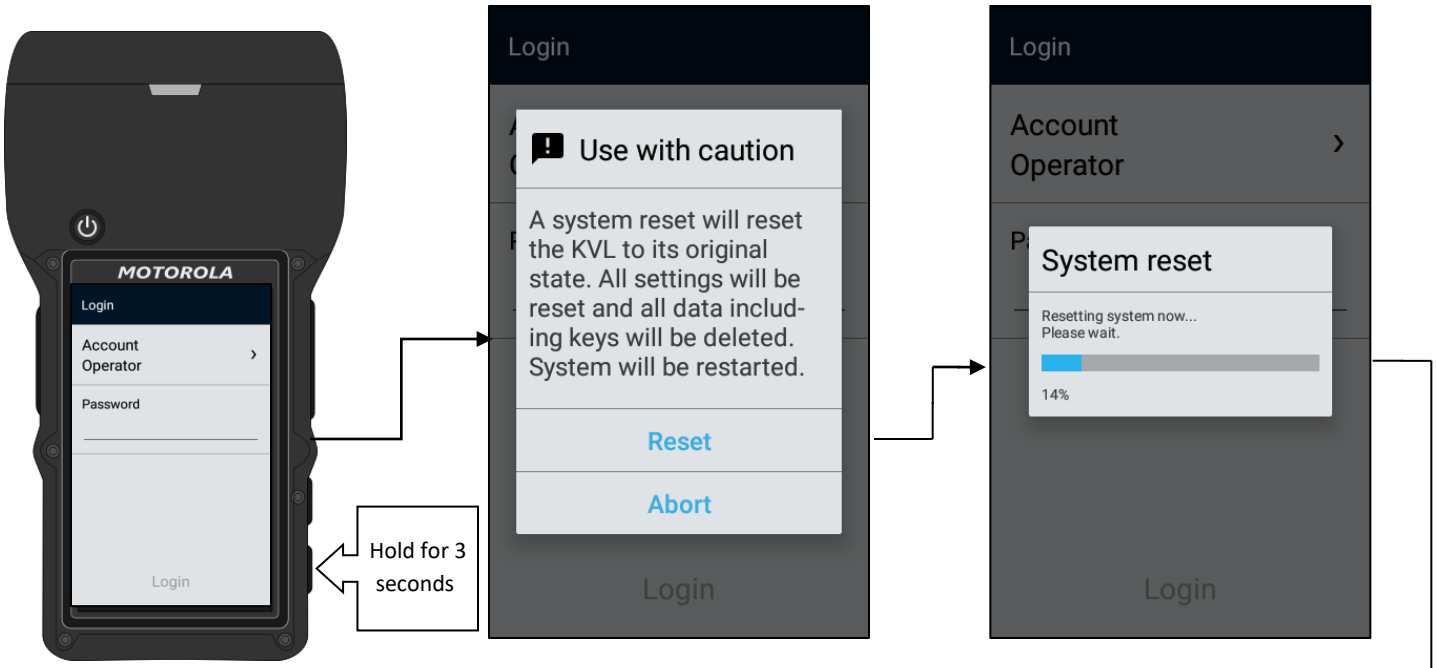
Led color	Meaning
Red	KVL is booting up
Yellow	Checking KVL data integrity
Green	KVL is ready for use
Yellow (flashing)	Formatting KVL memory. May take up to 2 minutes
Red (constant)	KVL may be in one of the states: HSM failure - KVL needs to be restarted HSM permanent failure (restart does not solve issue) – KVL needs to be sent for repair HSM stays in programming mode after upgrading (restart does not solve issue) - KVL needs to be sent for repair

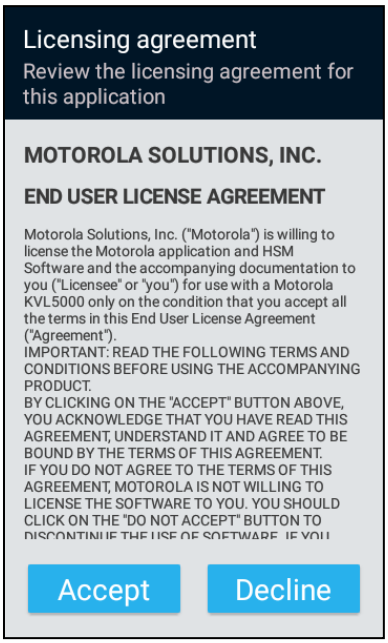
Clearing sensitive data

Perform system reset



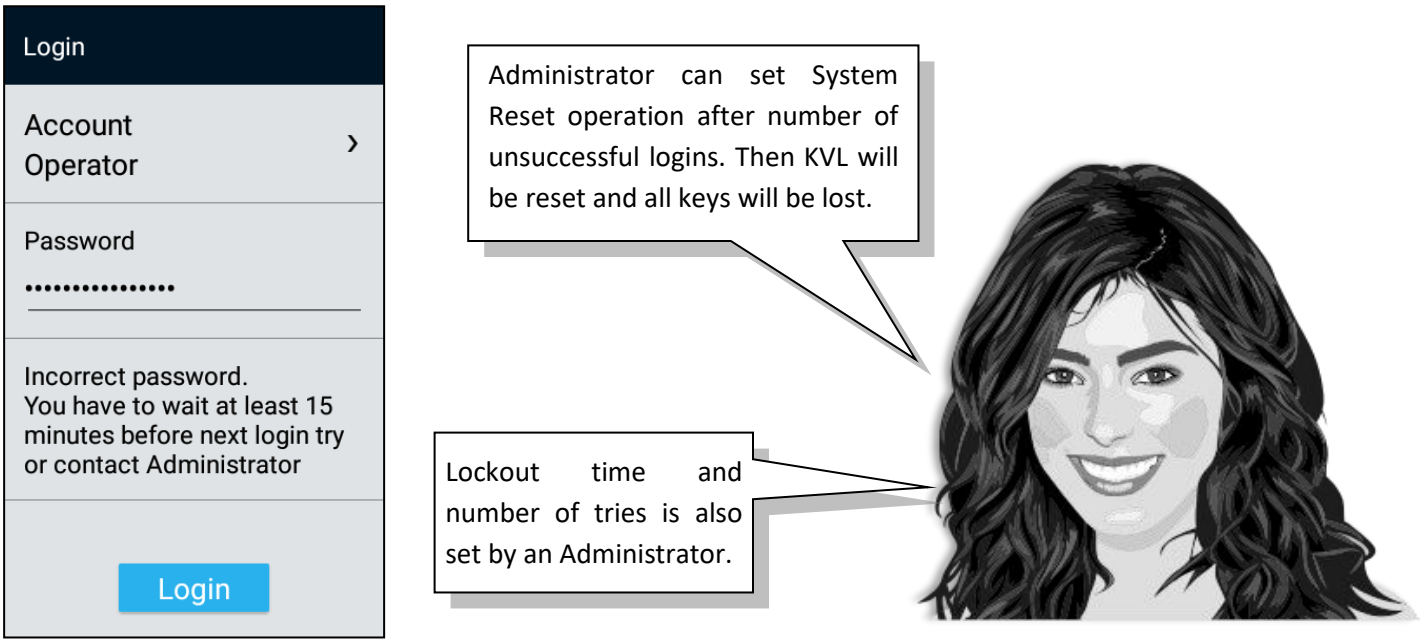
Perform system reset using hardware button





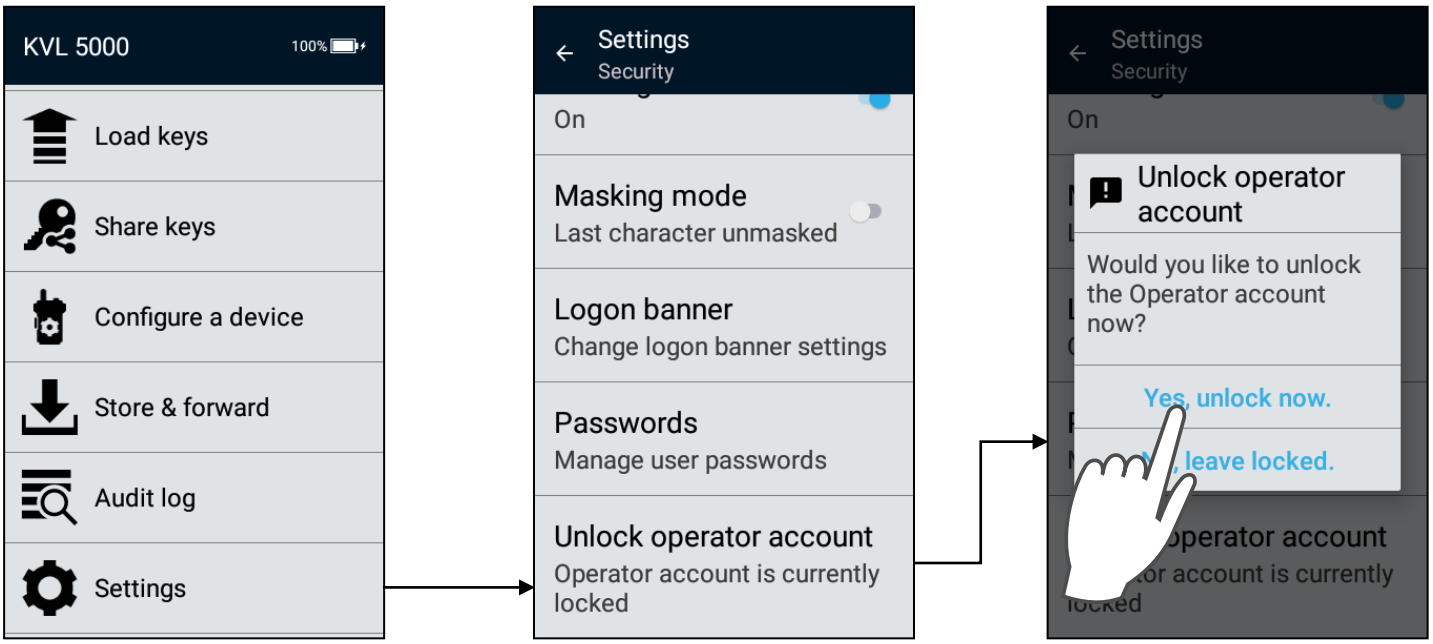
Operator Lockout

When trying to log in with wrong password more than set number of times, lockout is engaged.



Unlocking account

Administrator can unlock Operator's account in Settings.



Potential Radio Authentication issues

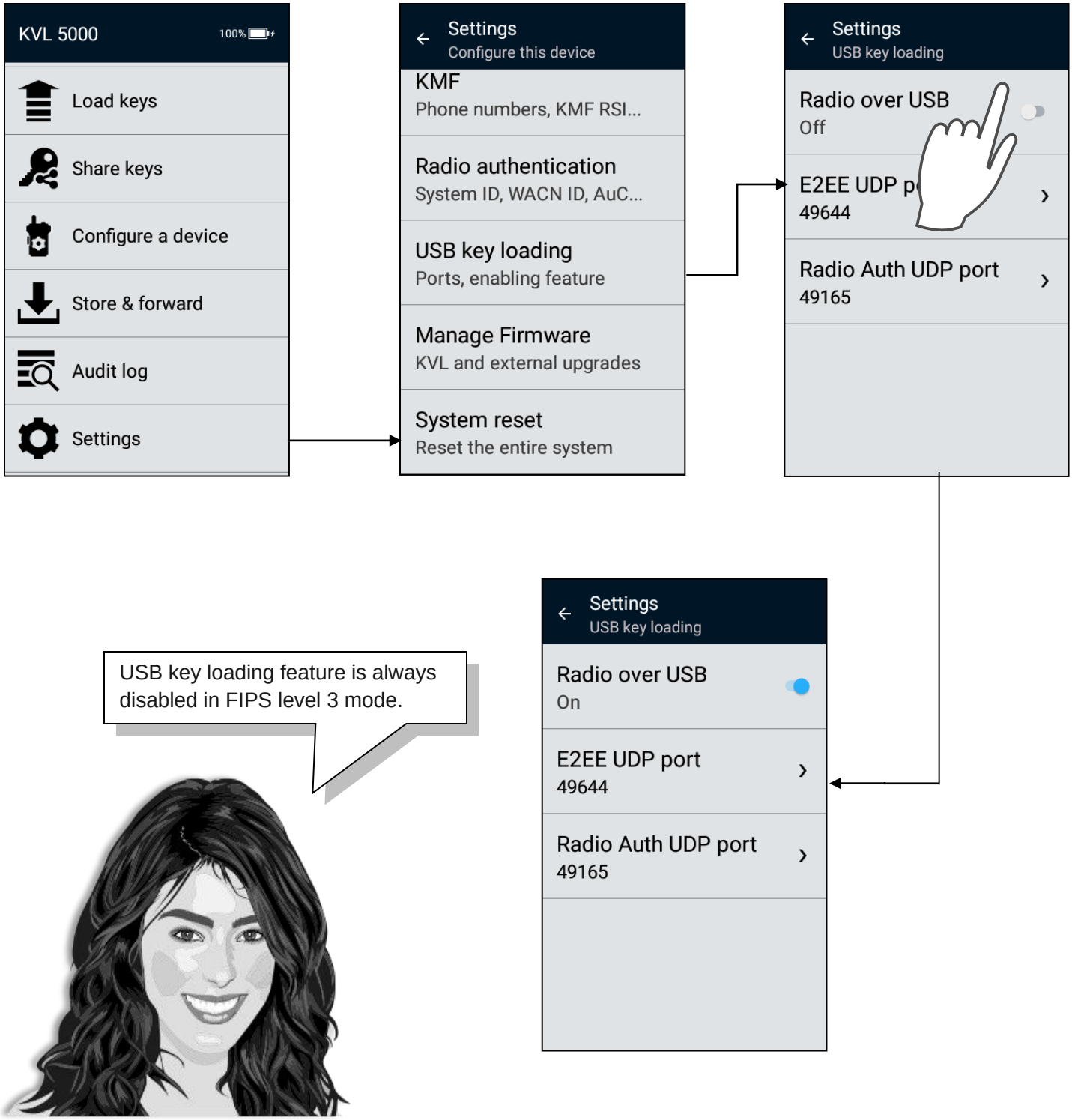
In case there is an issue with connecting KVL to radio for Radio Authentication operations, please make sure that the following conditions are met:

- Serial cable is used for connection between KVL and the radio.
- Radio has been configured for Radio Authentication feature (radio must have Radio Authentication turned on and set correct System ID, WACN ID, Radio Id and Radio port), especially the active profile on the connected radio (each profile can have assigned separate SUID).
- Please note that radio can turn off some of its functions when the battery is low

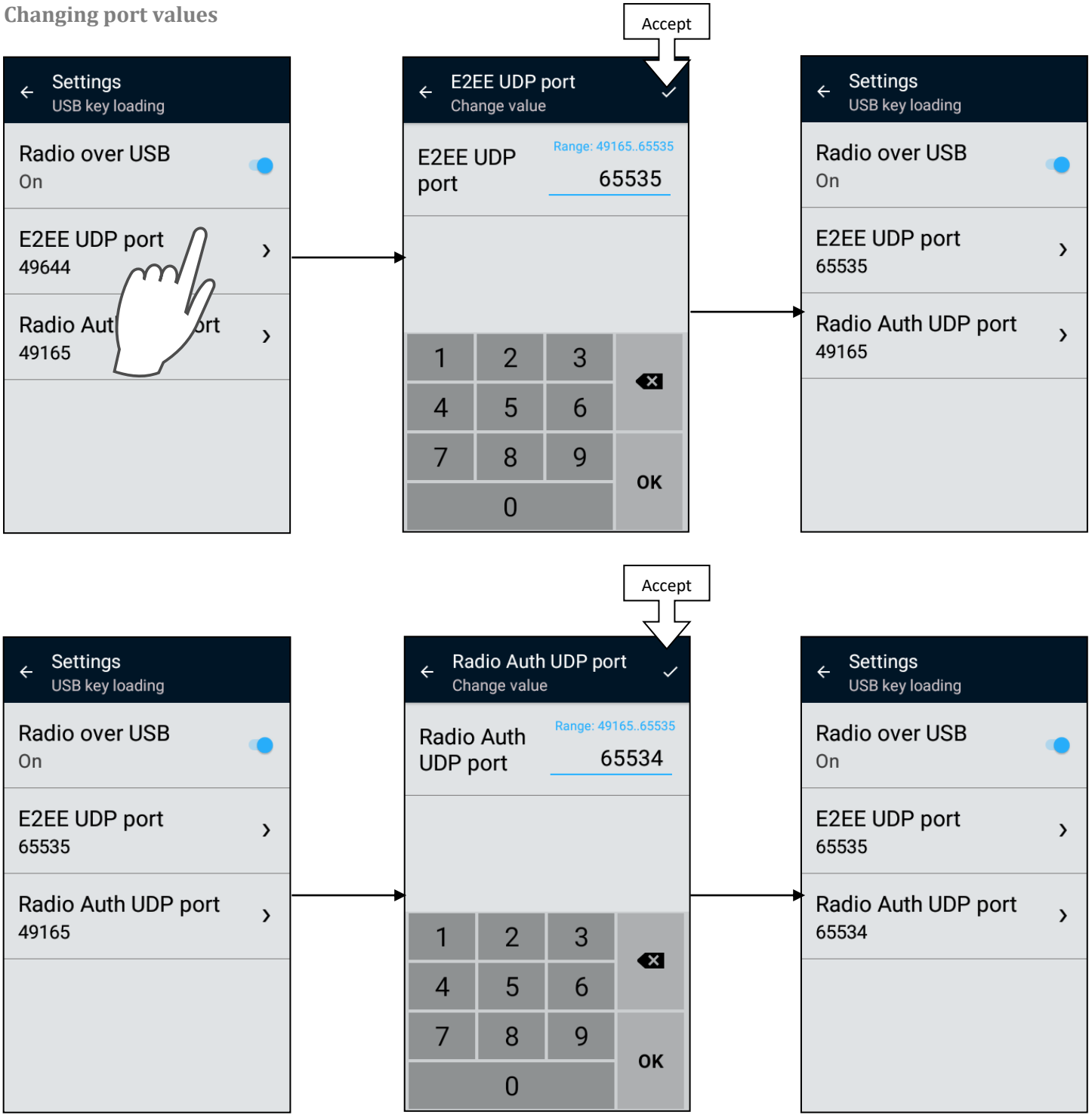
Note: SUID = System ID + WACN ID + Radio ID

USB key loading

Enabling USB key loading feature

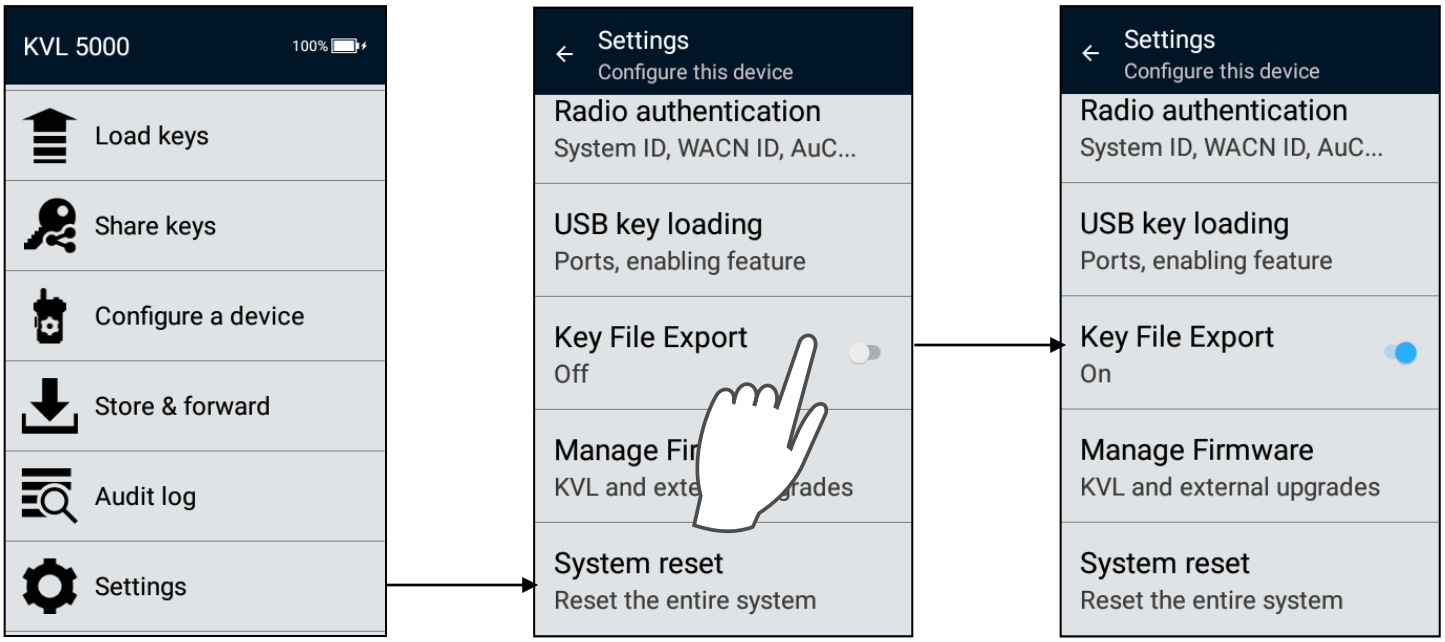


Changing port values

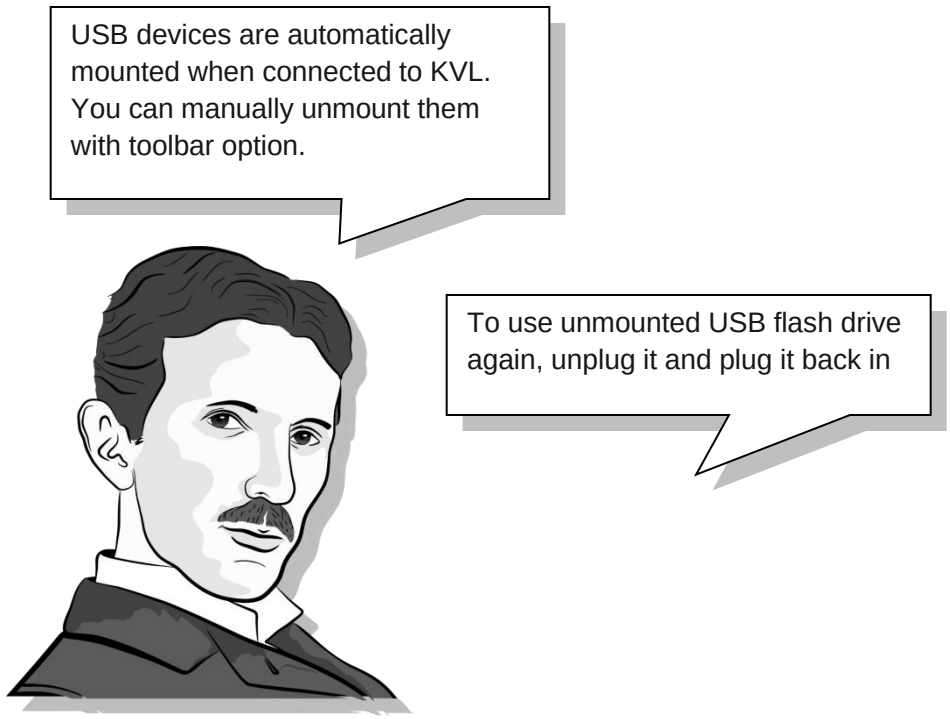


Key File Export

Enabling key file export feature



Unmounting USB flash drive



Key export file missing on USB flash drive

Some USB flash drives will not store exported key if USB flash drive was not unmounted properly. To ensure correct file saving please unmount USB stick after completing file export.

Potential Tactical OTAR issues

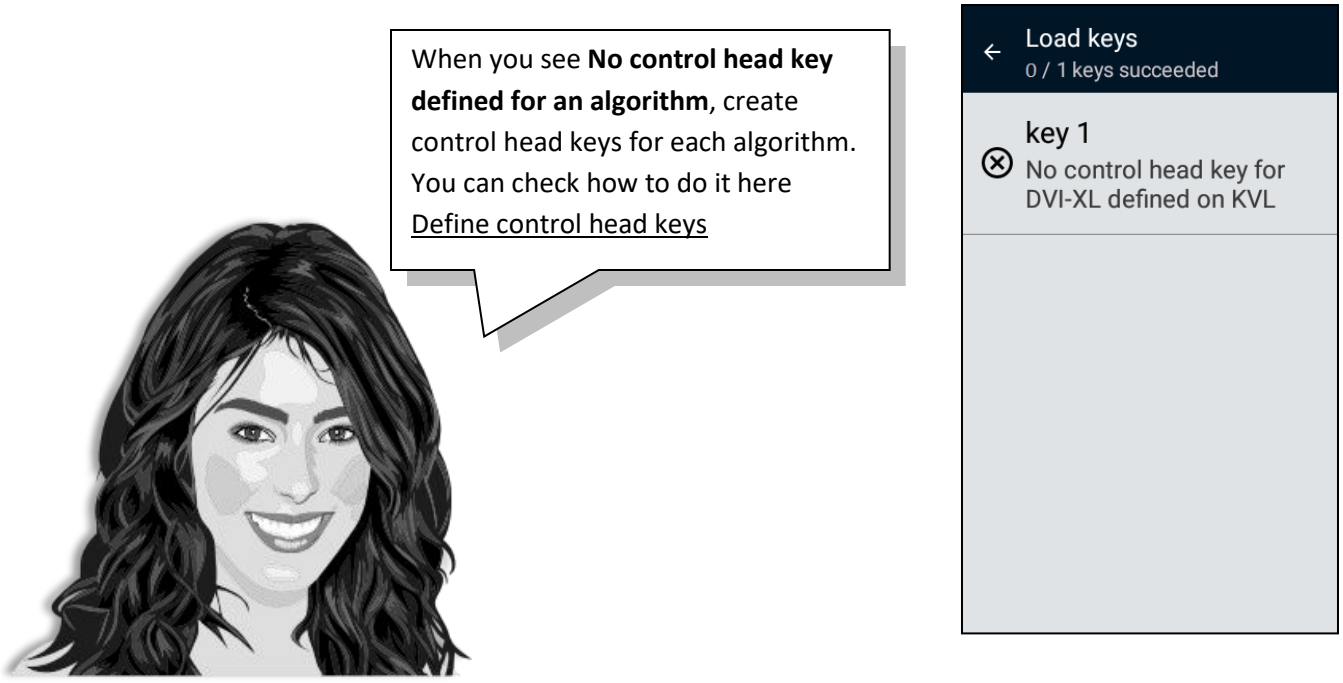
In case there is an issue with connecting KVL to radio for Tactical OTAR update operation, please make sure that the following conditions are met:

- Serial cable is used for connection between KVL and the radio.
- Radio serving as an RF modem must be equipped with the Tactical Rekey/OTAR feature
- Members to update are within range
- Please note that radio can turn off some of its functions when the battery is low

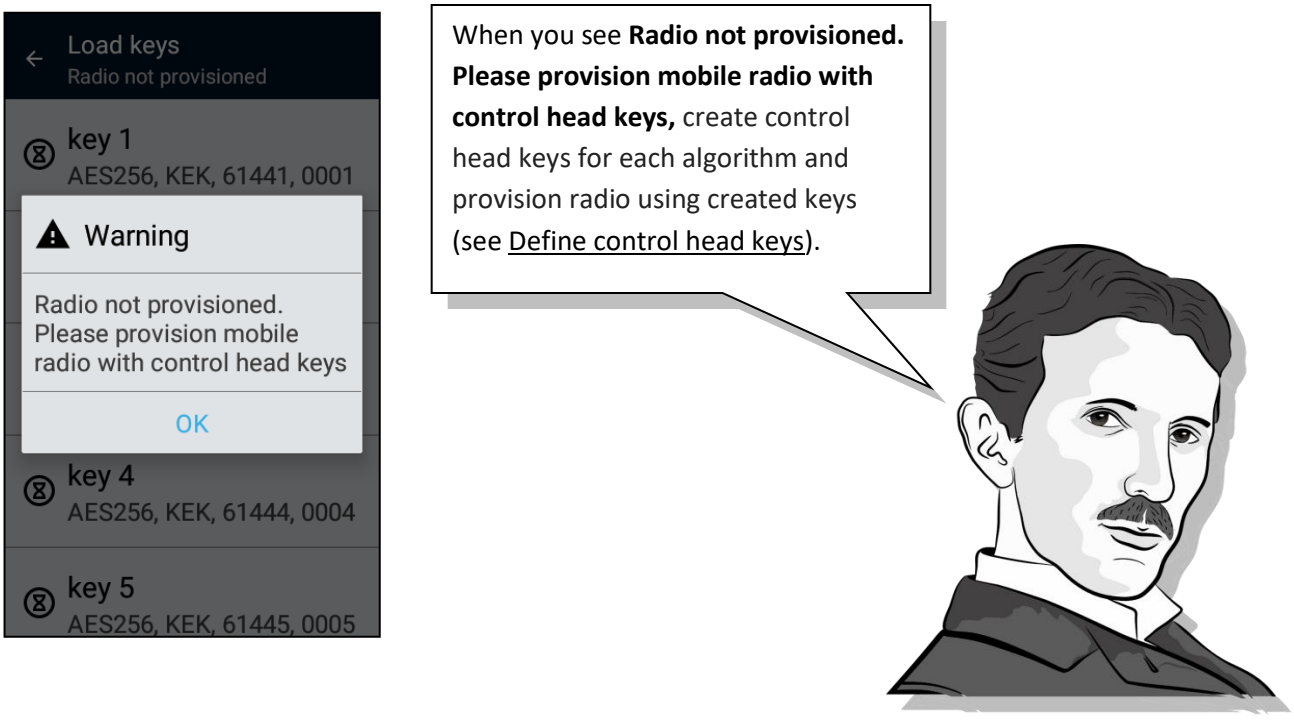
When you see **Missing KEK to decrypt** status add the member again to the Tactical OTAR group

Potential Control Head issues

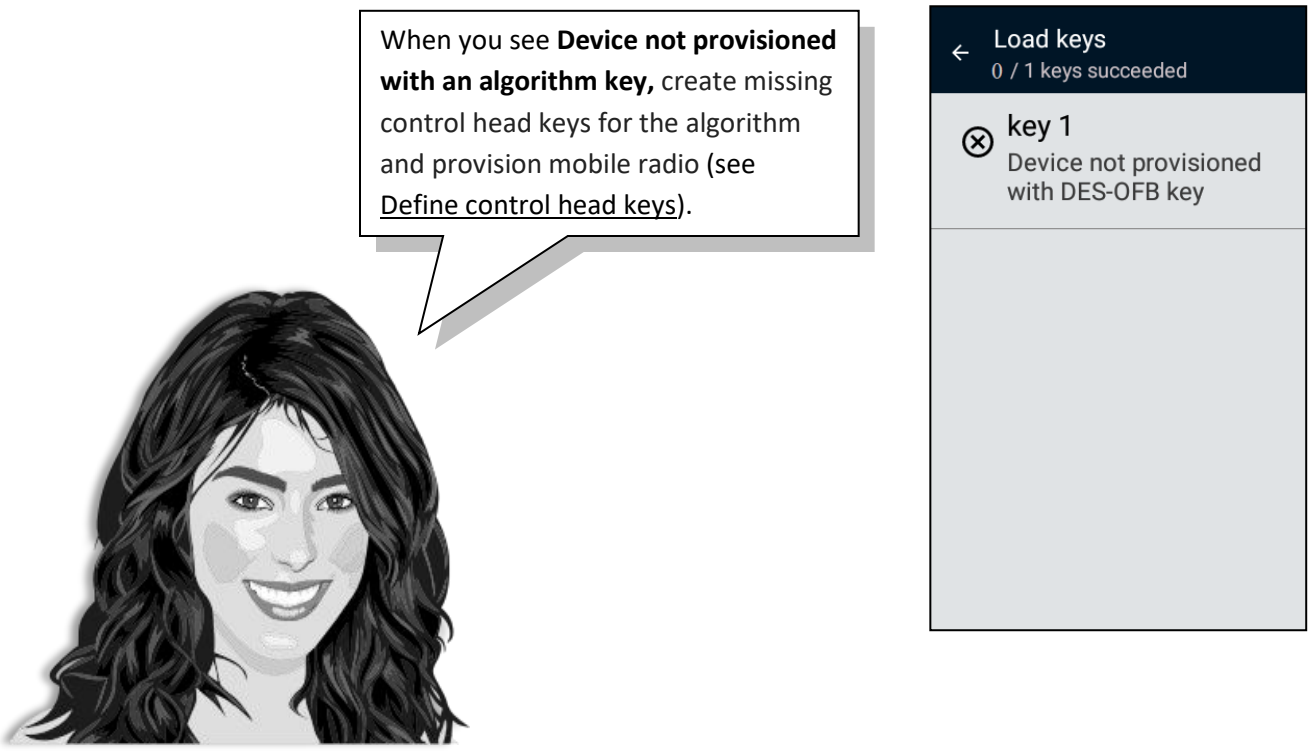
No control head key defined for algorithm



Radio not provisioned



Device not provisioned with algorithm key



Appendix: KVL Role based Action List

KVL Action	Admin has Access	Operator has access
Configure Radio		
View Target RSI(s) (Individual, Group)	yes	yes
Change Target Individual RSI	yes	yes
View Target KMF RSI	yes	yes
Change Target KMF RSI	yes	yes
View Target Keys	yes	yes
View Target Keysets	yes	yes
Change Target Active Keyset	yes	yes
View Target MNP	yes	yes
Change Target MNP	yes	yes
Remove Target Key	yes	yes
Remove Target Group	yes	yes
Remove All from Target	yes	yes
Load & Share		
Load Key	yes	yes
Load Key Group	yes	yes
Store and Forward Download	yes	yes
Store and Forward Update	yes	yes
View Targets to Update	yes	yes
Clear Targets to Update	yes	no
Load Automatic SU Auth Key	yes	yes
Load Manual SU Auth Key	yes	yes
Download K-SUID pairs to AuC	yes	yes
View SUID that have been loaded	yes	yes
Clear K-SUID pairs that have been loaded	yes	no

Manage Keys & Groups		
View Key	yes	yes
Add Key	yes	Only with Keys and Groups permission
Delete Key	yes	Only with Keys and Groups permission
Delete KMF / AUC UKEK Keys	yes	Only with Keys and Groups and KMF / AUC permissions
Edit Key	yes	Only with Keys and Groups permission
Add Group	yes	Only with Keys and Groups permission
Delete Group	yes	Only with Keys and Groups permission
Rename Key Profile	yes	no
Clear Key Profile	yes	no
Tactical OTAR		
View Tactical OTAR Groups	yes	yes
Add Tactical OTAR Group	yes	Only with OTAR Groups permission
Delete Tactical OTAR Group	yes	Only with OTAR Groups permission
Edit Tactical OTAR Group	yes	Only with OTAR Groups permission
Add Tactical OTAR Member	yes	Only with OTAR Groups permission
Remove Tactical OTAR Member	yes	Only with OTAR Groups permission
Tactical OTAR Full Update	yes	yes
Tactical OTAR Optimized Update	yes	yes

Appendix: KVL Role based Action List

Settings		
Change KVL RSI	yes	no
Change Theme	yes	yes
Change Inactivity Timeout	yes	no
Change FIPS Mode	yes	no
Change System Key	yes	no
Change Sharing Mode	yes	no
Change Banner Text	yes	no
Change Hardware Settings	yes	yes
Change Application Log Level	yes	yes
Export Application Log	yes	yes
Change Operator Password	yes	yes
Change Admin Password	yes	no
Clear Passwords	yes	no
Change KMF RSI	yes	Only with KMF permission
Change KMF MNP	yes	Only with KMF permission
Change KMF Baud Rate	yes	yes
Change Active KMF	yes	yes
Change KMF Phone #'s	yes	Only with KMF permission
Change KMF UKEK Setup	yes	Only with KMF permission
Enable USB Key Loading	yes	no
Change USB Port Numbers	yes	no
Enable Key File Export	yes	no
View Audit Log	yes	yes
Clear Audit Log	yes	no

Appendix: KVL Role based Action List

Settings		
System Reset	yes	yes
Change KVL Radio Auth ID	yes	Only with AuC permission
Change AuC Destination Port	yes	Only with AuC permission
Change Active AuC	yes	yes
Change SU Destination Port	yes	Only with AuC permission
Change AuC UKEK Setup	yes	Only with AuC permission
Change SU Auth System ID	yes	Only with AuC permission
Change SU Auth WACN ID	yes	Only with AuC permission
Manage Firmware		
Upgrade KVL	yes	no
Remove KVL Algorithms	yes	no
View KVL Firmware Version	yes	yes
Upgrade External Crypto Module	yes	no
Remove Algorithm From External Crypto Module	yes	no
View External Crypto Module Firmware	yes	yes
Control head		
Change MNP	yes	Only with control head permission
Define control head keys	yes	Only with control head permission
Provision mobile radio	yes	yes
Load keys and groups	yes	yes