

New SE350 Standard model

Service actions and differences with the original SE350 model

The Lenovo logo is positioned on the right side of the slide. It consists of the word "Lenovo" in a white, sans-serif font, oriented vertically. The background behind the text is a vertical gradient bar transitioning from green at the top to blue at the bottom.

SE350 Standard model

As of August 2021, there are two SE350 models (The machine type has not changed)

- SE350 with Security Pack
- SE350 Standard

SE350 with Security Pack	SE350 Standard (Security Pack disabled)
<ul style="list-style-type: none">• SE350 automatic data protection can be enabled – this includes the intrusion sensor and motion sensor• SED data access can be locked up at tamper events• The system will need to be claimed and activated in order to unlock and access data• Must be activated to boot up and become fully functional• The Secure Activation Code is used when claiming the system for activation or when the system board is replaced	<ul style="list-style-type: none">• SE350 automatic data protection is disabled• Data access will never be locked up, SED management is disabled, and the tamper setting is disabled• No activation is required• Claiming the system is optional, but the Secure Activation Code would be needed

Note: The Activation Code is printed on the asset tag and the flyer that was shipped with the server. Users can scan the QR code on the system board to get the Device key. Click the buttons to see more details.

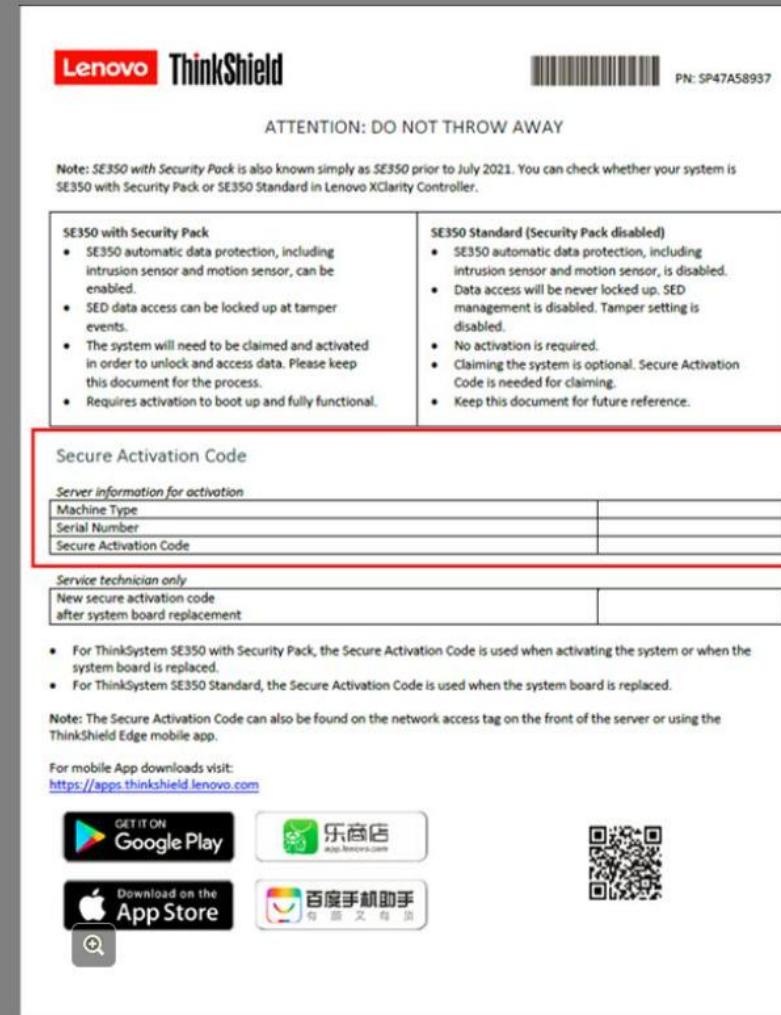
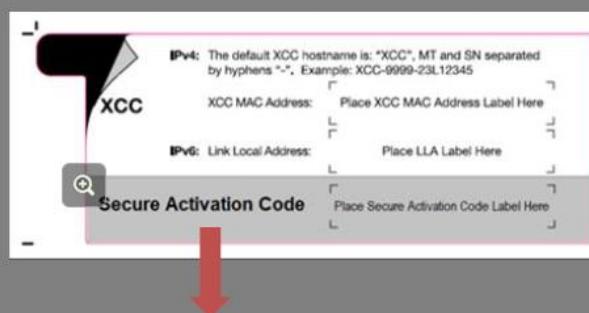
Asset tag and flyer

QR code

Secure Activation Code on the asset tag and flyer



A new field for the Secure Activation Code has been added to the pull-out asset tag and flyer.

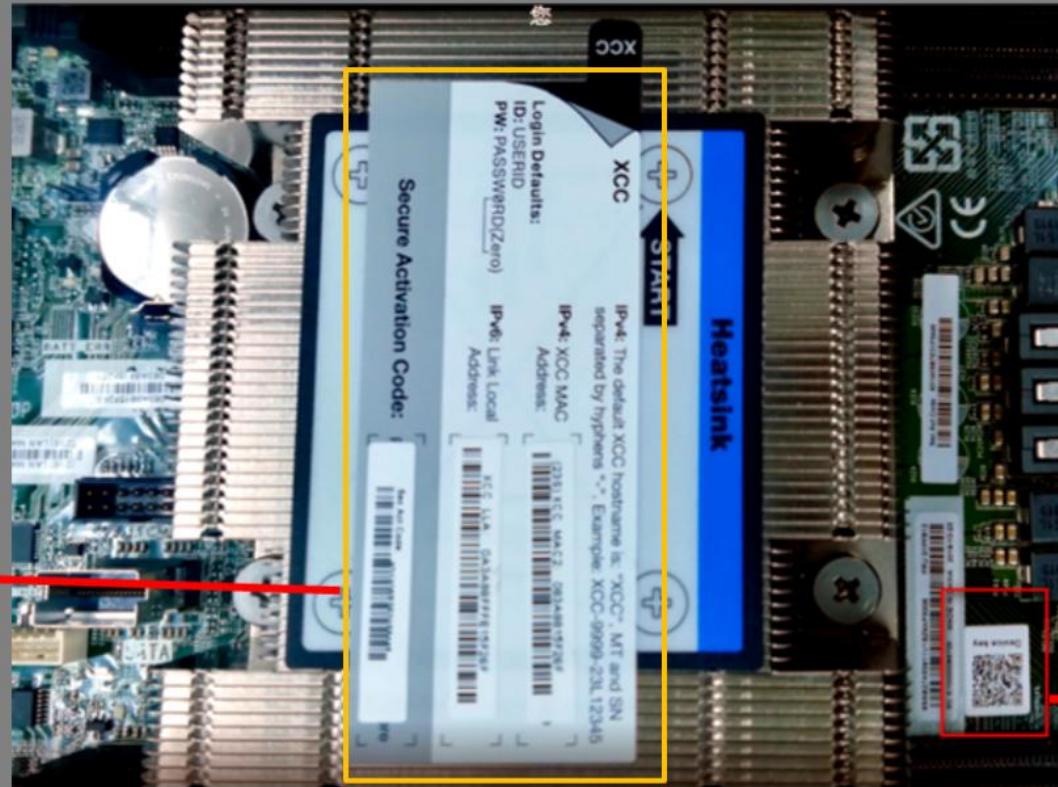




A QR code has been added to the system board. When you replace a system board, scan the QR code to get the Device key.

A Secure Activation Code sticker will be attached to the heat sink on the new system board. When you replace the system board, peel off the sticker and attach it to the pull-out asset tag.

Secure Activation
Code sticker



SE350 Device key
QR code



Identifying the two SE350 models

XCC can be used to check whether a system is an SE350 with Security Pack or an SE350 Standard. Authorized servicers can also use the ThinkShield Service Support account to log in to ThinkShield Key Vault Portal to check the SE350 device type.

Click the buttons below to see examples.

Checking with XCC:

- Login page [Click here](#)
- Home page [Click here](#)
- Lockdown mode configuration [Click here](#)
- SED management [Click here](#)

Checking with ThinkShield Key Vault Portal [Click here](#)

Checking with XCC – Web login page



With a Standard model, **System Lockdown Mode** will be shown as **Not Applicable**, and the Secure Activation Guide link will be removed.

Len

ThinkSystem SE350

System Events	3	1
Machine Type	7Z46	
Serial Number	1234567890	
Power State	Off	
BMC IP	10.240.219.133	
Location		
System Lockdown Mode	Not Applicable	

ThinkSystem

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2020. Lenovo is a trademark of Lenovo in the United States, other countries, or both.

SE350 Standard

Len

XClarity Controller

User name

Password

Login

Secure Activation Guide

Remove

Len

Hodaka Planner (2123IT CPU)

System Events	2
Machine Type	7Z46
Serial Number	PENTEST004
Power State	Off
BMC IP	10.240.219.120
Location	
System Lockdown Mode	Inactive

ThinkSystem

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021. Lenovo is a trademark of Lenovo in the United States, other countries, or both.

SE350 with Security Pack

Checking with XCC – Home page



With a Standard model, the **System Lockdown Mode**, **Motion Detection**, and **Intrusion Detection** quick links will be removed.

System Information and Settings

Hodaka Planner (2123iT CPU)	Power Off
Machine Type/Model	7Z46CTO1WW
Serial No.	PENTEST004
System Name	
Front Panel USB Port Management	Enabled
BMC License	Lenovo XClarity Controller Enterprise Upgrade
BMC IP Address	10.240.219.120
BMC Hostname	XCC-7Z46-PENTEST004
BMC Version	3.30 (Build ID: TEI379D)
UEFI Version	1.10 (Build ID: HYE115A)
LXPM Version	2.04 (Build ID: PDL133C)
Location	
System Lockdown Mode	Inactive
Motion Detection	Disabled
Chassis Intrusion Detection	Disabled

Quick Actions

- Power Action
- Location LED: Off
- Service

Power Utilization

33W	Output	
0W	0W	33W
CPU	Memory	Others

System Utilization

0%	0%	0%	0%
CPU	Memory	I/O	System

Remove

XCC Lockdown Mode configuration



Lockdown Mode settings have been removed from the BMC Configuration page.

The screenshot shows the BMC Configuration page for a ThinkSystem SE350 Planner. The left sidebar lists various configuration sections, with 'BMC Configuration' currently selected. The main content area displays a warning message about the removal of Lockdown Mode settings. A red dashed box highlights the 'System Lockdown Mode' section, which contains a warning message and configuration for Motion Detection and Chassis Intrusion Detection. A red arrow points to the 'LOCKDOWN' entry in the 'Quick Link' sidebar, with the text 'Remove' next to it, indicating that the Lockdown Mode configuration has been removed.

XClarity Controller

! ThinkSystem SE350 Planner ... System name:

Allow Third-Party Password Retrieval Disabled

System Lockdown Mode ?

De-asserted

Motion Detection ? Disabled

Chassis Intrusion Detection ? Enabled

Additional Configurations

Apply Cancel

ThinkShield Key Vault

Quick Link

- SSL
- SSH
- IPMI
- SYS FW
- TPM/TCM
- PWD MGR
- LOCKDOWN**
- SED AK

Remove

SED Authentication Key (AK) Manager ?

- Change the SED AK ?
- Backup the SED AK ?

SED key management



The SED key management page has been removed from BMC configuration as SED data would not be encrypted for the Standard model.



Checking with ThinkShield Key Vault Portal



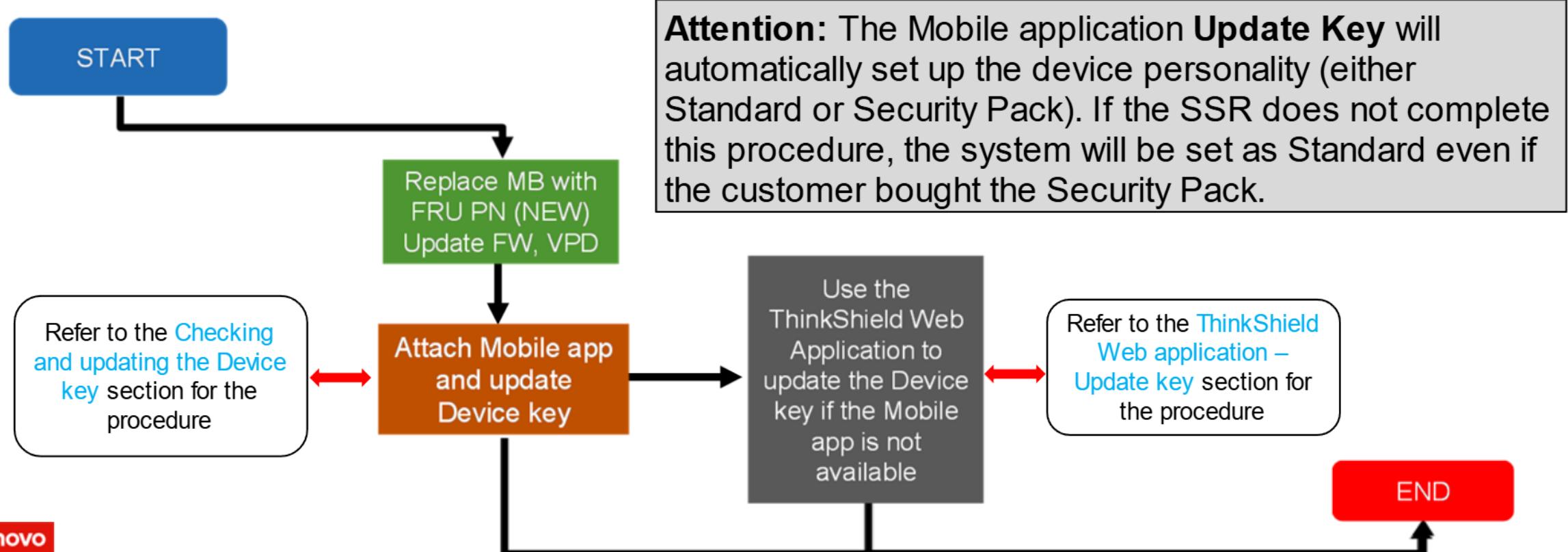
Use the ThinkShield Service Support account to log in to the ThinkShield Portal to check the SE350 device. The **MODE** will be displayed as either **Standard** or **Security Pack**.

The screenshot shows the ThinkShield Key Vault Portal interface. On the left, a sidebar has 'Device Manager' selected. The main area is titled 'Devices' and shows a table with columns: STATUS, MODE, DEVICE NAME, MACHINE TYPE, SERIAL NUMBER, and GROUP. A red box highlights the 'MODE' column, which contains buttons for 'Security Pack' and 'Standard'. The table data is as follows:

STATUS	MODE	DEVICE NAME	MACHINE TYPE	SERIAL NUMBER	GROUP
Active	Security Pack	343b	4f...	J30...	
Active	Security Pack	MST	7D5S	J30...	Lenovo...
Active	Standard	MST	7D5S	J30...	Lenovo...
Active	Security Pack	ADP	7Z46	J30...	
Active	Security Pack	Kevin	7D1X	J10...	
Manually Activated	Security Pack	Data	7Z46	J30...	

System board servicing procedure

As the SE350 Standard model cannot be locked and does not need activation, the procedure used to replace the system board is mostly the same as with ordinary Lenovo servers. However, the Device key still needs to be updated after a system board replacement. Users have the option of claiming a Standard model device, but the Secure Activation Code will still be needed to claim a device.



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.

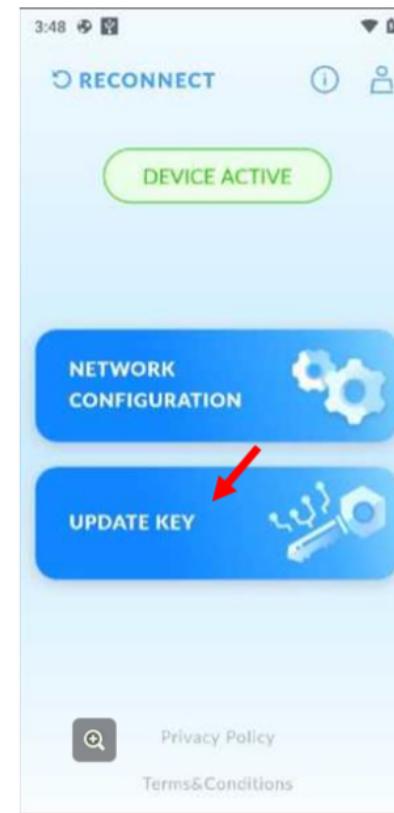
Click each number in turn to see the procedure.

Step

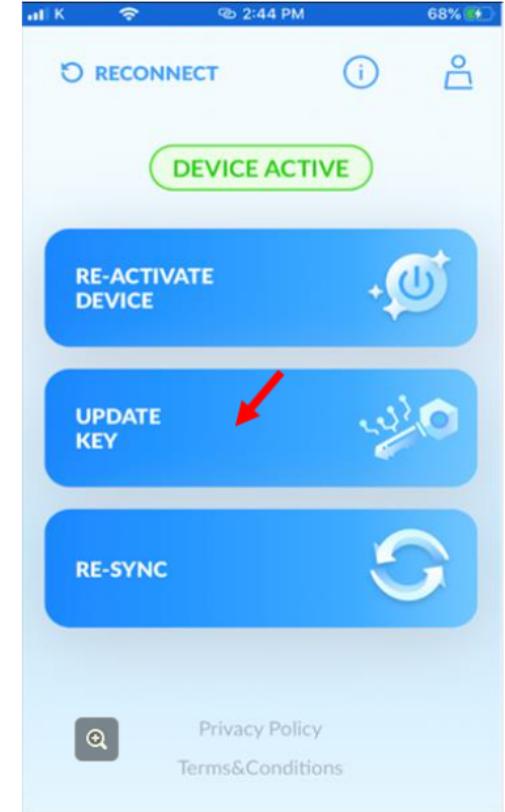


Checking and updating the Device key

- 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

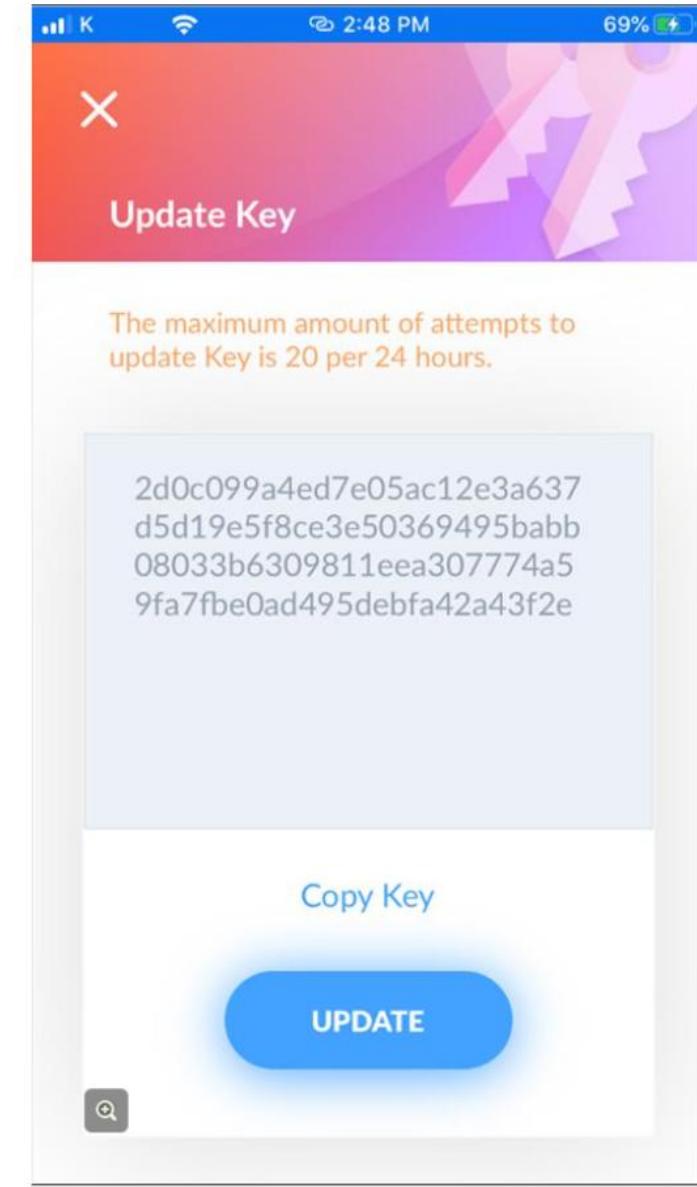


From customer's phone

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.

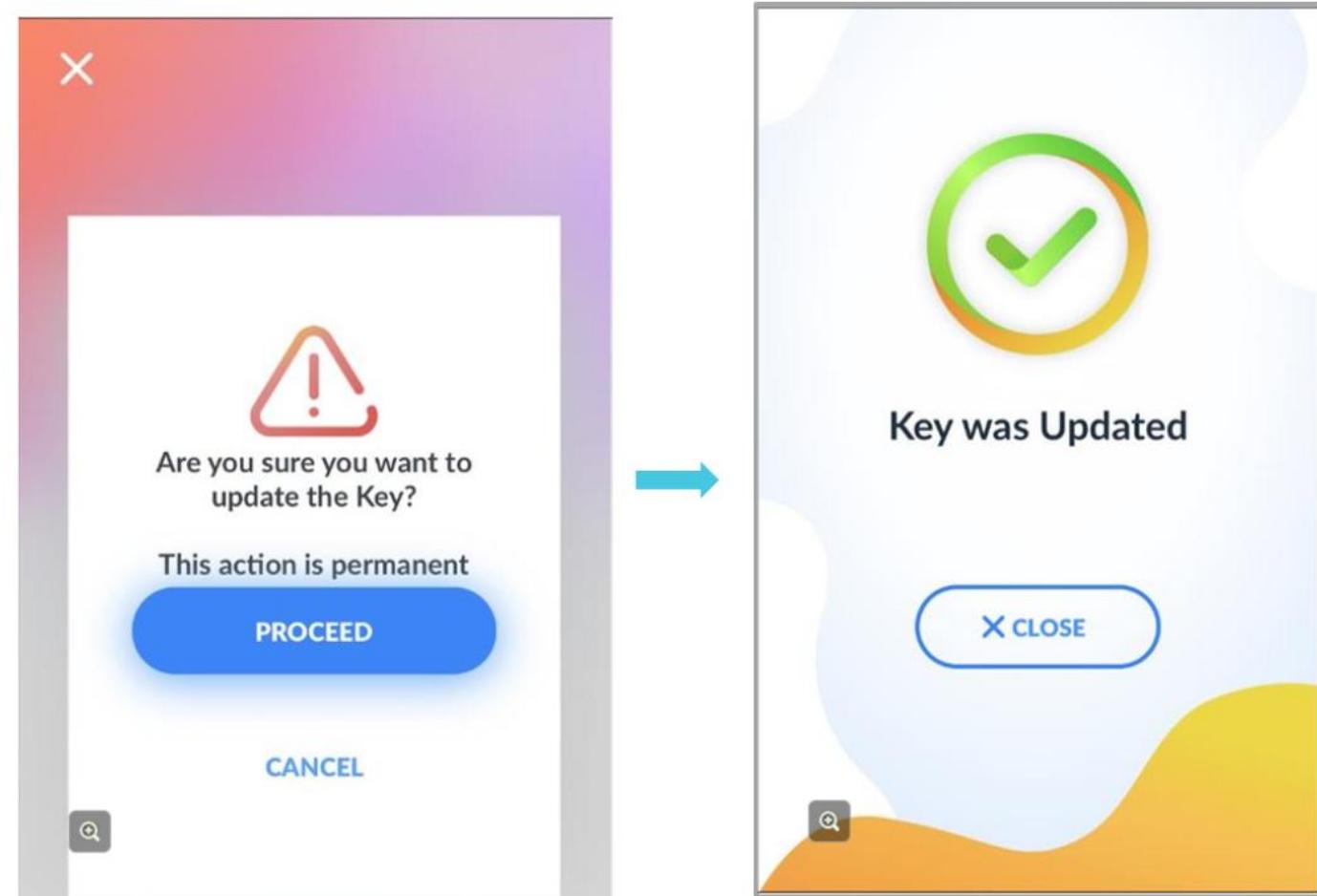
Note: You cannot attempt to update the key more than 20 times every 24 hours.



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). If the SSR does not complete this procedure, the system will be set as Standard even if the customer bought the Security Pack.



Step

