

New SE350 Standard model

Service actions and differences with the original SE350 model

The Lenovo logo is positioned in the top right corner of the slide. It consists of the word "Lenovo" written vertically in white, set against a rectangular background with a vertical color gradient from green at the top to blue at the bottom.

Lenovo

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.

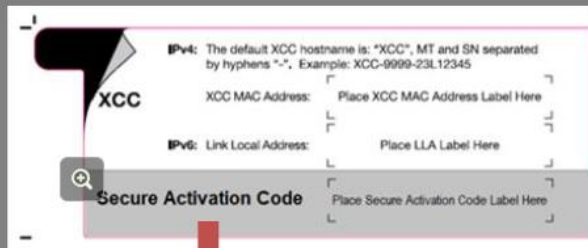
Asset tag and flyer

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.



Lenovo ThinkShield

PN: SP47A58937

ATTENTION: DO NOT THROW AWAY

Note: SE350 with Security Pack is also known simply as SE350 prior to July 2021. You can check whether your system is SE350 with Security Pack or SE350 Standard in Lenovo XClarity Controller.

SE350 with Security Pack

- SE350 automatic data protection, including intrusion sensor and motion sensor, can be enabled.
- 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. Please keep this document for the process.
- Requires activation to boot up and fully functional.

SE350 Standard (Security Pack disabled)

- SE350 automatic data protection, including intrusion sensor and motion sensor, is disabled.
- Data access will be never locked up. SED management is disabled. Tamper setting is disabled.
- No activation is required.
- Claiming the system is optional. Secure Activation Code is needed for claiming.
- Keep this document for future reference.

Secure Activation Code

Server information for activation

Machine Type	
Serial Number	
Secure Activation Code	

Service technician only

New secure activation code after system board replacement	
---	--

- For ThinkSystem SE350 with Security Pack, the Secure Activation Code is used when activating the system or when the system board is replaced.
- For ThinkSystem SE350 Standard, the Secure Activation Code is used when the system board is replaced.

Note: The Secure Activation Code can also be found on the network access tag on the front of the server or using the ThinkShield Edge mobile app.

For mobile App downloads visit:
<https://apps.thinkshield.lenovo.com>

GET IT ON
Google Play

乐商店
App Lenovo.com

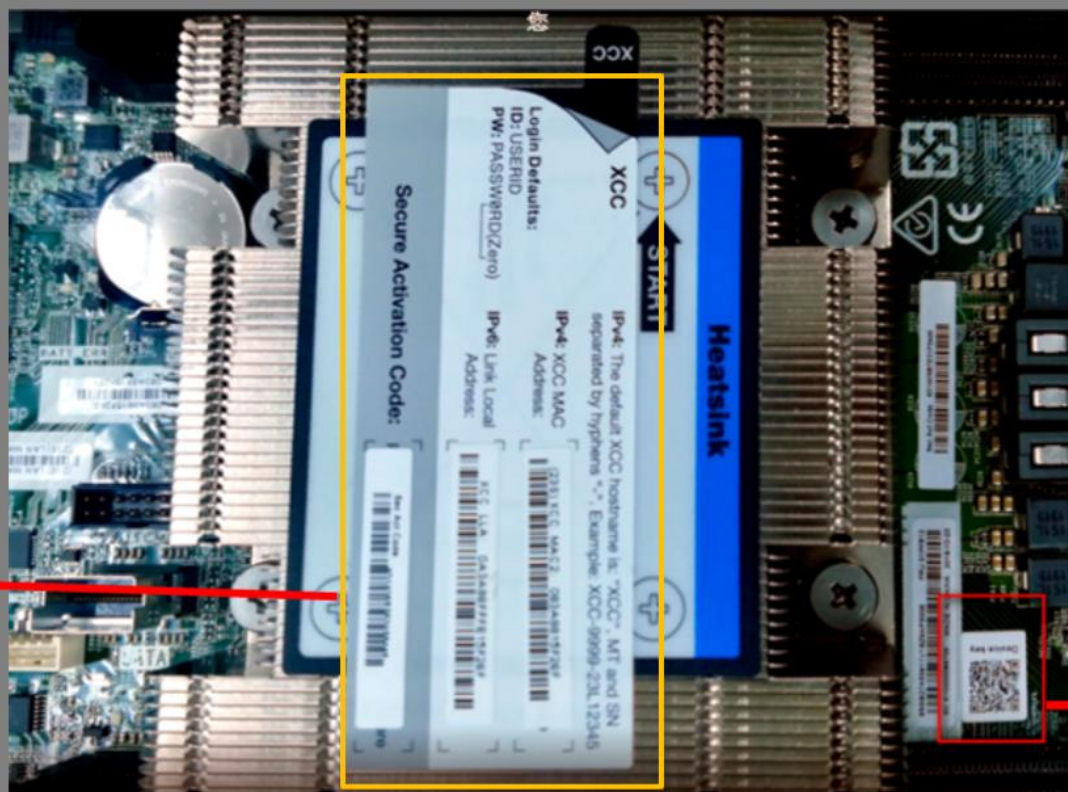
Download on the
App Store

百度手机助手
有 限 公 司



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:

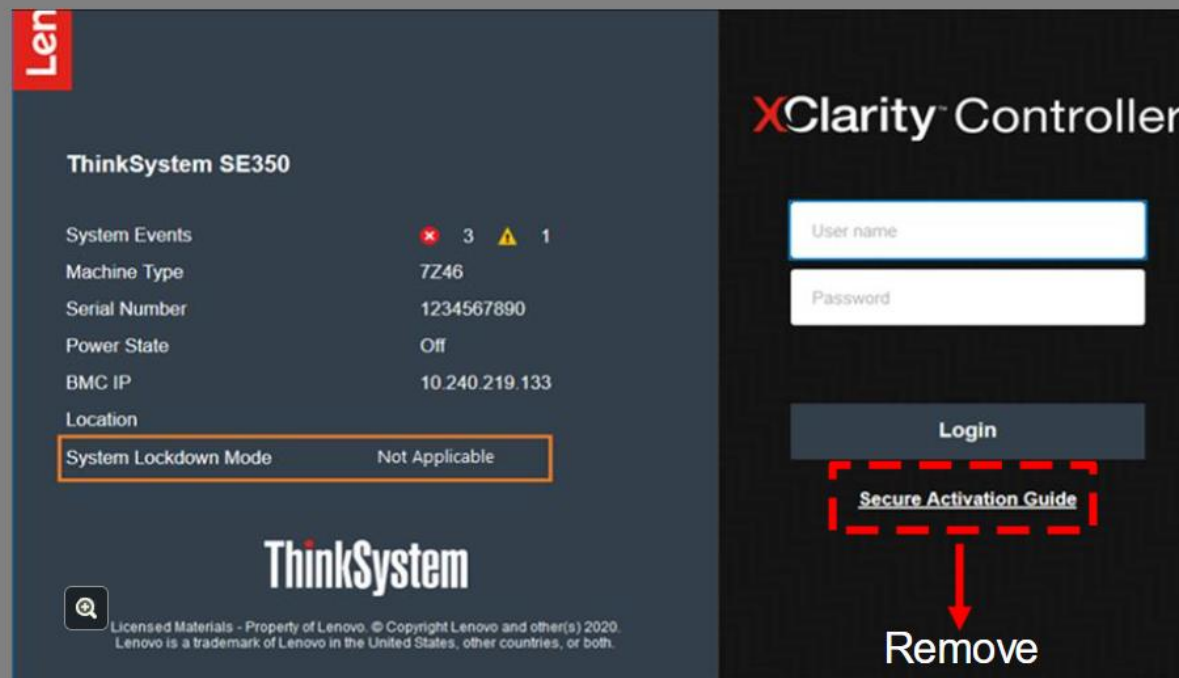
- Login page [Click here](#)
- Home page [Click here](#)
- Lockdown mode configuration [Click here](#)
- SED management [Click here](#)

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

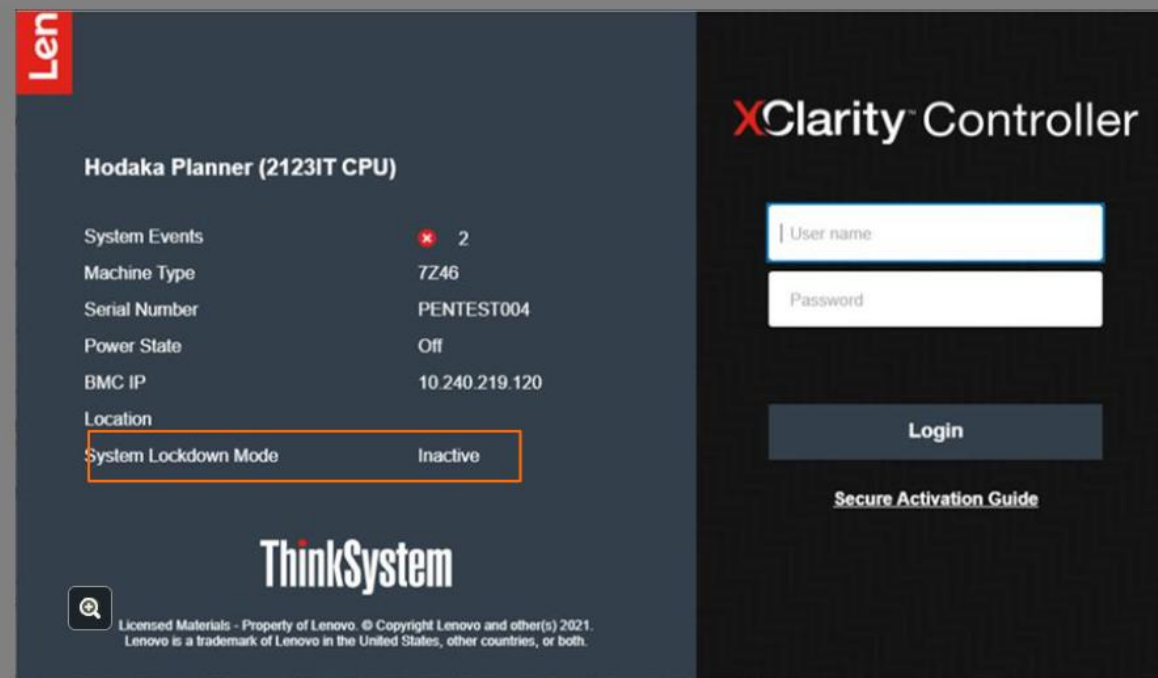
Checking with XCC – Web login page



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



SE350 Standard



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.

The screenshot shows the XClarity Controller Home page for a Standard model. The left sidebar contains navigation links: Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Edge Networking. The main content area is divided into several sections:

- Health Summary:** Displays the status of various components. CPU (1 / 1 installed) and Memory (1 / 4 installed) are green. Local Storage (Not Found) is grey. PCI (2 installed) is green. Fan (Not Found) is grey. System Board (2) is red. Others is green.
- System Information and Settings:** A table of system details. The last three rows are highlighted with a red dashed box: System Lockdown Mode (Inactive), Motion Detection (Disabled), and Chassis Intrusion Detection (Disabled). A red arrow points from the 'Remove' button next to these settings.
- Quick Actions:** Includes Power Action, ID Location LED: Off, and Service.
- Power Utilization:** Shows a bar chart for 33W Output, with CPU at 0W, Memory at 0W, and Others at 33W.
- System Utilization:** Shows four bar charts for CPU, Memory, I/O, and System, all at 0%.

The 'Remove' button is located to the right of the red dashed box, indicating that the highlighted settings can be removed from the interface.

XCC Lockdown Mode configuration



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

The screenshot displays the XClarity Controller interface for the ThinkSystem SE350 Planner. The left sidebar contains navigation links: Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Backup and Restore. The main content area shows the 'System Lockdown Mode' configuration, which is highlighted with a red dashed box. This configuration includes a 'De-asserted' toggle, a warning message about 'Motion Detection' being disabled, and toggles for 'Motion Detection' (Disabled) and 'Chassis Intrusion Detection' (Enabled). Below these are 'Additional Configurations' and 'Apply'/'Cancel' buttons. The 'ThinkShield Key Vault' logo is also visible. To the right, a 'Quick Link' sidebar lists various security features, with 'LOCKDOWN' highlighted. A red arrow points from the 'Remove' button to the 'LOCKDOWN' link in the sidebar.

XClarity Controller

ThinkSystem SE350 Planner ... System name:

Export USERID 3:25 PM

Allow Third-Party Password Retrieval Disabled

System Lockdown Mode De-asserted

! 'Motion Detection' is in disabled state, system now loses the capability to detect motion event and trigger lockdown mode automatically when someone moves system unexpectedly.

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.



Remove

Checking with ThinkShield Key Vault Portal



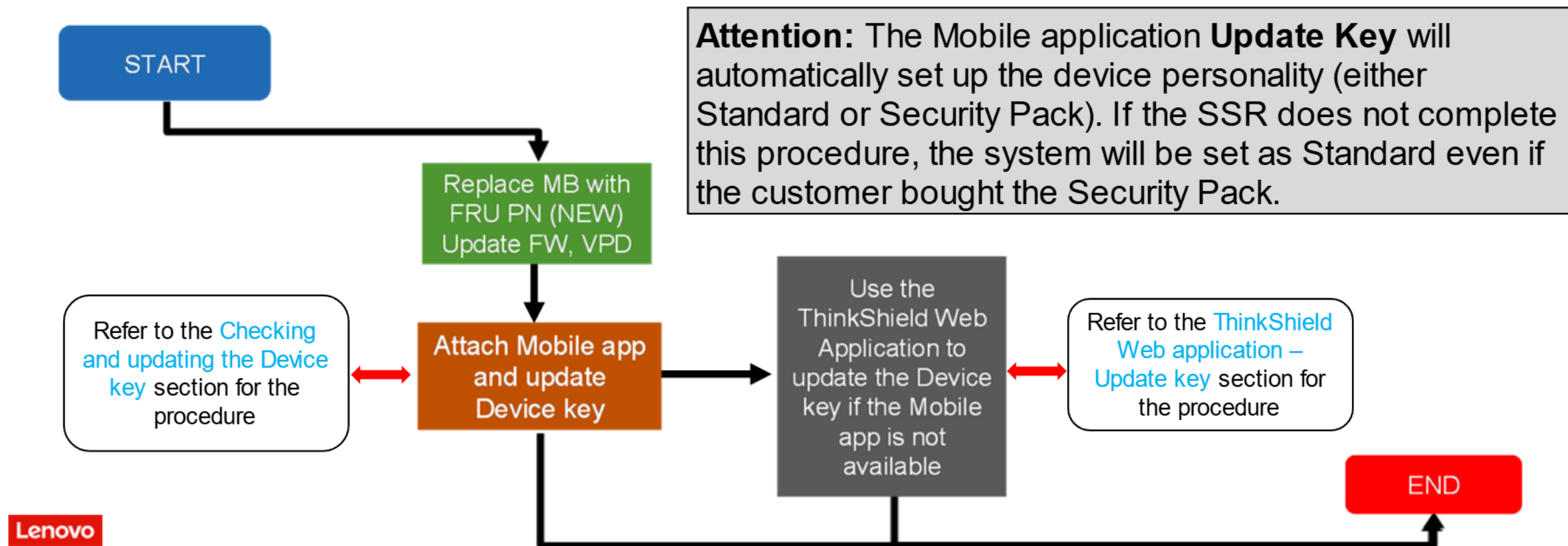
Use the ThinkShield Service Support account to log in to the ThinkShield Portal to check the SE350 device. The **MODE** will be displayed as either **Standard** or **Security Pack**.

The screenshot displays the ThinkShield Key Vault Portal interface. On the left is a dark sidebar with the 'ThinkShield Key Vault Portal' logo and a 'Device Manager' section. The main content area is titled 'Devices' and includes a 'Refresh' button and a search bar. A table lists several devices, with the 'MODE' column highlighted by a red rectangle. The modes shown are 'Security Pack' and 'Standard'. The table columns are: STATUS, MODE, DEVICE NAME, MACHINE TYPE, SERIAL NUMBER, and GROUP.

STATUS	MODE	DEVICE NAME	MACHINE TYPE	SERIAL NUMBER	GROUP
Active	Security Pack	3438...	7D1B	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



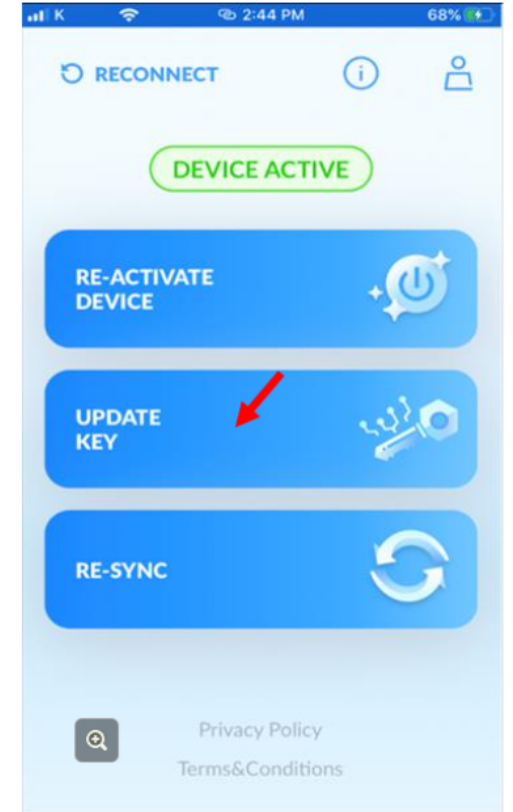
Checking and updating the Device key

- Using the ThinkShield Service Support credentials, log in to the **TSServiceSupport** organization on the ThinkShield Mobile application.
 - If the SSR can't use 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**.

Step **1** — **2** — **3** 



From SSR's phone



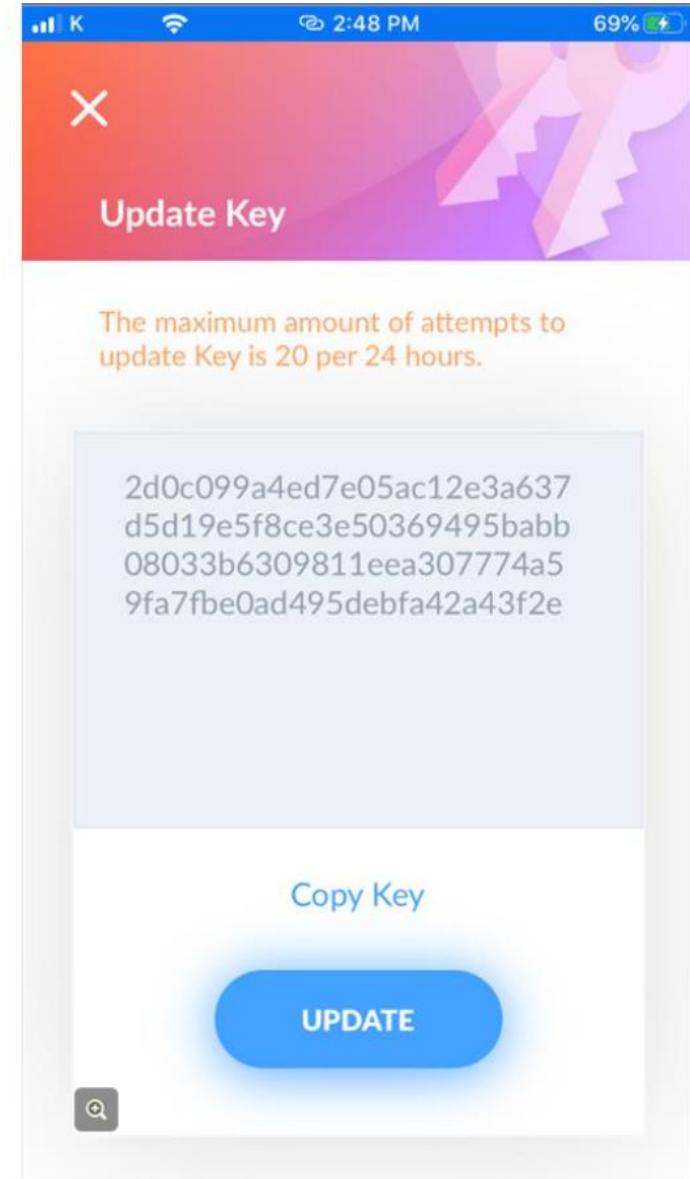
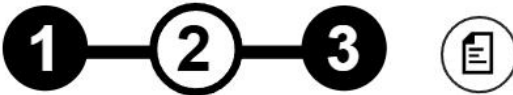
From customer's phone

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.

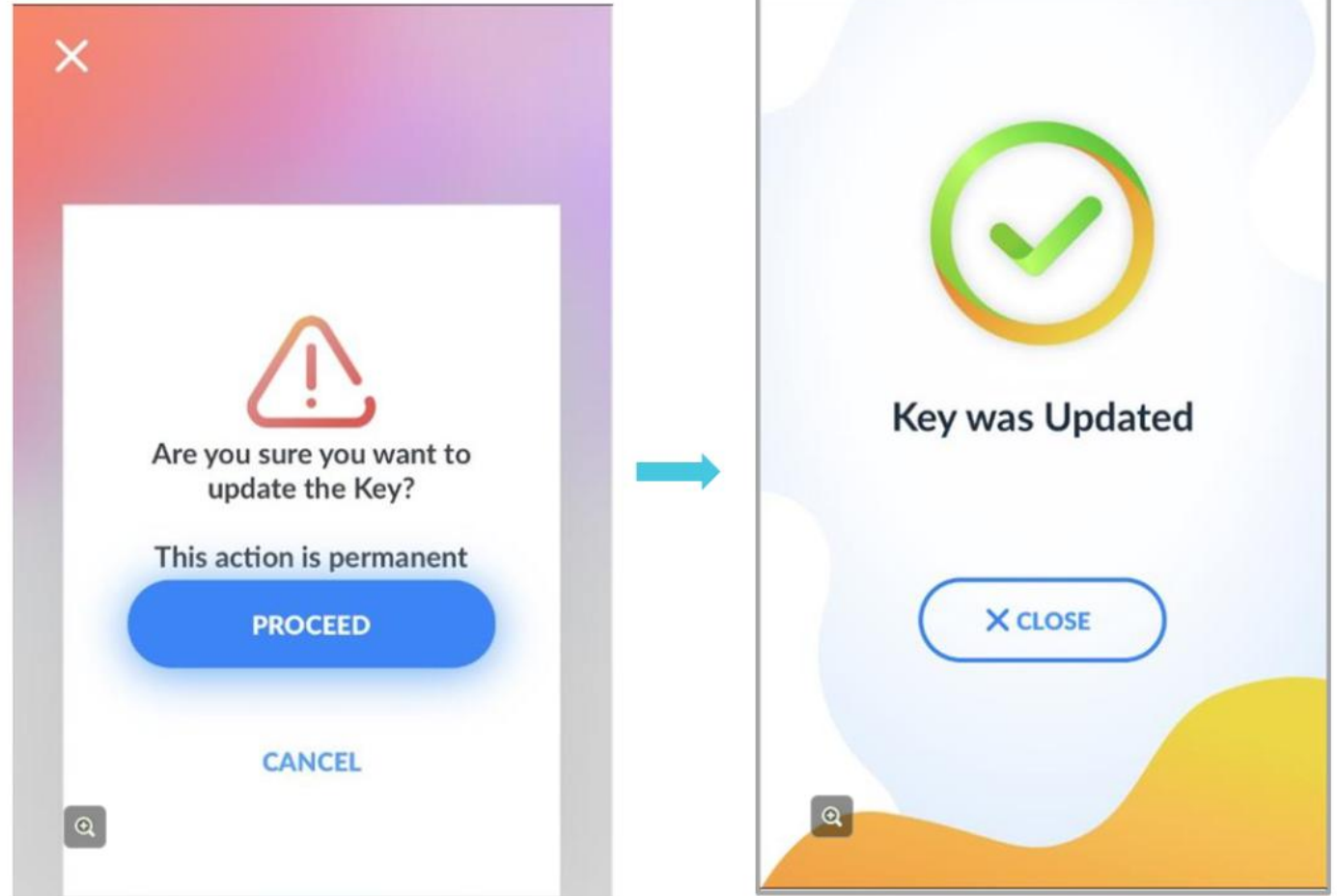
Step



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 **1** — **2** — **3** 