New SE350 Standard model

Service actions and differences with the original SE350 model

Lenovo

SE350 Standard model

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

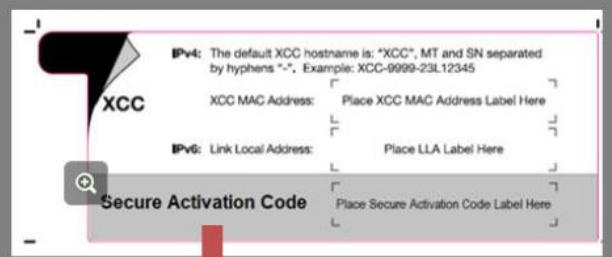
- SE350 with Security Pack
- SE350 Standard

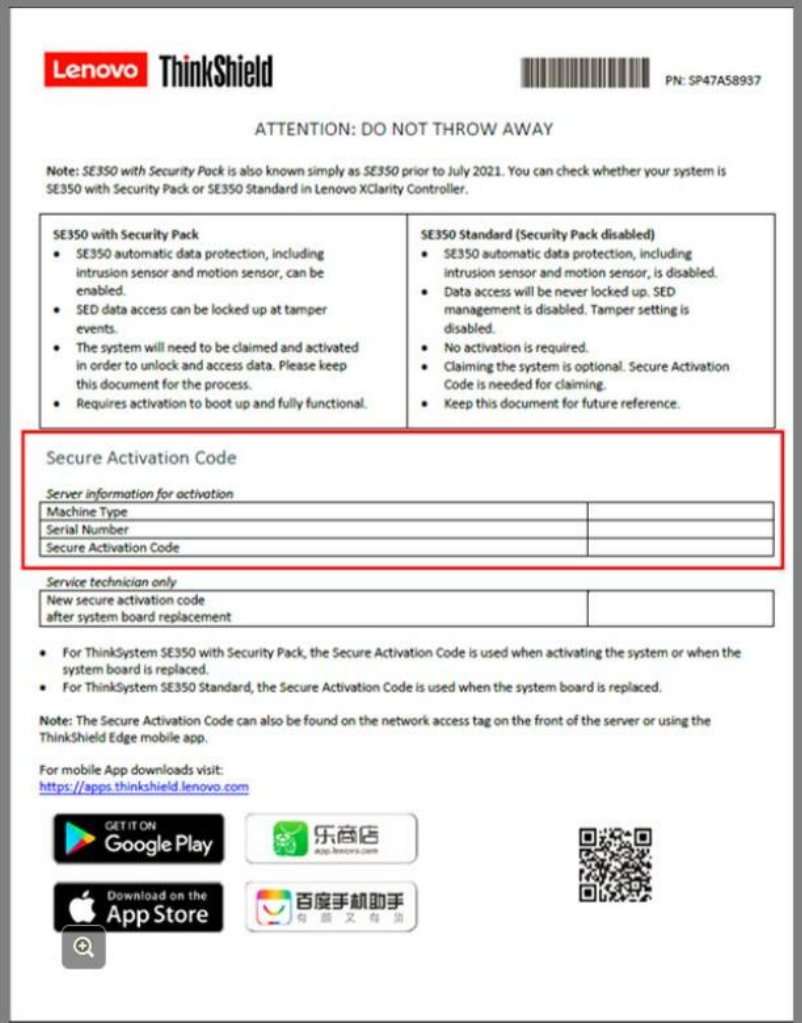
SE350 with Security Pack	SE350 Standard (Security Pack disabled)
• SE350 automatic data protection can be enabled – this includes the intrusion sensor and motion sensor • SED data access can be locked up at tamper events • The system will need to be claimed and activated in order to unlock and access 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	• 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

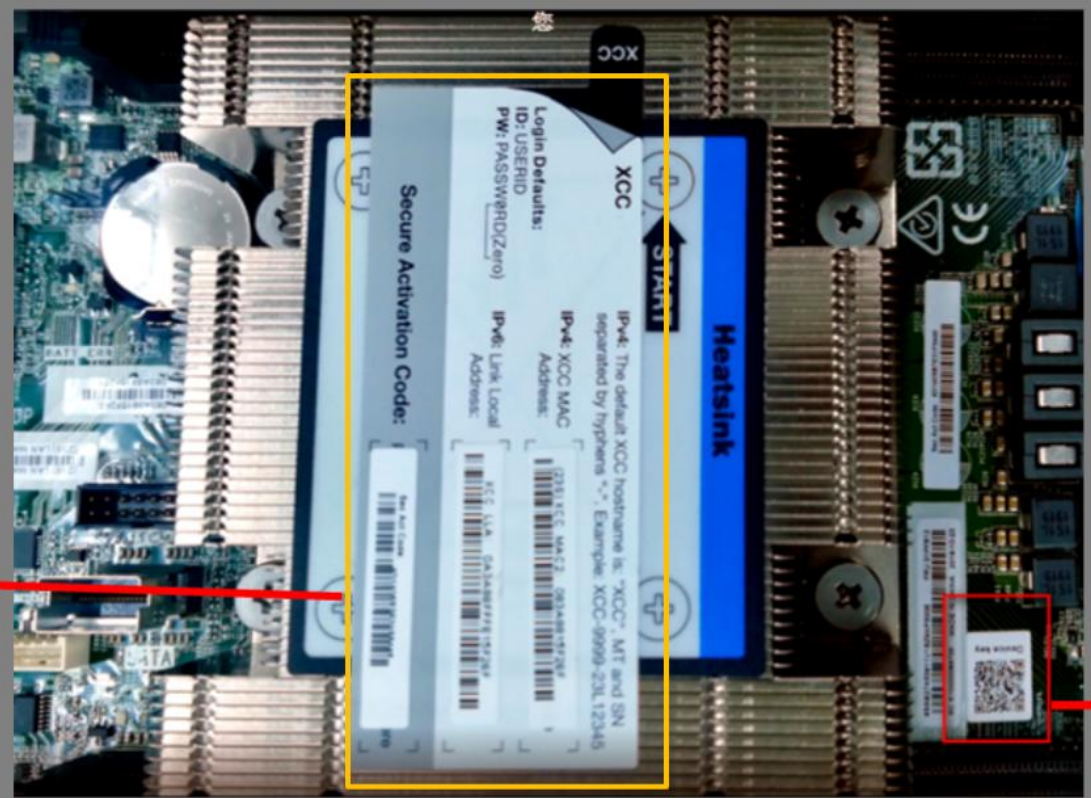
Secure Activation Code on the asset tag and flyer

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.



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.

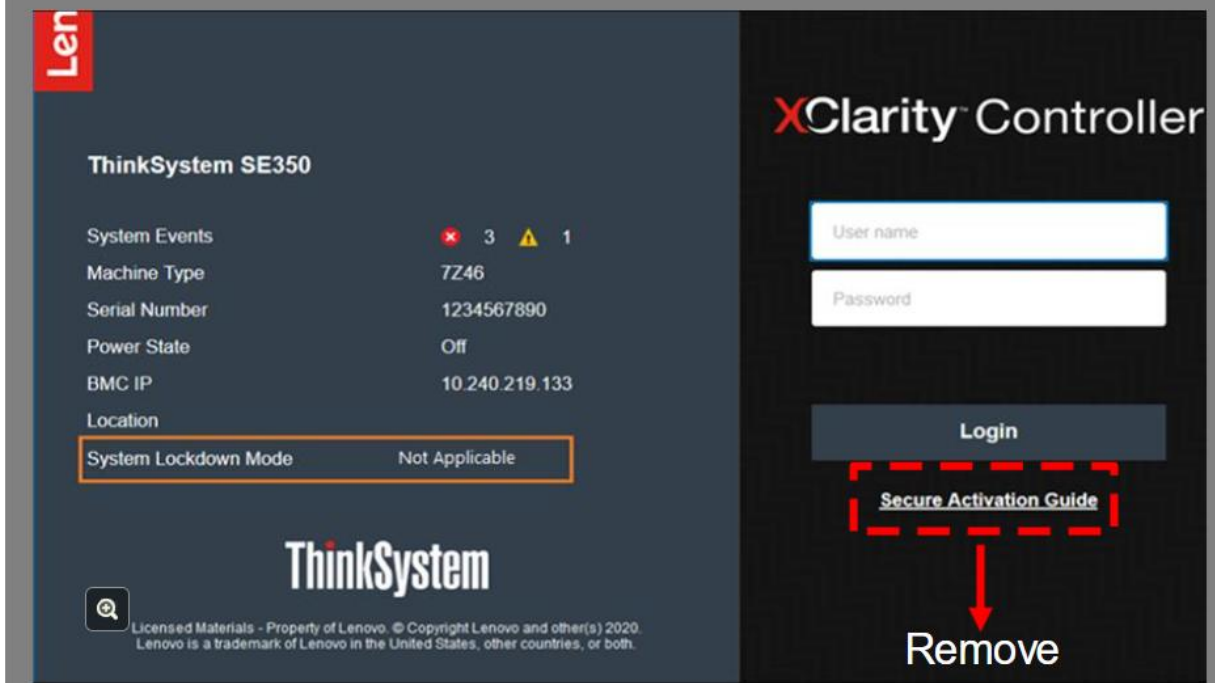
Checking with XCC:

- Login page Click here
- Home page Click here
- Lockdown mode configuration Click here
- SED management Click here

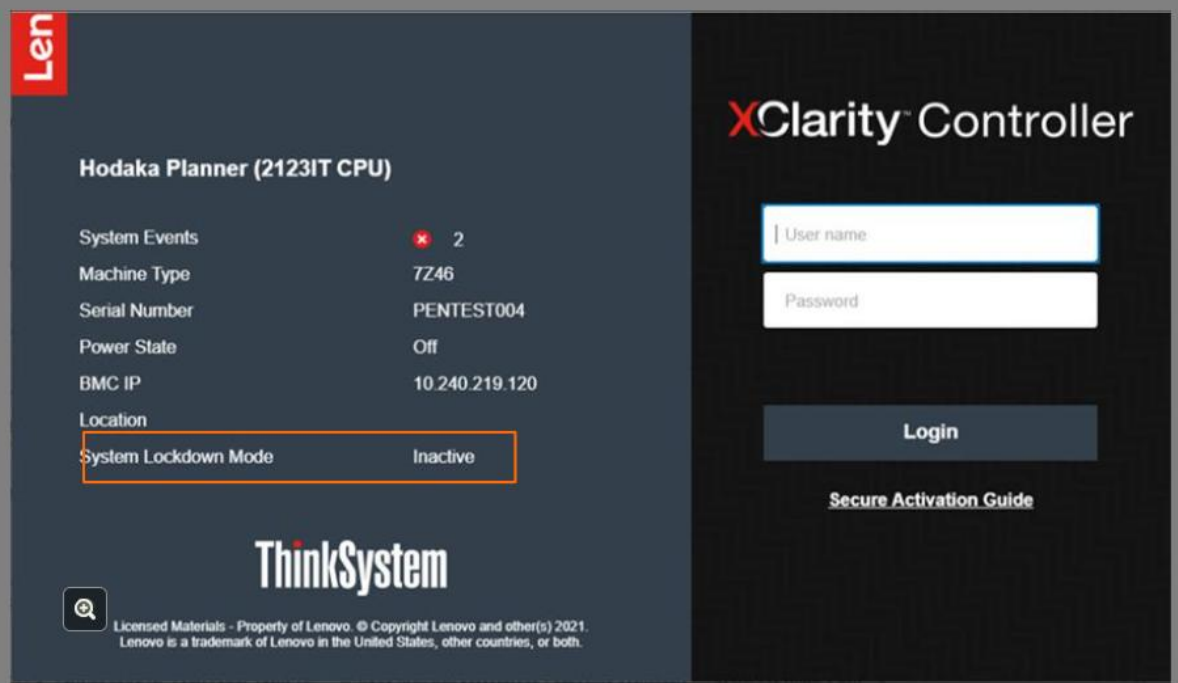
Checking with ThinkShield Key Vault Portal Click here

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.



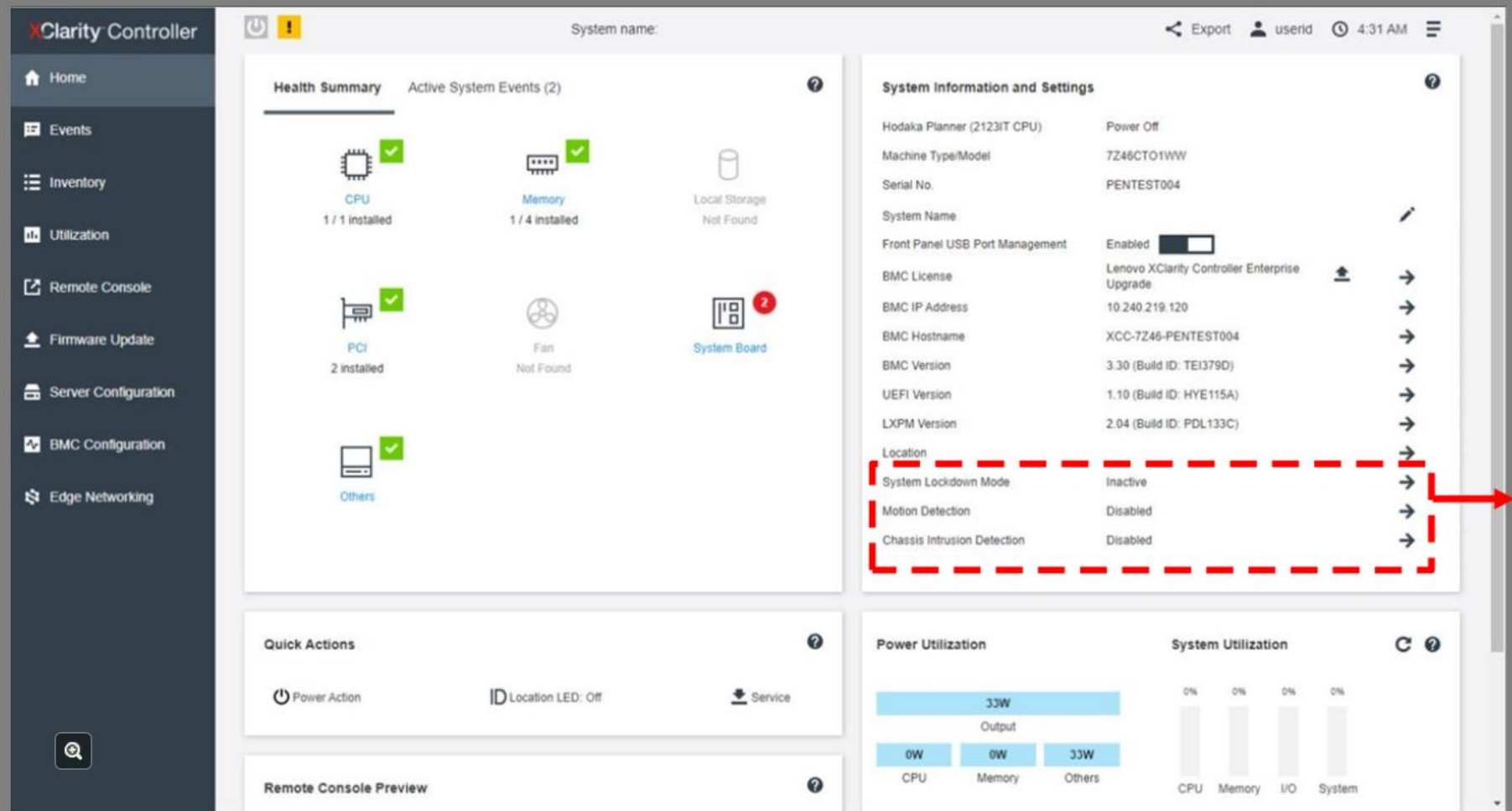
SE350 Standard



SE350 with Security Pack

Checking with XCC – Home page

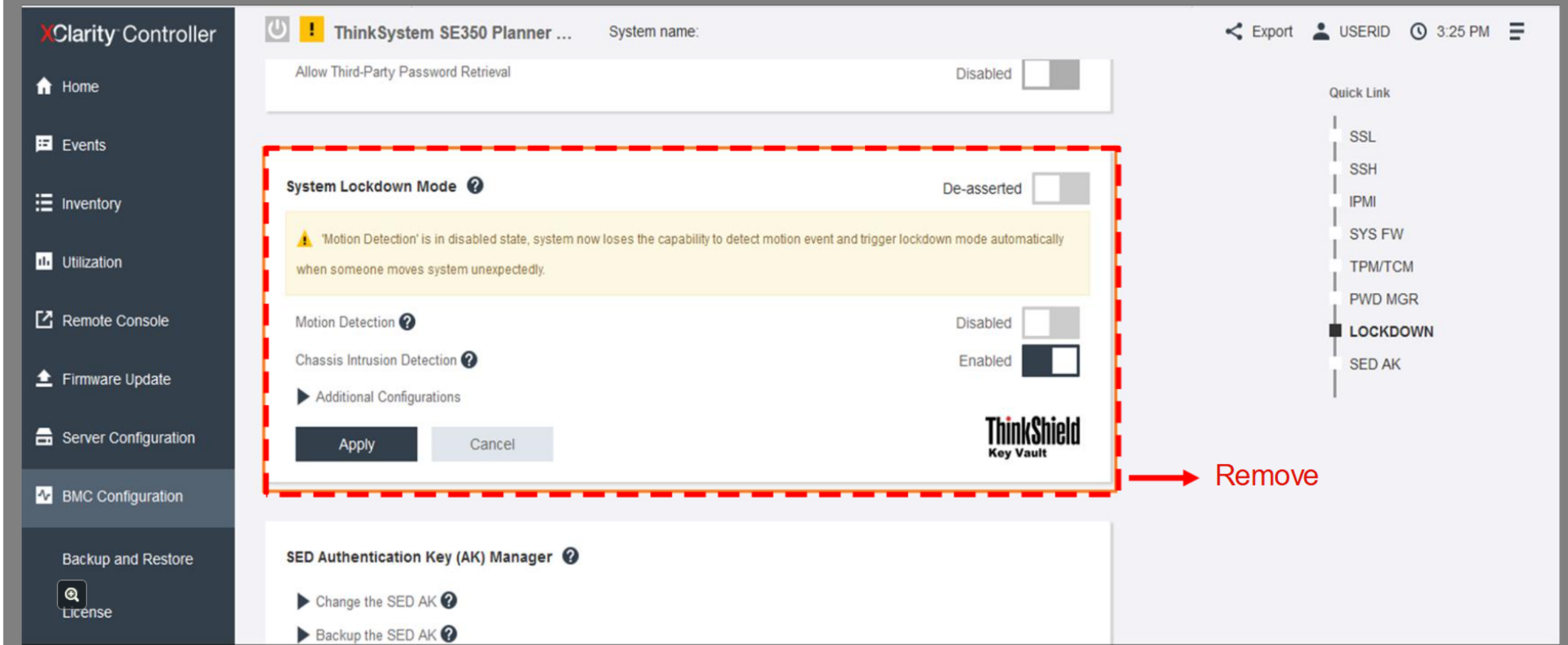
With a Standard model, the **System Lockdown Mode**, **Motion Detection**, and **Intrusion Detection** quick links will be removed.



New SE350 Standard model

XCC Lockdown Mode configuration

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

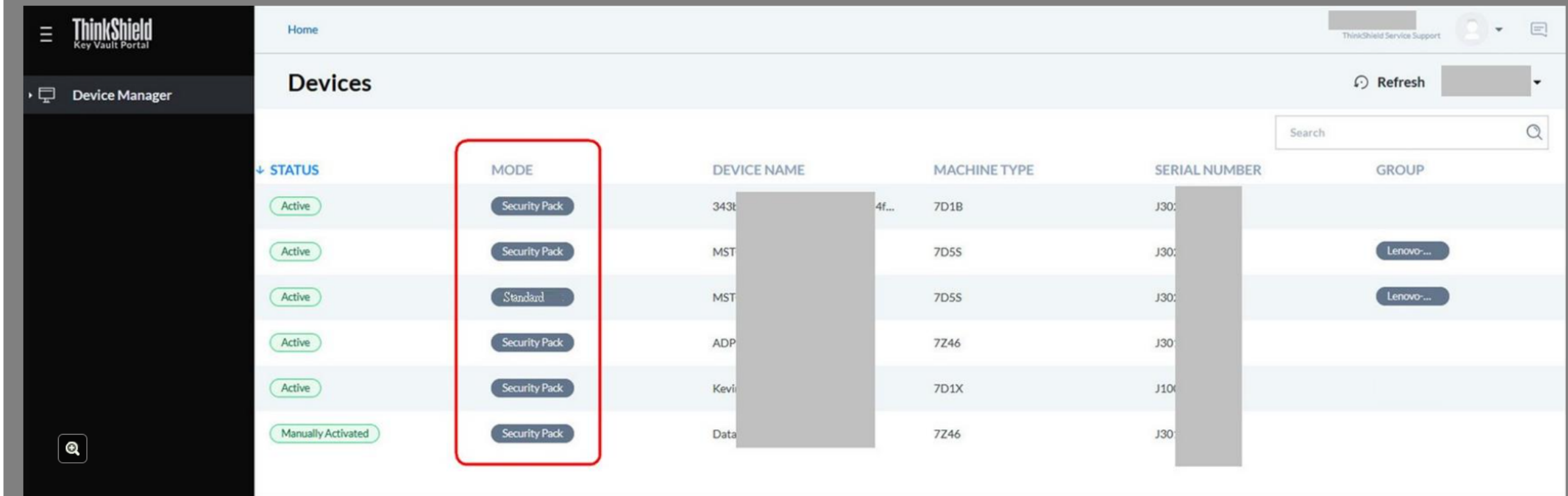


SED key management

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

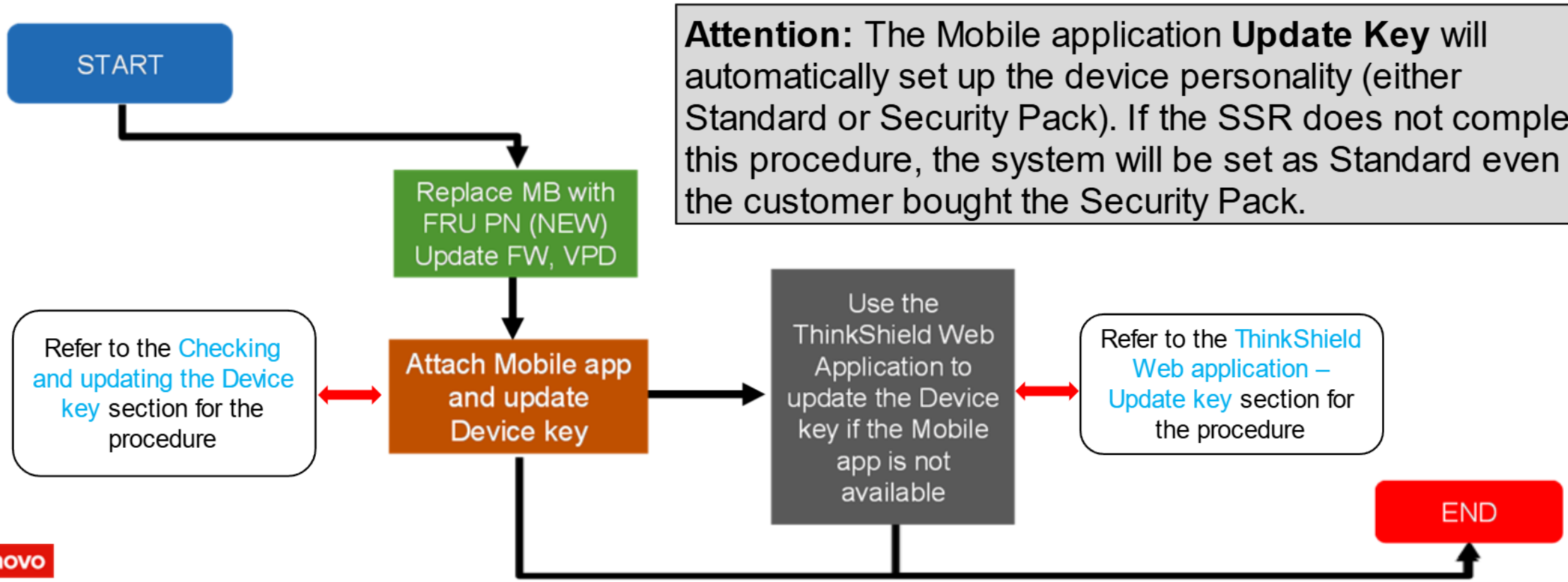
Checking with ThinkShield Key Vault Portal

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**.



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.



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.

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.

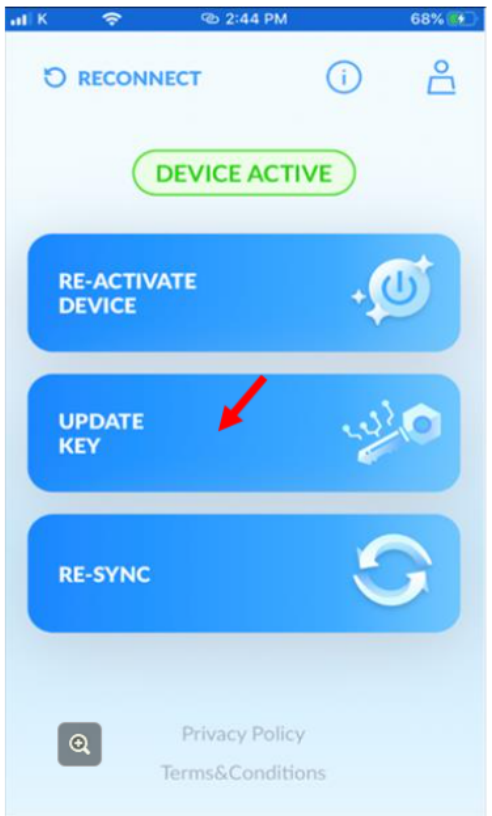
Click each number in turn to see the procedure.

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



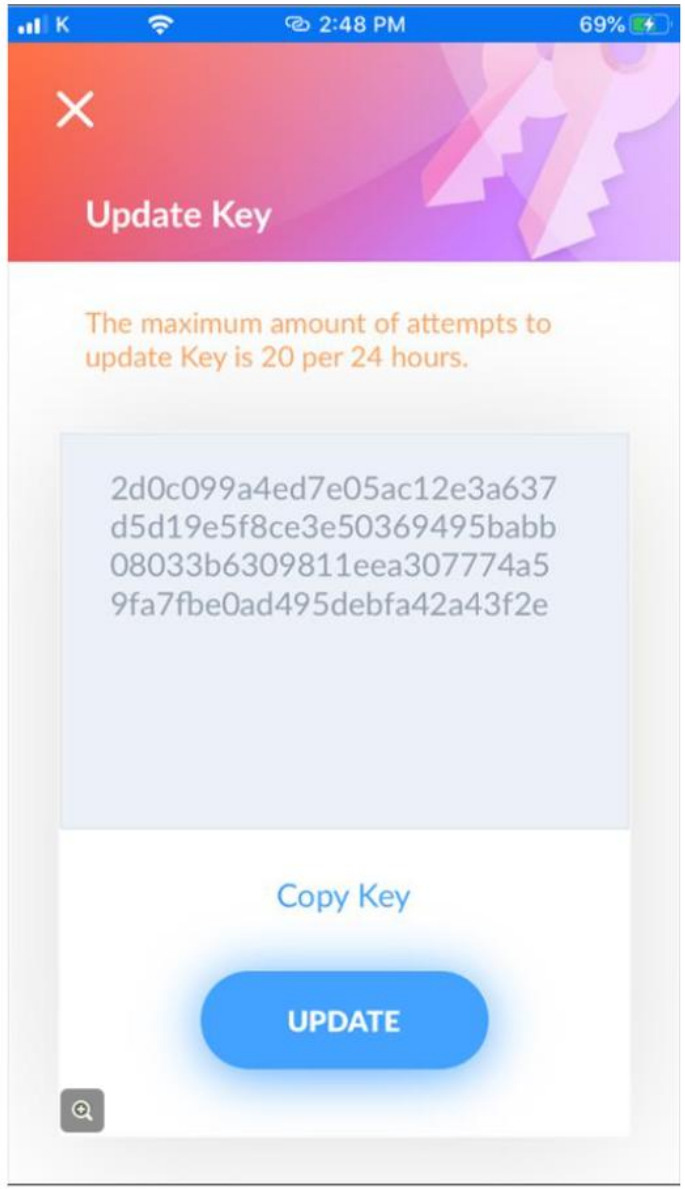
From customer's phone

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.

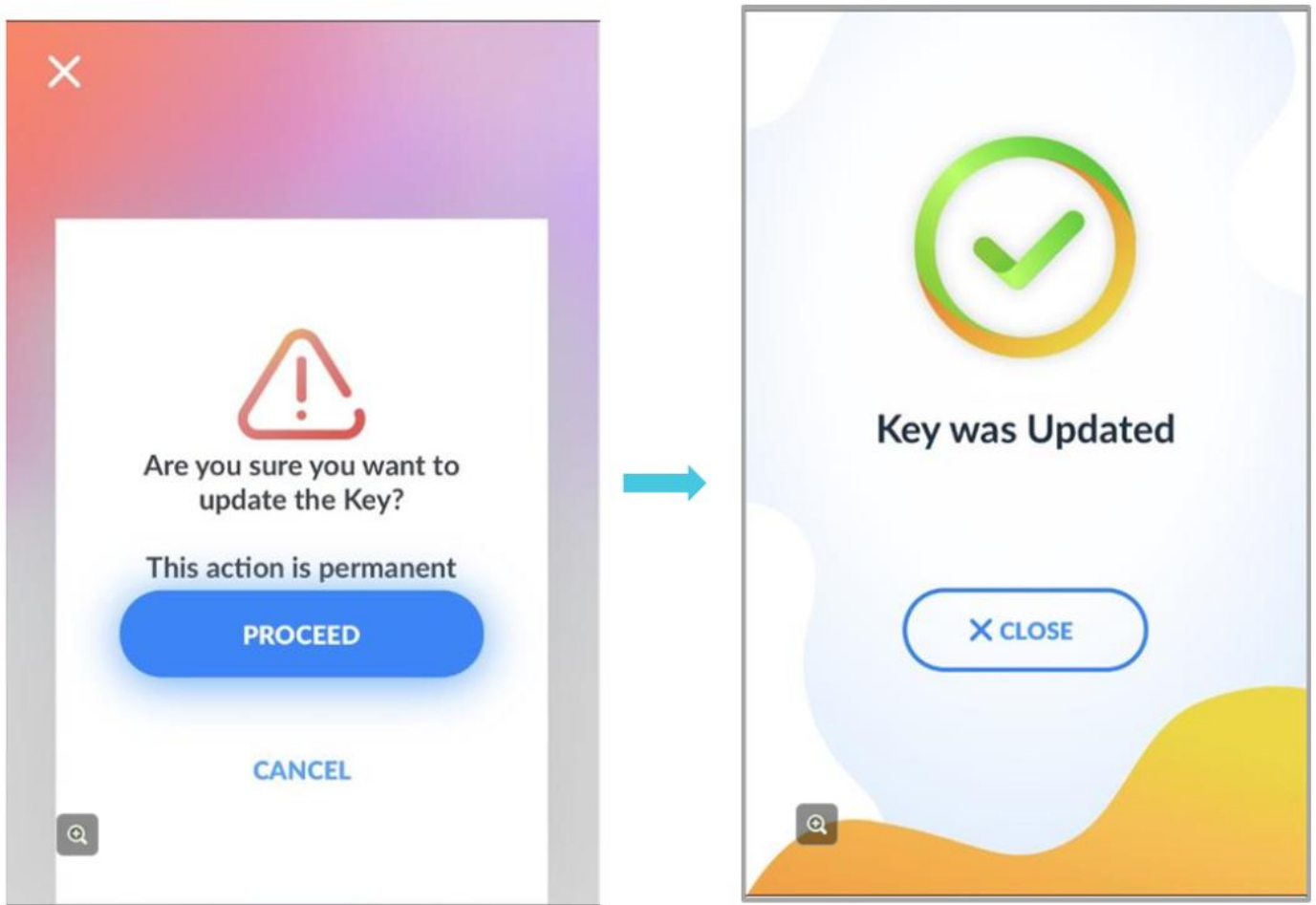


Step 1 2 3

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