

Security features

Security pack, SED AK management

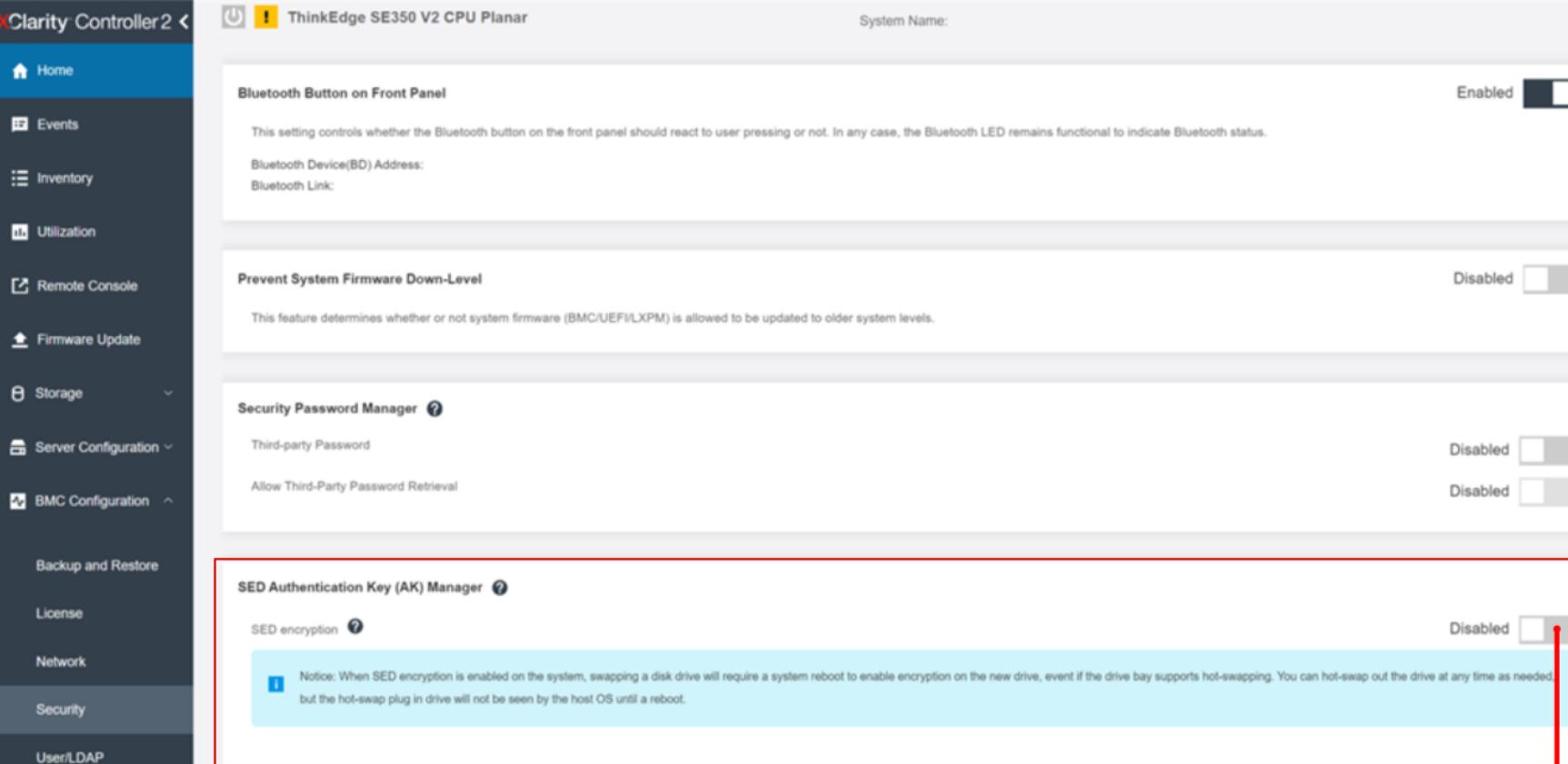
Lenovo

Security pack

- The Security Pack is a collection of security and activation features.
- It allows for the enablement of local self-encrypting (SED) authentication key (AK) management.
- The SE350 V2 and SE360 V2 will only support the security pack disable feature for the initial release.

Features	Initial release
Function set	<ul style="list-style-type: none">- Security pack disabled<ul style="list-style-type: none">• SED AK management based on a passphrase

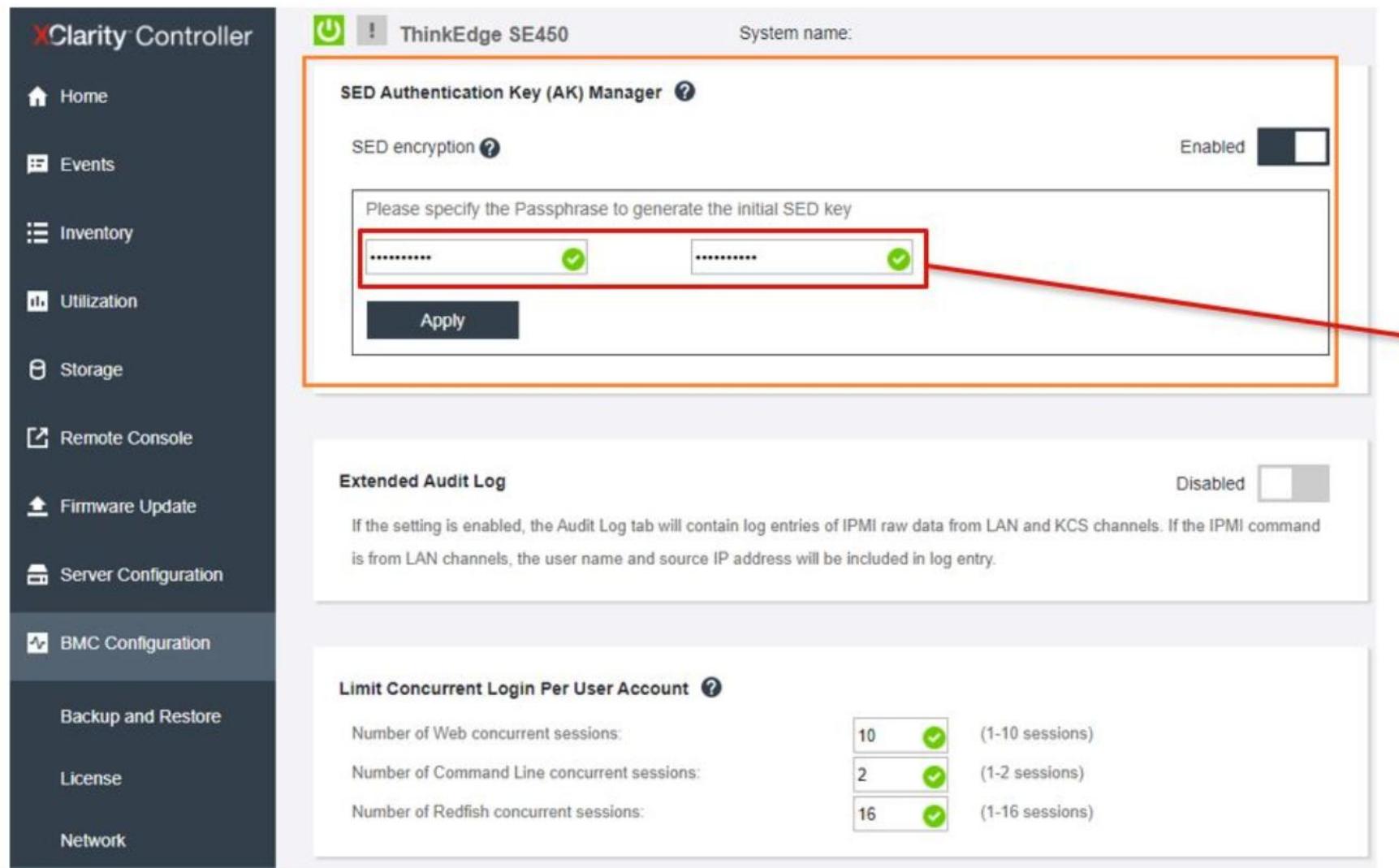
SED AK management – SED encryption disabled



The screenshot shows the XClarity Controller2 interface for a ThinkEdge SE350 V2 CPU Planar system. The left sidebar includes options like Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Storage, Server Configuration, BMC Configuration, Backup and Restore, License, Network, Security, and User/LDAP. The main content area displays several configuration sections: 'Bluetooth Button on Front Panel' (Enabled), 'Prevent System Firmware Down-Level' (Disabled), 'Security Password Manager' (Third-party Password: Disabled, Allow Third-Party Password Retrieval: Disabled), and 'SED Authentication Key (AK) Manager'. The 'SED encryption' setting under the AK Manager is highlighted with a red box and a red arrow pointing to the 'Disabled' status. A note below it states: 'Notice: When SED encryption is enabled on the system, swapping a disk drive will require a system reboot to enable encryption on the new drive, event if the drive bay supports hot-swapping. You can hot-swap out the drive at any time as needed, but the hot-swap plug in drive will not be seen by the host OS until a reboot.'

SED encryption
disabled

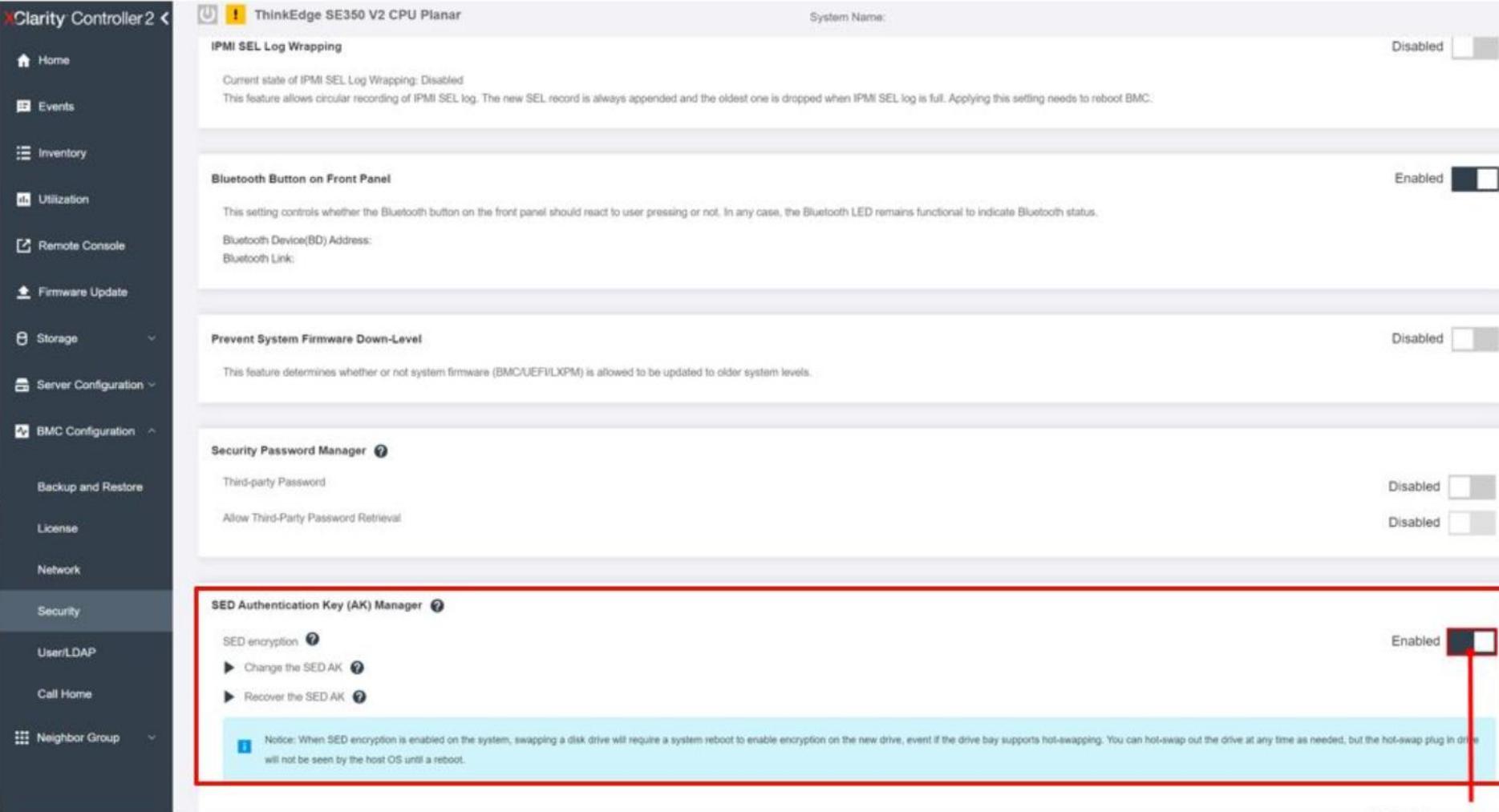
SED AK management – enabling SED encryption



The screenshot shows the BMC Configuration page of the XClarity Controller. The left sidebar lists various configuration tabs, and the main area is titled 'SED Authentication Key (AK) Manager'. It contains a section for 'SED encryption' where two passphrase fields are shown, both marked with a green checkmark. An 'Apply' button is below the fields. To the right of this section, a red box and a red arrow highlight the 'Enabled' toggle switch, which is currently in the 'Off' position. Below this section, there are other configuration options: 'Extended Audit Log' (disabled), and 'Limit Concurrent Login Per User Account' with settings for Web, Command Line, and Redfish concurrent sessions.

The security pack disabled mode supports SED AK management, and it can be activated with a passphrase through BMC Configuration.

SED AK management – SED encryption enabled



The screenshot shows the Clarity Controller 2 interface for a ThinkEdge SE350 V2 CPU Planar. The left sidebar is a navigation menu with the following items: Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Storage, Server Configuration, BMC Configuration, Backup and Restore, License, Network, Security (which is selected and highlighted in blue), User/LDAP, Cell Home, and Neighbor Group.

The main content area displays several configuration sections:

- IPMI SEL Log Wrapping:** Current state is **Disabled** (unchecked).
- Bluetooth Button on Front Panel:** Current state is **Enabled** (checked).
- Prevent System Firmware Down-Level:** Current state is **Disabled** (unchecked).
- Security Password Manager:** Contains two sub-options: "Third-party Password" and "Allow Third-Party Password Retrieval", both of which are **Disabled** (unchecked).
- SED Authentication Key (AK) Manager:** Contains two sub-options: "SED encryption" and "Change the SED AK". "SED encryption" is **Enabled** (checked), and "Change the SED AK" is **Disabled** (unchecked). A callout box below "SED encryption" provides a note: "Notice: When SED encryption is enabled on the system, swapping a disk drive will require a system reboot to enable encryption on the new drive, even if the drive bay supports hot-swapping. You can hot-swap out the drive at any time as needed, but the hot-swap plug-in drive will not be seen by the host OS until a reboot."

SED encryption
enabled

More SED AK management methods are supported when the system is configured to Security Pack mode.

Changing the SED AK

In security pack disabled mode, the passphrase is required when SED AK is changed or recovered.

SED Authentication Key (AK) Management

SED encryption 

Enabled 

▶ Change the SED AK 

▼ Recover the SED AK 

Note that you need to provide the corresponding SED AK passphrase.

Set password 

Confirm password 

Start Restore

SED Authentication Key (AK) Management

SED encryption 

Enabled 

▼ Change the SED AK 

Method: Generate SED AK from Passphrase

Set password 

Confirm password 

Re-generate

▶ Recover the SED AK 