

Security features

ThinkEdge security 2.0, LXCE UpdateXpress

Lenovo

ThinkEdge security 2.0 overview

ThinkEdge security 2.0 introduces a new method for activation.

- An XCC user with administrator privileges can activate the server in lockdown without ThinkShield Portal.

ThinkEdge security 2.0 decouples the security pack from individual security features

- All ThinkEdge servers will be shipped with SED disks.
- SED encryption and security sensors are configurable in XCC.
- If the security sensors are enabled, the system will lock down in the event of tamper detection.

There is no change in portal activation as it is still activated by ThinkShield Portal.

Users can promote the system from local activation to portal activation with LXCE UpdateXpress, but this process is irreversible.

There is an option to ship the system with either local activation or portal activation.

Note: The Security Pack 2.0 portal activation mode will be released in December. System Lockdown Mode in the XClarity Controller is currently available. Refer to the SE455 V3 user guide on [Lenovo Docs](#) to understand the procedure to activate or unlock the system.

ThinkEdge security 2.0 – XCC

The screenshot displays the XCC (XClarity Control Center) interface for ThinkEdge security 2.0. It is divided into two main sections: 'System Lockdown Mode' and 'SED Authentication Key (AK) Management'.

System Lockdown Mode: This section includes a toggle for 'Active' (currently on), a dropdown menu for 'Significant Motion' (highlighted with a red box), and a toggle for 'Enabled' (currently on, also highlighted with a red box). There are also links for 'Motion Detection', 'Chassis Intrusion Detection', and 'Additional Configurations', along with 'Apply' and 'Cancel' buttons.

SED Authentication Key (AK) Management: This section features a toggle for 'SED encryption' (currently on, highlighted with a red box) and a dropdown for 'Generate key using passphrase'. Below this, there is a section for 'Change the SED AK' which includes a dropdown for 'SED AK generation method' (set to 'Generate key using passphrase'), input fields for 'Input passphrase' and 'Confirm passphrase' (both highlighted with red boxes and marked with red 'x' icons), and a 'Re-generate' button. At the bottom, there are links for 'Backup the SED AK' and 'Recover the SED AK', and a blue informational banner.

— If system lockdown control is managed by XCC, users can activate the server by toggling this option. No interaction is required with ThinkShield Portal.

— When security sensors are enabled, the ThinkEdge server will lock down in the event of tamper detection.

— Enabling SED Encryption is an irreversible action. The user cannot disable SED encryption after it is enabled.

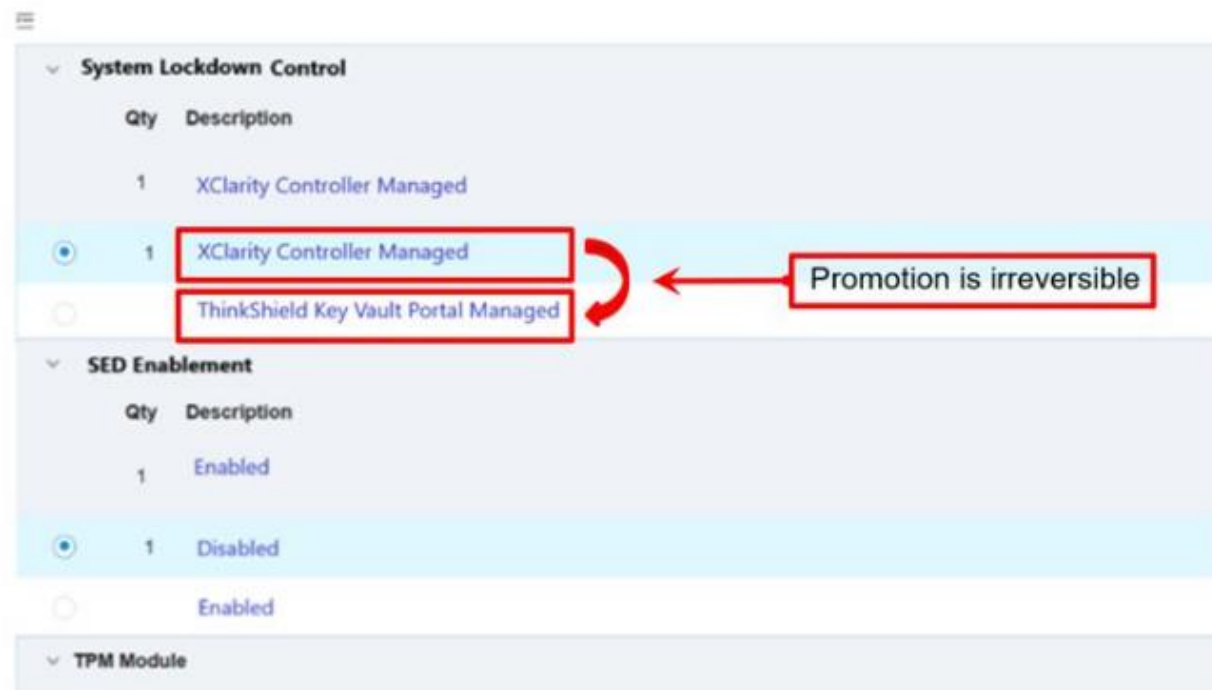
— Users can select either passphrase or random generation as the SED AK generation method.

LXCE UpdateXpress – system lockdown control

With ThinkEdge servers, LXCE UpdateXpress can be used to promote the system lockdown control from **XClarity Controller Managed** to **ThinkShield Key Vault Portal Managed**.

This promotion is irreversible, and users will not be able to demote the system lockdown control in the future.

LXCE will communicate with the portal to update the system lockdown control mode.



LXCE UpdateXpress – server security features

LXCE UpdateXpress can be used to perform the following tasks:

- Promote system lockdown controls for a ThinkEdge server from XCC-managed to ThinkShield Portal-managed
- Claim ThinkEdge servers in ThinkShield Portal
- Server activation
- Configure security sensors
- Manage SED encryption and AK

