

# Wave 2 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.

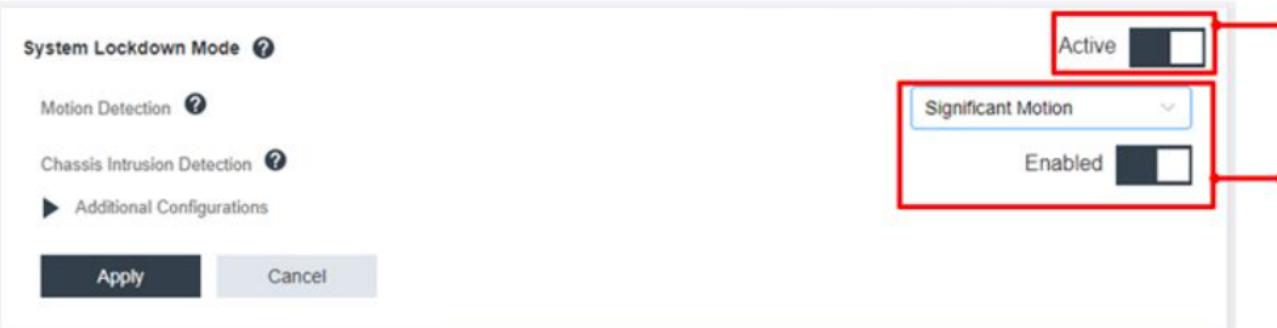
There is no change in portal activation, as it is still activated by ThinkShield Portal.

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 2023. System Lockdown Mode in XCC is currently available. Refer to the SE455 V3 user guide on [Lenovo Docs](#) to understand the procedure used to activate or unlock the system.

# ThinkEdge security 2.0 – XCC



System Lockdown Mode

Motion Detection

Chassis Intrusion Detection

Additional Configurations

Active

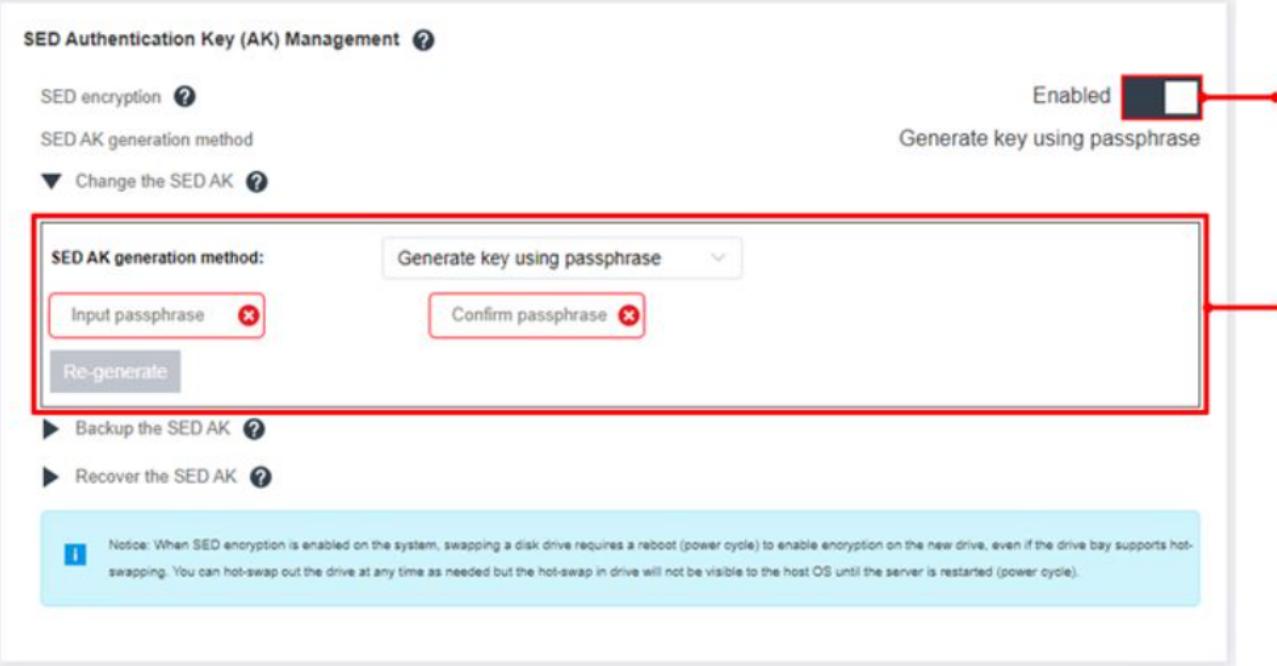
Significant Motion

Enabled

Apply Cancel

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.



SED Authentication Key (AK) Management

SED encryption

SED AK generation method

▼ Change the SED AK

Enabled

Generate key using passphrase

SED AK generation method:

Input passphrase

Confirm passphrase

Re-generate

Backup the SED AK

Recover the SED AK

Notice: When SED encryption is enabled on the system, swapping a disk drive requires a reboot (power cycle) 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 in drive will not be visible to the host OS until the server is restarted (power cycle).

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

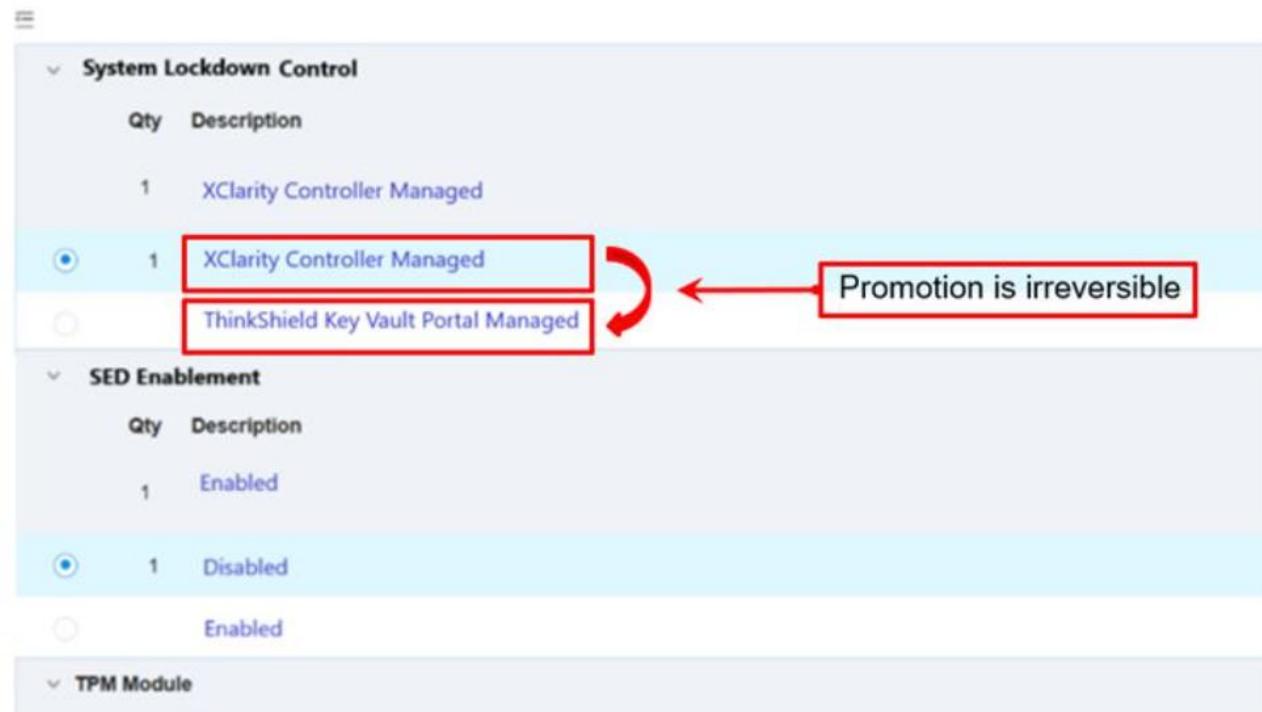
Users can select either passphrase or random generation as the SED AK generation method.

# 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

Lenovo XClarity Essentials UpdateXpress undefined

Active Machine Type: 7DA9

1. Welcome

2. Target Server

3. Task

4. Configure Security Features

5. System Lockdown Control

6. Finish

ThinkEdge Server Security Feature  
Select the tasks that you are interested in.

You can select more than one task. And they will be proceed in displayed order.

► ThinkEdge server security feature introduction

Claim server in ThinkShield portal [?]  
Claim server's ownership in ThinkShield Key Vault Portal.

Configure Security Sensors [?]  
Configure security sensors for tamper detection.

Manage the SED authentication key [?]  
Change/Backup/Recover the SED authentication key.

System Lockdown Control [?]  
Promote system lockdown control from XClarity Controller managed to ThinkShield portal managed.



## Field service action – system board replacement

The technician is required to update the public key after a system board replacement.

Refer to the following sections in course [ES71911C Servicing the ThinkSystem SE350 edge server](#):

- Updating the device key
- System board replacement flow

Refer to the following Lenovo Docs documents for system board replacement procedures:

- [SE350 V2 procedure for replacing the system board](#)
- [SE360 V2 procedure for replacing the system board](#)