

ThinkEdge Security

Planning / Implementation

Lenovo ThinkEdge Servers are a family of servers specifically designed to be used as compute endpoints at the edges of your network. They are designed to operate outside of a traditional data center, often in rugged environments. Central to the design is security, to ensure that customer data is secure even in less-controlled environments.



Figure 1. Lenovo ThinkEdge securely connects users to data at the Edge

The key focus of ThinkEdge security is data protection. There are many potential threats to data that are unique to edge environments. The threats include cases of attackers stealing entire ThinkEdge servers with storage media due to the servers' relatively compact design and their deployment outside of data centers.

In order to protect the data, ThinkEdge servers use Self-Encrypting Drive (SED) technology which encrypts all customer data automatically. There is a key (the SED Authentication Key, or AK for short) which controls access to SED. The ThinkEdge servers carefully protect the SED AK by storing it inside a secure element. The ThinkEdge servers only allow access to the SED AK after the system is properly authorized. Once the system is authorized, the SED AK unlocks the drive and allows the system and data to be accessed. When the ThinkEdge servers detect a tamper event, it locks access to the SED AK until the system is authorized again. If an attacker steals the SED media, since it is encrypted, the attacker cannot read the content.

In addition, the selected ThinkEdge servers contain sensors that further protect customer data against threats after the server is installed at its final location. If these sensors detect that the device is being tampered with, the ThinkEdge server locks the device so that the data becomes inaccessible.

Firmware versions

This Lenovo Press document describes the enhanced security features that are supported by all ThinkEdge servers with the XCC2 (XClarity Controller 2) service processor with firmware versions listed in the table below.

For ThinkEdge servers with firmware older than the versions listed, or for the ThinkSystem SE350 (any firmware version), refer the Lenovo Press document [ThinkEdge Security for SE350](#).

Table 1. Minimum firmware levels for enhanced security features

Server model	Firmware for enhanced security features
ThinkSystem SE350	No support for enhanced security features; Refer to document ThinkEdge Security for SE350 .
ThinkEdge SE450	USX381A or later
ThinkEdge SE350 V2	IYX321N or later
ThinkEdge SE360 V2	IYX321N or later
ThinkEdge SE455 V3	All firmware versions support enhanced security features
ThinkEdge SE100	All firmware versions support enhanced security features

Minimum firmware levels for the [Emergency XCC password reset](#) feature are listed in the following table.

Table 2. Minimum firmware levels for Emergency XCC password reset

Server model	Firmware for Emergency XCC password reset
ThinkSystem SE350	No support for Emergency XCC password reset; Refer to document ThinkEdge Security for SE350 .
ThinkEdge SE450	USX369B or later
ThinkEdge SE350 V2	IYX333C or later
ThinkEdge SE360 V2	IYX333C or later
ThinkEdge SE455 V3	MBX315C or later
ThinkEdge SE100	All firmware versions support enhanced security features

Data protection and SED key management

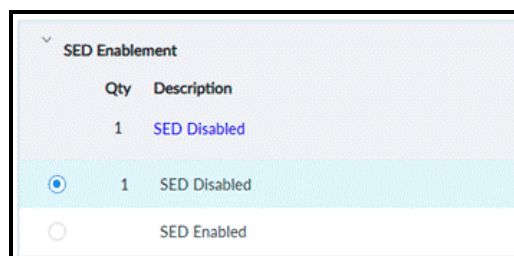
ThinkEdge servers support self-encrypting drives (SEDs) for local storage. SED provides benefits by encrypting data on-the-fly at the drive level with no performance impact, by providing instant secure erasure thereby making the data no longer readable, and by enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use. These features are essential for many businesses, especially those storing sensitive customer data.

The SED Authentication Key (SED AK) is unique to each SED drive. The SED AK controls access to the data on the SED.

There is established technology to manage the SED AK by a key management server, such as Thales KeySecure. However, ThinkEdge servers need to operate and access the SED regardless of network availability while typical end point device server cannot access SED when end point server cannot access key management server over network. ThinkEdge servers also need to control the SED access when hardware detects tamper event.

In order to support such unique requirements of ThinkEdge servers, ThinkEdge server manages SED AK locally. Each ThinkEdge server has hardware secure element, and the SED AK is stored in the secure element,

However, some customers may like to use a key management server or may not require a SED. In order to support both cases, ThinkEdge servers support “SED Enablement” as an option. Customer can select SED enablement from DCSC at ordering as below.

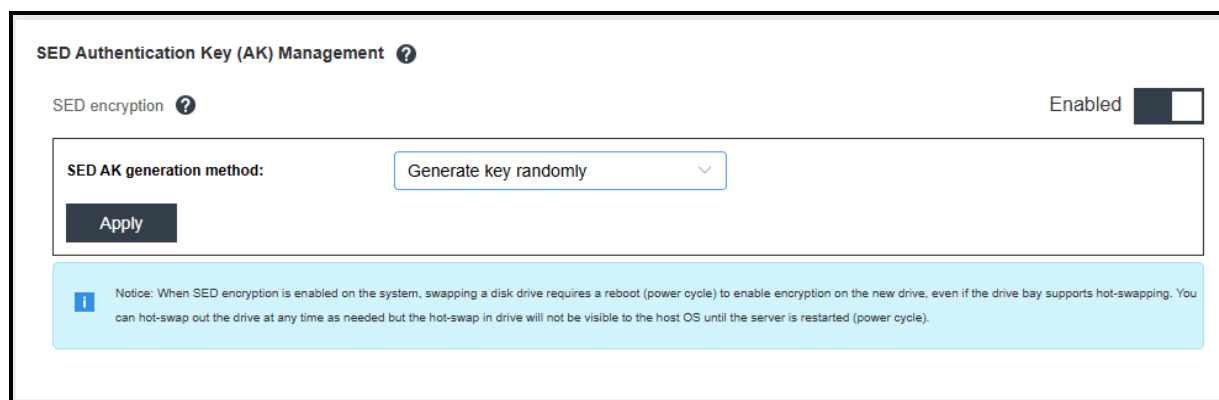


The screenshot shows a configuration window titled "SED Enablement". It contains a table with two columns: "Qty" and "Description". The table has two rows: the first row shows "1" in the Qty column and "SED Disabled" in the Description column; the second row shows "1" in the Qty column and "SED Enabled" in the Description column. The second row is highlighted with a blue background. To the left of the table, there are two radio buttons: the top one is selected (filled with blue) and corresponds to the "SED Disabled" row, while the bottom one is unselected (empty) and corresponds to the "SED Enabled" row.

Qty	Description
1	SED Disabled
1	SED Enabled

Figure 2. SED Enablement

A customer can also enable SED from XCC as shown below, however, once enabled, SED cannot be disabled.



The screenshot shows the "SED Authentication Key (AK) Management" interface. At the top, there is a title bar with a question mark icon. Below the title bar, there is a section labeled "SED encryption" with a question mark icon. To the right of this section is a toggle switch labeled "Enabled", which is currently turned on. Below the toggle switch is a form with a label "SED AK generation method:" and a dropdown menu showing "Generate key randomly". Below the dropdown menu is an "Apply" button. At the bottom of the interface, there is a light blue notification box with an information icon and text: "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)."

Figure 3. SED AK Management

Device ownership

Ownership is one of the most important concepts to review when discussing security. Devices must protect the data when handled by someone with unauthorized access, however, the owner of the device should be able to manage the device with ease. Similarly, devices must protect data when attackers (with unauthorized access) reach the device, whereas the owner (with authorized access), should be able to manage and access the device with ease.

In the case of edge computing, there are differences from servers located in a data center. The IT administrator tends to work in an IT office, far from devices at an edge location. For the edge, devices may be directly shipped to the edge location. In the case of a data center, a single IT administrator will receive hundreds of devices at a single data center, but in the case of edge computing, on-site personnel will receive 1 or 2 devices at hundreds of separate locations. How do we know who the rightful owner of each edge device is?

Defining Device Ownership

The ThinkEdge server owner defines who is able to claim ownership of the server initially and who is able to activate the server initially and, in the event, it is locked down due to a tamper. A major consideration for determining who should own the device is the location of the where the device is being managed from. If the device is being managed from where it is located then the owner is local and if the device is being managed from a remote location, then the device owner is remote.

ThinkEdge servers support XClarity Controller management when device owners are local and ThinkShield Key Vault Portal management when device owners are remote.

XClarity Controller management allows a XCC user with the proper privileges to claim and activate the device. All that is needed is access to the XCC. Special consideration is needed to properly protect the XCC credentials and account when this method is selected.

ThinkShield Key Vault Portal management first requires the Organization to be registered in the ThinkShield Key Vault then it requires the organization's administrator to claim and activate the device using the portal initially. Anytime the device needs to be reactivated a user with a properly privileged portal account must be authenticated to activate the device using any of the supported methods.

Other things to consider when selecting between XClarity Controller management and ThinkShield Key Vault Management is the physical security of the device. If a device is in an insecure location for example and could possibly be stolen or tampered with ThinkShield Key Vault management is a better choice because of the separation of the authentication method required to activate the server and the physical server itself. For example, if a server in an insecure location is stolen and locked down the person who stole the server would not be able to activate the server since they would not have an account in the ThinkShield Key Vault Portal. If XClarity Controller management was selected the person who stole the server may be able to gain access to the XCC account and activate the server and gain access to the data on the device.

ThinkEdge servers support the above two methods to define the ownership of servers and who can manage System Lockdown Control. The first method is called XClarity Controller Managed, and the other method is called ThinkShield Key Vault Portal Managed. Customers can preselect the ownership when ordering their ThinkEdge server as shown below.

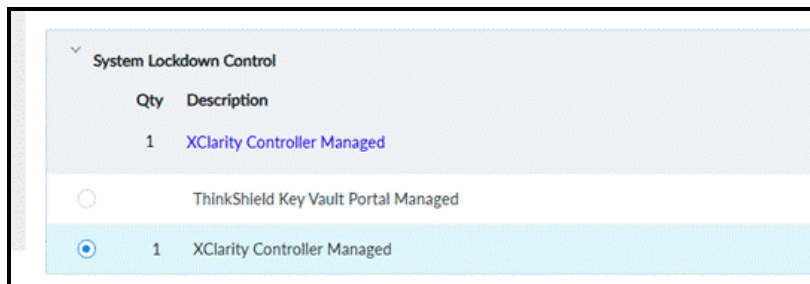


Figure 4. System Lockdown Control

Security Considerations for System Lockdown Control

Security considerations for the following situations:

- [Using XCC for System Lockdown Control](#)
- [Using ThinkShield Key Vault Portal for System Lockdown Control](#)

Using XCC for System Lockdown Control

When XCC-based Lockdown Control is selected, the XCC password becomes particularly important to protect your data in ThinkEdge servers. For example, while ThinkEdge servers can lock down data access when hardware detects tamper event, if you know the XCC password, you can unlock hardware to access the data.

ThinkEdge servers support hardware factory reset by UEFI by selecting **BMC Settings > Reset Factory Defaults Setting** as shown in the following figures.

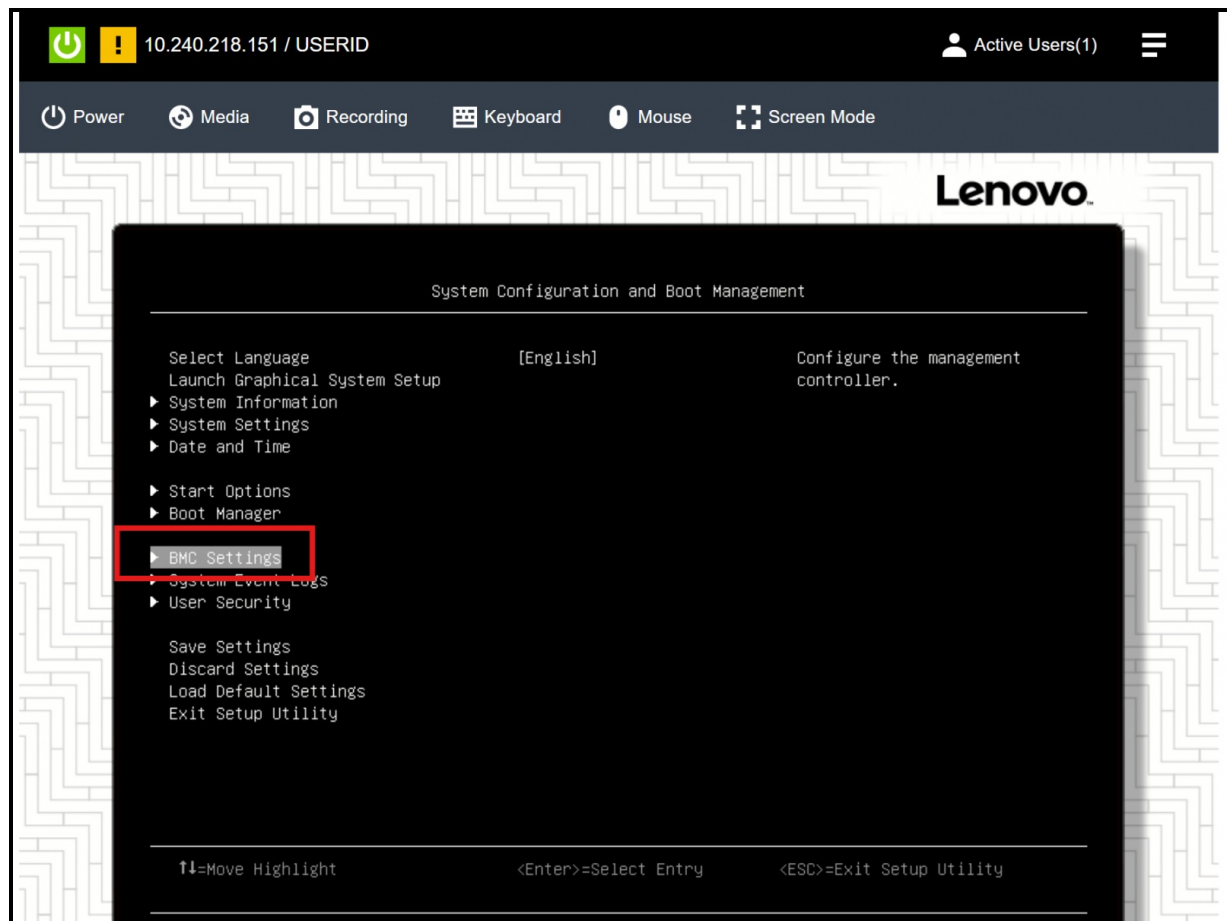


Figure 5. UEFI - System Configuration

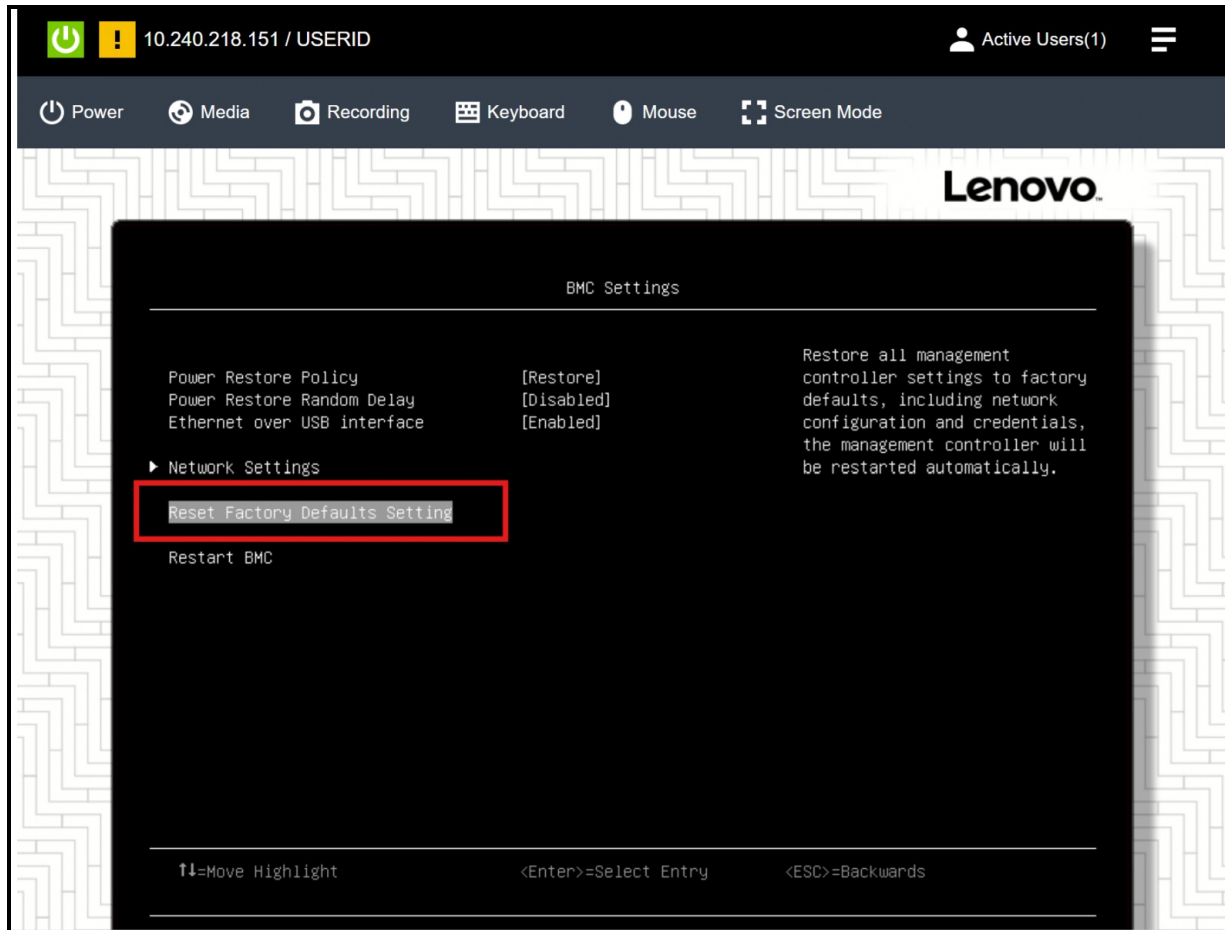


Figure 6. Reset Factory Defaults

It is very important to understand that once you perform factory reset, it will also reset XCC password then anyone can access the protected data in ThinkEdge servers (XCC can also support factory reset but this feature requires to know XCC password, however, factory reset by UEFI does not require XCC password). In order to prevent from anyone to run the UEFI password reset, it is highly recommended to assign UEFI password. Then, without knowing the UEFI password, nobody can reset XCC password by factory reset.

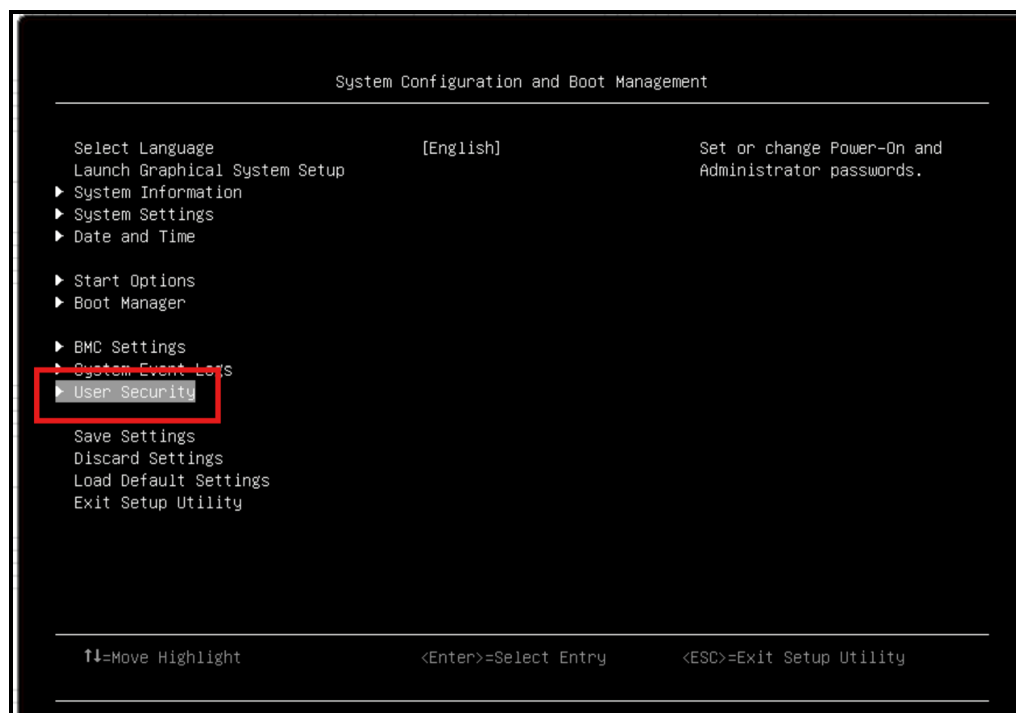


Figure 7. UEFI - System Configuration

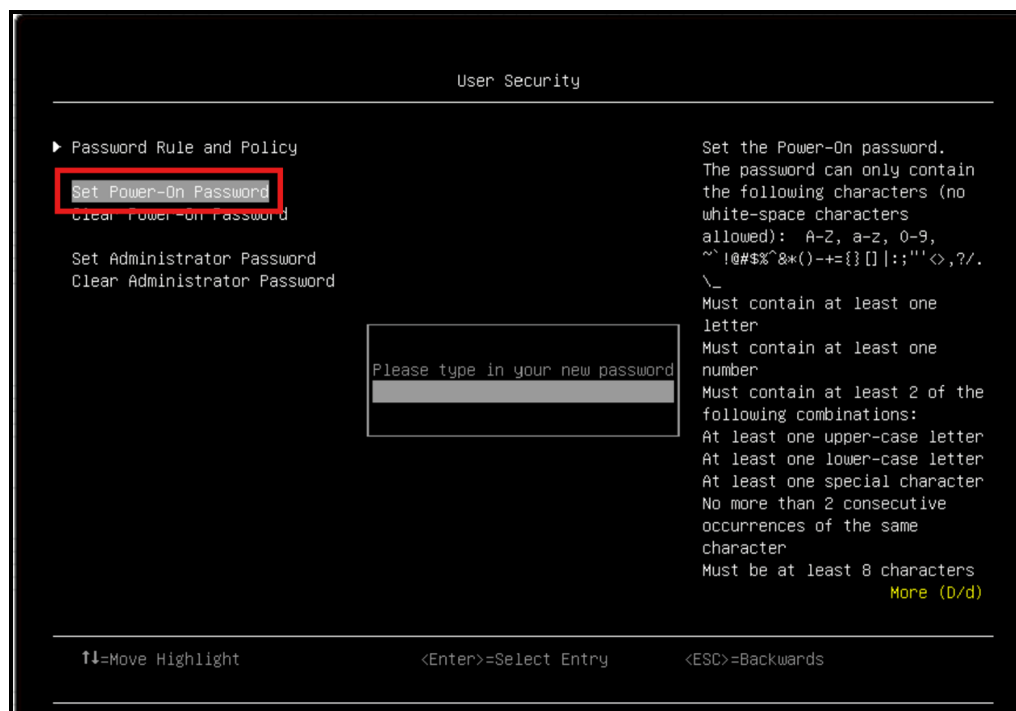


Figure 8. UEFI - User Security

In addition, selected ThinkEdge servers (SE450 and SE455 V3) supports an external diagnostics handset for enhanced systems management capabilities. User can also run XCC reset from the external diagnostics device without providing XCC password.

For SE450 (firmware version USX369B or later) and SE455 V3 (firmware version BX315C or later), the following security settings are adjustable. Make sure to configure the settings to prevent data loss:

- When reverting XCC to default by External Diagnostics Handset, the XCC password will be reset or not. (Default: The XCC password will not be reset.)
- When the XCC password is reset by External Diagnostics Handset or mobile app, the SED AK stored in the server will be cleared or not. (Default: The SED AK will be cleared.)

When customer set both XCC password and UEFI password, and lost both passwords together, ThinkEdge servers become inaccessible. In this case, you can reset the password securely. See the [Emergency XCC password reset](#) section for details. Note that this feature will clear the SED AK stored in the server to protect data from unauthorized access.

Using ThinkShield Key Vault Portal for System Lockdown Control

This ThinkShield Key Vault Portal can be used when the IT department desires to separate the duty of hardware management and security management. The ThinkEdge servers, in conjunction with [ThinkShield Key Vault Portal](#), provide the solution to the problems associated with device ownership, as described in the preceding section. To claim ownership, the IT administrator must register their organization in ThinkShield Key Vault Portal. With this portal, an IT administrator can manage on-site users and devices without needing to be on-site. This option provides stronger security protection and is good option to deploy ThinkEdge servers outside of Data Center type of environment.

The IT Administrator can also link their company's identity access management (IAM) system with the portal through Active Directory Federation Services (ADFS). This will increase the following:

1. Security by ensuring the organization's authenticity by ADFS
2. Ease-of-use by enabling on-site users to use their company user ID and password to log in to the portal

When edge users receive a ThinkEdge server, each server comes with a "Secure Activation Code." This is used to ensure proof of possession of the ThinkEdge server. The edge user can claim the device with the machine type, serial number, and this unique "Secure Activation Code." The ThinkShield Key Vault Portal can validate the Secure Activation Code which is unique to each device. Therefore, the Portal can claim the device only when the right information is provided. This "claiming" process makes the ownership association between the device and the organization claiming it.

Once claimed, an IT administrator can activate the device for operation. Until this activation process is completed, the ThinkEdge server locks the SED Authentication Key so that data is inaccessible and protected.

Device activation

Activation is a security feature of ThinkEdge servers that ensures that the system delivered from the factory is only used by its intended recipient and that all data and applications remain secure. An IT administrator can activate the server for operation, but until this activation process is completed, the ThinkEdge server locks the SED Authentication Key so that data on the SED drives is inaccessible and protected.

Activation method depends on ownership definition of ThinkEdge servers.

When a customer selects XCC Managed System Lockdown control, ThinkEdge servers are pre-activated. When ThinkEdge servers are deactivated, for example, by tamper event detection, customer can simply activate ThinkEdge server from XCC (GUI / Redfish API) by toggling the Active slider as shown in the following figure.

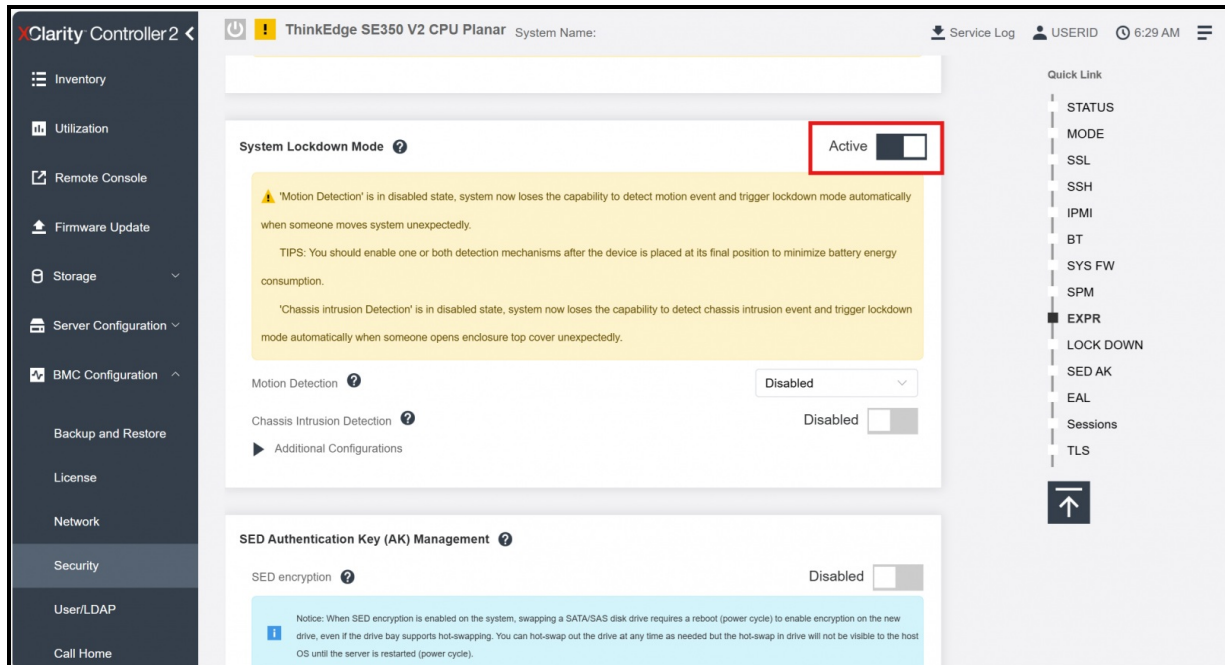


Figure 9. XCC - System Lockdown Mode

The System Lockdown Mode GUI shows the current lock down status. When it is locked down mode, the button shows “Inactive” as shown in the following figure. When the ThinkEdge system is under XCC Managed System Lockdown control, customers can toggle the button. After clicking **Apply**, the system will be unlocked, and the status will be changed to **Active**, as the figure above shows.

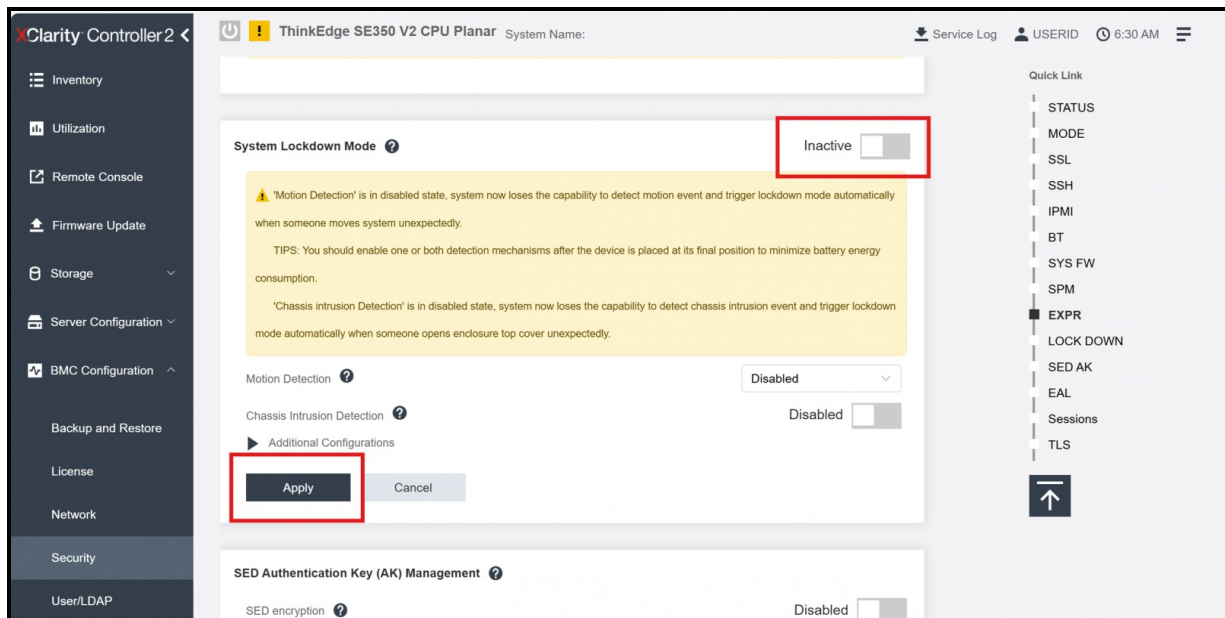


Figure 10. XCC - System Lockdown Mode

When customer selects ThinkShield Key Vault Portal Managed Lockdown control, ThinkEdge servers are shipped not activated, and activation is required.

There are four methods available to activate the device:

- Activation using LXCE UpdateXpress

The first method to activate a server is by using LXCE UpdateXpress. LXCE UpdateXpress is a software utility running on Windows laptop. It provides a GUI based wizard to guide on-site users to activate a ThinkEdge server. In order to activate server, the user need to make sure their laptop is in the same network as the server to be activated or connected directly to XCC port of the server with an Ethernet cable.

- Automatic / online activation

If the management port of the edge server is able to connect to Internet, the server can communicate with the ThinkShield Key Vault Portal, and the IT admin can activate the server there.

- Activation using the ThinkShield Edge Mobile Management Application

This method of activation allows an IT administrator to delegate the process to an on-site user (called Edge user in ThinkShield Key Vault portal). In this method the on-site user uses a mobile application to activate the device. To prevent exploitation of the mobile activation process, this method requires that the IT administrator assign the appropriate role to the on-site user in the ThinkShield Key Vault. Once assigned, the on-site user can claim and activate devices using the [ThinkShield Edge Mobile Management application](#) (for iOS and Android).

- Manual activation

This method involves both the on-site user and the IT Administrator manually exchanging information. This method is only used in cases where one of the other methods is not possible, such as when networking is neither available nor allowed and only when the end user can communicate by a phone.

When the ThinkEdge server is not activated and is in locked state, the server interrupts the boot process and displays a warning message "System is locked down and must be activated in order to complete booting" and will wait the activation / unlocking process as described above.

There are three ways to determine whether a ThinkEdge server is activated or not activated:

- Messages on the UEFI POST screen
- Messages on the XCC login screen
- Status of the Activation LED on the server

The following figure shows the UEFI POST screen of a server that is already activated.

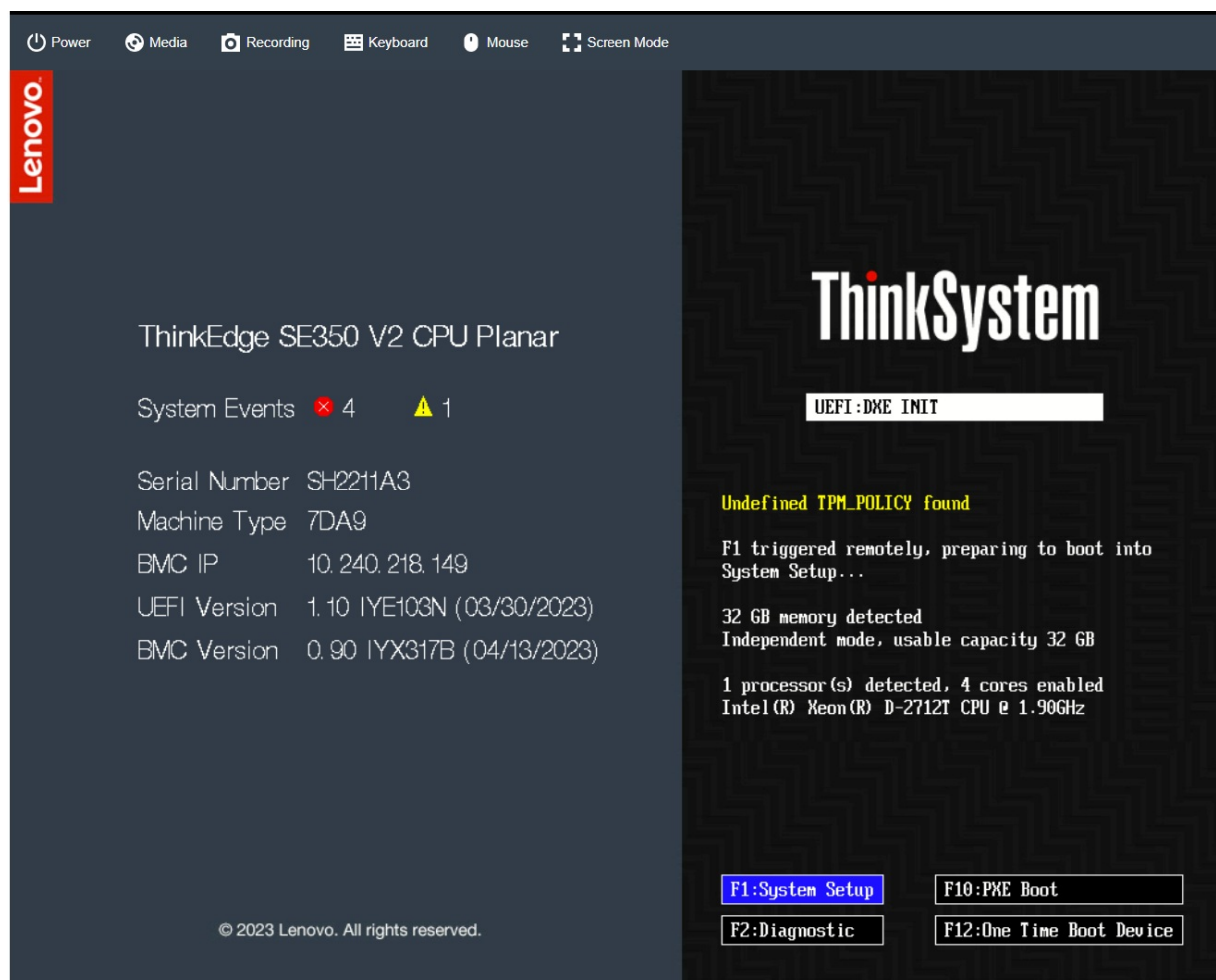


Figure 11. Activated ThinkEdge Server UEFI POST Screen

The following figure shows the UEFI POST screen of a server that is not yet activated.

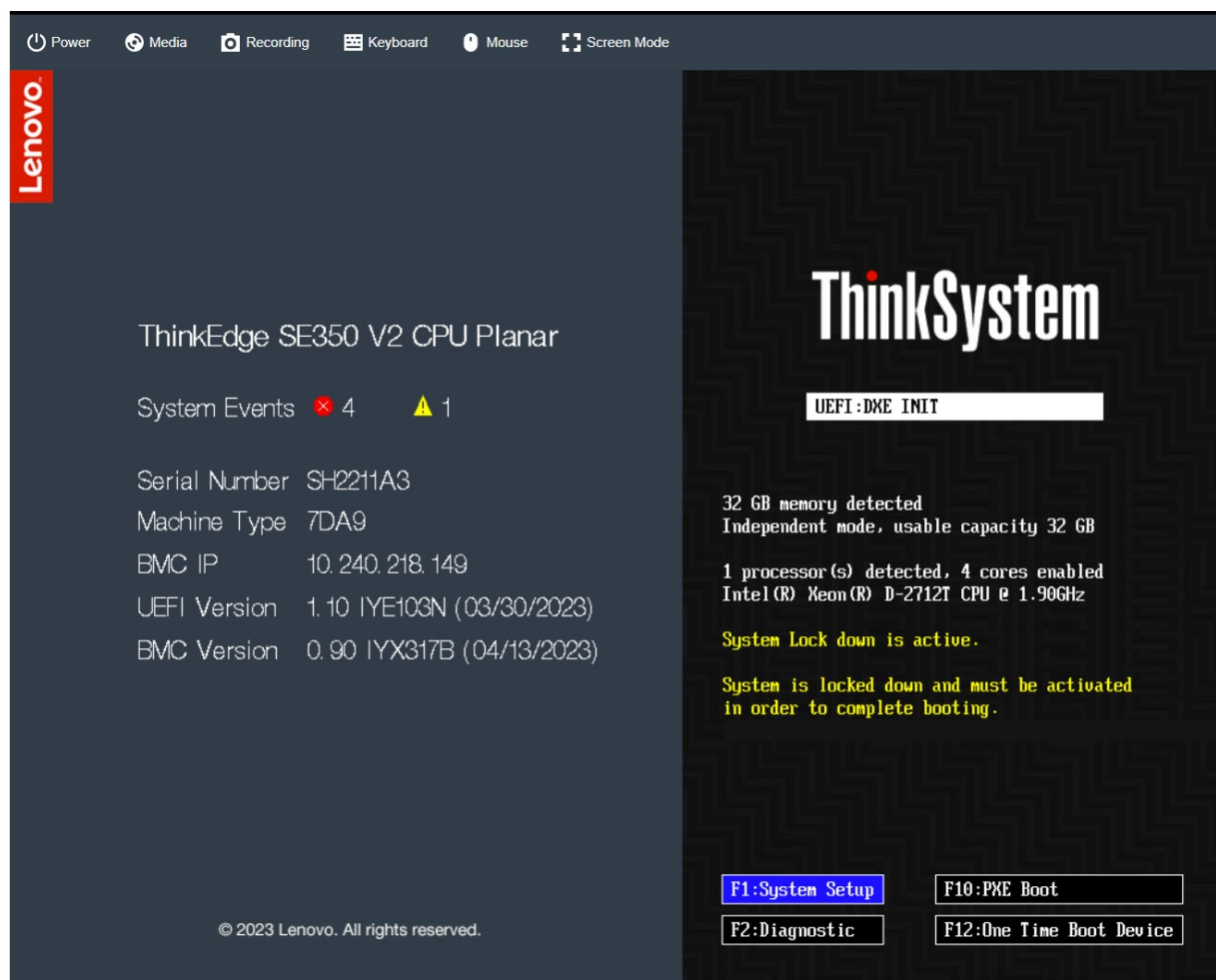


Figure 12. ThinkEdge Server UEFI POST Screen Waiting Activation

The following figure shows the XCC login screen of a server that is not yet activated.

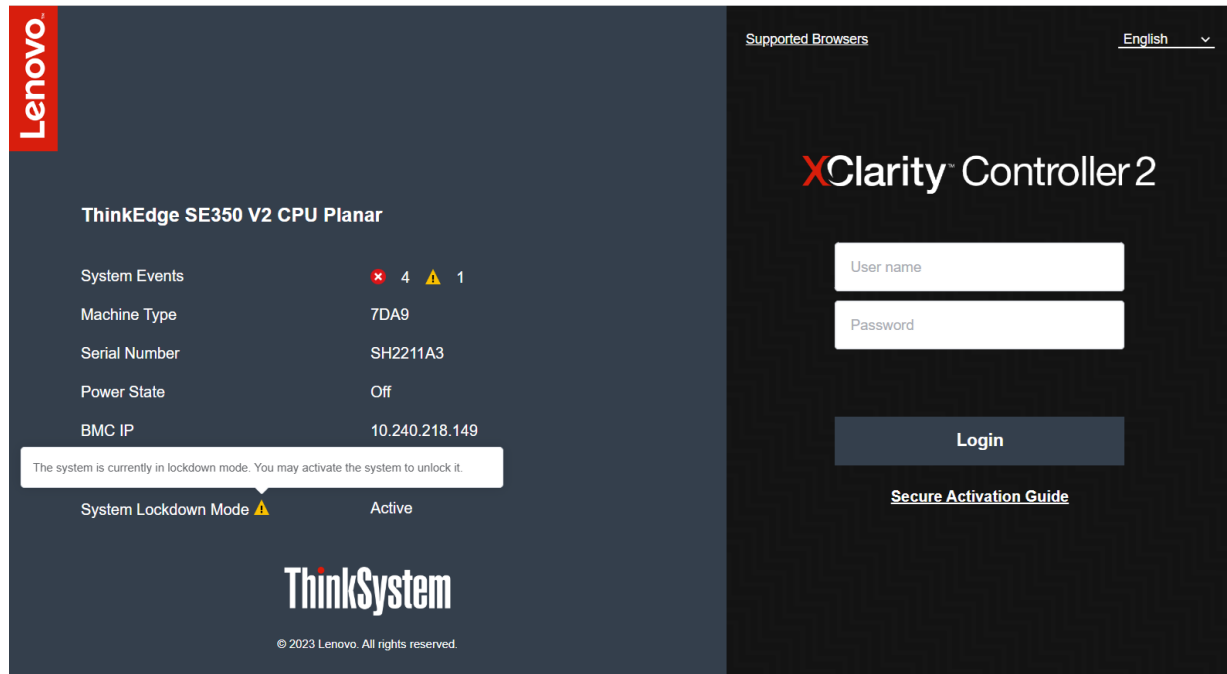


Figure 13. Activated ThinkEdge Server XCC Login Screen

The following figure shows the XCC login screen of a server that is already activated.

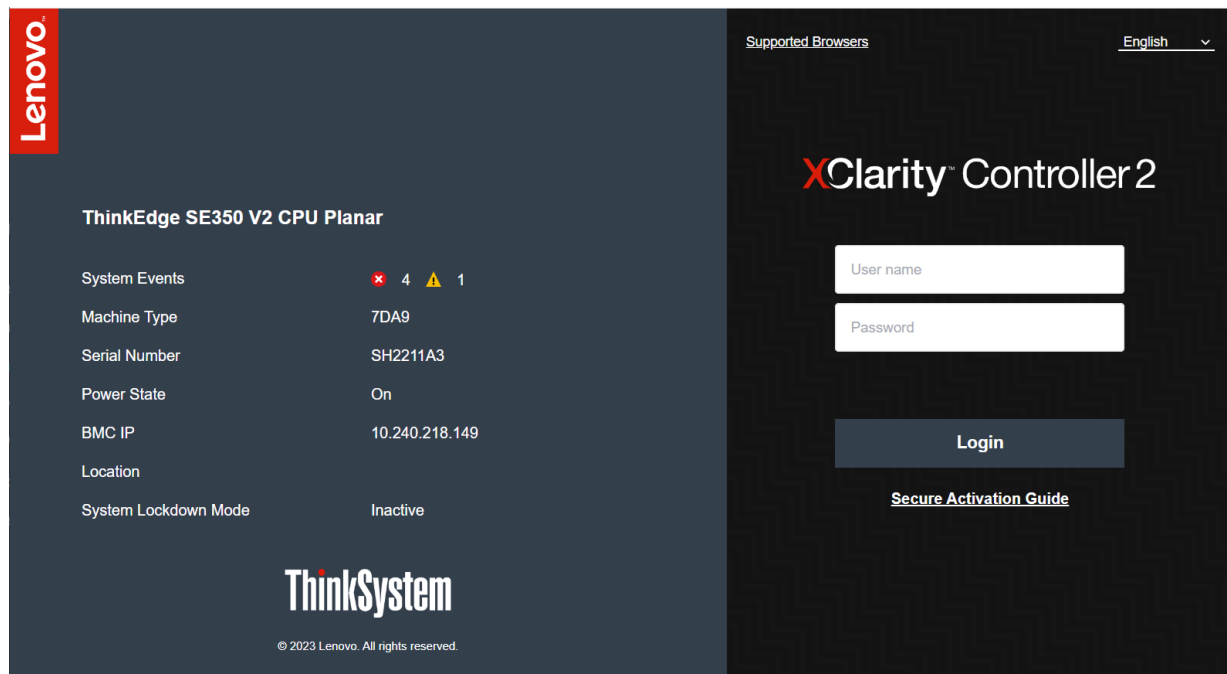


Figure 14. ThinkEdge Server XCC Login Screen Waiting Activation

The Security LED on the ThinkEdge server indicates the status of activation:

- LED is On = SED is enabled, or tamper detection (such as an intrusion sensor) is enabled, and server is activated
- LED is Blinking = Server is in lockdown mode, but server is not yet activated
- LED is Off = SED is disabled, and tamper detection is disabled, and server is activated (or SecurityPack is de-populated setup - SE450 only)

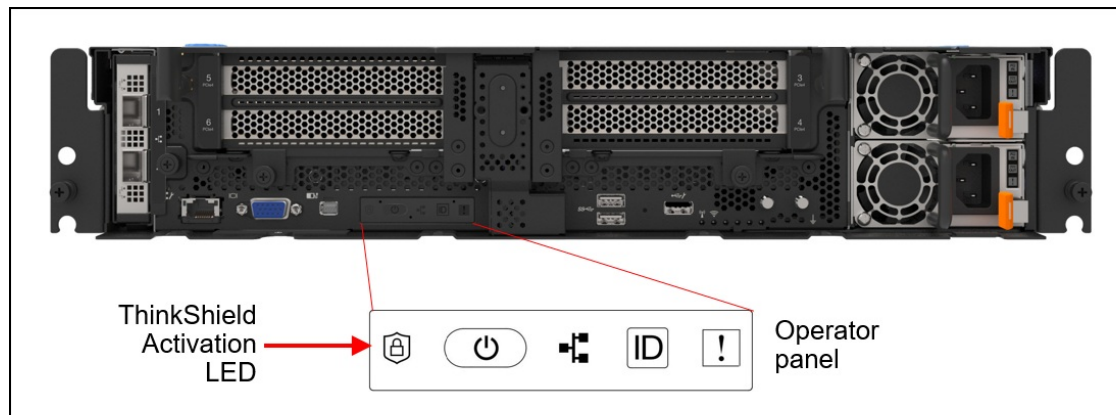


Figure 15. SE450 ThinkShield Activation LED

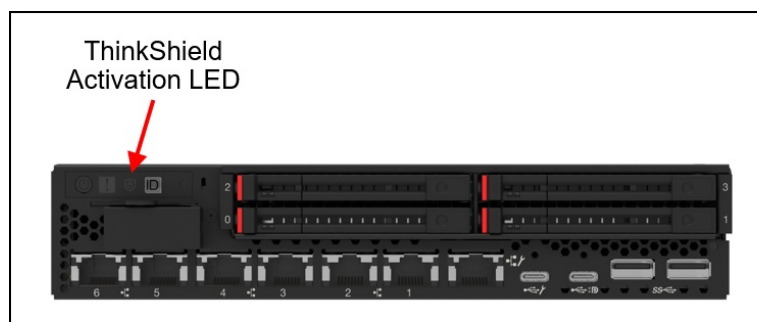


Figure 16. SE350 V2 ThinkShield Security LED

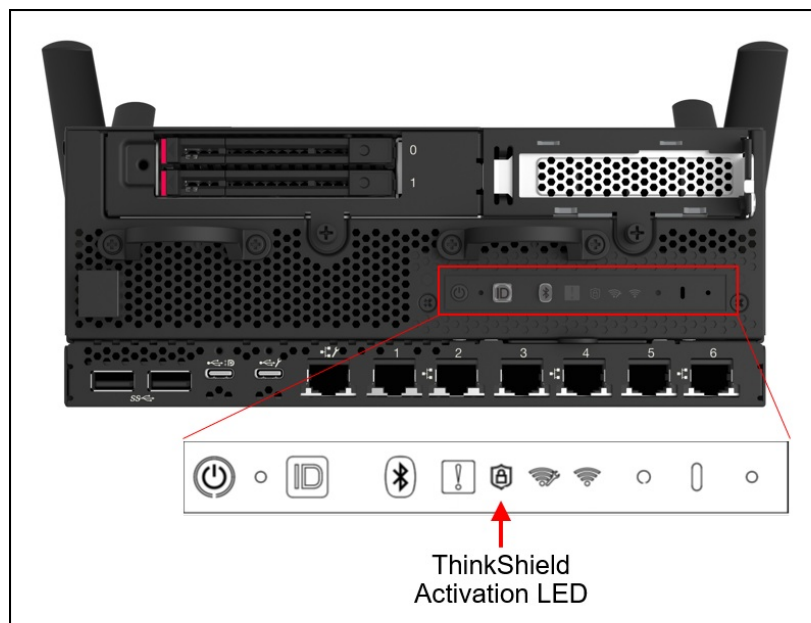


Figure 17. SE360 V2 ThinkShield Security LED (Front)



Figure 18. SE455 V3 ThinkShield Security LED

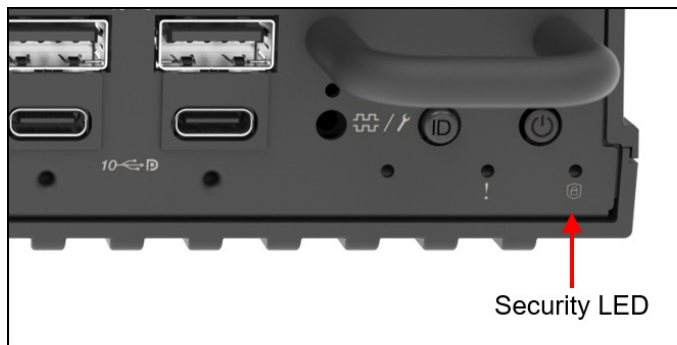


Figure 19. SE100 ThinkShield Security LED (front of server)

Checking System Lockdown Control in XCC

It is possible to determine the Activation Method that a Server is shipped and configured with using XClarity Controller. Once you login to the XCC web interface as an Administrator, the Home Page shows the current System Lockdown Mode (Active or Inactive) and the System Lockdown Mode Control (XClarity Controller or ThinkShield Portal), as shown in the following figures.

The following figure shows XCC as the System Lockdown Mode control.

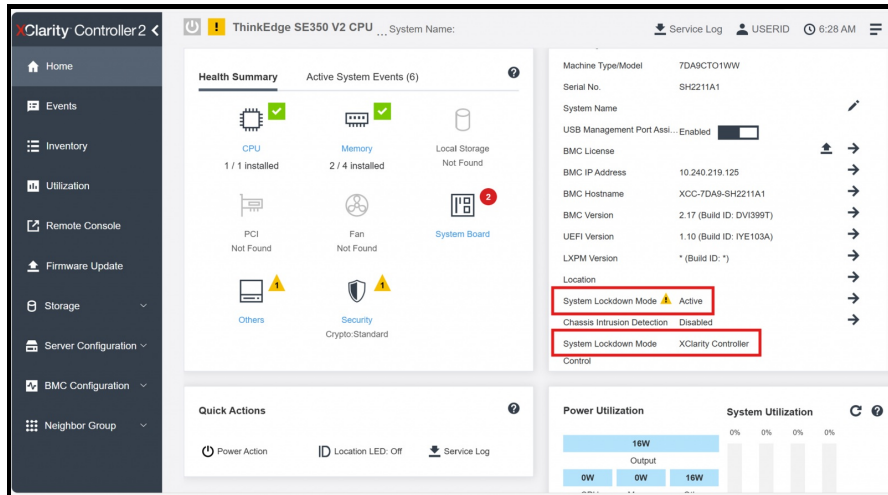


Figure 20. XCC Home showing XCC as the System Lockdown Mode control

The following figure shows ThinkShield Portal as the System Lockdown Mode control.

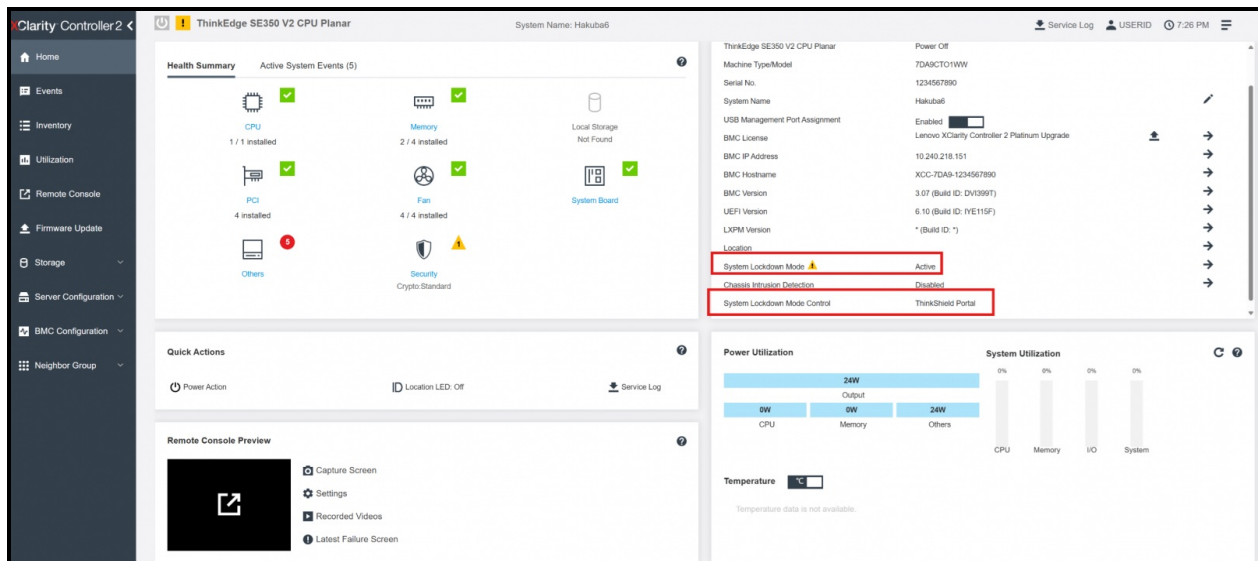


Figure 21. XCC Home showing ThinkShield Portal as the System Lockdown Mode control

ThinkShield Key Vault Portal

The [ThinkShield Key Vault Portal](#) is a web application that is designed to manage organizations, users, and devices when ThinkShield Key Vault Based Lockdown Control was selected.

The first action after ordering the first ThinkEdge server is to create a new organization where all the devices belong. To create the new organization, the administrator needs to create a Lenovo ID (see <https://passport.lenovo.com>) if they don't already have one.

When creating a new organization, the administrator can choose to authenticate their organization's users by linking their directory services using Active Directory Federation Services (ADFS) (recommended) or by using the Lenovo ID identity authentication services.

Create organization
All fields are required except where noted

PROFILE | SUBSCRIPTIONS

ORGANIZATION INFORMATION

Organization Domain Display Name Country/Region **United States**

Authentication Type **Lenovo ID**

ORGANIZATION ADMIN

Organization Admin Email First Name Last Name

Cancel **Continue**

Figure 22. Creating new organization using ThinkShield Key Vault Portal

Invite User
All fields are required except where noted

MANUAL INVITE | BULK INVITE

INFORMATION **CONTACT**

First Name John Email email@email.com

Last Name Doe

Role **Edge User**

Cancel **Invite**

Figure 23. Adding new user using ThinkShield Key Vault Portal

After creating a new organization, the administrator can define role-based access control for users who need access to their ThinkEdge servers. It is particularly important to follow the principal of least-privilege when assigning roles to users.

The following table shows a high-level view of the roles vs. functions. Detailed permissions can be found in the application user manuals.

Table 3. Roles and functions for user types in ThinkShield Key Vault Portal

Task	Organization Admin	Edge User	Base User	Maintenance User
Log into ThinkShield Key Vault Portal and have access to an Organization	Yes	Yes	Yes	Yes
Activate (on board and unlock) ThinkEdge servers	Yes	Yes	No	No
Manage Users	Yes	No	No	No
Manage Device	Yes	No	No	No
Update Key / Emergency XCC password reset	No	No	No	Yes

In addition to manually adding new users, when Active Directory Federation Service (ADFS) is in use and an unregistered user logs into Portal, the Portal will automatically register the user, however, only the Base user role (read-only) will be assigned. A Base user cannot perform any operation by default, so the IT administrator needs to change the role appropriately. From ThinkShield Key Vault Portal, a user with an appropriate role can manage users and ThinkEdge Servers.

Activation using the ThinkShield Edge Mobile App

Considering ease-of-use for non-IT skilled users at edge locations, and given that the number of devices to manage at the edge may be smaller, the ThinkEdge Server can be activated by the ThinkShield Edge Mobile Management app. The mobile app can be downloaded from [major Android stores](#) (Android) and from the Apple App Store (iOS).

The mobile app can interface with each ThinkEdge server in one of two ways:

- Physical connection to the dedicated USB service port on the front of the server
- Bluetooth (when wireless option is selected)

The USB service port is indicated with the management symbol  as shown in the following figures.

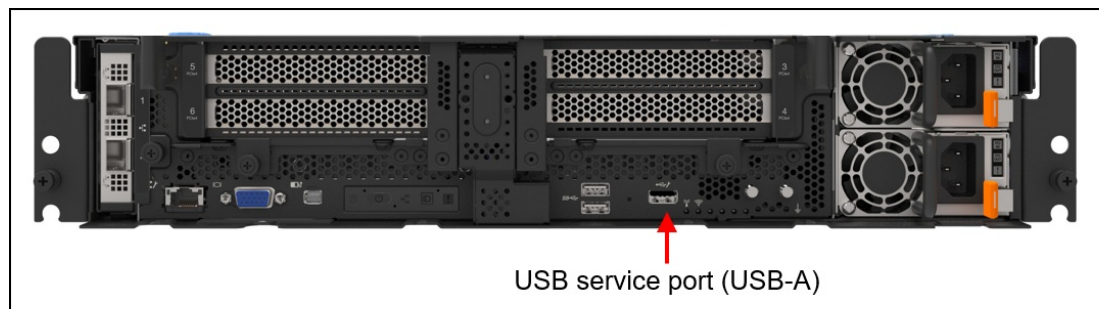


Figure 24. SE450 dedicated service USB Type-A port

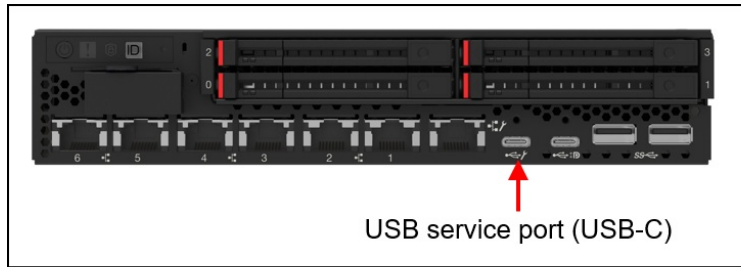


Figure 25. SE350 V2 dedicated service USB Type-C port

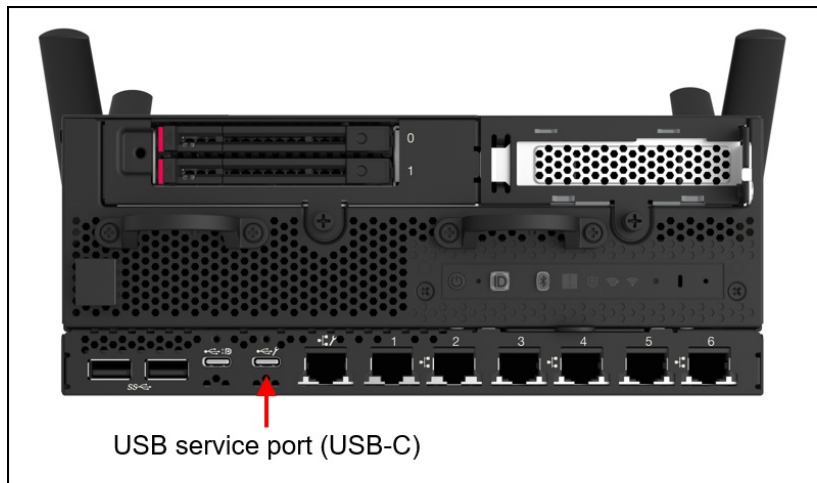


Figure 26. SE360 V2 dedicated service USB Type-C port



Figure 27. SE455 V3 dedicated service USB Type-A port

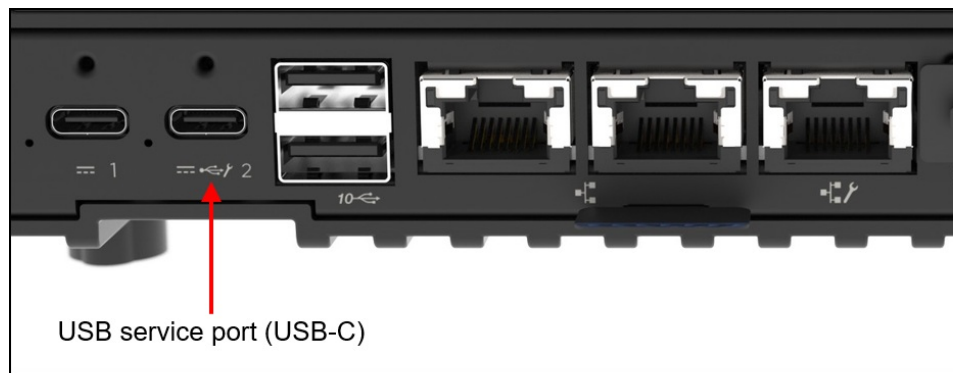


Figure 28. SE100 service USB Type-C port (rear of server)

On-site users (Edge Users) first need to be registered and provided the proper role by the IT administrator (Organization Admin) and prior to access, they need to login to the mobile app. A registered Edge user can use the mobile app to claim and to activate the devices.

The process to activate a ThinkEdge server using the Mobile app is shown in the following figure.

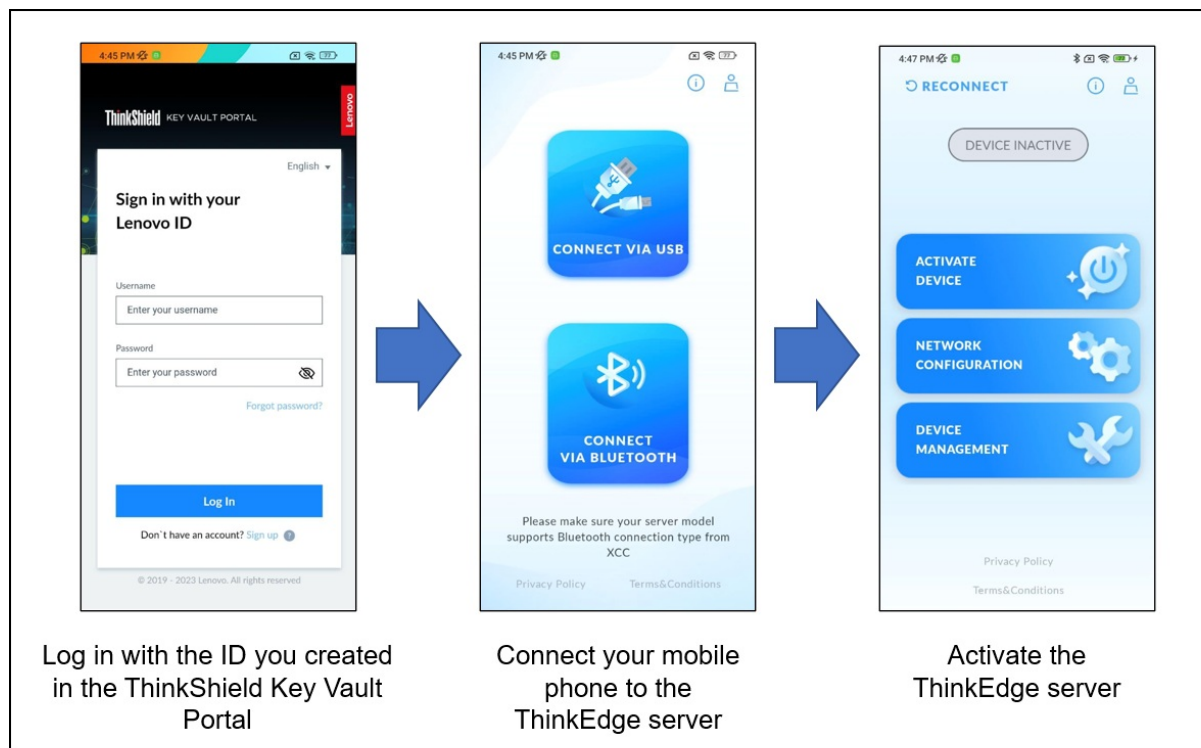


Figure 29. Activation flow using the ThinkShield Edge Mobile Management App

Activation using LXCE UpdateXpress

LXCE UpdateXpress can be downloaded from the UpdateXpress web page:

<https://support.lenovo.com/us/en/solutions/ht115051-lenovo-xclarity-essentials-updateexpress>

To activate ThinkEdge server in locked-down mode with LXCE UpdateXpress, connect your laptop to the management network or connect directly to the server's Remote Management port (XCC) with an Ethernet cable, and login to XCC as a user with Administrator permissions.

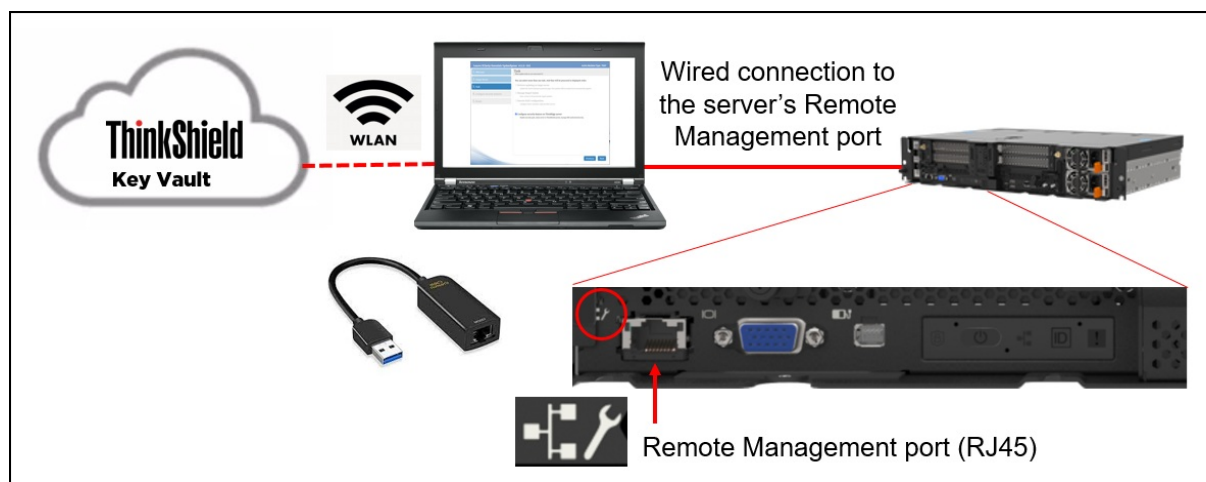


Figure 30. Connecting LXCE UpdateXpress to the ThinkEdge server

Activation of ThinkEdge server is part of functions to configure security feature on ThinkEdge server in LXCE UpdateXpress. If server's system lockdown control is managed by ThinkShield Key Vault Portal Managed, user has to be authenticated as member of organization owning that server in ThinkShield Key Vault Portal as the first step of server activation. Refer to [ThinkEdge server security features](#) on the Lenovo Docs site for details.

Lenovo XClarity Essentials UpdateXpress v4.2.0 - 01d

Active Machine Type: 7DA9

1. Welcome

2. Target Server

3. Task

4. Configure Security Features (3/3)

5. Enable Security Pack

6. Finish

Validate ThinkShield Portal Account

Complete account setting to the ThinkShield Portal for server activation.

You need to have valid Lenovo ID to be authenticated to the ThinkShield Portal. Please follow this [instruction](#) to create a Lenovo ID if you don't have it.

Ensure that your Lenovo ID and your device belong to the same organization in the ThinkShield Portal. To learn more about organization and how to create an organization ID, [click here](#).

If you forgot your organization ID, you can find it [here](#).

Organization ID

Lenovo ID

Password

Validate

Previous Next

Figure 31. Validated as server's owner in ThinkShield Key Vault portal

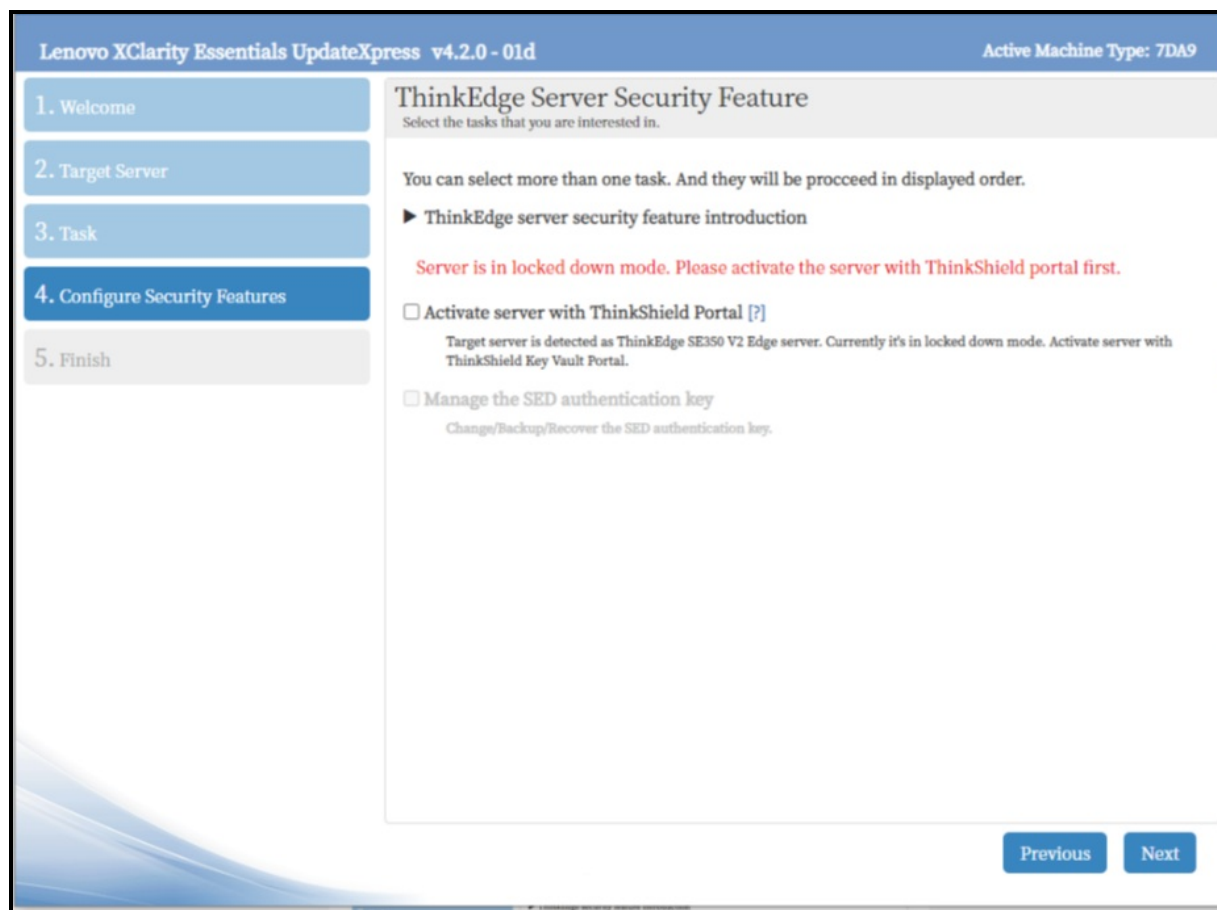


Figure 32. Activate ThinkEdge Server with LXCE UpdateXpress

SED Drive security and management

ThinkEdge servers support SED drives for local storage. Self-encrypting drives (SEDs) provide benefits by encrypting data on-the-fly at the drive level with no performance impact, by providing instant secure erasure thereby making the data no longer readable, and by enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use. These features are essential for many businesses, especially those storing sensitive customer data.

The SED Authentication Key (SED AK) is unique to each SED drive and Lenovo does not retain it. The SED AK controls access to the data on the SED. The IT administrator should make a backup of the SED AK for assurance of business continuity.

The ThinkEdge servers also support an auto SED AK backup feature as long as one of the following specific installed components is healthy:

- SE450: Either of these, depending on which is installed:
 - Firmware and TPM 2.0 Security Module
 - Firmware and Root of Trust Security Module
- SE350 V2: Either of these, depending on which is installed:
 - 4x 10/25Gb, 2x 2.5Gb (TSN) I/O Module
 - 4x 1Gb, 2x 2.5Gb (TSN) I/O Module
- SE360 V2: Either of these, depending on which is installed:
 - 4x 10/25Gb, 2x 2.5Gb (TSN) I/O Module
 - 4x 1Gb, 2x 2.5Gb (TSN) I/O Module

- SE455 V3:
 - Security mezzanine card (TPM / RoT)
- SE100
 - PCIe expansion riser card (Note: When SE100 is configured without PCIe expansion kit, SE100 does not take an automatic backup of the SED AK)

The automatic backup can be used to restore the SED AK in cases of hardware failure. This is only possible if both SED and above component are healthy. In this case, they can be installed into another ThinkEdge server, and the SED AK can then be restored. It is still imperative to make your own backup of the SED AK in cases where the above component is not healthy.

The following figure shows how you can use the XClarity Controller XCC web interface to backup your SED AK.

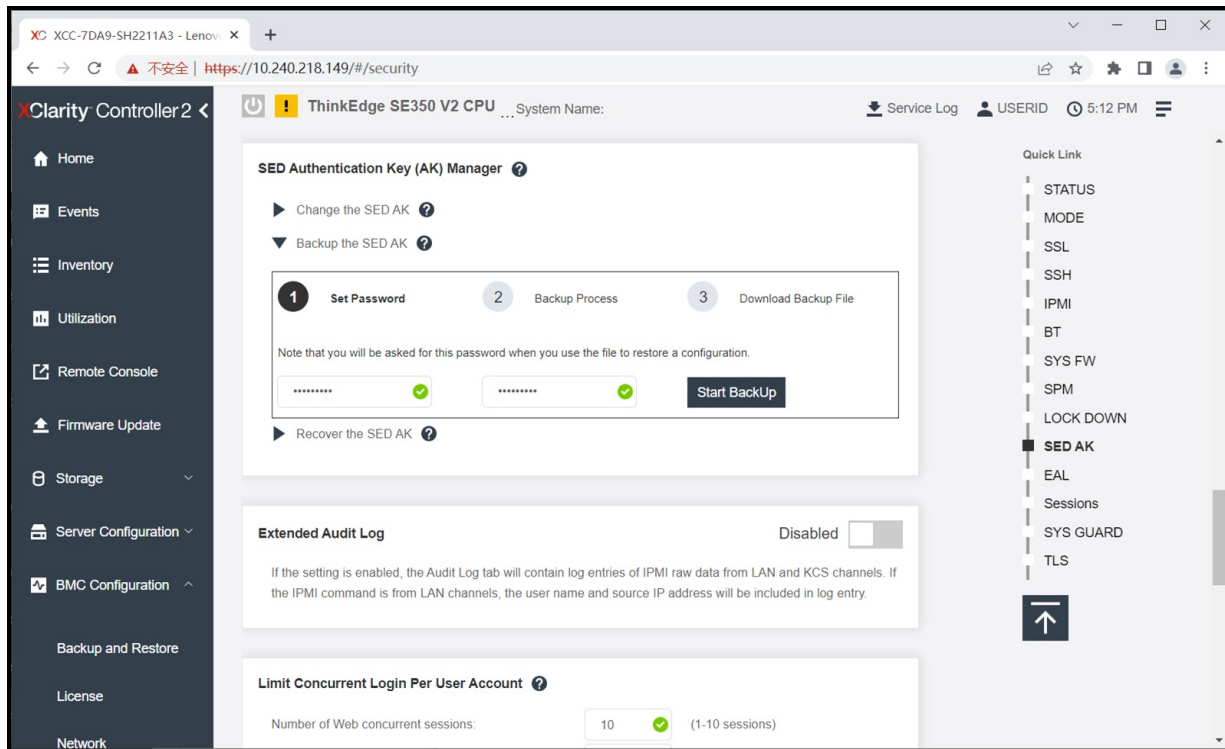


Figure 33. Backing up the SED Authentication Key using XCC

If sharing storage media across multiple ThinkEdge servers, a passphrase-based SED AK can be used instead of a random SED AK (the default). With the same passphrase, multiple ThinkEdge servers can share SED media. Changing to a passphrase can be performed via XCC as shown in the following figure.

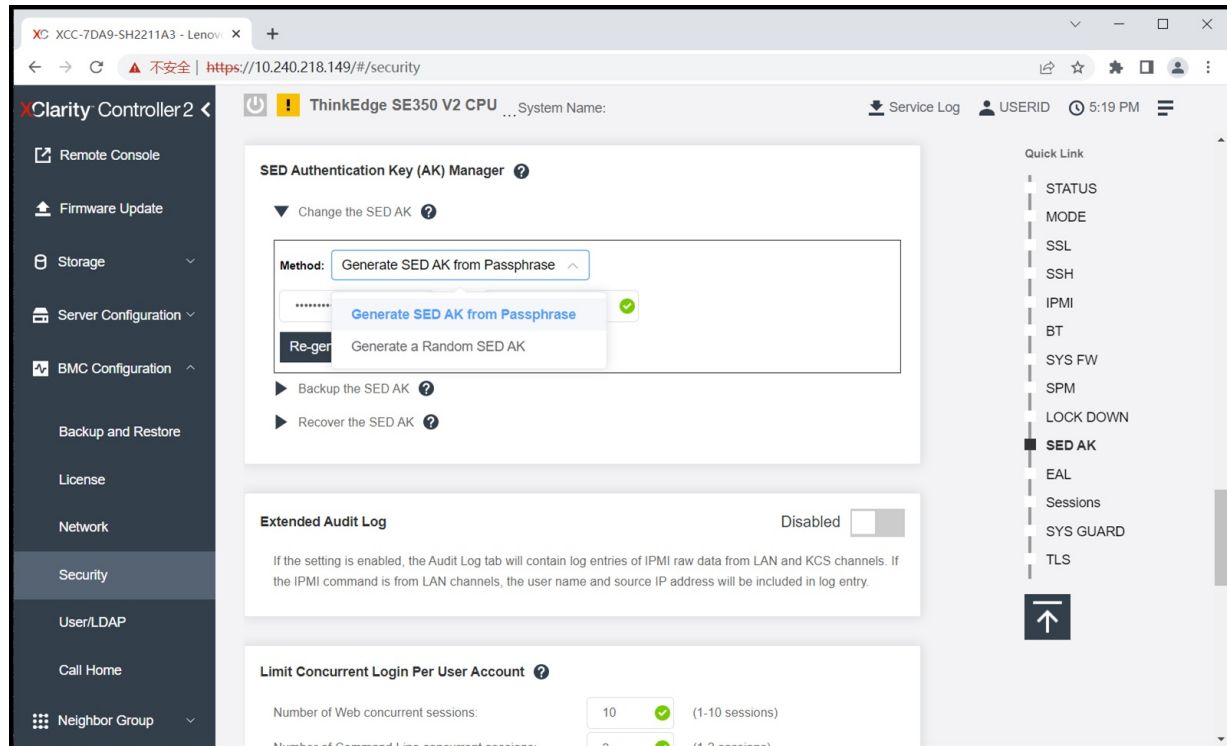


Figure 34. Changing SED AK to a Passphrase using XCC

The SED AK operations are very security sensitive; as a result, the XCC in ThinkEdge servers supports two administrator levels:

- Administrator
- Administrator+

When customer logs in ThinkEdge servers, the default user ID has Administrator+ privilege level. This is the user ID when customer first logs in with default ID / Password. Customers can create other users with other privilege levels, however, one ThinkEdge server can support only one Administrator+ privilege user. Only Administrator+ user (who is default user of local XCC) can manage the SED AK restore operation including to restore SED AK from automatic back up.

When the administrator first logs in to XCC in the ThinkEdge server, only the Administrator+ user (USERID) is registered as shown below.

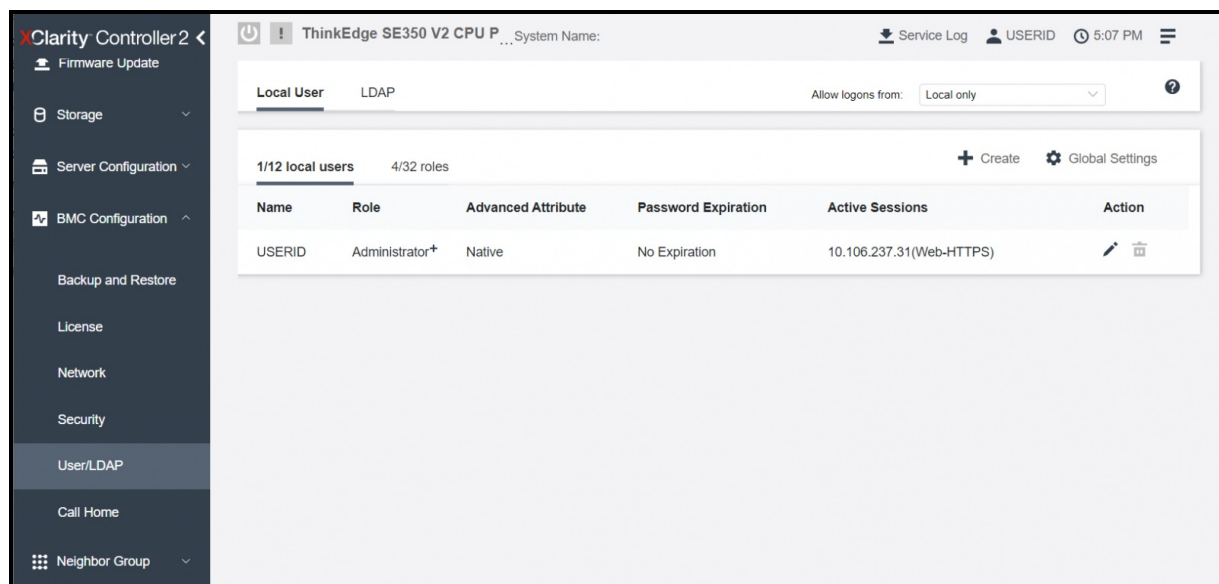


Figure 35. Default Administrator+ privilege user ID registered in ThinkEdge Servers

The administrator can create additional users, such as adding a user with Administrator privileges, as shown below.

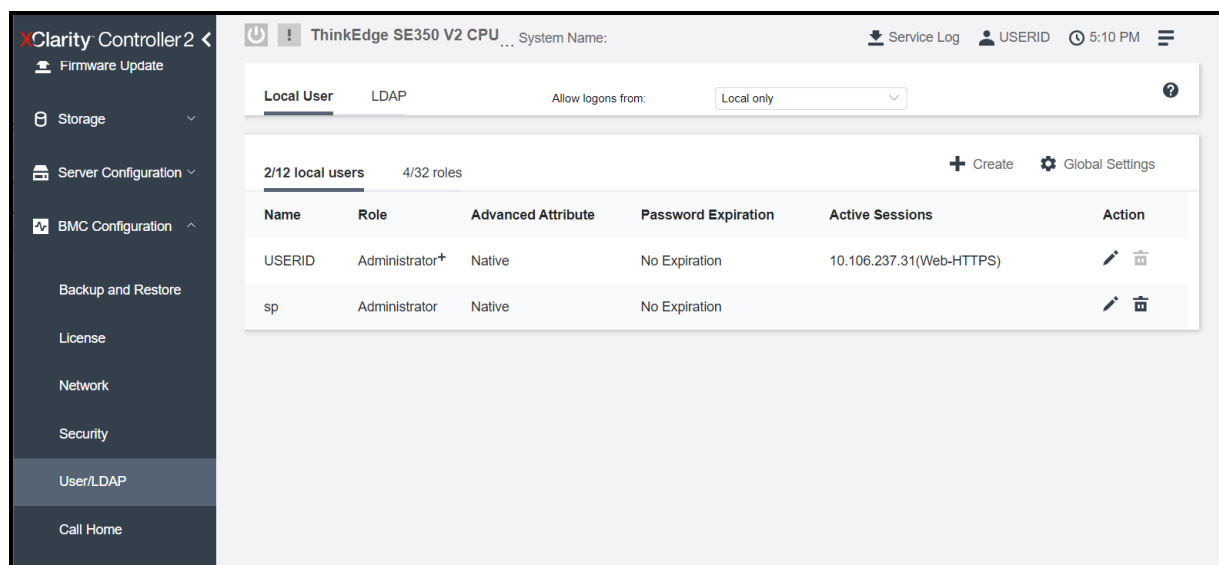


Figure 36. Administrator and Administrator+ ID registered in ThinkEdge Servers

For the account with Administrator+ privilege, the administrator can perform SED AK restore operation as indicated below.

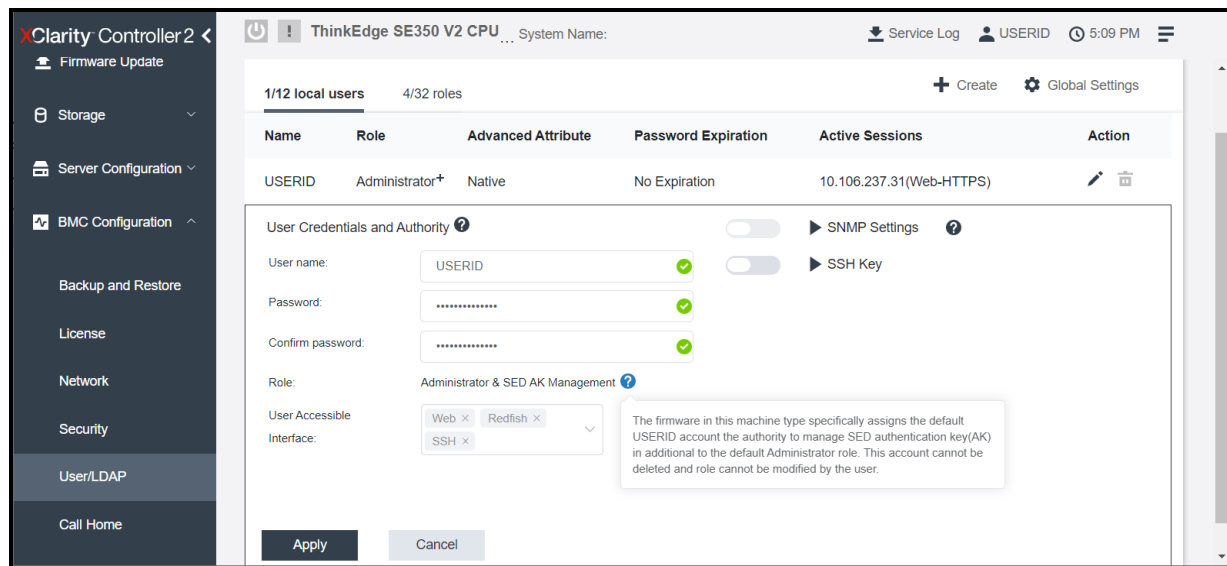


Figure 37. Administrator+ ID description from XCC GUI

Tamper and Intrusion Detection

Each ThinkEdge server has multiple sensors to detect tamper events to lock access to the SED. Each sensor can be configured using XCC, LXCE, LXCA, or the Redfish API. Since all sensors are disabled by default, be sure to enable and configure the sensors to initiate tamper event detection based on your needs.

Supported sensors used to lock SED drives are as follows:

- SE450: Intrusion sensor
- SE350 V2: Intrusion sensor, advanced motion detection sensor
- SE360 V2: Intrusion sensor, advanced motion detection sensor
- SE455 V3: Intrusion sensor
- SE100: Intrusion sensor

All ThinkEdge servers support the intrusion sensor which can detect when the opening of the top cover (top and bottom cover in case of SE360 V2). The SE350 V2 and SE360 V2 supports an advanced motion detection sensor where the user can define the motion event by the number of step counts which is nearly equal to the distance of movement.

The ThinkEdge SE350 V2, and SE360 V2 also support the ThinkEdge Anti-tampering Keylock Kit (it was also called as Tamper Detection Kit with the Security Lock option). When those options are selected, an intrusion event triggered by opening the top or bottom cover occurs only when the Kensington lock is attached (SE350 V2) or when the chassis is key locked (SE360 V2).

When the Kensington lock is removed (SE350 V2) or chassis key is unlocked (SE360 V2), top-cover access is permitted, the tamper event will not be triggered.

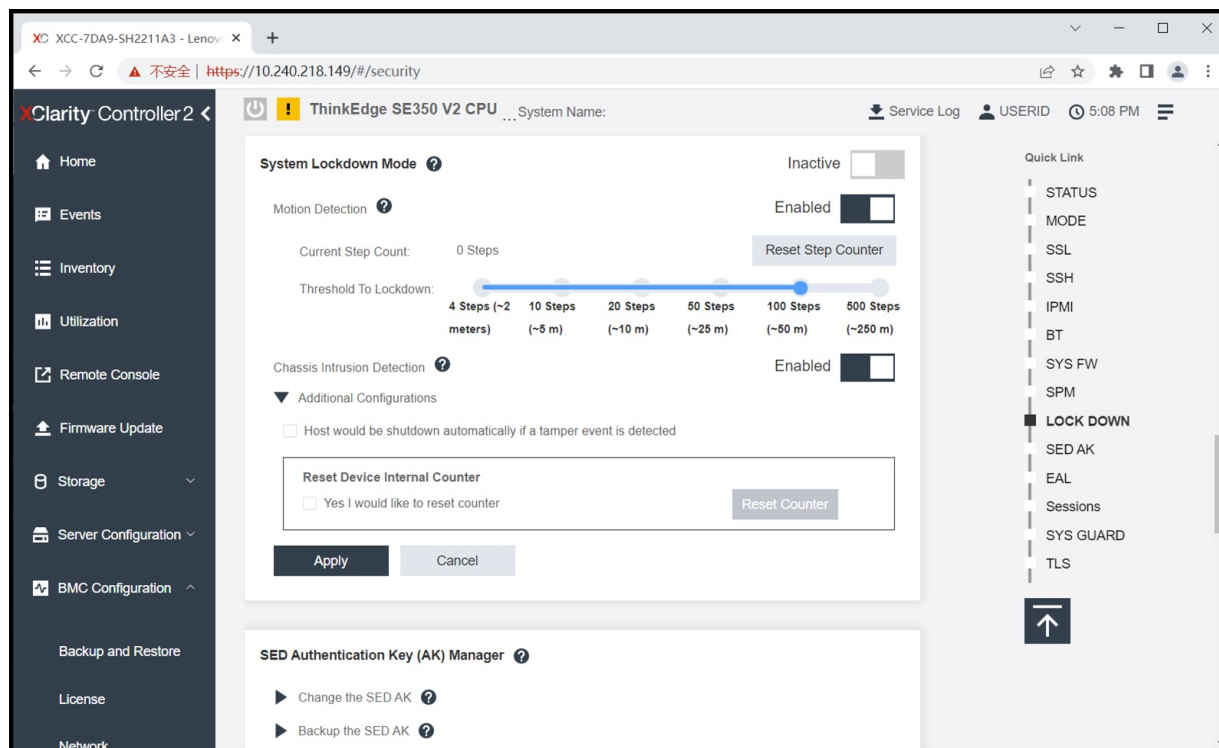


Figure 38. SE360 V2 Lockdown sensor management XCC GUI

Additional functions in LXCE UpdateXpress

In addition to activating ThinkEdge servers, LXCE UpdateXpress can also be used to configure other security features in ThinkEdge server listed as below:

- Claim ThinkEdge servers in ThinkShield Key Vault Portal
- Configure Security Sensors for tamper detection in ThinkEdge servers.
- Promote System Lockdown Control from XClarity Controller managed to ThinkShield Key Vault Portal managed.
- Manage (change, backup, and restore) SED authentication keys (requires Admin+ user privileges in XCC)

For the SE350 V2 and SE360 V2, Lenovo XClarity Essentials UpdateXpress provides a new feature to convert a system lockdown control from XCC managed to ThinkShield Key Vault Portal . This delayed promotion will support the case when customers need to access ThinkEdge server without device on boarding, for example, to install and configure software servers at a secure location, then deploy fully secured ThinkEdge servers to an unsecured location after promoting them to Security Pack Enabled.

Note: Once System Lockdown Control in ThinkEdge server is “promoted” from XClarity Controller managed to ThinkShield Key Vault Portal managed, it cannot be “demoted” back to XClarity Controller managed.

These functions can be accessed from “Configure Security Features on ThinkEdge server” from the task main menu in LXCE UpdateXpress. Please refer to [ThinkEdge sever security features](#) in Lenovo Docs.

Lenovo XClarity Essentials UpdateXpress v4.2.0 - 01d Active Machine Type: 7DA9

1. Welcome

2. Target Server

3. Task

4. Configure Security Features

5. Finish

Task
What update task are you interested in?

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

- ☐ Perform updating on target server
Update the server selected at previous page. The updates will be acquired and automatically applied.
- ☐ Manage Staged Update
Start, cancel or list previously staged updates.
- ☐ Remote RAID configuration
Configure RAID controller using the BMC service.
- ☒ Configure security feature on ThinkEdge server
Enable security pack, claim server to ThinkShield portal, manage SED authentication key.

Previous Next

Figure 39. LXCE UpdateXpress Task menu

The following figure shows details functions in LXCE UpdateXpress for security management of ThinkEdge servers.

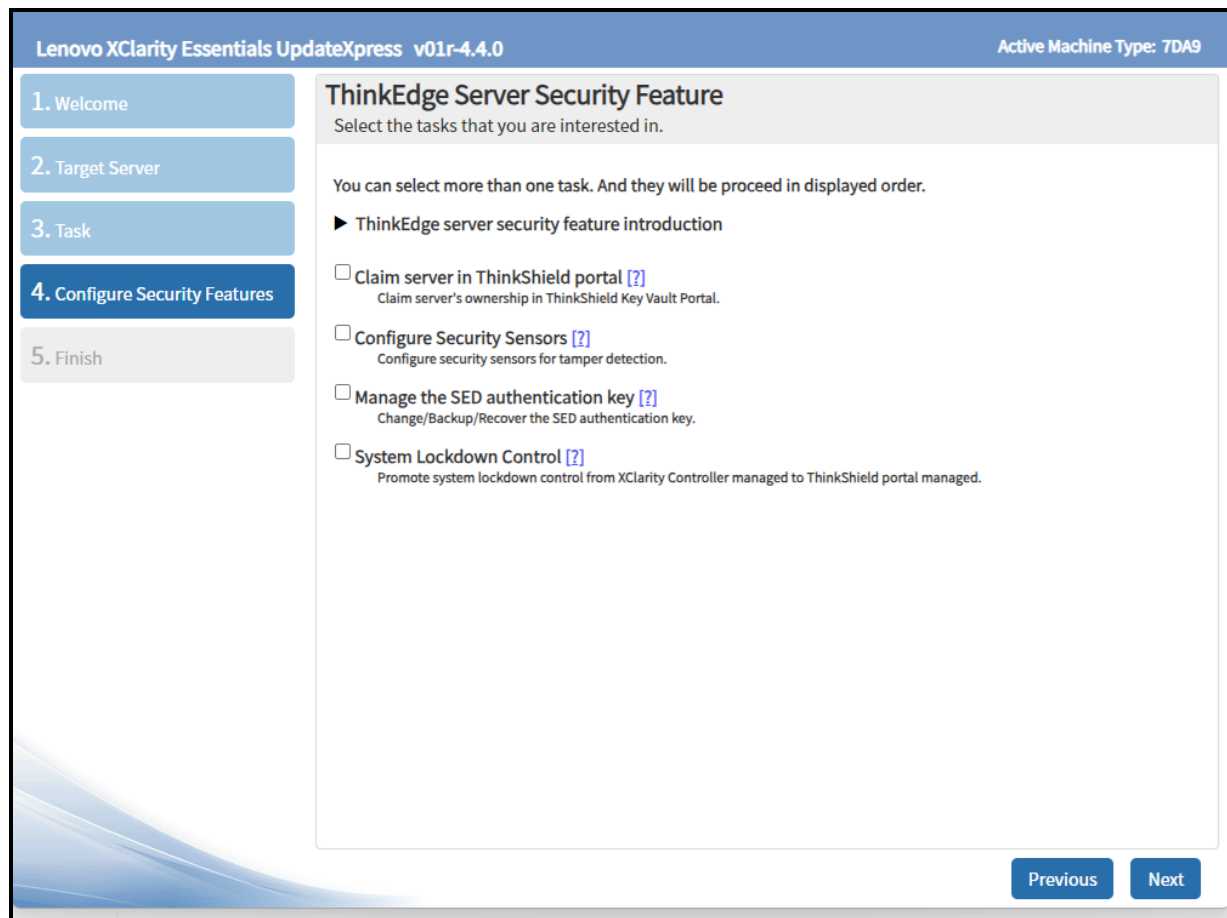


Figure 40. Additional functions in LXCE UpdateXpress for ThinkEdge server securities

Additional functions with ThinkShield Key Vault Portal

ThinkShield Key Vault Portal can also support more advanced management features.

- [Viewing all devices owned by an organization](#)
- [Viewing all users](#)
- [Manual claiming](#)
- [Manual activation](#)
- [Bulk user registration and server claims](#)
- [Transferring ownership](#)
- [Emergency XCC password reset](#)

Viewing all devices owned by an organization

The Portal can show all claimed and activated ThinkEdge Servers owned by the organization, as shown in the following figure.

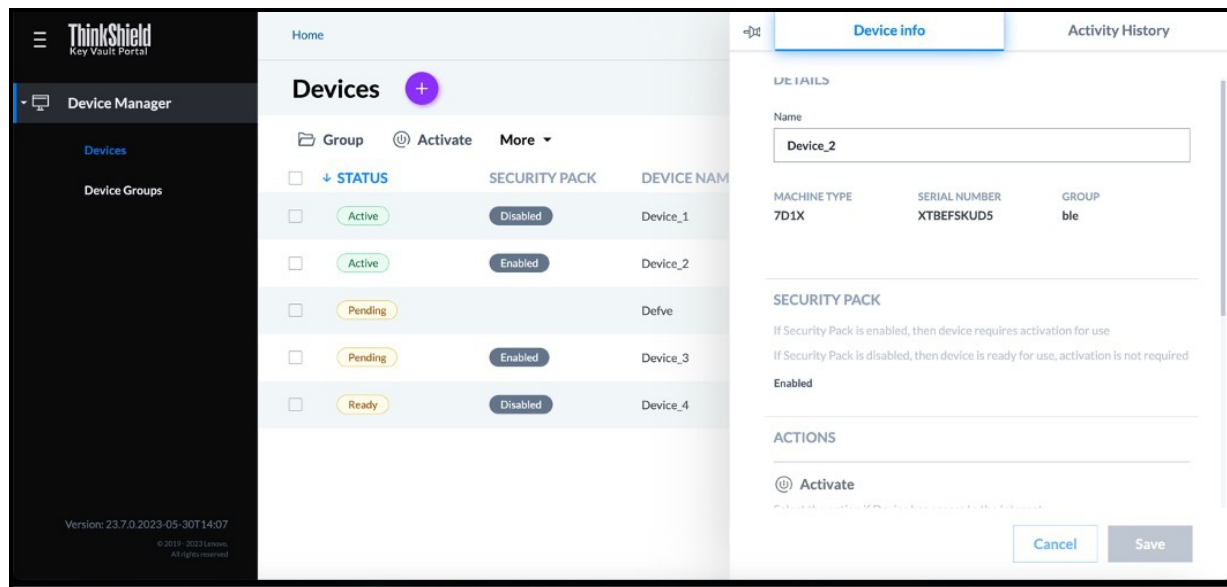


Figure 41. Displaying ThinkEdge server information under the organization

Viewing all users

ThinkShield Key Vault Portal can also be used to show the users and their roles that belong to the organization.

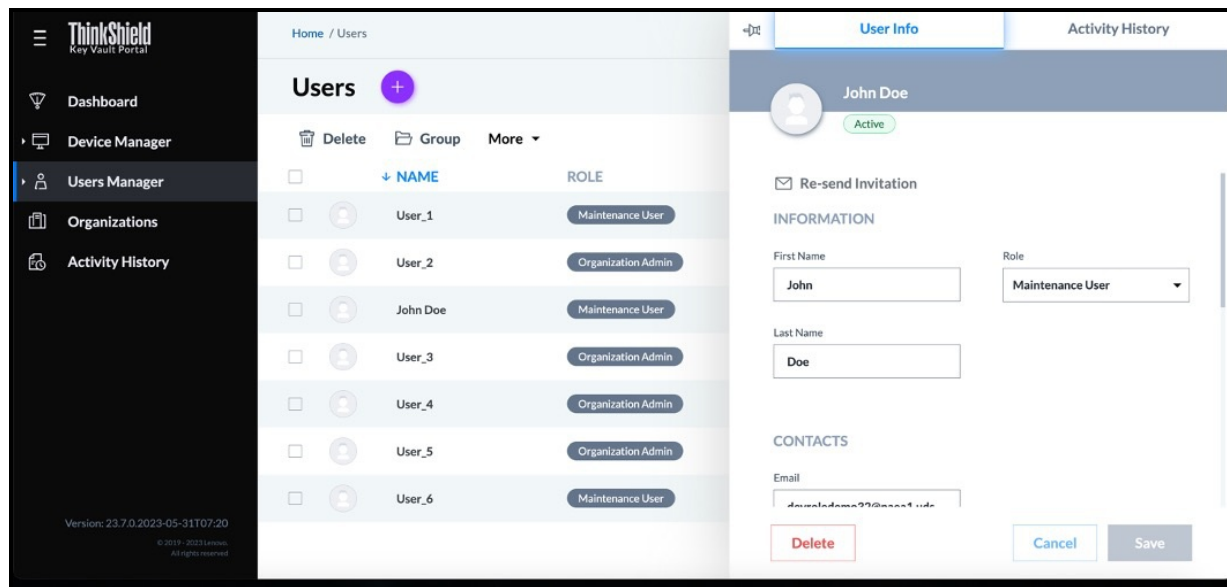


Figure 42. Displaying user information belongs to the organization

Manual claiming

When it is more appropriate to minimize activation effort by on-site personnel, the customer can also select automatic activation. Prior to automatic activation the administrator must manually claim each device. For this they need on-site user to provide them the Secure Activation Code.

The Secure Activation Code is physically located on the server:

- Printed on the pull-out information tab at the front of the server

- Printed on a sticker on the system board
- Printed on the activation flyer that ships with the server

If none of these is accessible, the administrator can also retrieve an activation code from ThinkShield Edge Mobile Management App or by using IPMI command to XCC. For details about using IPMI, see [Lenovo Support Tip HT10992](#).

The secure activation code is located either on the pull-out tab or on the system board, adjacent to the processor.

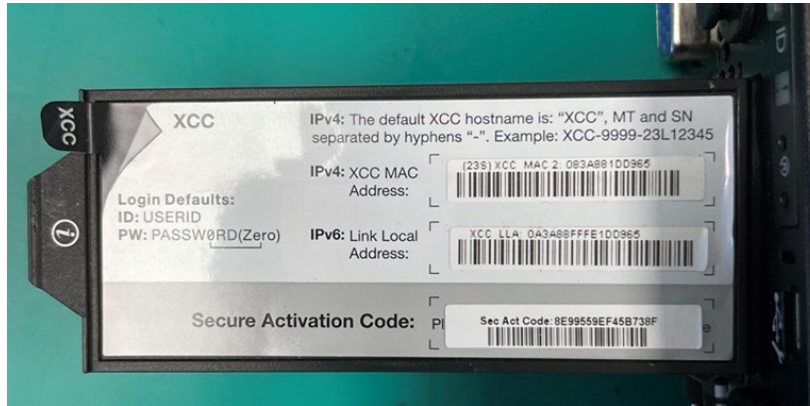


Figure 43. Secure Activation Code from the pull-out information tab

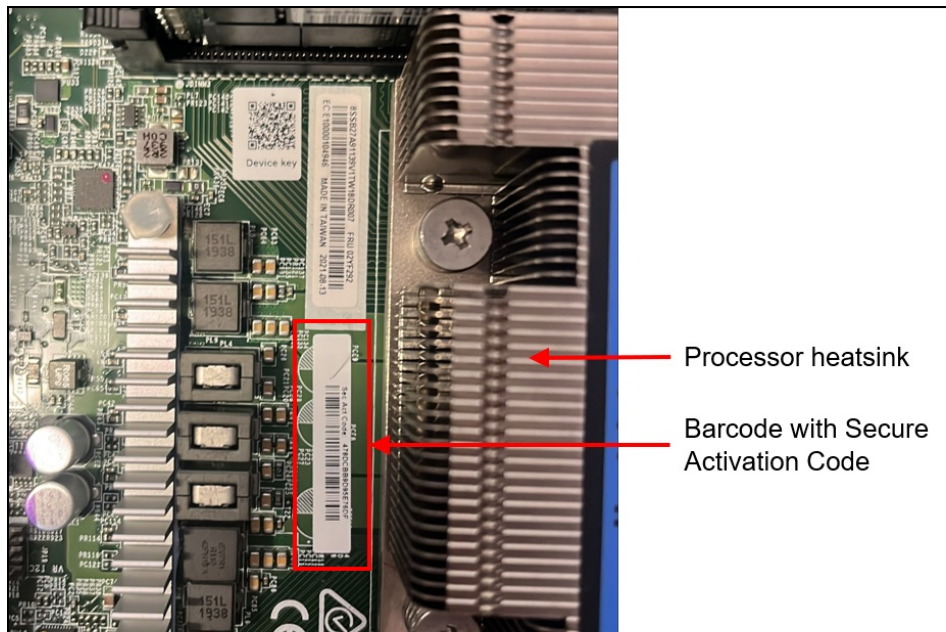


Figure 44. Secure Activation Code in bar code from the system board

The administrator will also need the machine type and serial number of the server. These are printed on a label on the server.

Enter the secure activation code, machine type, and serial number into the ThinkShield Key Vault Portal via **Device Manager > Devices > Claim**, as shown in the following figure, then click **Submit**.

Home / Devices

Claim a Device

All fields required except where noted otherwise.

MANUAL CLAIM BULK CLAIM

Manually claim a device by entering its Machine Type, Serial Number and Secure Activation Code.

Machine Type	Secure Activation Code
<input type="text" value="7DA9"/>	<input type="text" value="1DBC-F2E3-C6A2-E51C"/>
Serial Number	Name <i>optional</i>
<input type="text" value="AAAA24574"/>	<input type="text"/>

Figure 45. Claiming a ThinkEdge Server

Now select the new server and click the **Activate** button as shown in the following figure. The ThinkShield Key Vault Portal will update device status from Pending to Ready for Activation.

The last step is to connect the BMC Ethernet port of the ThinkEdge server to the Internet so it can communicate with the ThinkShield Key Vault portal, and then power on the server. The ThinkEdge server will communicate with ThinkShield Key Vault Portal, and the server will be activated automatically.

Tip: If the ThinkEdge server was powered on prior to connecting the BMC to the Internet you may need to power it off and back on again for activation to occur.

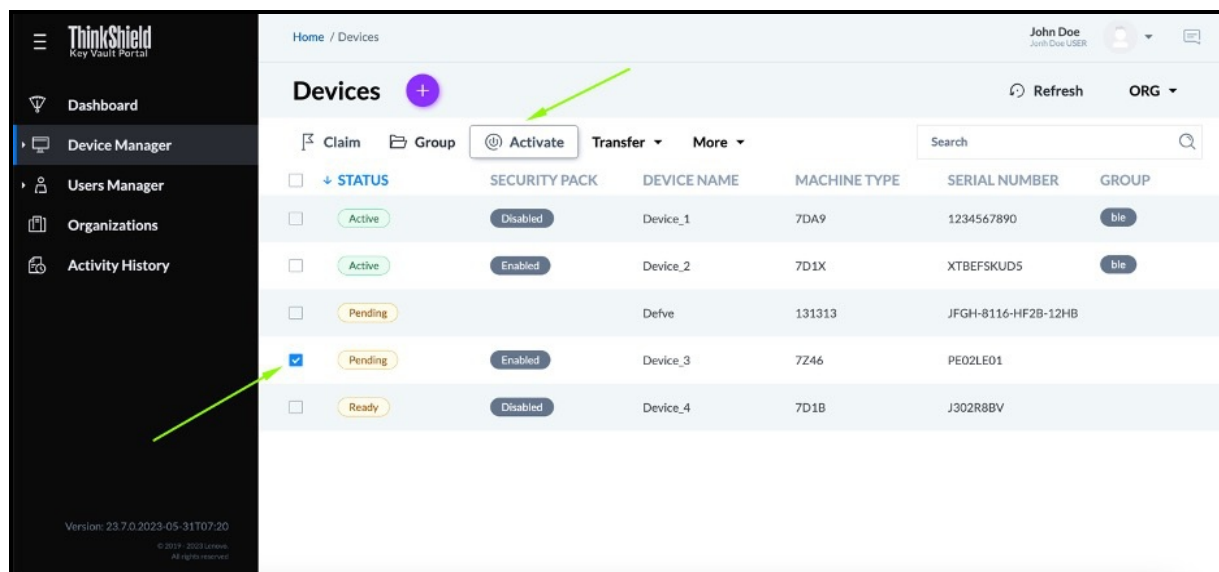


Figure 46. Activating a ThinkEdge Server

Manual activation

When the local admin in the edge location is unable to activate the ThinkEdge server via an Internet connection (automatic activation, or through the use of LXCE UpdateXpress or the ThinkShield Edge Mobile Management App), another approach is a manual method where the local admin manually enters the required information from XCC into ThinkShield portal.

With manual activation, the local admin uses XCC on the ThinkEdge server to obtain the challenge information. This information is then entered into the ThinkShield Portal, which then provides a response code. The local admin then enters the response information to XCC, which will activate the edge server. The exchange of challenge and response can be performed locally by a single person or remotely by an on-site person and a remote admin.

For more information, see the ThinkShield Key Vault Portal User Guide. The links to the user guide and troubleshooting guide are listed in the [Related links](#) section.

Bulk user registration and server claims

When the administrator needs to register multiple users at the same time or to claim multiple ThinkEdge servers at the same time, the administrator can enter the user information (e.g. name, email address, role) or server information (e.g. MT/SN, activation code) into a CSV file and upload that file to the ThinkShield Key Vault Portal.

For more information see the ThinkShield Key Vault Portal Web Application User Guide. The link for the guide is in the [Related links](#) section.

Transferring ownership

If a customer needs to transfer the ownership of a ThinkEdge server to another organization, the ThinkShield Key Vault Portal can be used to execute a secure device transfer. This method avoids the risk and effort of re-claiming ThinkEdge servers.

First, the sender selects the ThinkEdge servers they wish to transfer using the ThinkShield Key Vault Portal. Once selected, they initiate the transfer process. The ThinkShield Key Vault Portal will generate a CSV file containing the selected ThinkEdge server information which the sender downloads. When the sender downloads the file, the ThinkShield Key Vault Portal provides a passphrase which will expire in 24hours. Then the sender will share the CSV file and the passphrase securely to the receiver. The receiver then uploads the CSV file and provides the passphrase, the ThinkShield Key Vault portal verifies the passphrase and finally transfers ownership of ThinkEdge servers from the sender to the receiver.

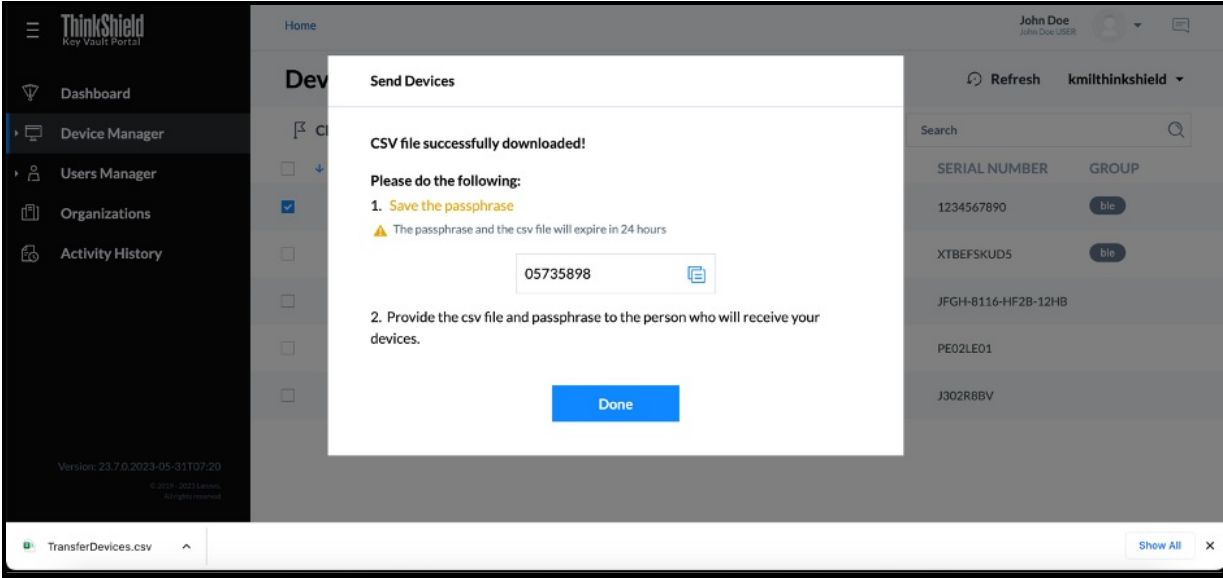


Figure 47. Transferring multiple ThinkEdge servers by CSV file with secure one-time password

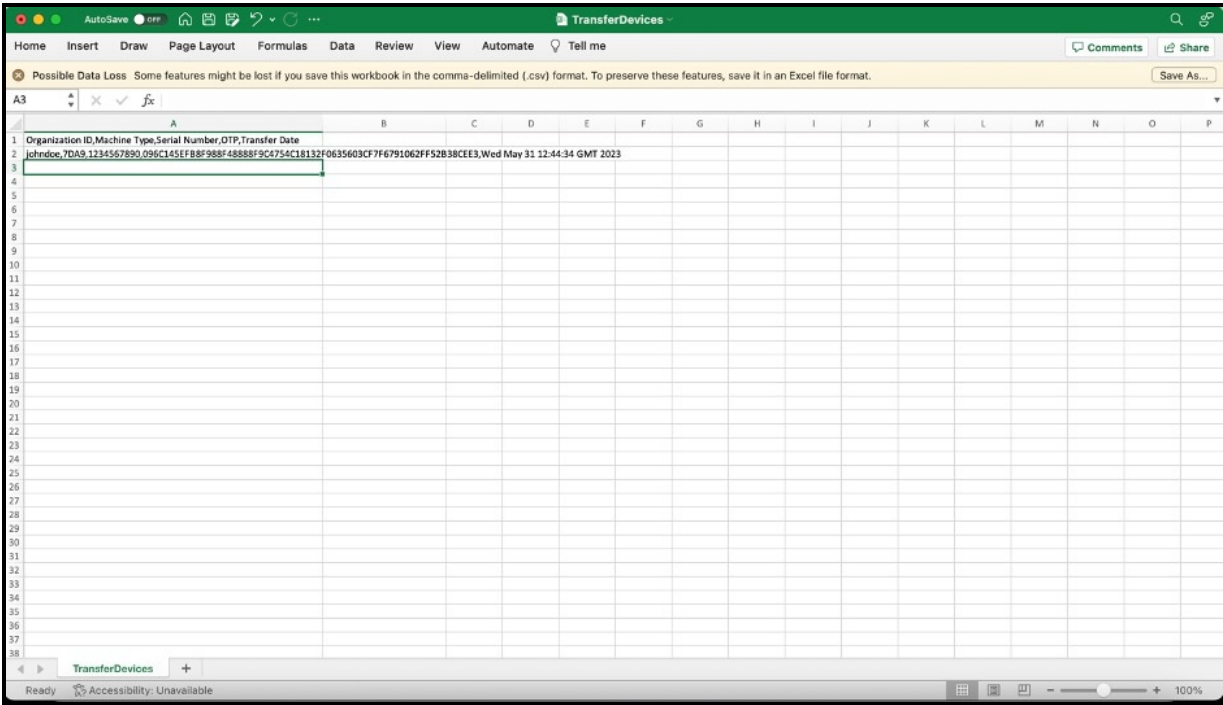


Figure 48. Device transfer CSV file example

Emergency XCC password reset

Firmware requirements: The Emergency XCC password reset feature has minimum firmware requirements as listed in the [Firmware versions](#) section.

When XClarity Controller based Lockdown Control is selected, XCC password becomes particularly important to protect your data in ThinkEdge servers. To protect the XCC password, it is also highly recommended to assign UEFI password. However, if both XCC and UEFI password are lost, the ThinkEdge server becomes inaccessible. In this case, emergency XCC password reset feature allows the user to regain the access by resetting XCC password. Emergency XCC password reset feature does not include the normal XCC password reset methods, which can be performed with authorized access to tools like XCC, UEFI, BoMC, OneCLI, etc. See the following information to learn the capability of emergency XCC password reset feature.

When SED encryption is enabled, if emergency XCC password reset is performed, the SED AK stored in the server will be cleared as the default action. Data stored on the SED will no longer be accessible unless the SED AK is restored. Backing up the SED AK is strongly advised to reduce the risk of data loss.

In order to perform emergency password reset, ThinkShield Key Vault Portal and Edge Mobile Management Application need to be prepared as the same process of ThinkShield Key Vault Portal Control. After setting up the organization, maintenance role user should be prepared. When the maintenance user attaches Edge Mobile Management Application to the ThinkEdge server, the maintenance user can access emergency XCC password reset from the menu as below.

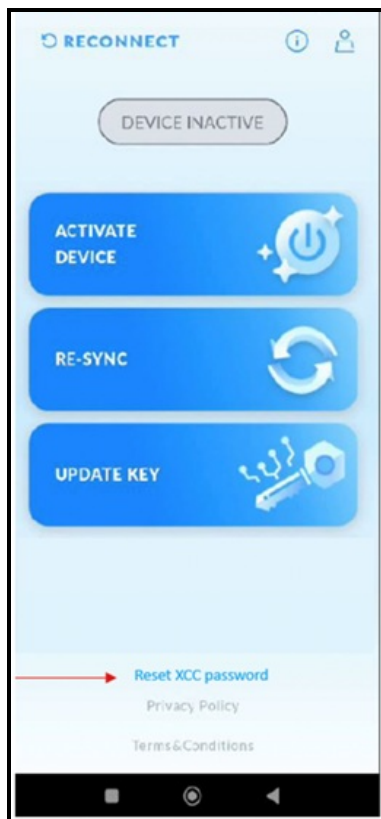


Figure 49. LXC - XCC password reset

Serviceability considerations

To support the security design, each ThinkEdge server has a unique security key stored in hardware, and the ThinkShield Key Vault Portal tracks the matching device key information for each device. When the Lenovo service representative replaces a motherboard in a ThinkEdge server, the matching device key must be updated in the ThinkShield Key Vault Port. The Lenovo service representative will make the update after service action. An on-site user who has the Maintenance User role can also make the update if needed.

The new device key is printed on the motherboard and provided by QR code, and the portal has the update key function only available for the Maintenance User Role, as referenced in the table of user roles in the [ThinkShield Key Vault Portal](#) section.

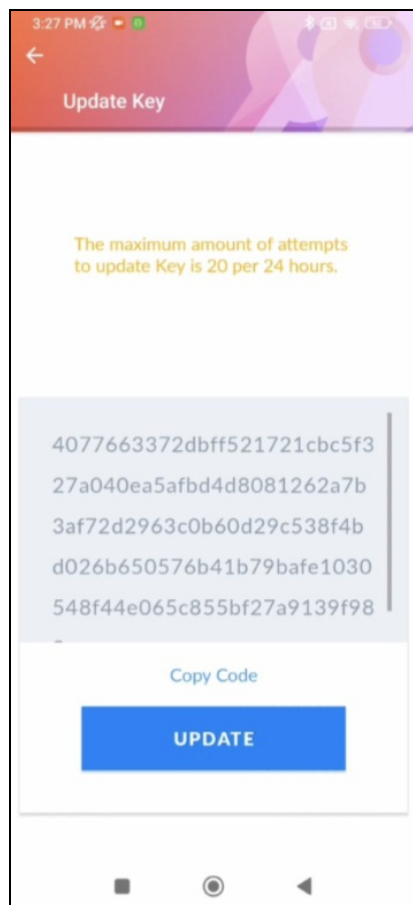


Figure 50. Mobile app updating device key by Lenovo service representative or Maintenance role user after replacing ThinkEdge system motherboard

Related links

See the following links for additional information:

- LXCE UpdateXpress User's Guide
http://sysmgt.lenovofiles.com/help/topic/ux_essentials/ux_book.pdf
- LXCE UpdateXpress home page
<https://support.lenovo.com/us/en/solutions/ht115051-lenovo-xclarity-essentials-updatexpress>
- ThinkShield Key Vault Portal
<https://portal.thinkshield.lenovo.com>
- ThinkShield Key Vault Portal Web Application User Guide
https://download.lenovo.com/servers_pdf/thinkshield-web-application-user-guide-v2.pdf
- ThinkShield Edge Mobile Management Application User Guide
https://download.lenovo.com/servers_pdf/thinkshield-mobile-application-user-guide-v6.pdf
- ThinkShield Key Vault Portal Web Application Troubleshooting Guide
https://download.lenovo.com/servers_pdf/thinkshield-web-application-troubleshooting-guide-v2.pdf
- ThinkShield Edge Mobile Management Application Troubleshooting Guide
https://download.lenovo.com/servers_pdf/thinkshield-mobile-application-troubleshooting-guide-v2.pdf
- SE450 User Guide
<https://pubs.lenovo.com/se450/>
- SE350 V2 User Guide
<https://pubs.lenovo.com/se350-v2/>
- SE360 V2 User Guide
<https://pubs.lenovo.com/se360-v2/>
- SE455 V3 User Guide
<https://pubs.lenovo.com/se455-v3/>
- SE100 User Guide
<https://pubs.lenovo.com/se100/>
- Lenovo XClarity Controller (XCC) User Guide
<https://pubs.lenovo.com/lxcc-overview/>
- UEFI User Guide
<https://pubs.lenovo.com/uefi-overview/>
- Lenovo XClarity Administrator (LXCA) User Guide
https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_overview.html?cp=1_0

Authors

Makoto Ono is a Distinguished Engineer of Lenovo ISG Edge Computing, and a System Architect of ThinkEdge server products.

Mike Demeter is a Senior Product Security Architect with the Lenovo Infrastructure Solutions Group's Product Security Office. His product security background expands over 20 years as a security architect and software engineer. His focus is on ensuring that security is built into data center products throughout the entire secure development lifecycle. He has been the product security architect responsible for the Lenovo ISG ThinkEdge products since their inception.

Related product families

Product families related to this document are the following:

- [ThinkEdge SE100 Server](#)
- [ThinkEdge SE350 V2 Server](#)
- [ThinkEdge SE360 V2 Server](#)
- [ThinkEdge SE450 Edge Server](#)
- [ThinkEdge SE455 V3 Server](#)

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2025. All rights reserved.

This document, LP2189, was created or updated on May 23, 2025.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
<https://lenovopress.lenovo.com/LP2189>
- Send your comments in an e-mail to:
comments@lenovopress.com

This document is available online at <https://lenovopress.lenovo.com/LP2189>.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at <https://www.lenovo.com/us/en/legal/copytrade/>.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®

ThinkEdge®

ThinkShield®

ThinkSystem®

XClarity®

The following terms are trademarks of other companies:

Active Directory® and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.