ThinkEdge Security for SE350

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 processor. 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.

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 device is?

Initial steps

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.

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.

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 – https://apps.thinkshield.lenovo.com).

- 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.

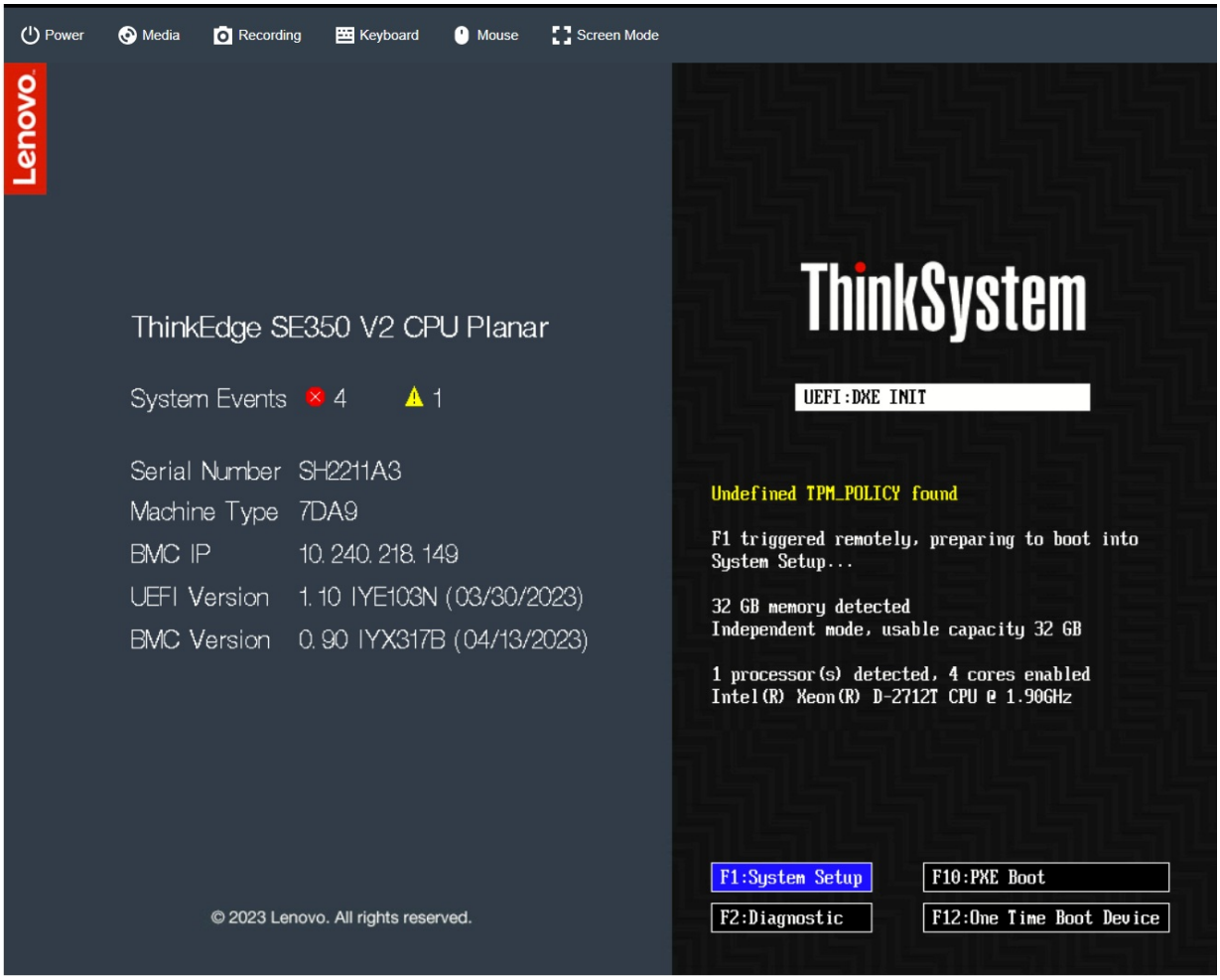

Figure 2. Activated ThinkEdge Server UEFI POST Screen

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

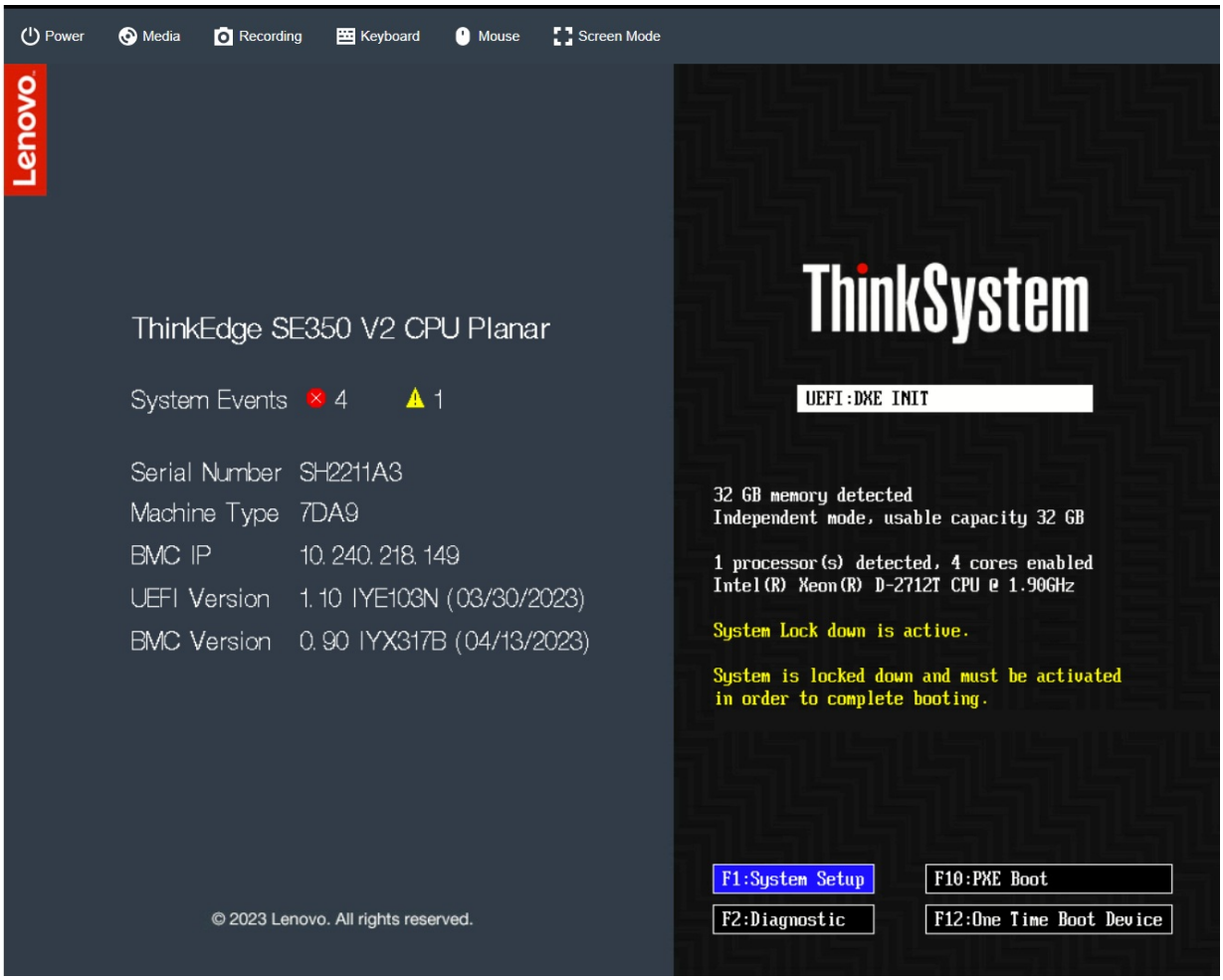

Figure 3. ThinkEdge Server UEFI POST Screen Waiting Activation

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

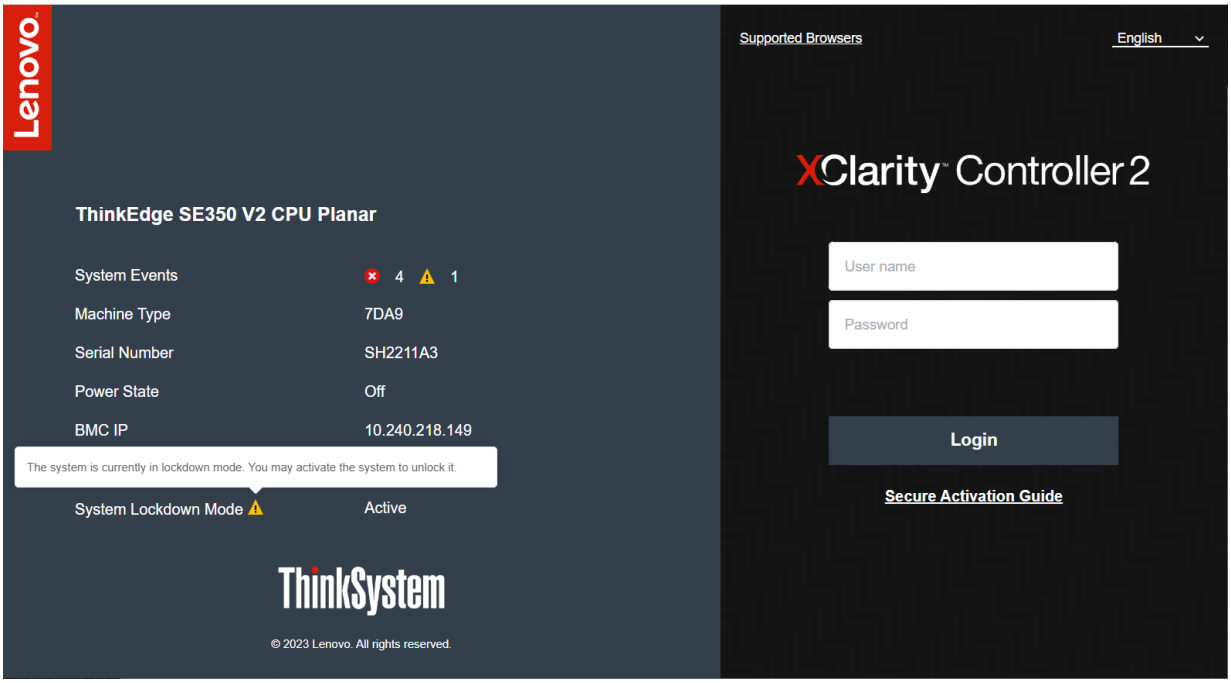

Figure 4. Activated ThinkEdge Server XCC Login Screen

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

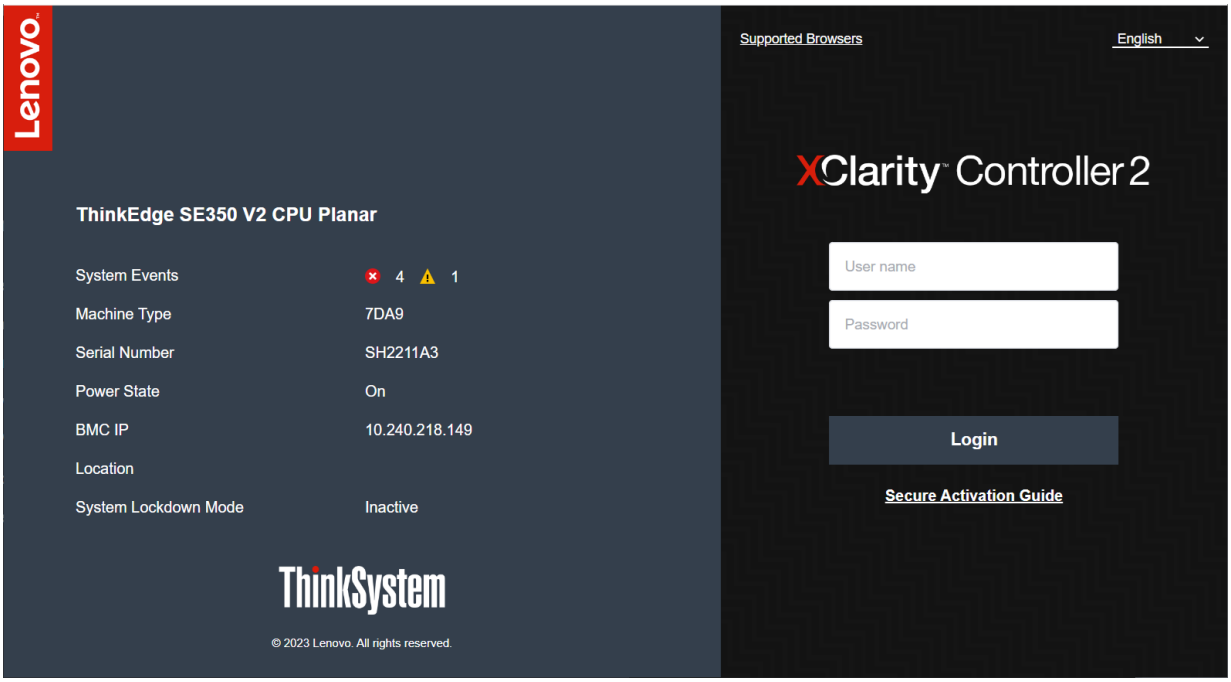

Figure 5. ThinkEdge Server XCC Login Screen Waiting Activation

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

- LED is On = Security Pack is enabled, and server is activated
- LED is Blinking = Security Pack is enabled but server is not yet activated
- LED is Off = Security Pack is disabled or de-populated setup (SE450)

Tip: The SE350 does not have an Activation LED.

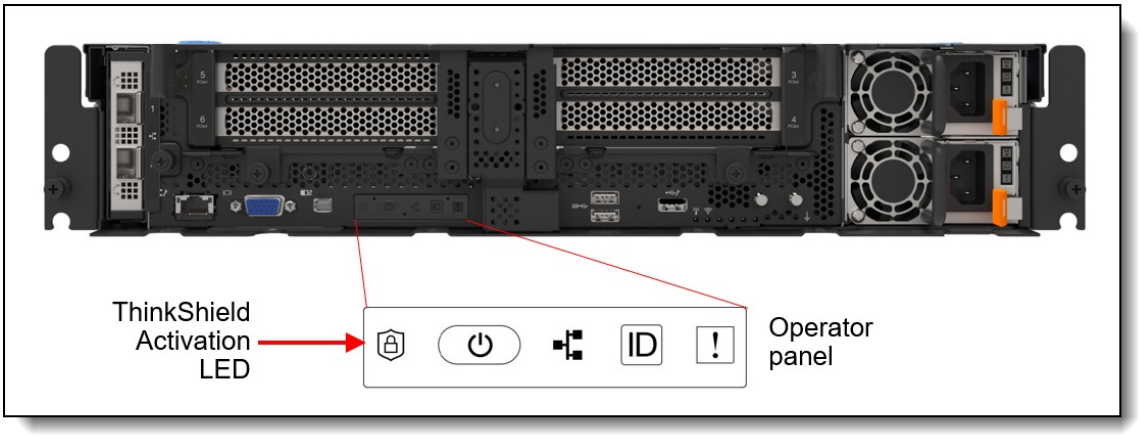

Figure 6. SE450 ThinkShield Activation LED

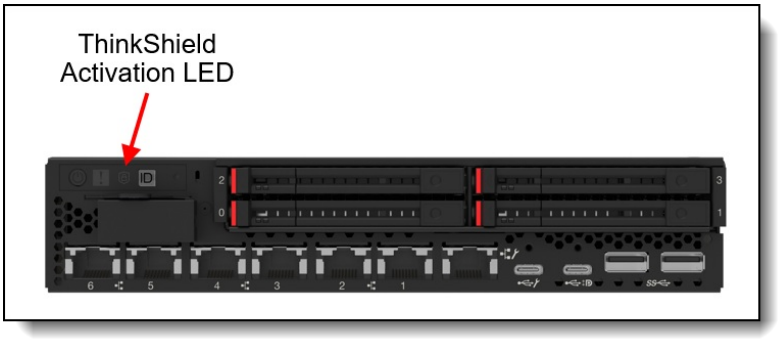

Figure 7. SE350 V2 ThinkShield Activation LED

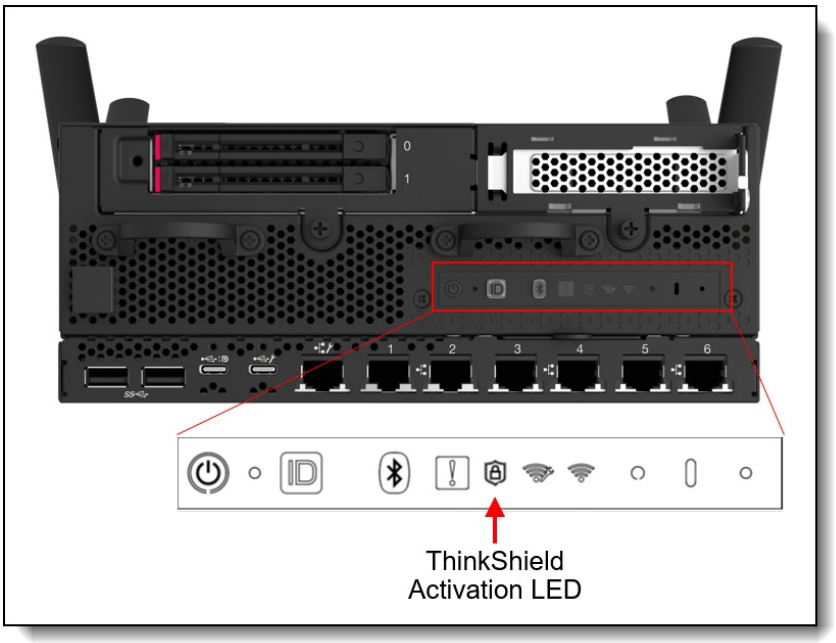

Figure 8. SE360 V2 ThinkShield Activation LED (Front)

Security Pack

Security is very important at the edge and Lenovo ThinkEdge servers are designed to provide new security features as described above. However, some customers may wish to deploy ThinkEdge servers in secured environment where strong hardware security may not be required.

To match customer's security requirements, ThinkEdge servers provide the following Security Pack selections at the time of order:

- Security Pack Enabled:

  All ThinkEdge unique security features are enabled by default. These include automatic SED AK management and automatic SED lock up by tamper events. These features are enabled as part of the mandatory self-service device onboarding process (user registration, device claiming, device activation) to unlock ThinkEdge server.

- Security Pack Disabled:

  All ThinkEdge security features are disabled so that self-service on boarding process is not required. Selected ThinkEdge server can support manual SED AK installation.

- Security Pack Depopulated:

  All ThinkEdge unique security features are disabled so that self-service on boarding process is not required. Manual SED AK installation is also disabled.

Customers can make the following selections:

- SE350:
  - Security Pack Enabled
  - Security Pack Disabled
- SE450:
  - Security Pack Enabled
  - Security Pack Depopulated
- SE350 V2 and SE360 V2:
  - Security Pack Disabled
  - Security Pack Enabled (planned for future release)

Security Pack is one-time selection for SE350 and SE450 at order, and customer will not be able to change the selection after manufacturing.

The following figure shows how to enable the Security Pack in the SE350 and time of order, using the DCSC configurator.

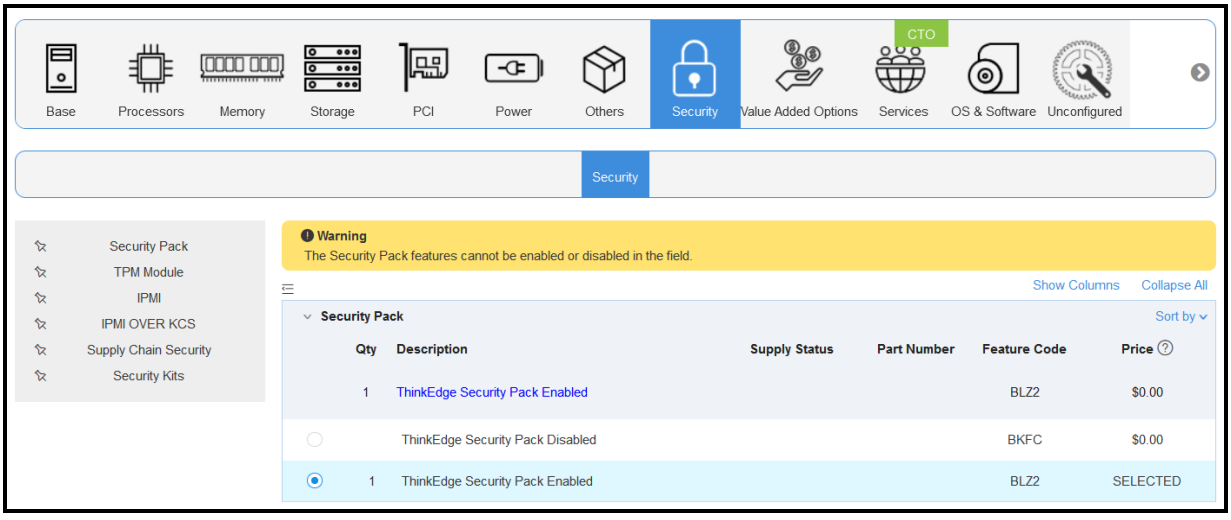

Figure 9. DCSC - SE350 order with Security Pack Enabled

The following figure shows how to depopulate the Security Pack in the SE450 and time of order, using the DCSC configurator.

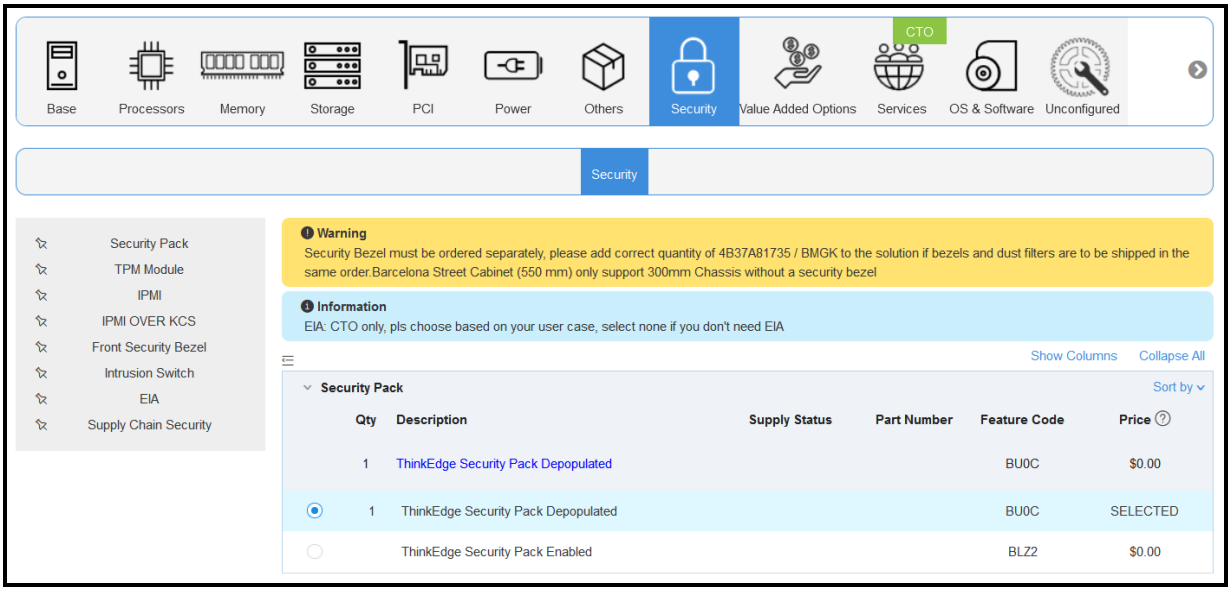

Figure 10. DCSC - SE450 order with Security Pack Depopulated

Note: Once Security Pack is enabled on a server it is not possible to disable it.

ThinkShield Key Vault Portal

The ThinkShield Key Vault Portal is a web application that is designed to manage organizations, users, and devices.

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.

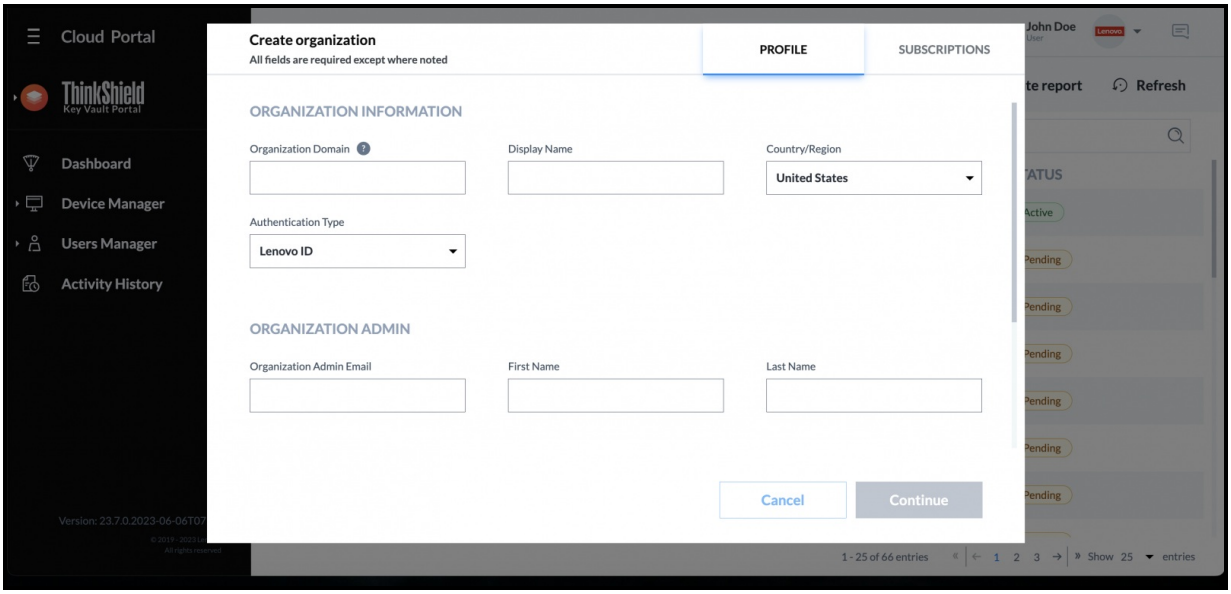

Figure 11. Creating new organization using ThinkShield Key Vault Portal

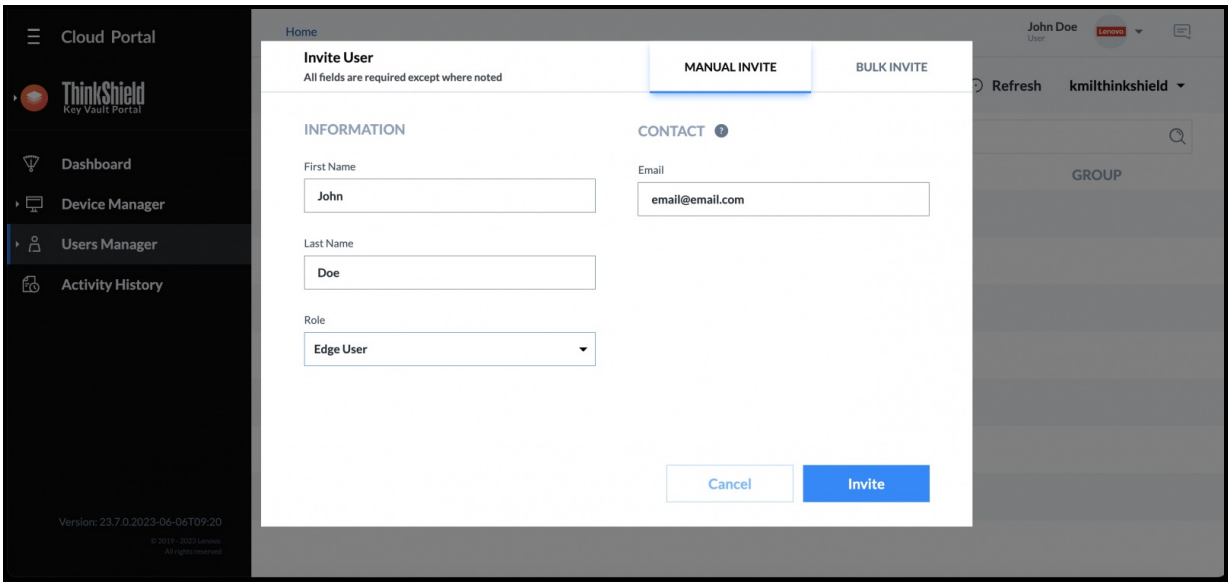

Figure 12. Adding new user using ThinkShield Key Vault Portal

After creating a new organization, the administrator can define role-based access control for users who need access to their ThinkEdge servers. It is very 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 1. 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	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.

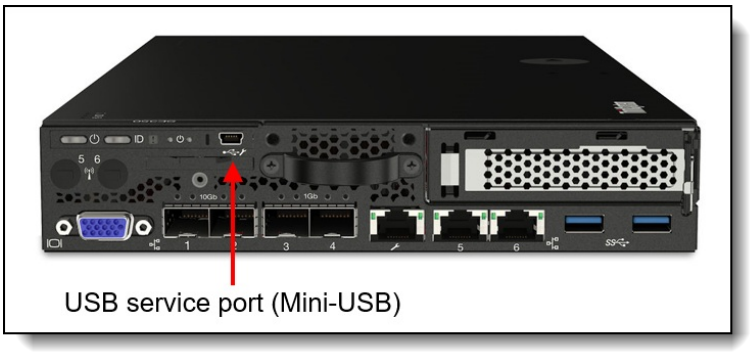

Figure 13. SE350 dedicated service mini-USB port

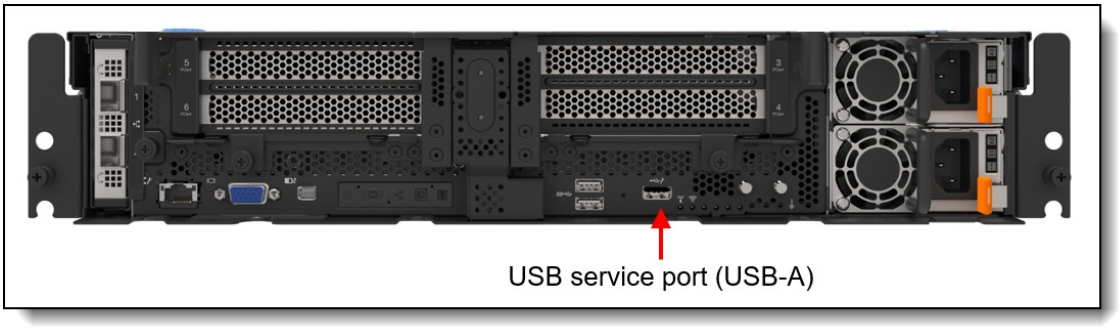

Figure 14. SE450 dedicated service USB Type-A port

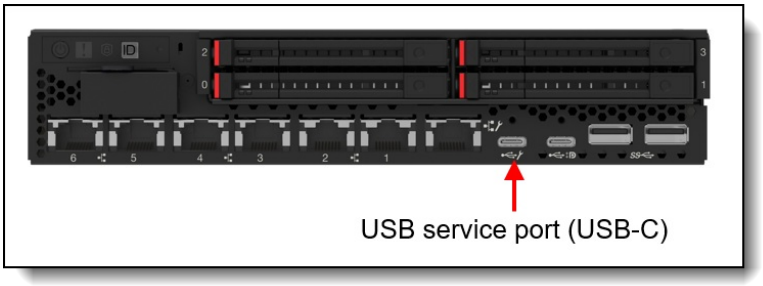

Figure 15. SE350 V2 dedicated service USB Type-C port

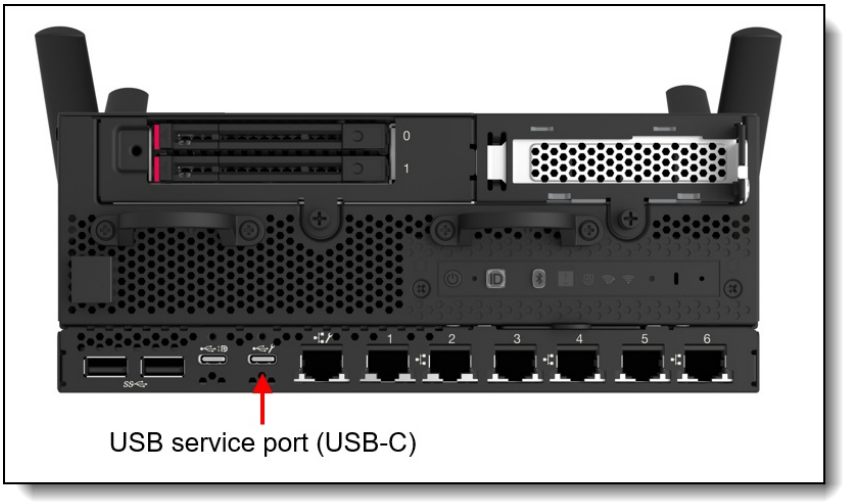

Figure 16. SE360 V2 dedicated service USB Type-C port

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.

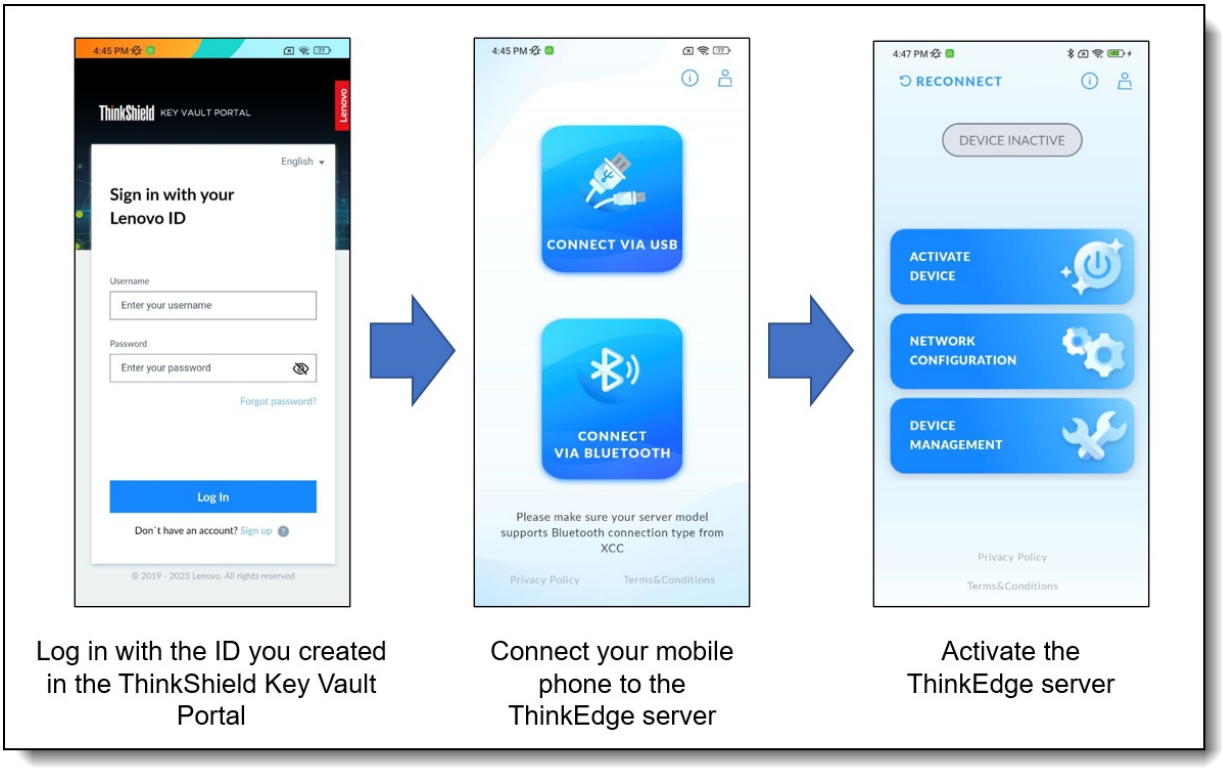

Figure 17. Activation flow using the ThinkShield Edge Mobile Management App

Activation using LXCE UpdateXpress

The on-site user can activate a ThinkEdge SE450 server by using Lenovo XClarity Essentials UpdateXpress (LXCE UpdateXpress) running on an administrator's laptop running Windows 10 or Windows 11.

ThinkEdge SE450 only: LXCE UpdateXpress can currently only be used to claim and activate ThinkEdge SE450. LXCE UpdateXpress does not support the SE350. LXCE UpdateXpress will be able to be used to claim and activate ThinkEdge SE350 V2 and SE360 V2 once Security Pack Enabled is supported on those servers.

LXCE UpdateXpress can be downloaded from the UpdateXpress web page:
https://support.lenovo.com/us/en/solutions/ht115051-lenovo-xclarity-essentials-updatexpress

To activate ThinkEdge server with LXCE UpdateXpress, connect your laptop to your 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.

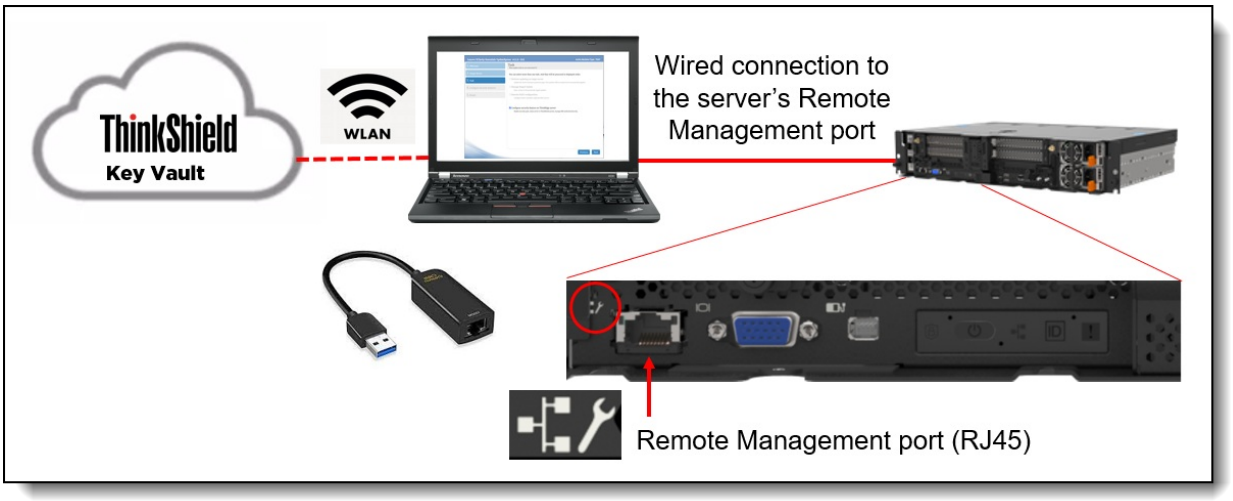

Figure 18. Connecting LXCE UpdateXpress to the ThinkEdge server

As part of activation using LXCE Update Express, users must first be added to the organization owning the server with Edge User permission.

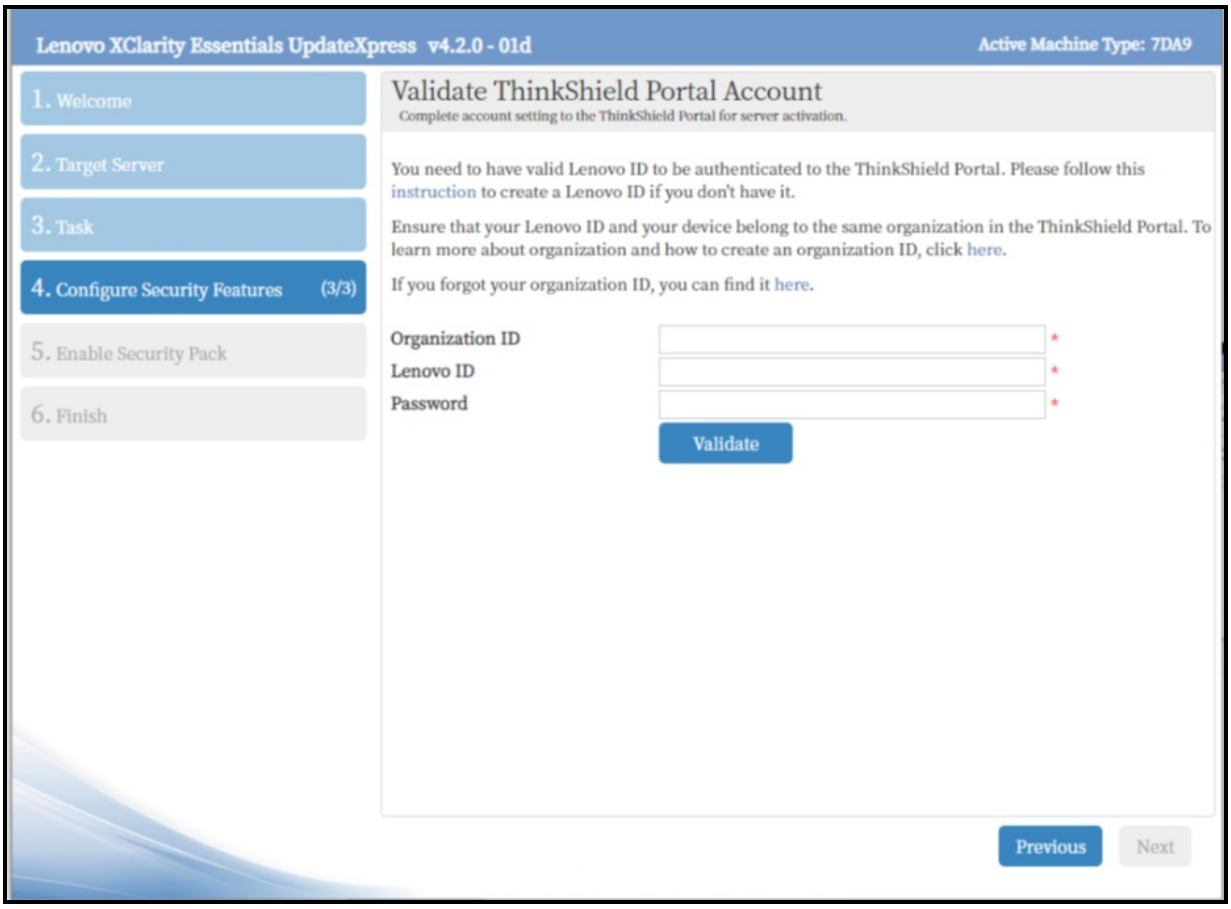

Figure 19. Validate ThinkShield Key Vault portal Account

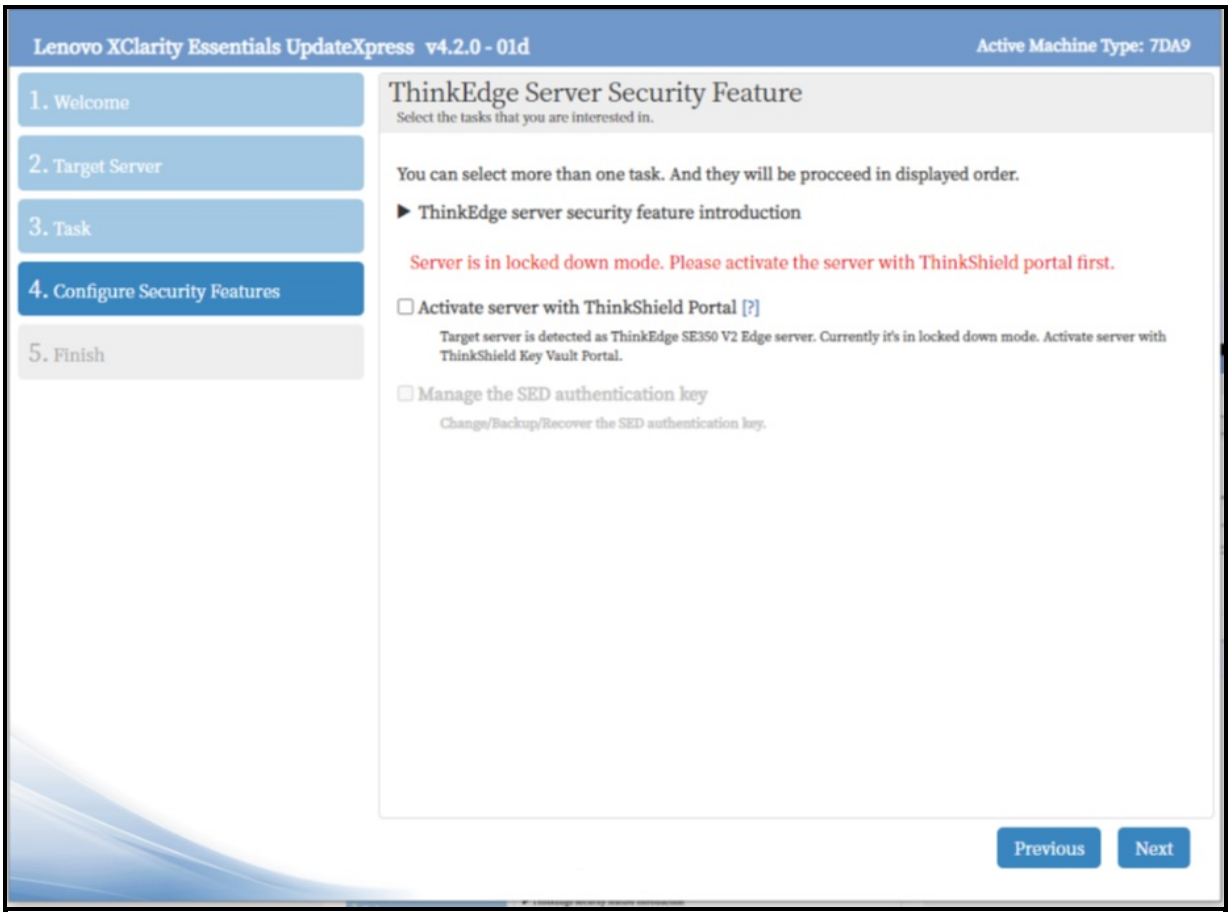

Figure 20. Activate ThinkEdge Server with LXCE UpdateXpress

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:

- SE350: Either of these, depending on which is installed:
  - ThinkSystem M.2 Enablement Kit
  - ThinkSystem M.2 Mirroring Enablement Kit
- 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

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.

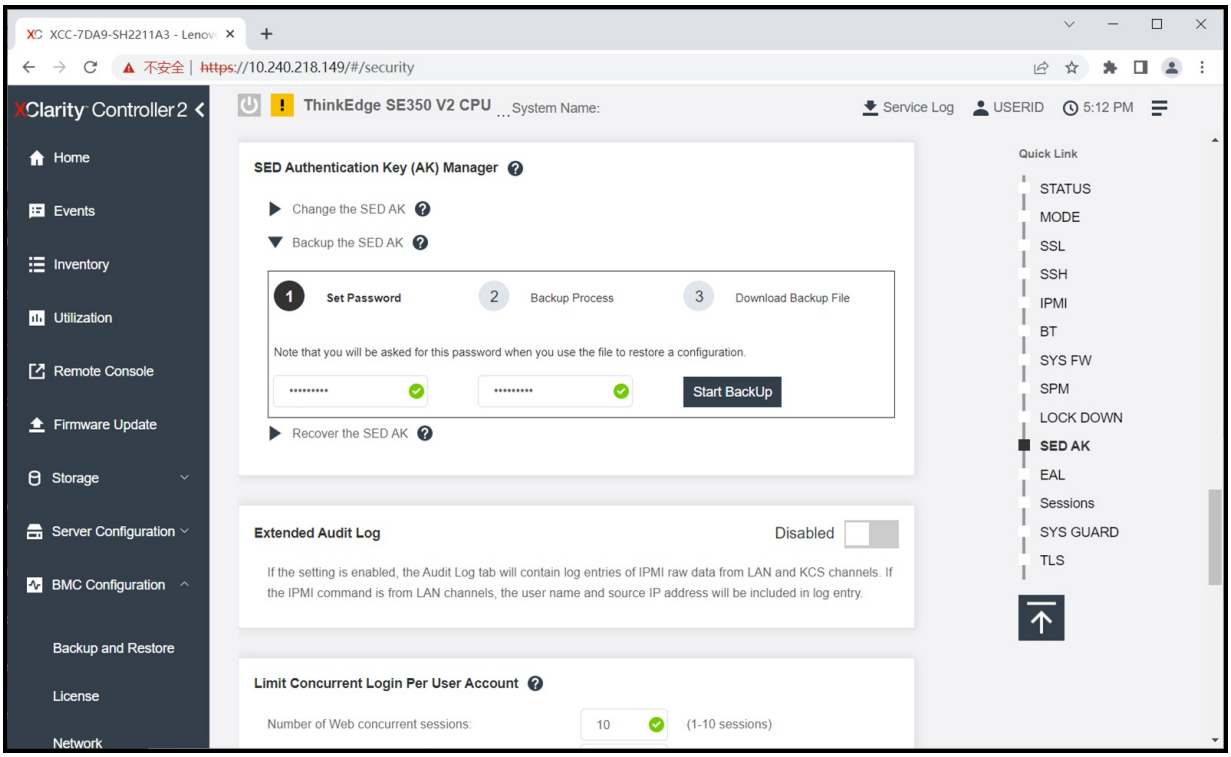

Figure 21. Backing up the SED Authentication Key using XCC

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.

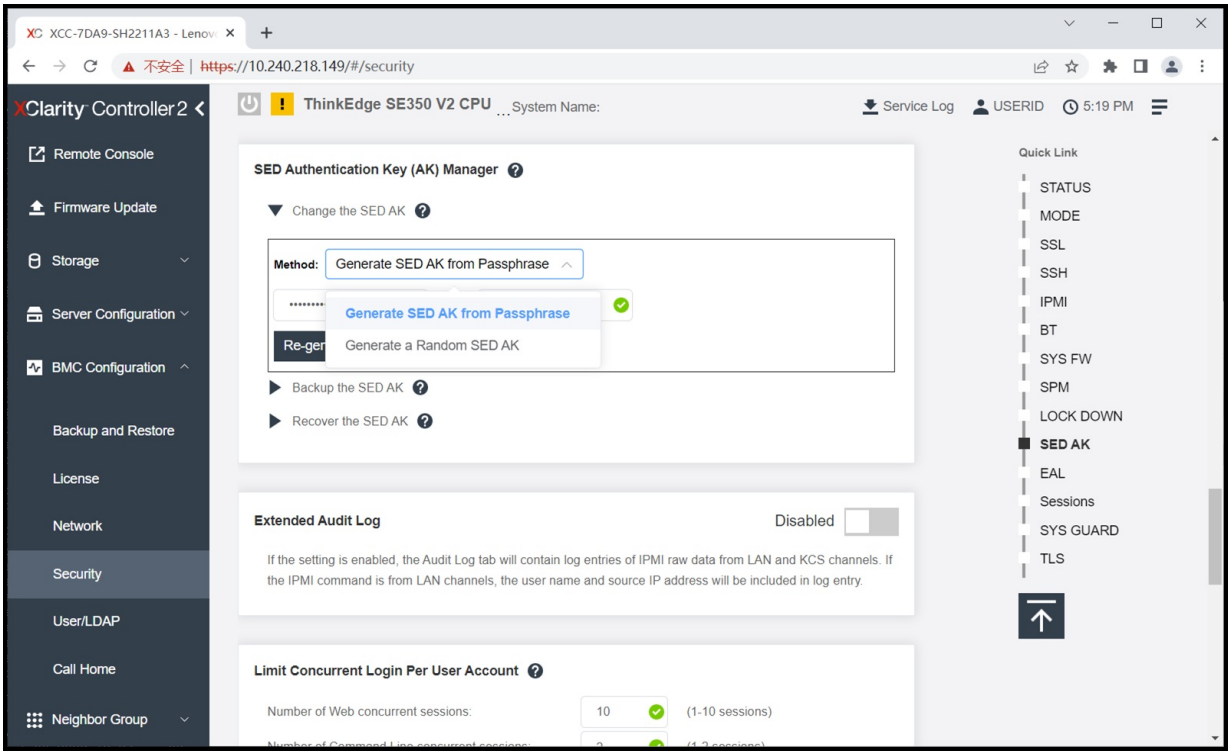

Figure 22. Changing SED AK to a Passphrase using XCC

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.

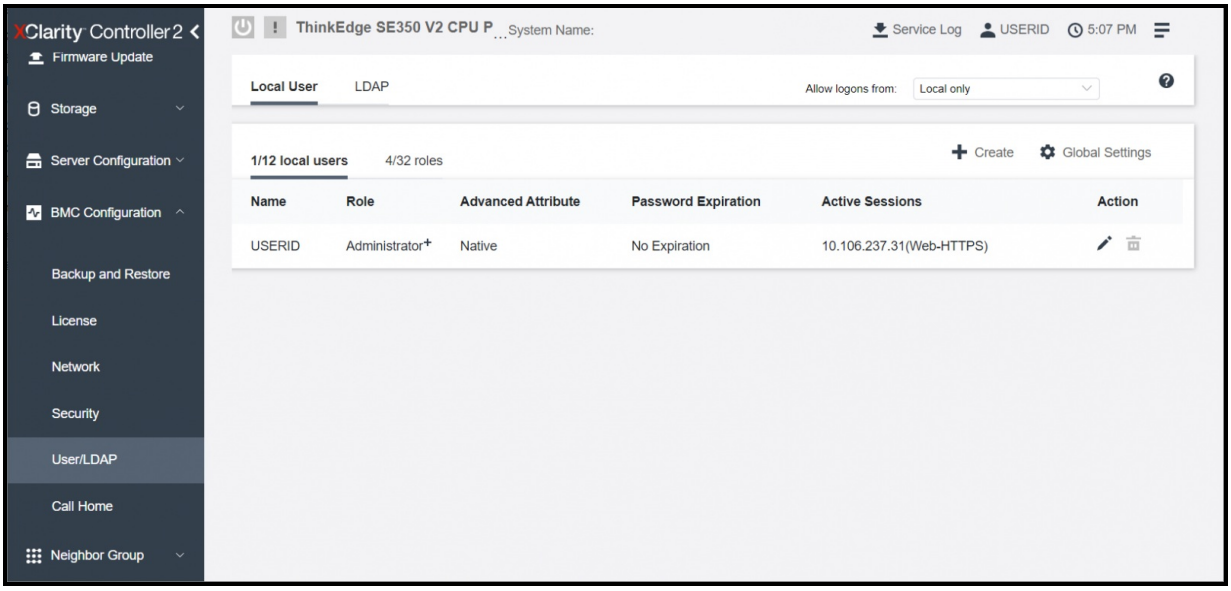

Figure 23. Default Administrator+ privilege user ID registered in ThinkEdge Servers

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

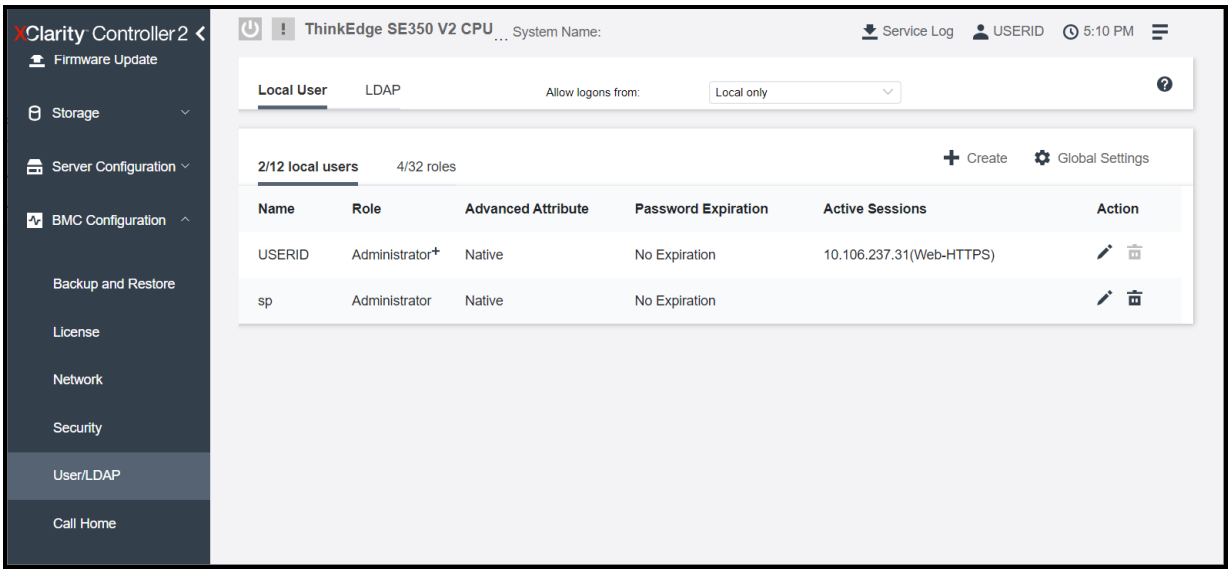

Figure 24. Administrator and Administrator+ ID registered in ThinkEdge Servers

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

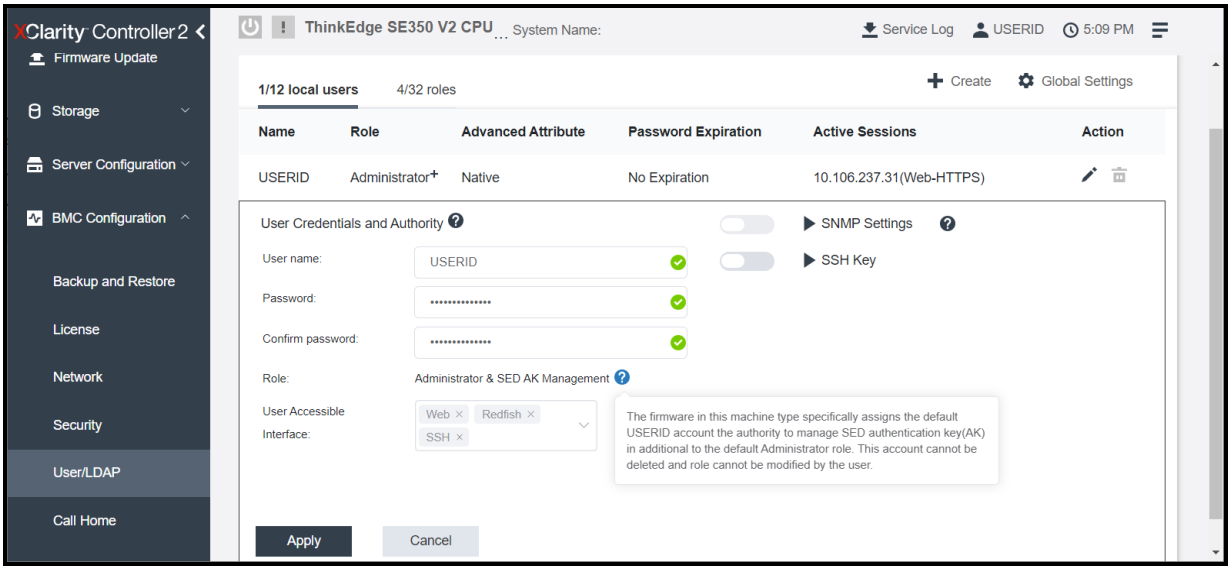

Figure 25. Administrator+ ID description from XCC GUI

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:

- SE350: Intrusion sensor, motion detection sensor
- SE450: Intrusion sensor
- SE350 V2: Intrusion sensor, advanced motion detection sensor
- SE360 V2: Intrusion sensor, advanced motion detection 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 supports a motion detection sensor, which can detect when the SE350 receives a motion event defined by the orientation and magnitude of the movement. 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, 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 and SE350 V2) or when the chassis is key locked (SE360 V2).

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

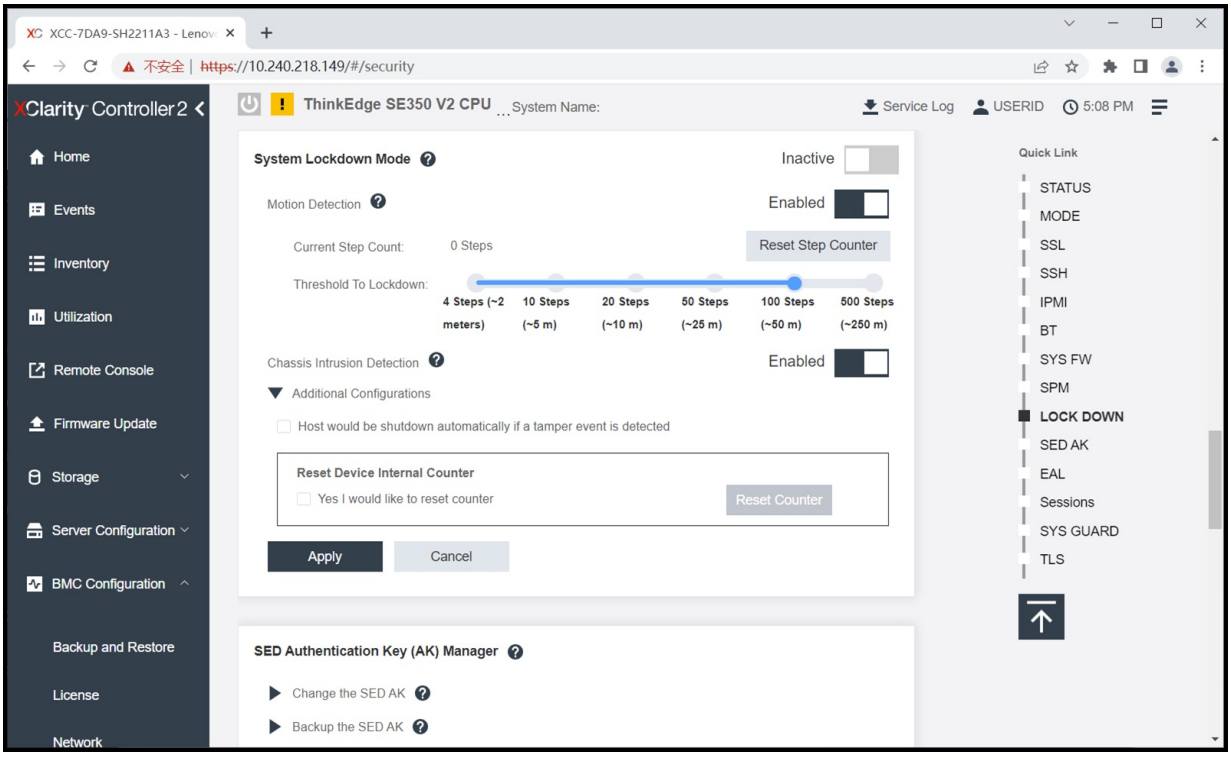

Figure 26. SE360 V2 Lockdown sensor management XCC GUI

Additional functions with LXCE UpdateXpress

In addition to claiming and activating ThinkEdge servers, LXCE UpdateXpress can also:

- Enable Security Pack (if not already enabled from the factory) (SE350 V2 and SE360 V2 only)
- Manage (change, backup, and restore) SED authentication keys after security pack is enabled (requires Admin+ user privileges in XCC)

For the SE350 V2 and SE360 V2, an upcoming release of Lenovo XClarity Essentials UpdateXpress will provide a new feature to convert a system from Security Pack from Disabled to Security Pack Enabled. 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 Security Pack is enabled on a server it is not possible to disable it.

These functions are accessed in UpdateXpress as shown in the following figure.

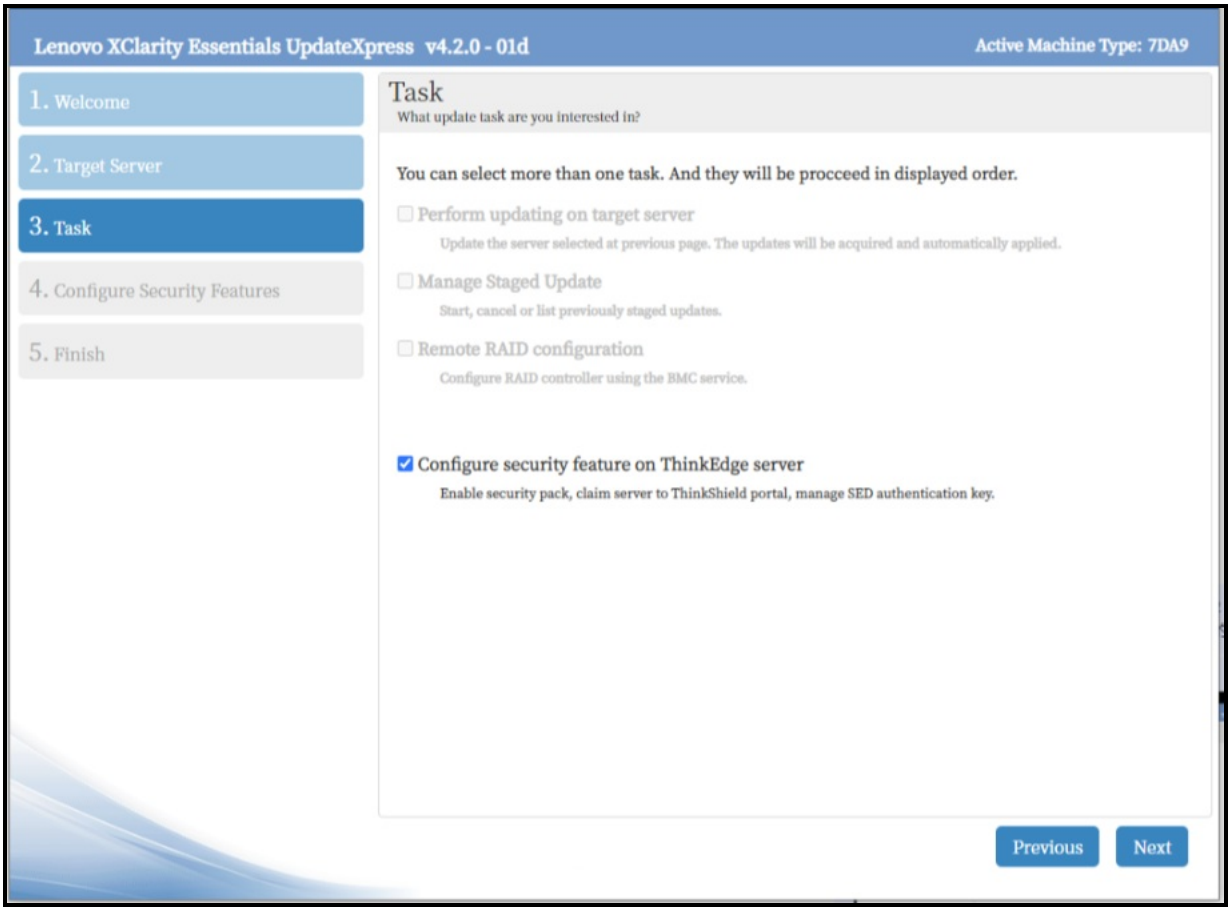

Figure 27. LXCE UpdateXpress Task menu

The following figure shows SED key management using LXCE UpdateXpress.

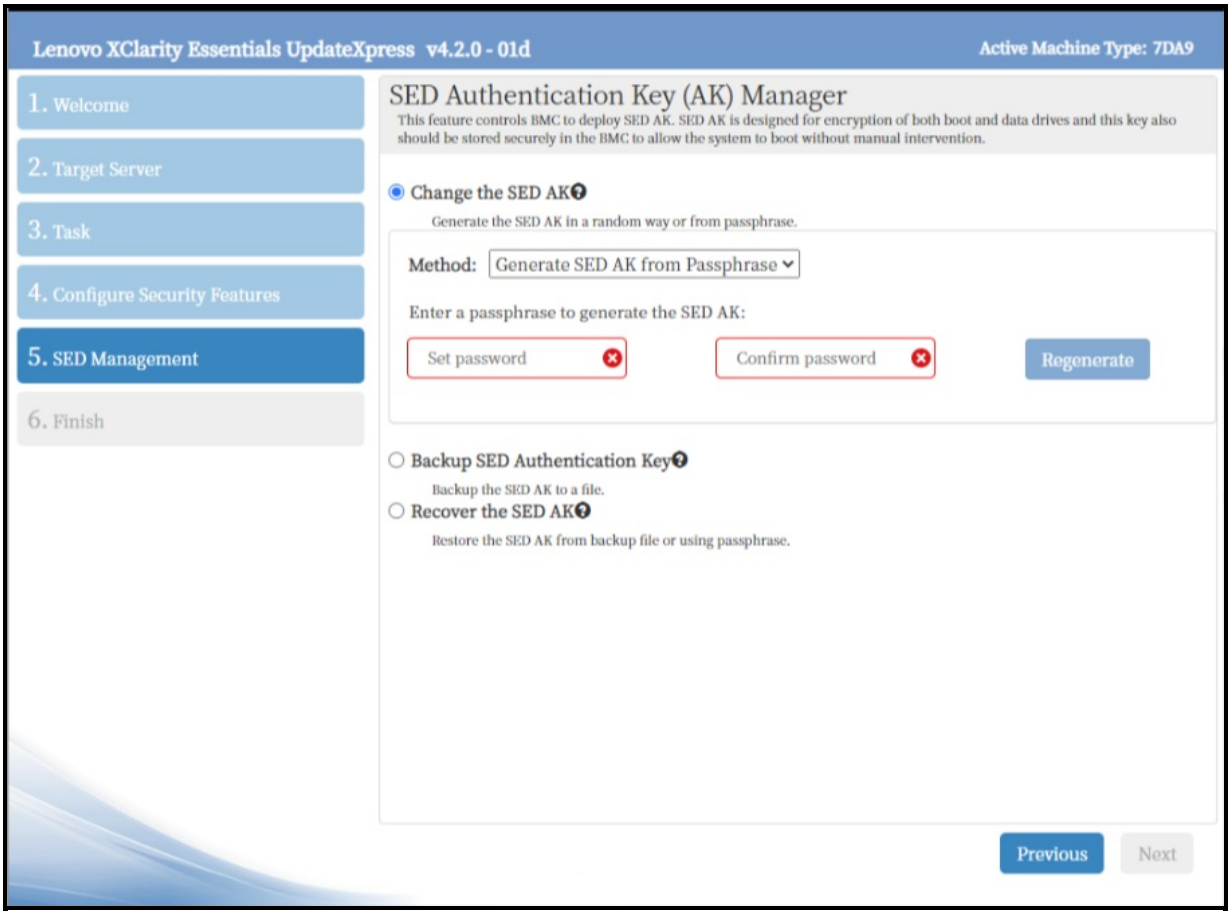

Figure 28. LXCE UpdateXpress SED Authentication Key Management

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

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.

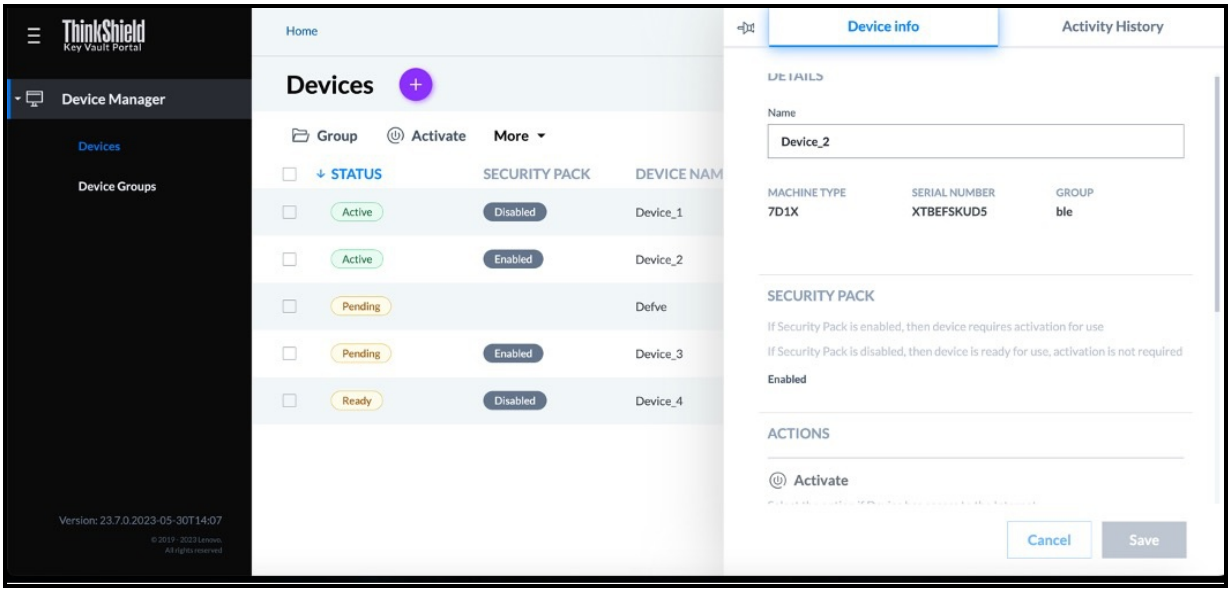

Figure 29. Displaying ThinkEdge server information under the organization

Viewing all users

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

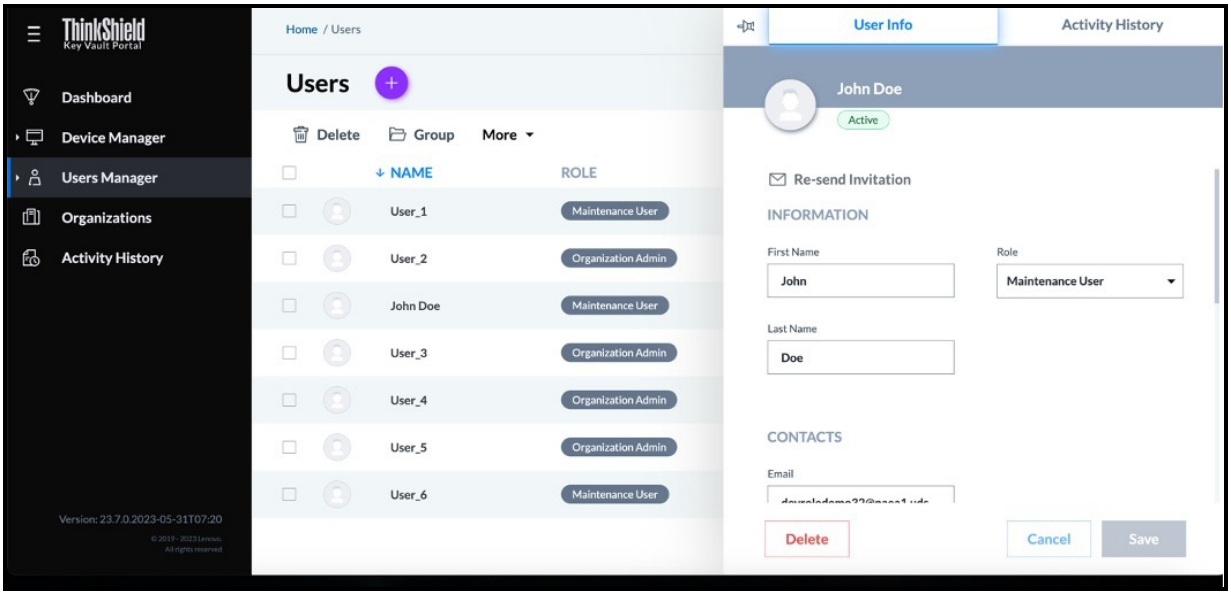

Figure 30. Displaying user information belongs to the organization

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.

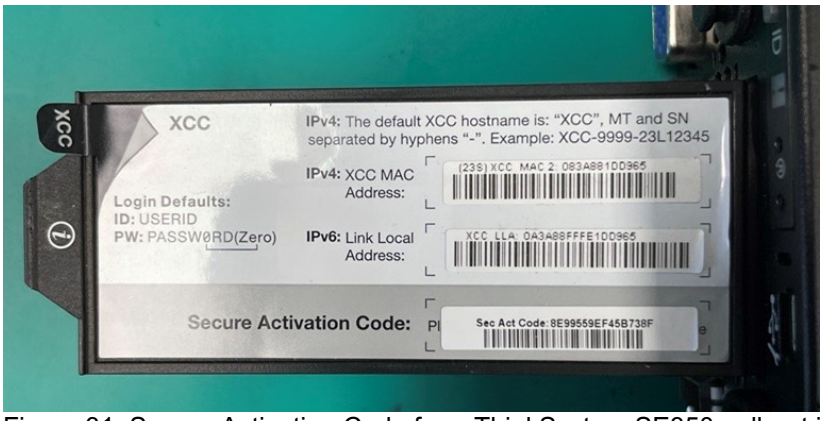

Figure 31. Secure Activation Code from ThinkSystem SE350 pull-out information tab

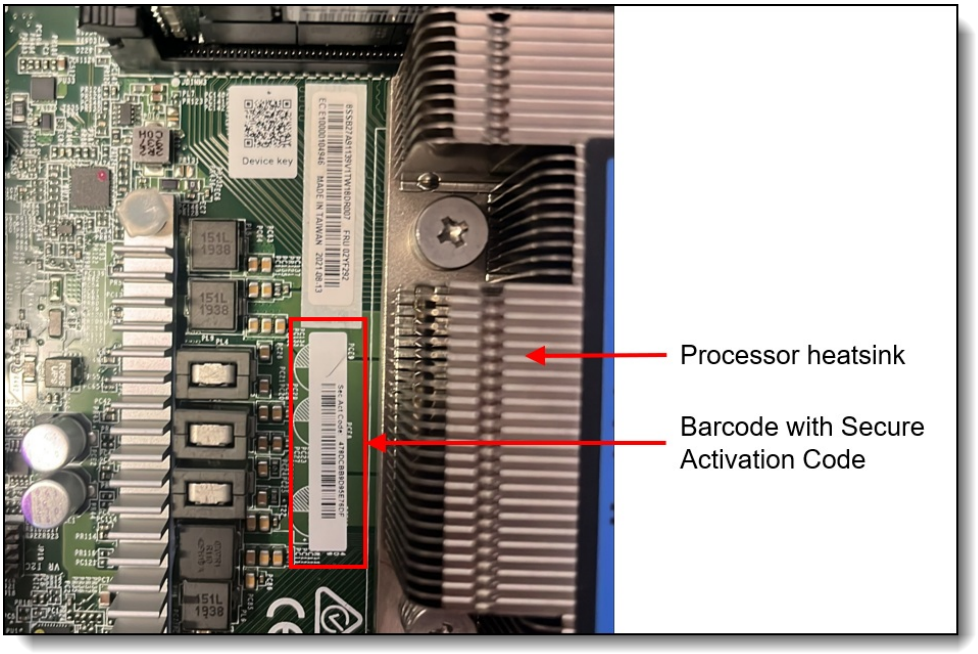

Figure 32. Secure Activation Code in bar code from ThinkSystem SE350 system board (near CPU and fan cage)

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**.

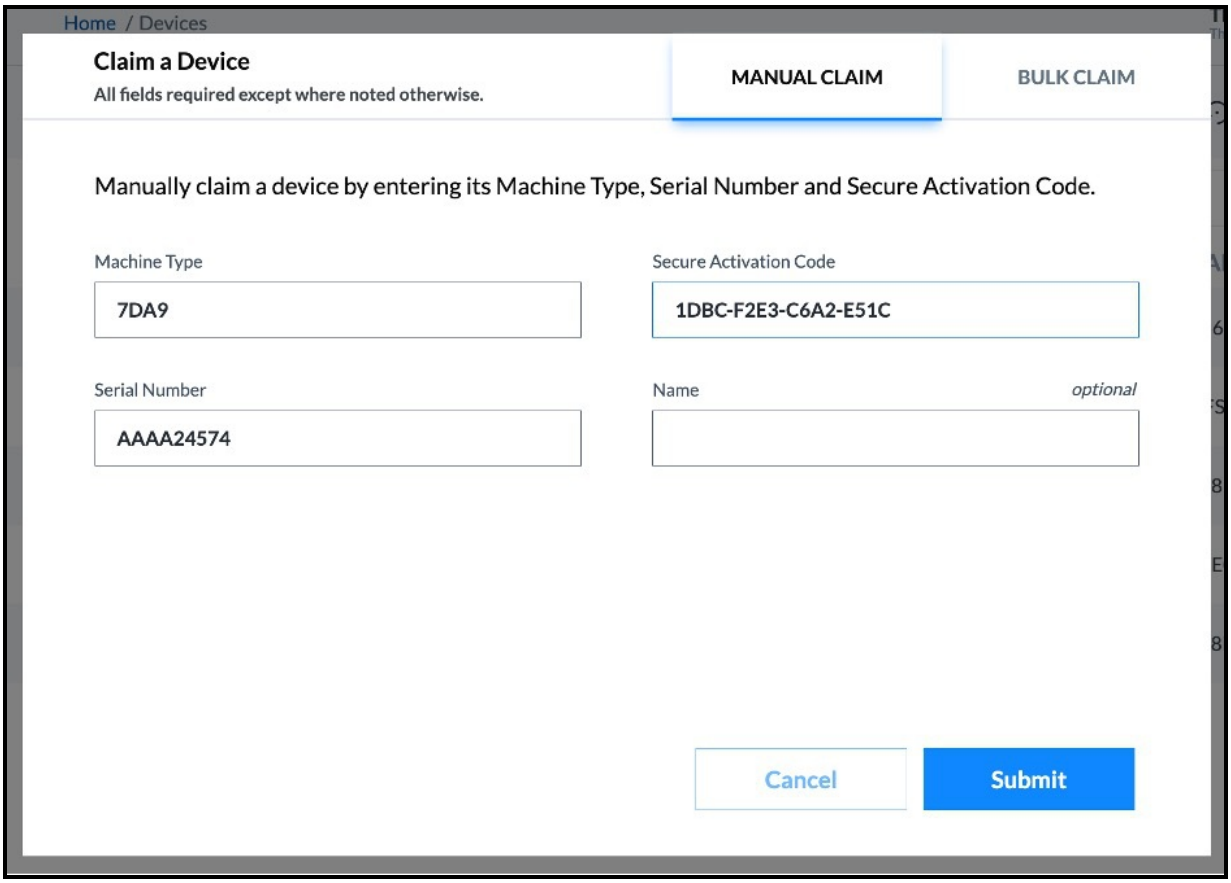

Figure 33. Claiming a ThinkEdge Server

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 final 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 many need to power it off and back on again for activation to occur.

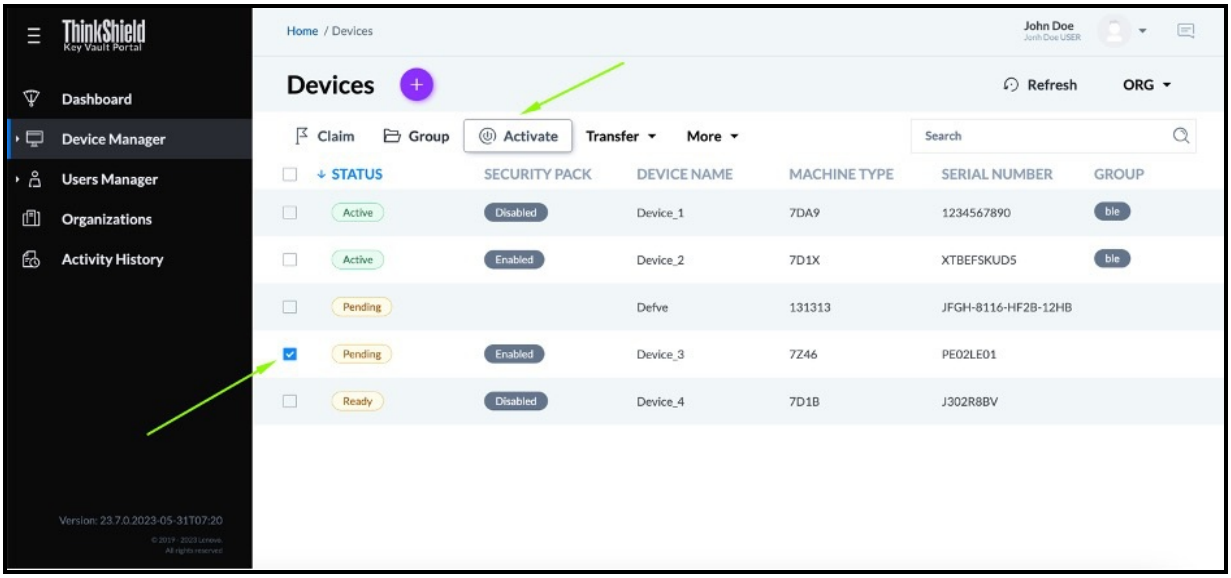

Figure 34. Activating a ThinkEdge Server

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.

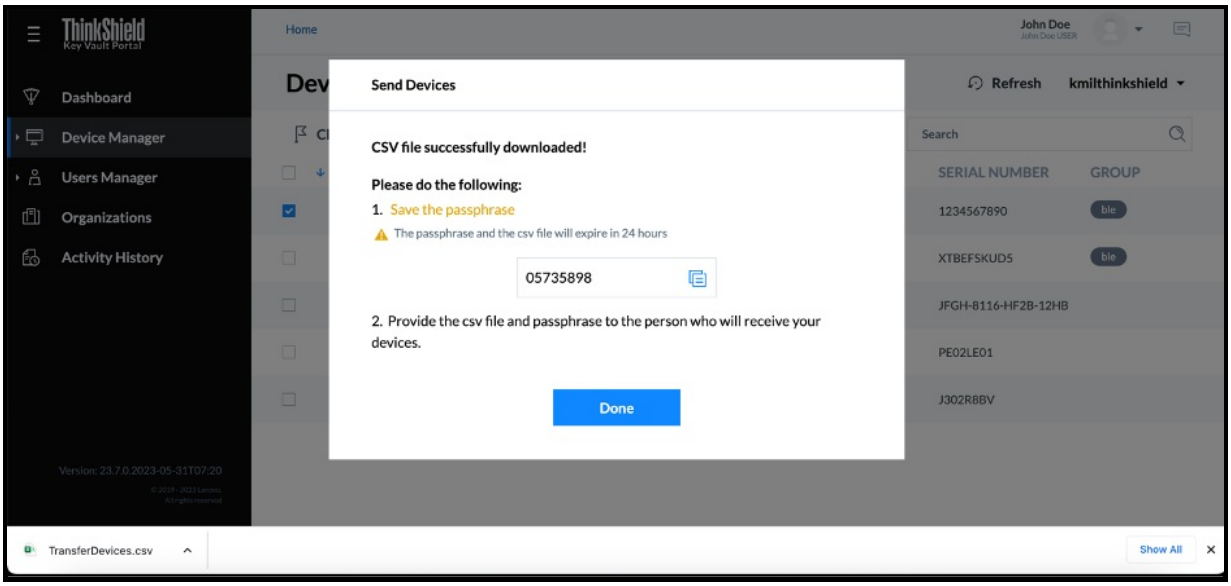

Figure 35. Transferring multiple ThinkEdge servers by CSV file with secure one-time password

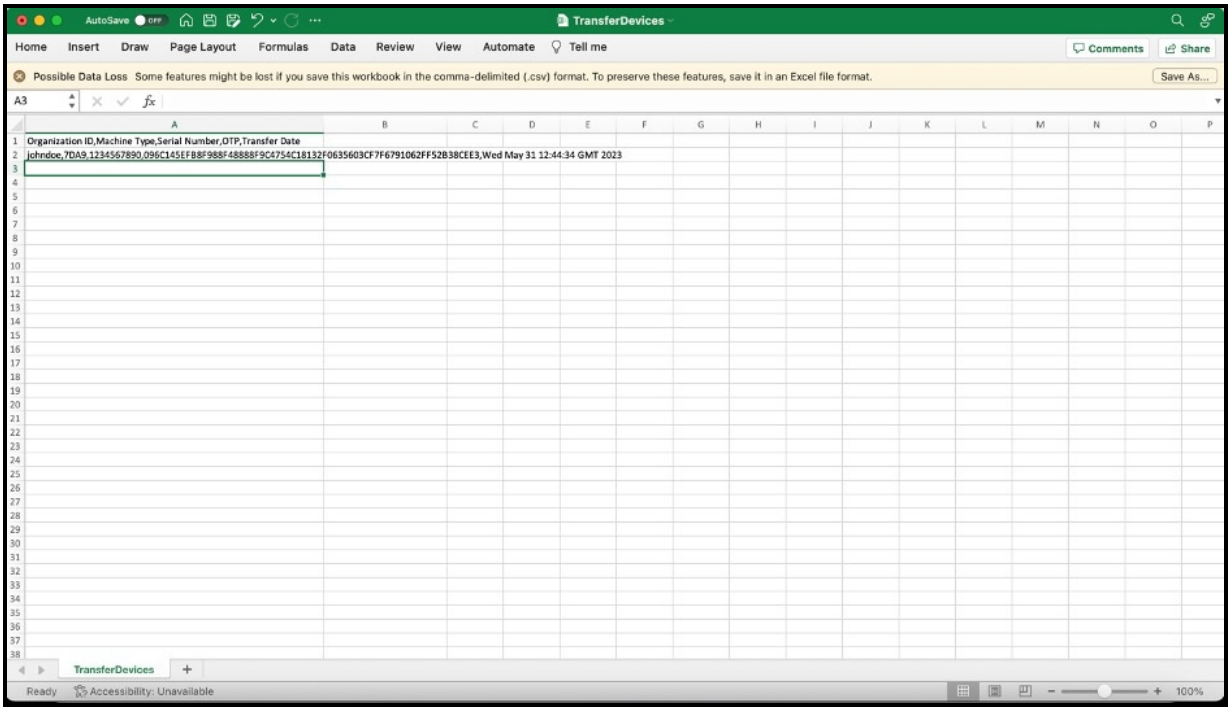

Figure 36. Device transfer CSV file example

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.

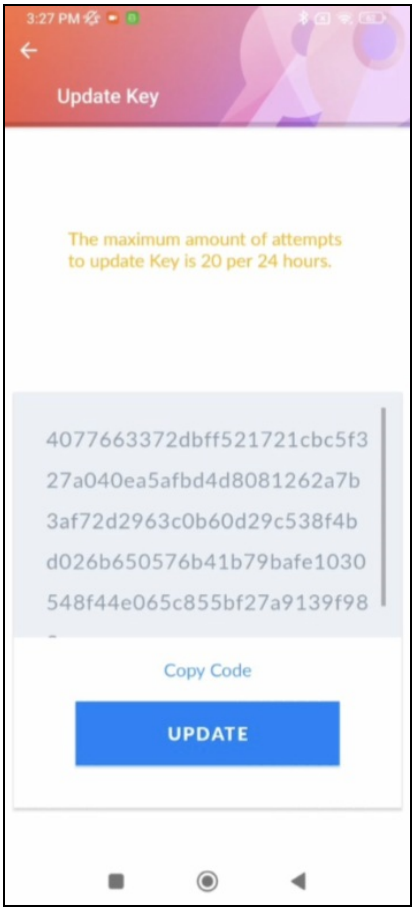

Figure 37. Mobile app updating device key by Lenovo service representative or Maintenance role user after replacing ThinkEdge system motherboard

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
- SE350 User Guide
  https://pubs.lenovo.com/se350/
- 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/
- 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 SE350 V2 Server
- ThinkEdge SE360 V2 Server
- ThinkEdge SE450 Edge Server
- ThinkSystem SE350 Edge 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.

This document, LP1725, was created or updated on August 9, 2023.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1725
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1725.

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.