Reference Architecture for Secure Edge Infrastructure with Lenovo ThinkEdge Servers and SUSE Linux Enterprise Micro

Last update: 20 Feb 2024
Version 1.0

Reference architecture to build infrastructure at Edge where security is important

Describes best practice for OS provision and Hardware/Firmware configuration at remote Edge site

Target for small size deployment in far-edge location

Include Bill of Materials for recommended configuration

Bill Zheng Sun, Lenovo

LENOVO PRESS

Table of Contents

1 Introduction

Edge computing is a new way of processing data that is growing in popularity. Rather than sending data to the cloud to be processed, edge computing uses devices that are located nearer to the data source. This can be useful in situations where real-time processing is required or when there is a need to reduce latency.

Gartner predicts that by 2025, more than 50% of enterprise-managed data will be created and processed outside the datacenter or cloud, with an over $500 billion increase in the edge computing market by 2030. Organizations deploy workloads in locations that are near the places where data is produced to get faster insight about the data without suffering latency of sending data to the cloud for processing.

Depending upon where the edge infrastructure is located, we can segment the Edge landscape into three logical areas: Near, Far and Tiny.

Near Edge

Computing infrastructure that is between the datacenter and the far edge. For example, Cell tower-based compute, Telecom Central Offices, and Campus compute facilities.

Far Edge

Edge computing infrastructure which is deployed in a location furthest from the datacenter. This will be on-site and close to the end-point devices (from a network latency perspective). Examples of Far Edge include:

- Commercial sector: Retail (shop or mall), Hospitality (hotel), Banking (local branch office), Education (school), Healthcare (medical center)
- Industrial sector: Agriculture, Oil and Gas (drilling location), Manufacturing (factory floor), Transportation (aircraft, trains), Energy (wind turbines), Utilities (electricity, water facilities)

Tiny Edge

The end-point itself (e.g. microcontroller enabled sensors, actuators, fixed function devices, etc.). Often referred to as “edge devices” – the Internet of Things (IoT) fits here. The tiny edge is typically within the same network as a Far edge service.

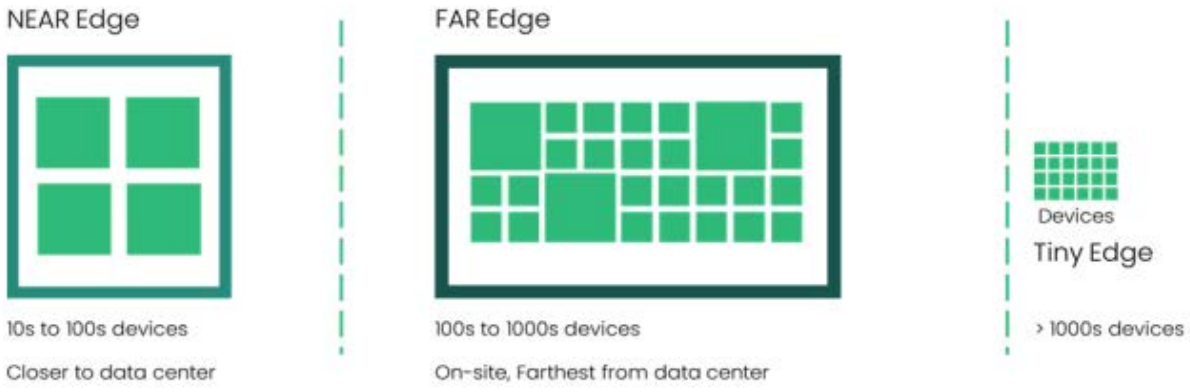


Figure 1.1 Edge Computing Categories

For Near Edge computing, typically computing resources (servers, storage and network equipment) are deployed in either regional datacenter or on-premise IT rooms. Given that the deployment environment of Near Edge is similar to traditional datacenter, current practice of management and deployment of IT infrastructure for the datacenter can be leveraged for Near Edge deployment.

However, in Far Edge deployment, computing infrastructure is deployed outside the datacenter, which lacks necessary facilities and personnels with the required IT skills on-site to manage the IT infrastructure. This shift in deployment practices brings lots of challenges to IT managers and administrators, especially on security, as it removes edge computing resources from the physical access and network security protection provided by a datacenter.

In this document, we'll describe the major challenges being faced by IT administrators for far edge deployments, discuss features in Lenovo next generation of ThinkEdge servers and SUSE Enterprise Linux Micro (SLE Micro) to address the security concerns in Edge deployment. In addition, we'll give a reference architecture of a single node K3S server built upon the SLE Micro operating system and a ThinkEdge server, as well as the best practice to deploy that single node K3S server in a secure manner at the Far Edge site.

The target audience for this Reference Architecture (RA) is system administrators or system architects. Some experience with Linux and Kubernetes may be helpful, but it is not required.

2 Business Challenges and Key Benefits

From recent practice in helping customers to deploy thousands of servers in Far Edge site, we noticed following challenges in Far Edge deployment:

Connectivity

Typically, only the outbound network is available at Far Edge sites. It's may not be easy or even possible for IT admin to connect to Edge servers in a Far Edge site remotely from corporate IT locations as they are often behind NAT or firewall. Network connection from Far Edge site to public cloud is not considered to be reliable.

Limited Capability

IT professionals are not available on-site to facilitate the deployment and maintenance of IT infrastructure in Far Edge sites. Unlike datacenters, Far Edge sites don't have required facilities, tools and processes to manage the IT infrastructure efficiently.

Security

Traditional datacenters are built with strict security control like 24x7 video surveillance, identity authorization, access management or tracking. In Far Edge sites, Edge server will normally be deployed in open space without any restriction on the access to the equipment. It is pretty easy for an attacker to steal the server or important parts of the server (like SSD disk). So it's vital to design the edge infrastructure with capability of self-protection (for example, tamper detection and encrypted storage) against potential attacks from various sources, and apply policy-driven configuration enforcement for security hardening at necessary levels.

Another trend in Edge computing is containerization of applications or workloads to be deployed at Edge site. With a large community of developers and rich features and capabilities, Kubernetes is emerging as the de-facto standard for a container orchestration platform. As a result, it's crucial to provide a reliable and sustainable container hosting platform at Edge.

3 Architecture Overview

In this document, we're proposing deploying a single node K3S cluster on Lenovo ThinkEdge SE350 V2 or SE360 V2 server. K3S will be deployed directly on SUSE SLE Micro operating system without hypervisor layer.

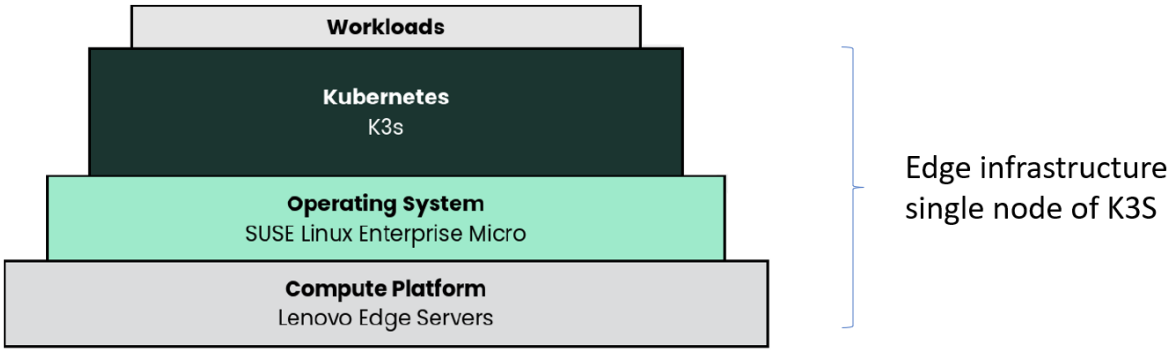


Figure 3.1 Architecture of Single Node K3S deployment

3.1 Compute Platform – Lenovo ThinkEdge Systems

Lenovo ThinkEdge SE350 V2

Figure 3.2 Lenovo ThinkEdge SE350 V2

Lenovo ThinkEdge SE350 V2 is a rugged, compact-sized Edge server with a focus on smart connectivity, business security, and manageability for the harsh environment.

Equipped with Intel® Xeon-D® processor, 1U height, half width and short depth case, Lenovo ThinkEdge SE350 V2 can be deployed in tight spaces. Mount it on a wall, ceiling or install it in a rack. It can handle anything from 0-55°C as well as full performance in high-dust and vibration environments. Lenovo ThinkEdge SE350 V2 is designed to provide industrial networking connectivity options with 1G/2.5G/10G/25G wired connection ability. This purpose-built compact server is reliable for a wide variety of Edge workloads.

Lenovo ThinkEdge SE360 V2

Figure 3.3 Lenovo ThinkEdge SE360 V2

Lenovo ThinkEdge SE360 V2 has been designed and built with the unique requirements to address AI@Edge applications for Edge servers. Same as ThinkEdge SE350 V2, it's based on Intel® Xeon-D ® processor. With 2U height, half-width, and a short depth case, it provides best support for GPU or accelerators from various vendors, like Nvidia A2 and L4, Intel® Data Center GPU Flex 140, and Qualcomm Cloud AI 100.

Lenovo ThinkEdge SE360 V2 can handle temperature changes from 0°C to 55°C as well as high dust and vibration environments. It also supports extreme extended temperature -20°C to 65°C with certain configurations and with marine certification. It also supports secure wireless WLAN and Bluetooth for easy connection.

Hardware Configuration Recommendation

For single node deployment, we recommend having a least 8 core CPU with 32GB memory for container workload. For internal storage, both Lenovo ThinkEdge SE350 V2 and Lenovo ThinkEdge SE360 V2 can be configured with M.2 drive for boot and 2.5-inch 7mm or 15mm drive bays for hot-swap SSD disks. As best practice, normally operating system will be installed on a mirrored (RAID1) M.2 bootable NVMe drive, enabled by Intel VROC onboard RAID. 2.5-inch SSDs can be used for storage of user data.

Tables listed below are recommended hardware configuration of Lenovo ThinkEdge SE350 V2 and ThinkEdge SE360 V2 for single node K3S to host typical container workload. Please refer to appendix A for detailed BOM structure.

CPU	Intel Xeon D-2733NT 8C 80W 2.1 GHz
MEM	32GB TruDDR4 3200 MHz x 2
Bootable Drive	M.2 7450 PRO 480GB x 2 (Configured as RAID 1 by Intel VROC)
Data Drive	7mm U.3 7450 MAX 800GB Mixed Use NVMe PCIe 4.0 x4 HS SSD x 2 7mm S4520 1.92TB Read Intensive SATA 6Gb HS SSD x 2

Table 3.1 Hardware Configuration for ThinkEdge SE350 V2

CPU	Intel Xeon D-2733NT 8C 80W 2.1 GHz
MEM	32GB TruDDR4 3200 MHz x 2
Bootable Drive	M.2 7450 PRO 480GB x 2 (Configured as RAID 1 by Intel VROC)
Data Drive	7mm U.3 7450 MAX 800GB Mixed Use NVMe PCIe 4.0 x4 HS SSD x 2 7mm S4520 1.92TB Read Intensive SATA 6Gb HS SSD x 2

Table 3.2 Hardware Configuration for ThinkEdge SE360 V2

Lenovo ThinkEdge servers are designed for insecure environments. Secured with physical tamper-detection and data encryption, Lenovo ThinkEdge servers are equipped with the ability to withstand conditions of all kinds. Lenovo ThinkEdge servers put increased processing power, storage and network closer to where data is generated, allowing actions resulting from the analysis of that data to take place more quickly. All of these features are unique to ThinkEdge server, not available in typical general-purpose rack server, making it an ideal computing platform for running workloads at the edge, such as in remote office or branch office locations, as well as in geographically disbursed retail locations and similar environments.

3.2 Operating System – SUSE SLE Micro

SUSE Linux Enterprise Micro (SLE Micro) is a lightweight and secure operating system purpose built for containerized and virtualized workloads.

It leverages the enterprise hardened security and compliance components of SUSE Linux Enterprise and merges them with a modern, developer-friendly OS platform. As a result, you get an ultra-reliable infrastructure platform that is also simple to use and comes out-of-the-box with best-in-class compliance.

Shipped as a small footprint and with architecture designed as an immutable OS, SLE Micro is well suited for any decentralized computing environment such as Edge deployments. Using SUSE Linux Enterprise Micro, you can build and scale differentiating Edge systems across a wide range of industries including aerospace, telecom, automotive, defence, healthcare, hospitality, and manufacturing.

SUSE SLE-Micro is an open source, cloud native solution for full stack edge infrastructure management, with the following 3 foundations:

Lightweight cloud-native edge stack

SUSE Edge utilises K3s - a CNCF sandbox project that delivers lightweight Kubernetes distribution fit for resource constrained and remote locations. K3s was built by the SUSE Rancher team and was donated to the CNCF in August 2020. K3s is a highly available, certified Kubernetes distribution specifically designed for production workloads in unattended, resource-constrained, remote locations. K3s is packaged as a tiny, single binary that reduces the dependencies and steps needed to install, run and auto-update a production Kubernetes cluster. All of these features make K3S an ideal platform for running containerized workloads at the Edge, especially for single node deployments.

Reliable & secure edge infrastructure

With 100% open source and built using open standards, SLE Micro provides a reliable and secure OS Platform for the Edge. SLE Micro is built from the ground up to support containers and microservices. SLE Micro leverages the enterprise-hardened technology components of SUSE Linux Enterprise and merges that with what developers want from a modern, immutable OS platform to provide an ultra-reliable infrastructure platform that is also simple to use.

SLE common code base provides FIPS 140-2, DISA SRG/STIG, integration with CIS and Common Criteria certified configurations. Fully supported security framework (SELinux) with policies included. Both Arm and x86 architectures are supported so you have architectural flexibility in deploying a broad range of edge applications.

Aim for maintenance-free infrastructure

SLE Micro uses transactional updates to upgrade from one version to the next. So the system is always in a defined state. Administrators can recover the system with a simple “rollback” via system tools, no backup or restore are needed.

In this document, we will illustrate architecture of one node of K3s cluster deployed on top of Lenovo next generation Edge server: ThinkEdge SE350 V2 and ThinkEdge SE360 V2, with SLE Micro as operating system, with more focus on the security of different layer of infrastructure. In addition, we will provide some guidance on security hardening of different components in the infrastructure, and best practice for deployment at Edge. By following these guidance and best practices, IT administrators can make better choices in designing edge infrastructure where security matters, and planning the edge deployment in a systematic manner.

Download the latest version of SUSE SLE Micro from SUSE official website. Format the hard disk (at least root partition) with btrfs file system to support snapshot and rolling upgrade. As data encryption will be provided at hardware level (enabled by Self-encrypted Disk, which will be discussed in more details in later chapters), encryption of data in a particular partition is not necessary.

As the best practice, the operating system will be installed on mirrored M.2 bootable NVMe drives. User data are stored in hot-swapped 7mm SSD disks. Make sure you pick the right disk for OS installation:

Figure 3.4 SLE Micro OS installation

3.3 Container Platform – K3S

K3s is a Lightweight Kubernetes. Easy to install, half the memory, all in a binary of less than 100 MB. K3s is a fully compliant Kubernetes distribution with the following enhancements:

- Packaged as a single binary.
- Lightweight storage backend based on sqlite3 as the default storage mechanism. etcd3, MySQL, Postgres are also available.
- Wrapped in a simple launcher that handles a lot of the complexity of TLS and options.
- Secure by default with reasonable defaults for lightweight environments.
- Simple but powerful "batteries-included" features have been added, such as:
  - local storage provider
  - service load balancer
  - Helm controller
  - Traefik ingress controller.

Operation of all Kubernetes control plane components is encapsulated in a single binary and process. This allows K3s to automate and manage complex cluster operations like distributing certificates.

External dependencies have been minimized (just a modern kernel and cgroup mounts needed). K3s packages the required dependencies, including:

- containerd
- Flannel (CNI)
- CoreDNS
- Traefik (Ingress)
- Klipper-lb (Service LB)
- Embedded network policy controller
- Embedded local-path-provisioner
- Host utilities (iptables, socat, etc)

More information can be found at https://k3s.io

For a single node K3S cluster, Kubernetes control plane as well as application workload will be hosted in the same server node. Single node of K3S cluster is suitable for running container workloads where service availability is not a mandatory requirement. Running three K3S server nodes is required to build a full high-availability K3S cluster, which is recommended for missing critical workload.

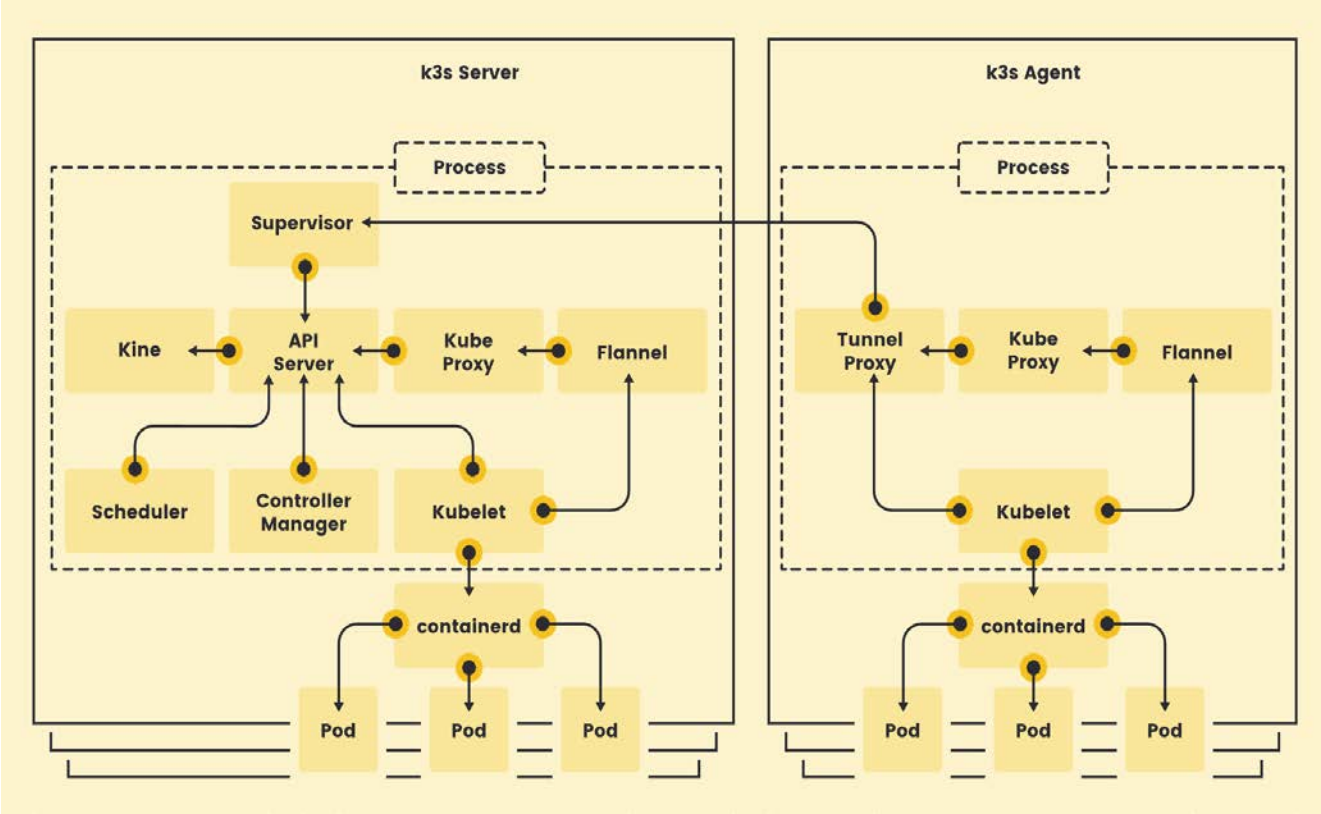


Figure 3.5 SUSE K3S architecture

In K3S single node deployment, local storage will be used for data persistence. K3s comes with a default Local Path Provisioner that allows creating a PersistentVolumeClaim backed by host-based storage. Typically, K3S persistent volume is located under /var partition, so enough space should be allocated for K3S persistent volume.

4 Enhanced Security at the Edge

4.1 ThinkEdge Server Security Features

The ThinkEdge SE350 V2 and SE360 V2 servers are shipped with following security features:

Support for a Kensington lock and cable	ThinkEdge server has a slot on the rear side of the server which a customer-supplied Kensington lock and cable can be attached to, to help prevent theft of the server.
Front bezel with lock	Optional component that mounts on the front of the server that restricts access to networking connectors on the front of the server. (not available in ThinkEdge SE360 V2)
Chassis Intrusion detection	ThinkEdge servers are equipped with an intrusion switch to detect unexpected removal of server's cover. If Chassis intrusion detection is enabled in server's BMC (XClarity Controller), the server will be locked down if the server's top cover is removed.
Motion detection	ThinkEdge servers are also equipped with security sensors to detect unexpected movement of the server. When motion detection is enabled in server's BMC (XClarity Controller), ThinkEdge server will be locked down if server is moved beyond predefined ranges.
Intrusion arm / disarm	The security keylock can be used as an electronic switch to disarm the intrusion switch detection, so that authorized servicing of the hardware can be performed without triggering the security actions.
Integrated password protection	Administrator password and power-on password stored in UEFI ensure that the server will not boot unless the password is entered correctly.
Onboard Trusted Platform Module (TPM)	Supports TPM 2.0 and enables advanced cryptographic functionality in the operating system and applications. For users in China, the server has an internal TCM port that supports a Nationz TPM 2.0 module.
Support for Secure Boot	To ensure only immutable and signed software are loaded during the boot time. The use of Secure Boot helps prevent malicious code from being loaded and helps prevent attacks

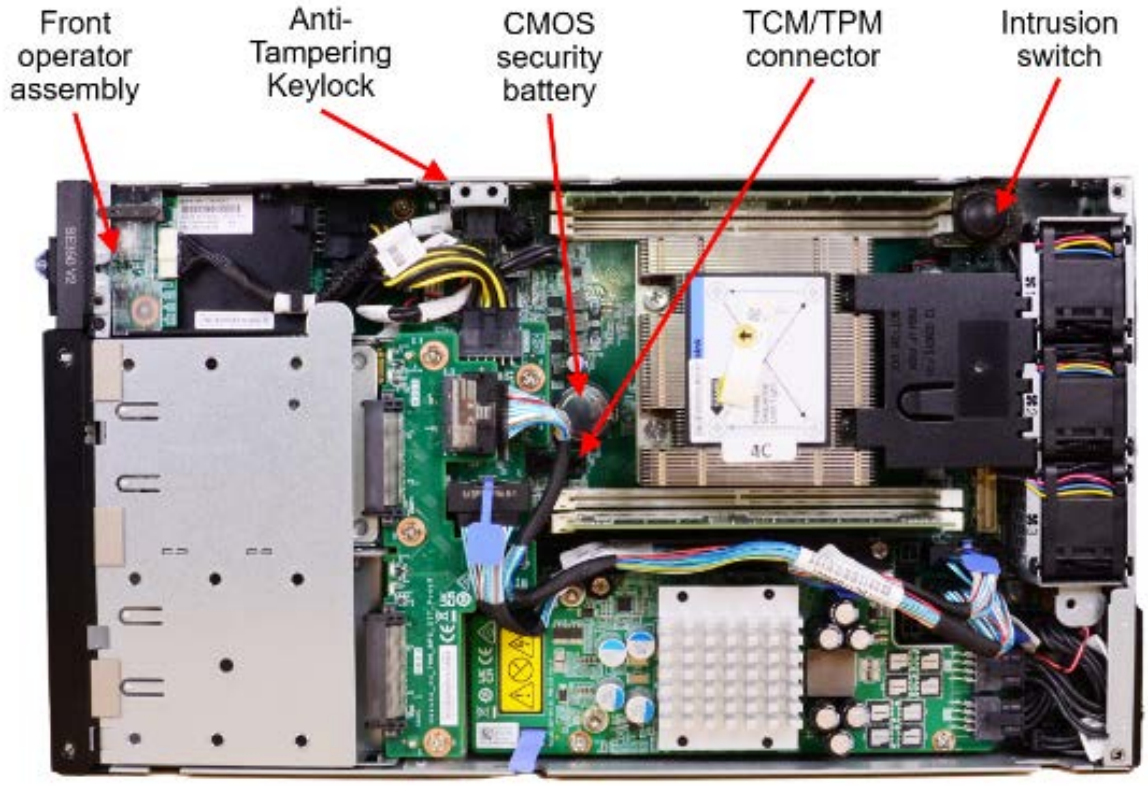


Figure 4.1 Security features of the SE350 V2

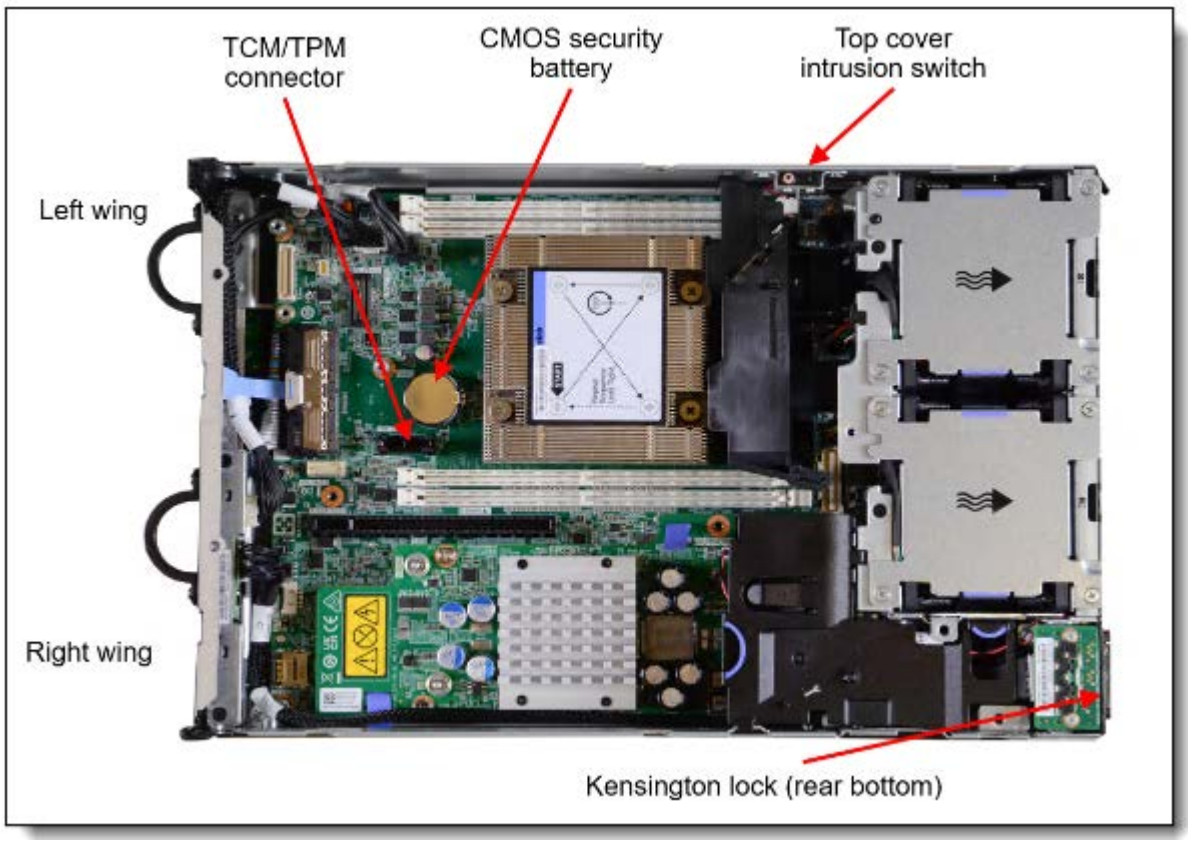


Figure 4.2 Security features of the SE360 V2

4.1.1Data Protection with Self Encrypted Drives

The key focus of ThinkEdge security is data protection. There are many potential threats to data that are unique to edge environments. Attackers could steal the whole ThinkEdge server, or just pull out the disk drive in the front panel.

In order to protect user's data, ThinkEdge servers are equipped with Self-Encrypting Drives (SED). SED drive has encryption hardware built into the drive controller, which will automatically encrypt all data as it is written to the drive and decrypt all data as it is read from the drive. Data stored on SEDs are always fully encrypted by a data encryption key (DEK), which is stored on the drive's hardware and cannot be accessed by the host operating system or unauthorized users.

Because SEDs use hardware-based full disk encryption, both the encryption and decryption processes occur in the disk hardware. This separation from the host operating system makes hardware encryption more secure than software encryption. Moreover, unlike software encryption, hardware encryption does not require extra CPU resources. If a SED is physically stolen or lost, it becomes practically impossible to obtain intelligible information from the SED.

While SED drives use Data Encryption Key (DEK) to encrypt data in disk drive, Authentication Key (AK) is used to unlock the drive and manage the access to DEK in the SED drive. 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, SED AK unlocks the access to DEK in

SED drives, so encrypted data in SED drive can be decrypted by DEK for access. If an attacker steals the SED drive, given that the data in the SED drive is encrypted, the attacker cannot read the content in the drive.

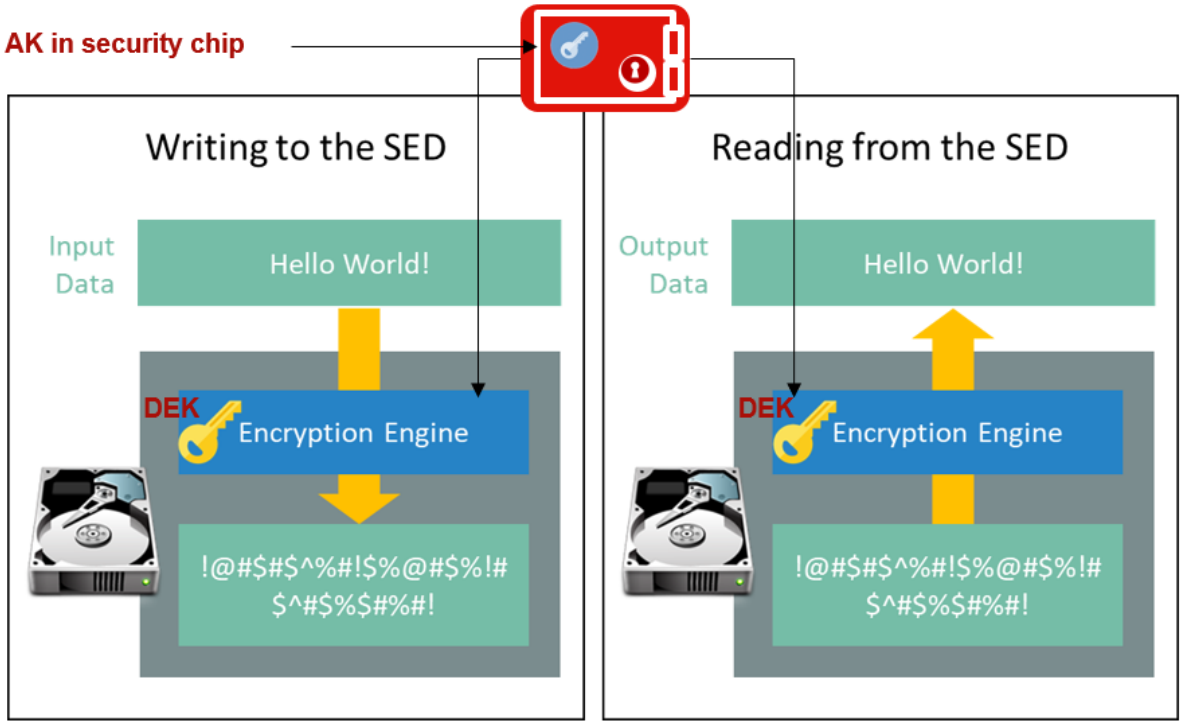


Figure 4.3 Data Encryption by SED Drive

For ThinkEdge SE350 V2 and SE360 V2, SED Encryption needs to be enabled in order to encrypt the data stored in the SED drives. SED Encryption is offered as CTO (configure to order) option, or it can be enabled at later time in XClarity Controller. SED encryption can't be disabled after it is enabled in manufactory or in XClarity Controller. If SED Encryption is not enabled, data will not be encrypted in SED Drive.

Feature code	Name	Description
BYBS		If SED Enablement is enabled in CTO, SED encryption will be enabled in manufactory. A randomly generated AK will be used to control access to DEK for data encryption.

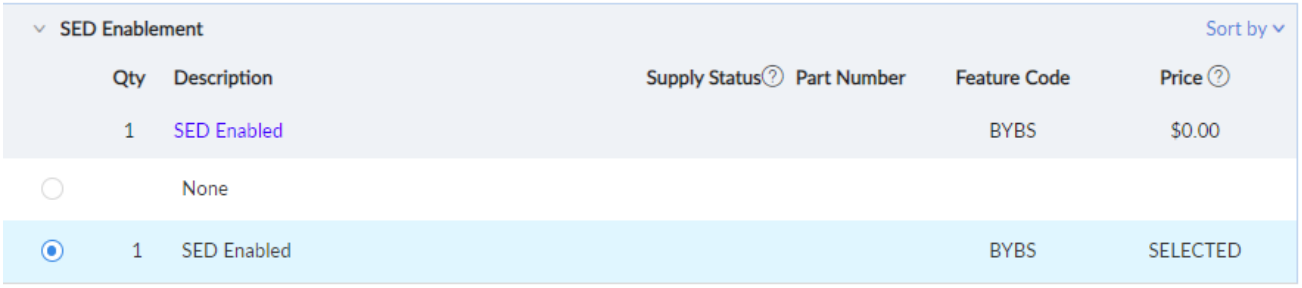


Figure 4.4 SED Enablement in DCSC configuator

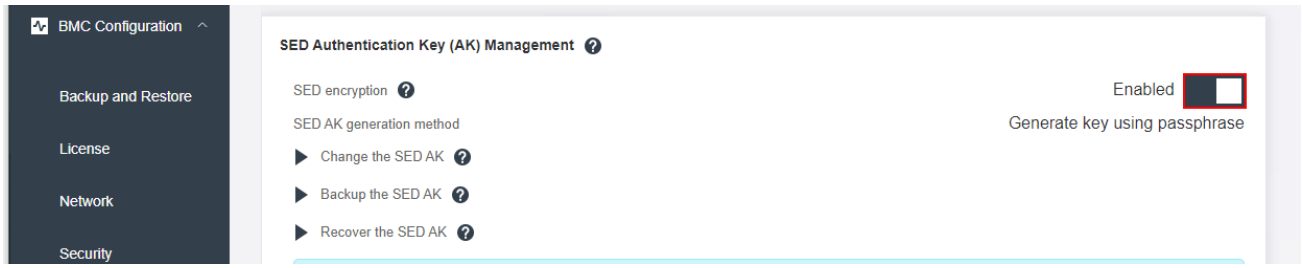


Figure 4.5 Enable SED Encryption in XClarity Controller

4.1.2System Lockdown and activation

If security sensors (Chassis Intrusion Detection or motion detection) are enabled in XClarity Controller, ThinkEdge server will be locked down when tamper events (open top cover, unexpected movement of the server) are detected. When ThinkEdge server is locked down, the system can't be rebooted. Access to SED AK stored in the security chip is blocked, therefore user data stored in the SED drive can't be accessed even if the whole system is stolen.

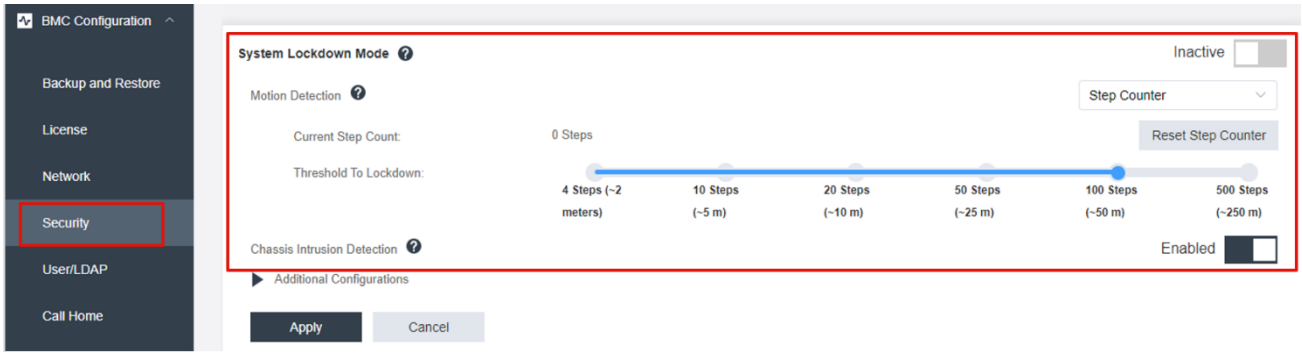


Figure 4.6 Security Sensors Configuration

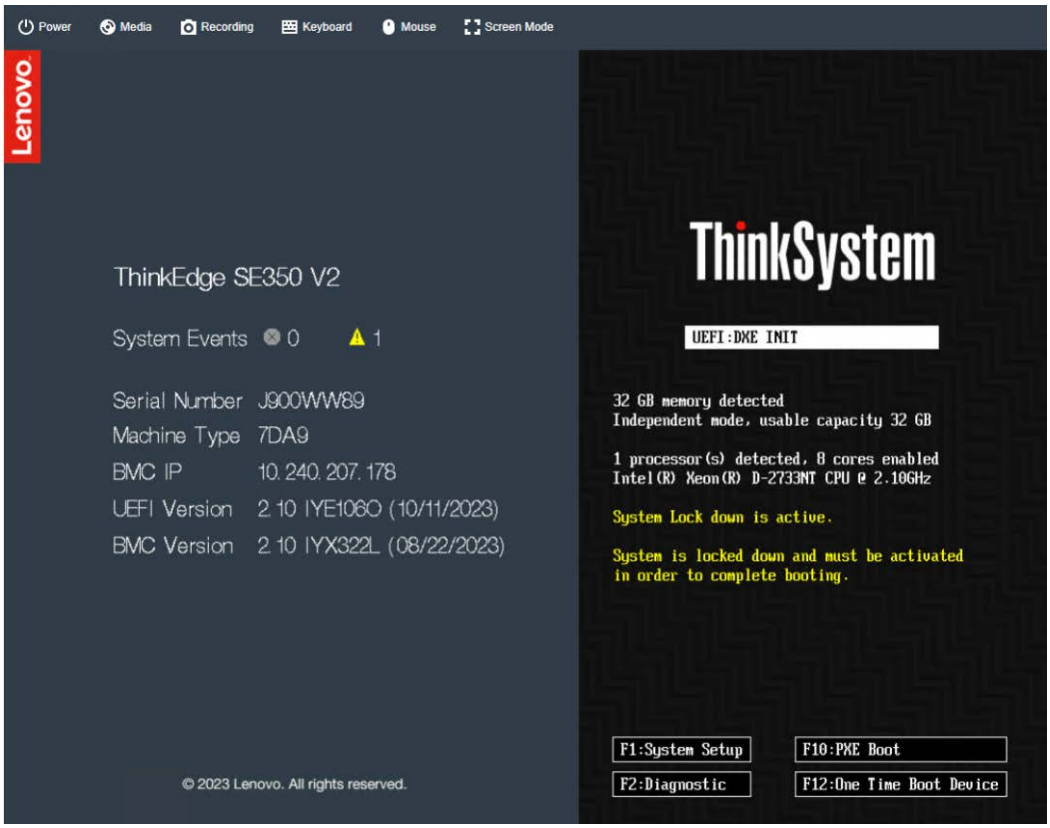


Figure 4.7 Console Screen of ThinkEdge server in Lockdown Mode

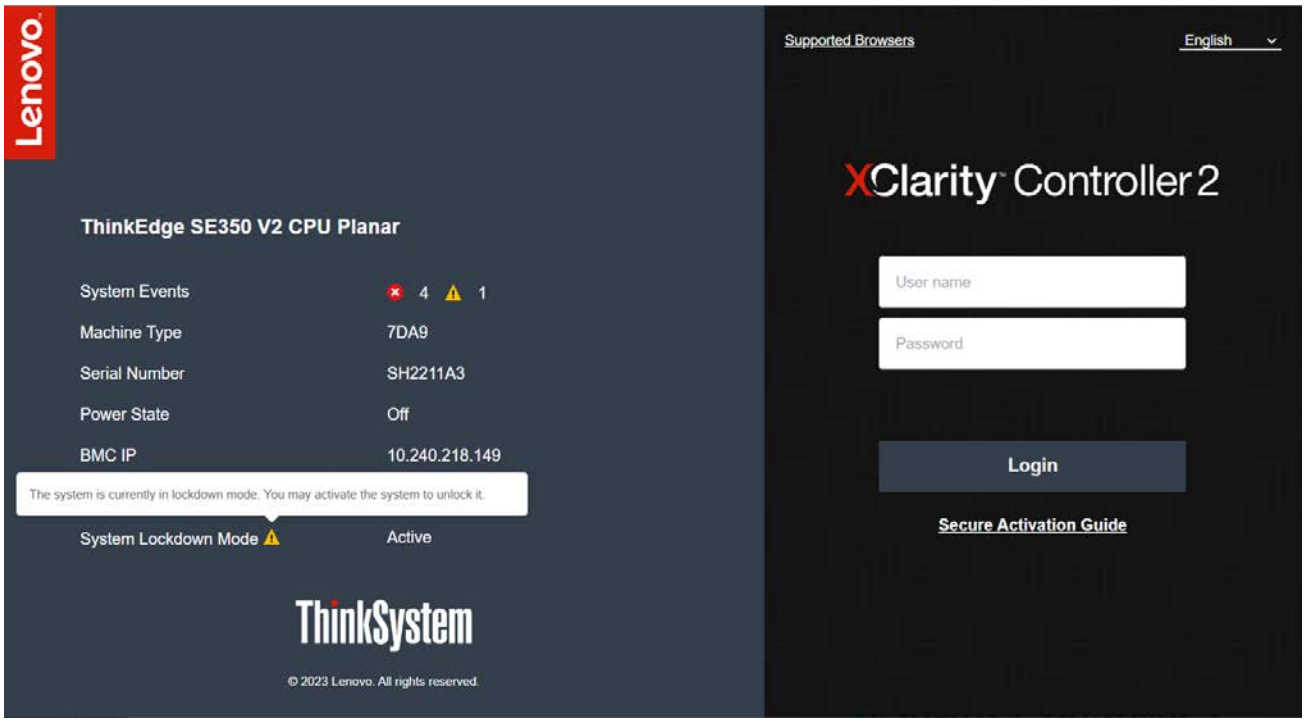


Figure 4.8 XClarity Controller of ThinkEdge server in lockdown mode

Users can also tell whether the server is in lockdown mode from the Activation LED in the server's front panel. If the Activation LED is blinking, the server is in a locked down model and needs to be activated.

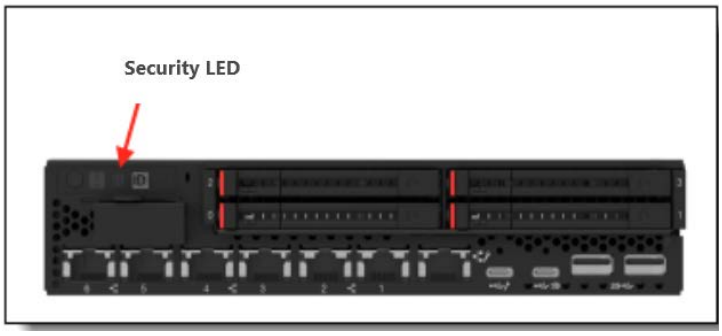


Figure 4.9 ThinkEdge SE350 V2 Security LED

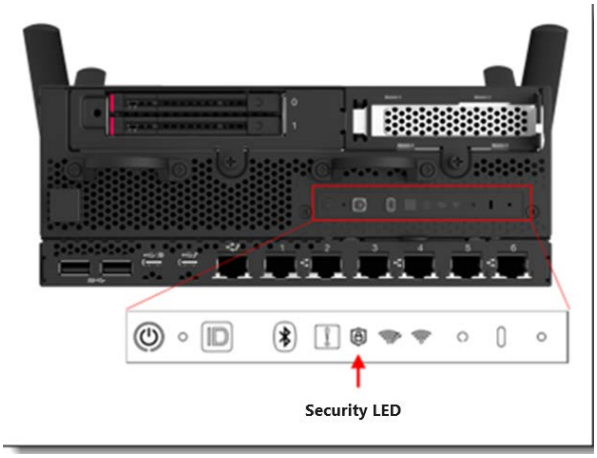


Figure 4.10 ThinkEdge SE360 V2 Security LED

Under Additional Configuration in System Lockdown Mode, users can choose whether Host OS will be shutdown with system lockdown. This option is enabled by default. Uncheck this option if Host OS needs to be kept running when the system is locked down. If this option is not enabled, Host OS will not be shutdown when system is locked down in the event of tamper detection, but the system can't be rebooted.

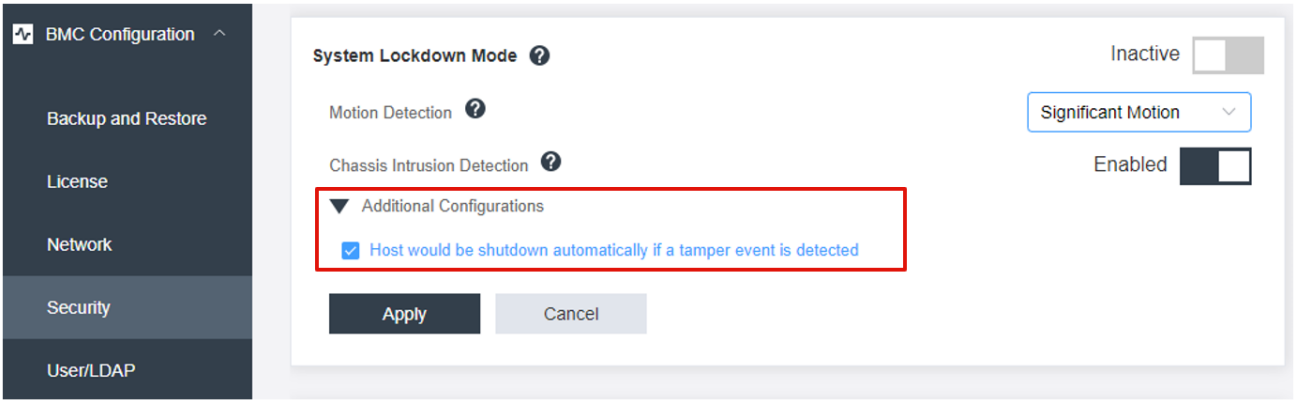


Figure 4.11 Additional Configuration for System Lockdown

4.1.3Activation of Server in Lockdown mode

When the ThinkEdge server is locked down in the event of tamper detection, user needs to activate the server in order to allow the system to reboot, and restore the access to encrypted data stored in SED drives. ThinkEdge servers are shipped with two options in terms of how the system is managed in lockdown mode, which are defined by System Lockdown Control in CTO configuration in https://dcsc.lenovo.com/ when the system is ordered.

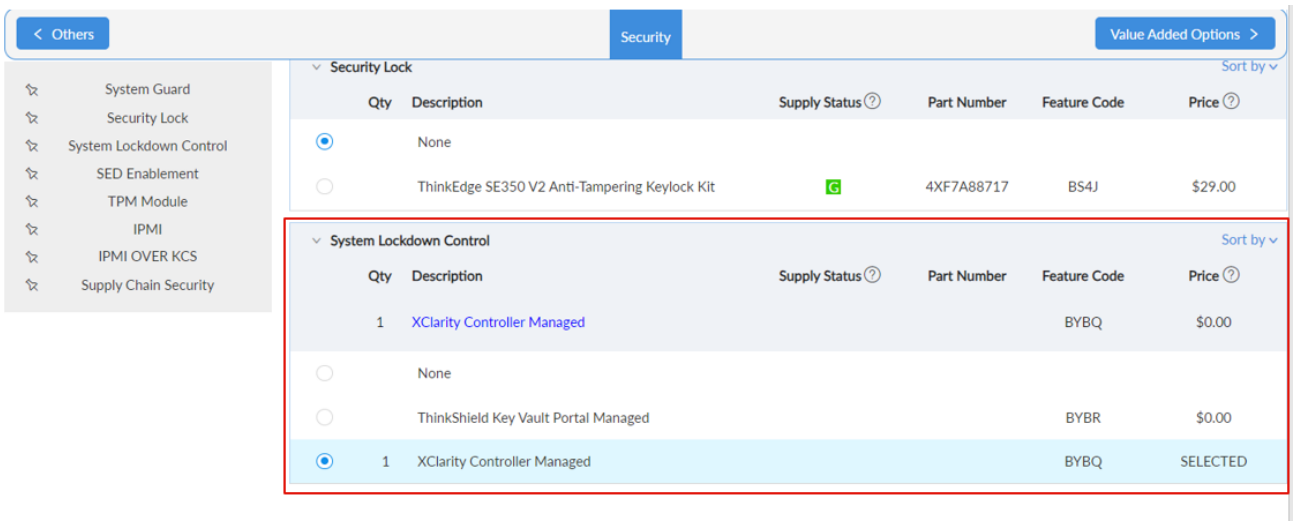


Figure 4.12 DCSC Configurator for System Lockdown Control

Feature Code	System Lockdown Control	Definition
BYBQ	XClarity Controller Managed	ThinkEdge server in lockdown mode can be activated by user with administrator privileges in XClarity Controller Web Console (refer to Figure 4.12 for details)
BYBR	ThinkShield Key Vault Portal Managed	ThinkEdge server in lockdown mode can only be activated by user authenticated with ThinkShield Key Vault portal.

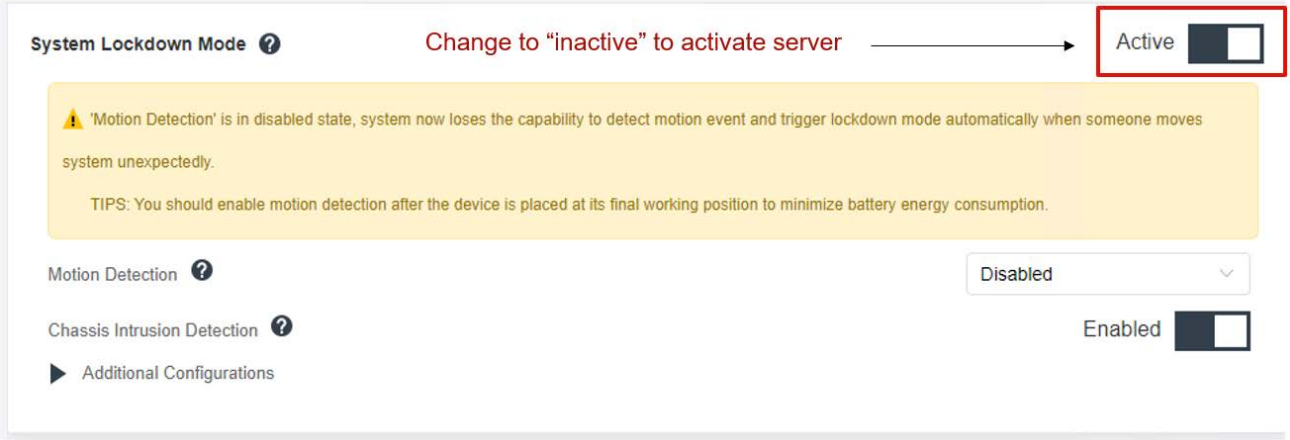


Figure 4.13 Activate Server in lockdown mode in XClarity Controller (XCC) Web Console

ThinkEdge server ordered with Feature Code BYBR (System Lockdown Control is managed by ThinkShield Key Vault Portal) will be shipped in lockdown mode from manufacturing. When the server arrives at a deployment site, it will not be powered on and complete the Power On Self Test until it has been successfully activated with ThinkShield Key Vault Portal.

ThinkShield Key Vault Portal

ThinkShield Key Vault Portal (https://portal.thinkshield.lenovo.com/) is a web service designed by Lenovo to facilitate management of the ownership of devices deployed outside datacenter. It is used to ensure only owner of the ThinkEdge server can manage and activate Edge servers deployed outside datacenter.

Similar to other public cloud services (like Amazon AWS or Microsoft Azure), ThinkShield Key Vault Portal supports multi-tenants. Each tenant is called “organization” in ThinkShield Key Vault Portal, which is used to manage the ownership of the device (Edge server), as well as users who can activate Edge servers at remote Edge site.

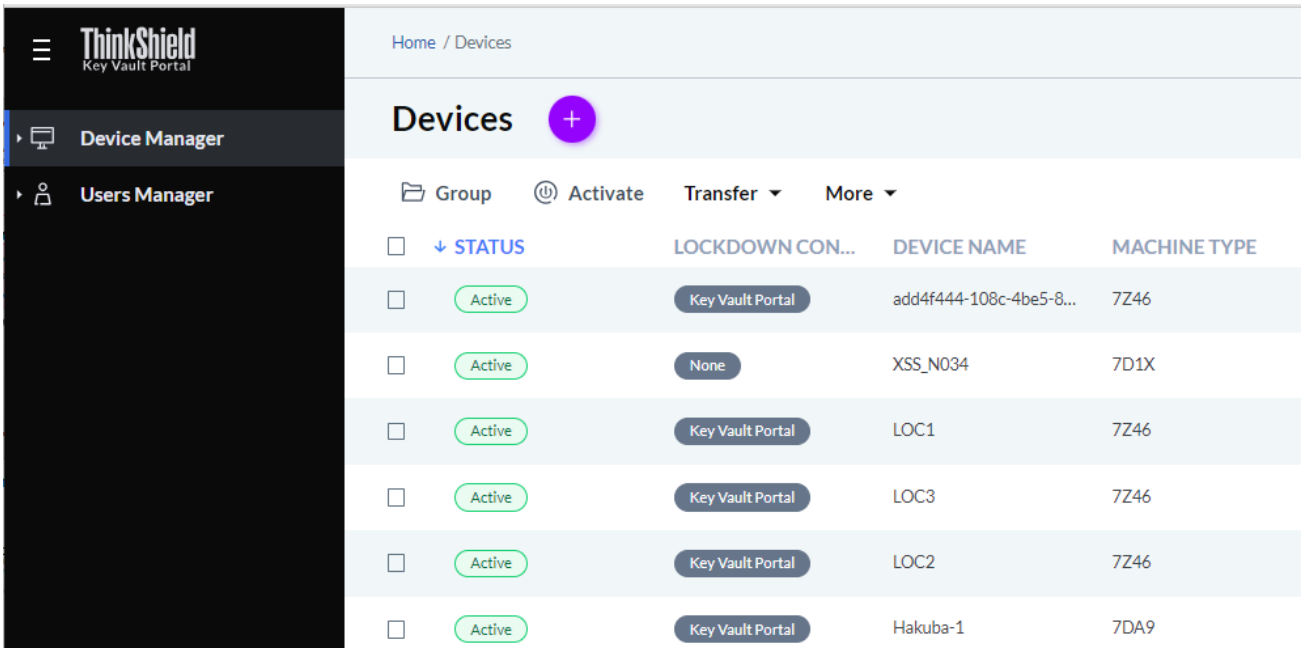


Figure 4.14 ThinkShield Key Vault Portal

IT administrators can add more users to their organization. These users will be able to activate ThinkEdge server in lockdown mode at remote site, if these server were shipped with Feature Code BYBR (System Lockdown Control is managed by ThinkShield Key Vault Portal), or its System Lockdown Control is changed from XClarity Controller Managed to ThinkShield Key Vault Portal Managed at field with promotion process done in LXCE UpdateXpress.

New users can be added to the organization by IT administrators. Organization users are able to add ThinkEdge servers to this organization by claiming the ownership of the server with “Secure Activation Code” shipped with the system. Users can add multiple servers to his organization. But once the Edge server is added in an organization, it can’t be added to other organizations as its ownership is tied to that organization. Transfer of the ownership of the server is possible and can be initiated by IT admin in current owner organization of the server.

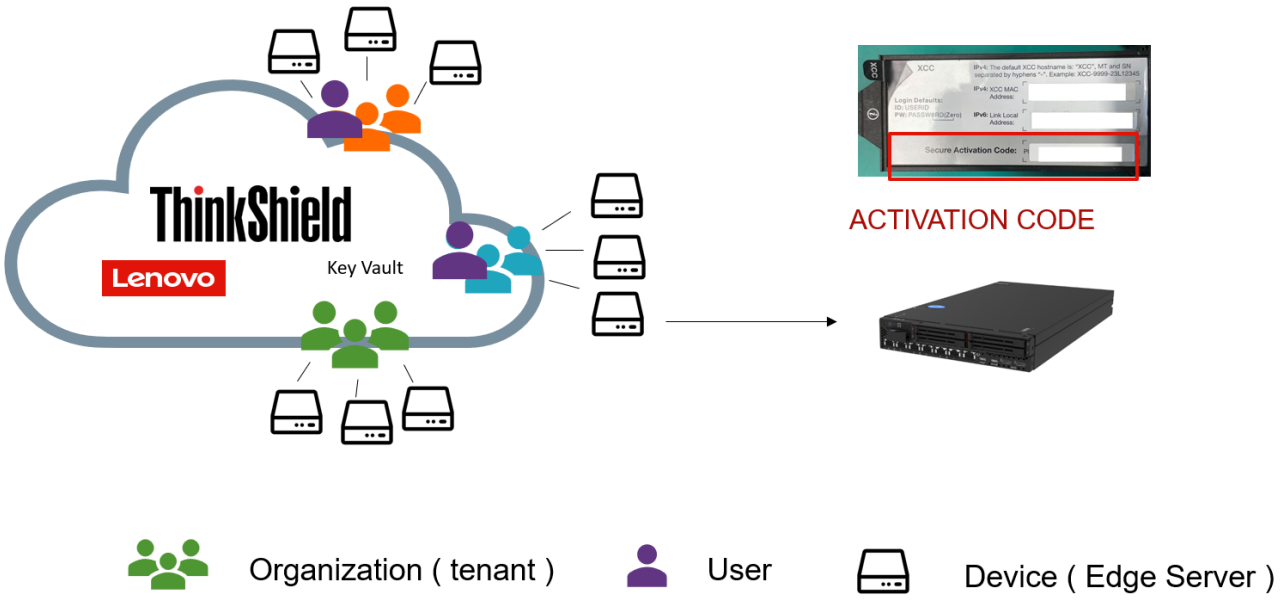


Figure 4.15 Claim Device's Ownership

User can use its Lenovo ID to login to ThinkShield Key Vault Portal. Additionally, IT Administrators can also link their company's identity access management (IAM) system with the portal through Active Directory Federation Service (ADFS), so that on-site users can use their own company user ID ThinkShield log in.

Please refer to following links to learn more about how to create Lenovo ID and organization in ThinkShield Key Vault Portal.

- How to create an organization on ThinkShield Key Vault Portal
- How to create a Lenovo ID

Activation with ThinkShield Key Vault Portal

When ThinkEdge servers with System lockdown Control configured as ThinkShield Key Vault Portal Managed is locked down in the event of tamper detection, it can only be activated by the owner of that server. User need to be authenticated by ThinkShield Key Vault Portal to make sure he is in the same organization with the ThinkEdge server.

Normally, activation of ThinkEdge server with ThinkShield Key Vault Portal can be done in three ways:

1. If ThinkEdge server system management port (BMC) is connected to network and able to access ThinkShield Key Vault portal in public Internet, users can activate that server directly at ThinkShield Key Vault portal Web console. More details can be found at https://support.lenovo.com/pt/en/solutions/ht509292

2. If on-site Edge user has a Windows laptop and is able to connect to ThinkEdge server system management (BMC) port by IPv4 address or directly with Ethernet cable, he can activate ThinkEdge server using Lenovo XClarity Essentials UpdateXpress (LXCE UpdateXpress). LXCE UpdateXpress can be downloaded from: https://support.lenovo.com/us/en/solutions/ht115051-lenovo-xclarity-essentials-updatexpress

3. If it's not possible to access system management port of ThinkEdge server, and the server's management port is not able to access Internet, on-site Edge user can activate ThinkEdge server using ThinkShield mobile App. The mobile app can be downloaded from major Android stores (Android) and from the Apple App Store (iOS). You can learn more about how to activate ThinkEdge server with mobile App from https://support.lenovo.com/us/en/solutions/HT509033.

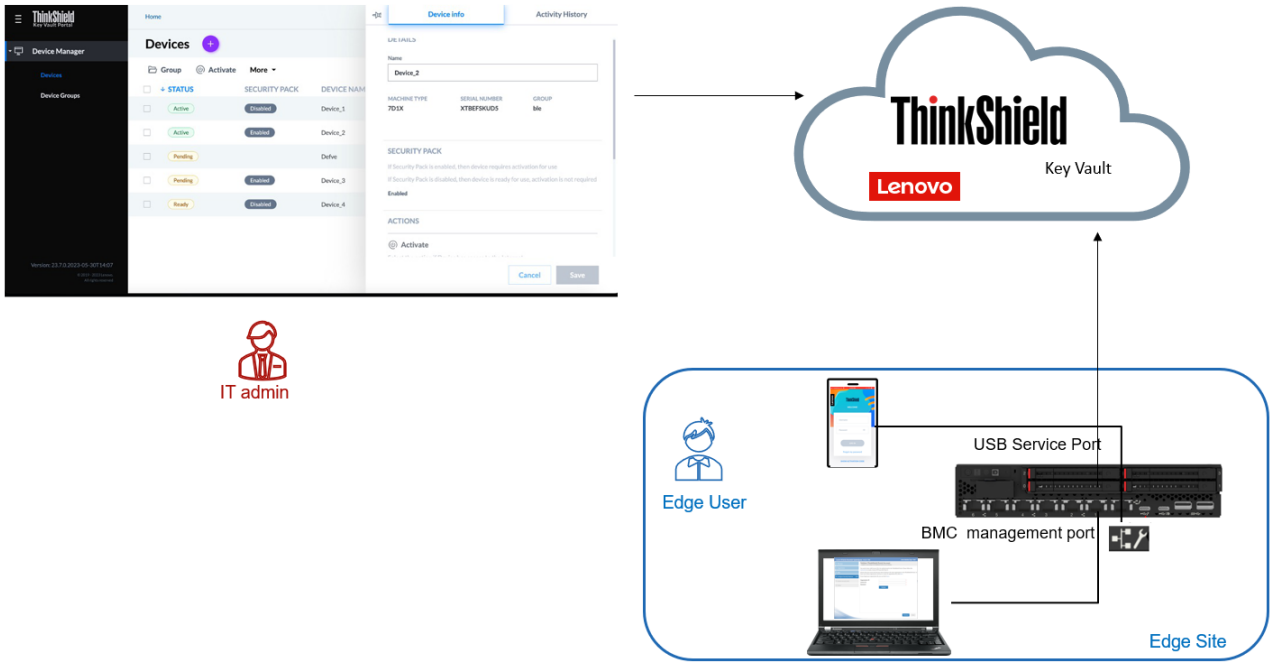


Figure 4.16 Activation of ThinkEdge server with ThinkShield Key Vault Portal

4.2SLE Micro Security Features

4.2.1SLE Micro Key Features

Immutable OS. SLE Micro is a lightweight immutable OS that's optimized for edge use cases. Its immutable design ensures the OS is not altered during runtime and runs reliably every single time. Further, SLE Micro leverages enterprise hardened SLE common code base to provide enterprise grade quality and reliability.

Small Footprint and Modular Architecture. SLE Micro's size is optimized for small footprint installations without compromising on enterprise-grade security or quality. SLE Micro's modular architecture maximizes developer agility and flexibility. You can start with just the Linux kernel and add required modules to create a custom image (using KIWI, Open Build Service, and SUSE Solid Driver Program) that is tailored for your application. You have full control over the footprint of the OS image.

Containers. SLE Micro is built from ground up to support containers and microservices. All applications/workloads are run as containers and separated into dedicated containers. This provides several advantages – new installation of workloads can be done without reboot, atomic updates are easier to support (create new workload, kill old workload) and it is easy to rollback when an update or configuration change goes wrong. From a security perspective, workloads are isolated from the core filesystem to guard against malicious applications compromising the system.

4.2.2Security & Compliance

Built-in Security Framework. Includes fully supported security framework – SELinux with policies. SELinux provides a mechanism for supporting access control security policies, including United States Department of Defense style mandatory access controls (MAC). Container runtime (Podman) is adjusted to support auto-generation of SELinux policies for container workloads.

Air-gapped use case support. Allows users to download container and workload images from trusted registries as well as transfer and integrate them for use in air-gapped environments. This allows for the creation of processes where direct access to registries is either not desired or not possible and the implementation of compliance checks in the process of transferring the images into the air gapped environments.

Secure Device Onboarding. Using integrated secure device onboarding clients, MSPs (Managed Service Providers) or IHVs/ISVs can ship an appliance directly to the end customer, and subsequently, while operating the device remotely, onboard it securely. This helps reduce deployment time and manual process while improving security for onboarding appliances/devices.

Secure Updates. Updates are always security signed and verified. Additionally, the updates are easy to rollback if an update fails or is not needed.

Kernel Live Patching. You can apply updates to a running kernel without the need to reboot. This helps you avoid costly downtime per device and reduce risk of cyber attack, by applying the security updates as soon as available, without waiting for a maintenance window.

Certifications. SLE Micro leverages SLE common code base, to provide FIPS 140- 2, DISA SRG/STIG, integration with CIS and Common Criteria certified configurations. In addition, SLE Micro is listed at NIAP as under evaluation for FIPS 140-3 certification and Common Criteria.

Aiming for Zero Maintenance. SLE Micro is built with the goal of zero maintenance. All routine maintenance functions like patches, updates, config changes are designed to be seamless for the system administrator.

4.2.3Reliable Updates

Secure download. Updates are always downloaded using https.

Signed. Packages and repositories are security signed – Intruder cannot exchange good, new packages with old or insecure packages.

Verified. Packages are verified before usage. System is not updated if conflicts occur. Snapshots get immediately deleted if updates terminate with an error.

Transactional updates. Each update is atomic and uses transactional update technology. Transactional updates along with rollback provide a fail-safe environment. Using Btrfs with snapshots provides a very space efficient method. The updates are flexible - no new package format is necessary and no size limitation for partition or OS. The transactional update process also can be enhanced to perform additional tasks during installation of updates.

Health Check. Built-in health checks ensure an optimized run time environment. Automated checks are done for errors during booting and snapshots. When error is detected, you have multiple options, such as rollback to working snapshot, reboot, or inform administrator. The health checks can also be easily extended by user supplied plugins and scripts. So, you can customize the health checks as per your needs.

Support for Edge devices. Support for 4G/5G modems strengthens the support for edge devices with SLE Micro.

Real Time Support. Real time kernel is optional on x86-64. Real time kernel can be used for real time applications.

High Availability in edge deployments. Keepalived and haproxy are included to offer High Availability functionality in edge deployments.

Long Term Support. SLE Micro is prepared to support long product life cycles .

Lifecycle Management. You can manage using Rancher by SUSE, SUSE Manager or using Cockpit for 1:1 Web based management or integrate with open-source management tools.

5 Secure Hardening Recommendation

In the previous chapters, we discussed security features generation of Lenovo ThinkEdge servers (ThinkEdge SE350 V2 and SE360 V2). We also introduced SUSE Linux Enterprise Micro and its key features specially designed for Edge deployment. In this chapter, we're going to give recommendations on security hardening of the full stack of Edge infrastructure: hardware, firmware in ThinkEdge server (UEFI and XClarity Controller for system management), as well as SLE Micro and K3S based on the best practices.

5.1 ThinkEdge server – Hardening UEFI

UEFI configuration can be done by pressing F1 key after system is rebooted. LXCE OneCLI command line tool can also be used to configure UEFI when applicable.

Enable Secure Boot

Secure boot is functionality built in to UEFI's specification. When Secure Boot is enabled and properly configured, it protects computers against attacks and infections from malware that installs rootkits and boot kits.

Secure Boot detects when software like the boot loader and key operating system files and other things like option ROMs have been tampered with. It does this by validating each component's digital signature. Any component whose digital signature verification fails is not loaded during the boot process. Depending upon the OS and drivers you are using on the server it may not always be possible to enable secure boot.

The parameter can be set in the following ways:

F1 menu:
System Settings -> **Security** -> **Secure Boot Configuration**

OneCLI:
`SecureBootConfiguration.SecureBootSetting "Enabled"`

Configure the Trusted Platform Module

Onboard Trusted Platform Module (TPM) is a component of most modern computer systems. It is classified as a secure crypto processor, toenable advanced cryptographic functionality in the operating system and applications. TPM 2.0 is supported in ThinkEdge SE350 V2 and SE360 V2.

The parameter can be set in the following ways:

F1 Menu:
System Settings -> **Security** -> **Trusted Platform Module**

OneCLI:
`TrustedComputingGroup.DeviceOperation "Update to TPM2.0 compliant"`

Set Boot Mode to UEFI

Boot Mode determines which mode the system used to boot. Setting boot mode to UEFI is the most secure value for Boot Mode. When set to UEFI the system runs UEFI drivers and boots a UEFI OS loader. This setting is automatically set to UEFI mode if Legacy BIOS is disabled in System Settings > Legacy BIOS

The parameter can be set in the following ways:

F1 Menu:
Setup -> **Boot Manager** -> **Boot Modes**

OneCLI:
`BootModes.SystemBootMode "UEFI"`

Review and update boot order

The boot order determines the order the system searches for bootable media as part of the boot process. The system follows the order specified until it finds a device that is bootable. Once it does it boots the system from that device.

Remove any unnecessary boot options that are not required. Systems normally will contain a network boot option such as PXE boot or HTTPS boot as part of the boot order. Network boot is typically used for initial deployment of the host operating system. After initial deployment of the host operating system, network boot options should be removed from the boot order.

The parameter can be set in the following ways:

F1 Menu
Setup -> **Boot Manager** -> **Change Boot Order**

OneCLI:
`BootOrder.BootOrder "comma delimited list"`

Review and remove unnecessary boot options

Verify the boot options and that all are required and remove the boot options that are not necessary. Carefully consider removing USB Storage from BootOrder if you do not need to boot from a USB device.

The parameter can be set in the following ways:

F1 Menu:
Setup -> **Boot Manager** -> **Delete Boot Option**
OneCLI:
`BootOrder.BootOrder "comma delimited device list"`

Review and update boot priority for each device type

Verify the priority/order for each type of boot device to ensure the correct device of each type receives the highest priority.

The parameters can be set in the following ways:

F1 Menu:
Setup -> **Boot Manager** -> **Set Boot Priority**

OneCLI:
BootOrder.HardDiskBootOrder *"comma delimited device list"*
BootOrder.USBBootOrder *"comma delimited device list"*
BootOrder.NetworkBootOrder *"comma delimited device list"*

Disable booting using the network stack

The Network Stack controls whether the system uses any network option for booting. If you do not require any network boot setting, then disable the entire network stack. This is not only the most secure setting it also helps speed up the boot process.

The parameter can be set in the following ways:

F1 Menu:
Setup -> **System Settings** -> **Network Settings** -> **Network Stack Settings -> Network Stack**

OnceCLI:
NetworkStackSettings.NetworkStack "Disable"

Disable PXE Boot

PXE boot allows a system to boot from a server on a network that supports PXE booting instead of from a local hard drive. If you are not able to disable booting using the network stack, disable PXE boot if you do not need it.

The parameters can be set in the following ways:

F1 Menu
Setup -> **System Settings** -> **Network Settings** -> **Network Stack Settings** -> **Disable IPv4 PXE Support**
Setup -> **System Settings** -> **Network Settings** -> **Network Stack Settings** -> **Disable IPv6 PXE Support**

OneCLI:
NetworkStackSettings.IPv4PXESupport "Disable"
NetworkStackSettings.IPv6PXESupport "Disable"

Disable HTTPS Boot

HTTPS boot allows a system to boot from a server on a network that supports HTTPS booting instead of from a local hard drive. If you are not able to disable booting using the network stack, disable HTTPS boot if you do not need it.

The parameters can be set in the following ways:

F1 Menu
Setup -> **System Settings** -> **Network Settings** -> **Network Stack Settings** -> **Disable**

IPv4 HTTP Support
Setup -> **System Settings** -> **Network Settings** -> **Network Stack Settings** -> **Disable IPv6 HTTP Support**

OneCLI:
NetworkStackSettings.IPv4HTTPSupport "Disable"
NetworkStackSettings.IPv6HTTPSupport "Disable"

Set an administrator password

Setting an administrator password deters unauthorized users from changing configuration settings. When an administrator password is set, you are prompted to enter a valid password each time you try to access the Setup Utility program. The Setup Utility program cannot be accessed until a valid password is entered.

Given that ThinkEdge servers are deployed outside data center, it is at risk of being accessed by none authorized person. It is very important to set an administrator password for UEFI, in particular for ThinkEdge server shipped with Feature Code BYBQ (System Lockdown Control is managed by XClarity Controller).

For ThinkEdge server shipped with Feature Code BYBQ, when it is locked down in the event of tamper detection, it can be activated in XClarity Controller Web Console. If UEFI administrator password is not set, attacker can easily go into the UEFI Setup Utility and change the password of XClarity Controller to factory default, thus obtain the access to XClarity Controller to activate the server.

If both the power-on password and administrator password are set, you can enter either password. However, you must use your administrator password to change any configuration settings.

The parameter can be set in the following ways:

F1 Menu:
User Security -> **Set Administrator Password**
OneCLI:
IMM.UefiAdminPassword "Uefi Admin Password"

5.2 ThinkEdge server – Hardening XClarity Controller (XCC)

Harden the network settings of XCC

Do not connect the Lenovo XClarity Controller (XCC) network interface to untrusted networks. Restricting XCC network access to only trusted networks reduces its attack surface and makes it more difficult for attackers to exploit any weaknesses it might have.

Configure IPv4

Select the proper method for determining the IPv4 address of the XCC interface. For example, if you do not wish the IPv4 address to be obtained from a DHCP server then do not select that option.

The parameters can be set in the following ways:

XCC WebUI:
BMC Configuration -> **Network**-> **Ethernet Configuration** -> **IPv4**

OneCLI – IPv4 Settings for Network Interface 1:
IMM.Network1 "Disabled" | "Enabled"
IMM.DHCP1 "Disabled" | "Enabled"
IMM.HostName1 *"hostname for the network"*
IMM.HostIPAddress1 *"static ipv4 address"*
IMM.HostIPSubnet1 *"static ipv4 netmask"*
IMM.GatewayIPAddress1 *"static ipv4 gateway"*

Configure IPv6

Select the proper Method for determining the IPv6 address of the XCC interface. If your organization does not use IPv6 then you should disable it. If you are using IPv6, then select the address configuration method used by your organization.

The parameters can be set in the following ways:

XCC WebUI
BMC Configuration -> **Network**-> **Ethernet Configuration** -> **IPv6**

OneCLI Settings – IPv6 Settings for Network Interface 1:
IMM.IPv6Network1 "Disabled" | "Enabled"
IMM.IPv6Static1 "Disabled" | "Enabled"
IMM.IPv6DHCP1 "Disabled" | "Enabled"
IMM.IPv6Stateless1 "Disabled" | "Enabled"
IMM.IPv6HostIPAddressWithPrefix1 *"ipv6 address value"*
IMM.IPv6GatewayIPAddress1 *"ipv6 gateway address value"*
IMM.IPv6LinkLocalIPAddress1 *"ipv6 link local address value"*
IMM.IPv6StatelessIPAddress1 *"ipv6 gateway address value"*
IMM.IPv6StatelessGateway1 *"ipv6 stateless gateway value"*

Disable or configure Ethernet over USB

Ethernet over USB is used for in-band communication between the host server and XCC. This feature provides an in-band channel for applications on the host server to communicate with XCC and vice-

versa. This means that a user logged in to the host can use applications on XCC that can communicate over this channel.

To prevent applications that are running on the server from accessing XCC via this interface, you should disable the USB in-band interface. If you do disable the USB in-band interface, you cannot perform an in-band update of the XCC firmware, the UEFI firmware, the embedded provisioning tool, and certain adapter firmware by using the XClarity Essentials in-band update utility.

The parameter can be set in the following ways:
XCC WebUI:

BMC Configuration -> **Network**-> **Ethernet over USB**

OneCLI Settings

```
IMM.LanOverUsb "Disabled" | "Enabled"
```

SNMP Configuration

SNMP can be used to manage and monitor XCC using the SNMP protocol. If you enable SNMP, then only enable those items that you need. For example, if you do not need SNMPv1 traps then ensure it is disabled.If you do need to use an SNMP Agent, then enable the SNMPv3 Agent only.

The parameters can be set in the following ways:
XCC WebUI:
BMC Configuration -> **Network**-> **SNMP setup**
OneCLI:

```
IMM.SNMPv3Agent "Disabled" | "Enabled"
IMM.SNMPTraps "Disabled" | "Enabled"
```

Disable unnecessary services

The following table shows the network services that are available within XCC. To reduce XCC's attack surface disable any service that your organization does not require. Certain services are required by XCC and cannot be disabled. Those are noted below.

Port	Service	When to disable	How to disable in XCC	OneCLI setting
427	SLP	Used by Lenovo XClarity Administrator (LXCA) and other Lenovo tools to discover devices on the network. If you do not use LXCA or another Lenovo tool that uses SLP, disable this protocol.	BMC Configuration → Network → Service Enablement	IMM.SLPPortControl "Closed"
546	DHCPv6 Client	Disabled if you do not use DHCPv6 for IPv6 Interface Configuration	BMC Configuration → Network → Ethernet Configuration	IMM.IPv6DHCP1 "Disabled"
623	IPMI over LAN	Disable IPMI over LAN if you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol.	BMC Configuration → Network → Service Enablement	N/A
1900	SSDP	Used by Lenovo XClarity Administrator (LXCA) and other	BMC Configuration → Network → Service	N/A

		Lenovo tools to discover devices on the network. If you do not use LXCA or another Lenovo tool that needs SSDP, disable this protocol.	Enablement	
5989	DHCPv6 Client	Used by LXCA and other Lenovo tools to configure the server. If you do not use LXCA or another Lenovo tool that needs CIM-over-HTTPS, disable this protocol.	BMC Configuration → Network → Service Enablement	IMM.CIMXMLOverHTTPS_Enable "Disabled" IMM.CIMOverHttpsPortControl "Closed"

Block List and Time Restriction

Block Lists and Time Restrictions are used to further restrict access to XCC. Use the Block List settings and configure the IPs and MAC addresses of those systems that do not need access to XCC. Use the Time Restrictions and configure the times that XCC cannot be accessed.

The parameter can be set in the following ways:

XCC WebUI:
BMC Configuration –> **Network**–> **Block List and Time Restriction**

OneCLI:
Not Available

Configure XCC SSL certificate

The SSL certificate is the server certificate used by the XCC WebUI, the Redfish Service and the CIM Service. By default, XCC will generate a self-signed certificate for the server. Self-signed certificates typically cause errors or warnings in browsers that the server cannot be trusted.

When possible, use a valid CA signed certificate as it is preferred and is considered a security best practice. To do this, use XCC to generate a certificate signing request, get it signed by the CA of your choosing and then upload the CA signed certificate into XCC.

The parameter can be set in the following ways:

XCC WebUI:

BMC Configuration –> **Security** –> **SSL Certificate Management**

Disable IPMI over Keyboard Controller Style (KCS) Access

The IPMI over KCS channel allows a host user, who is an administrator user on the host, full access to the IPMI commands supported by XCC without any form of XCC authentication. If you are not running any tools or applications on the server that access the XClarity Controller through the IPMI protocol, it is highly recommended that you disable the IPMI-over-KCS access for improved security of XCC.

When using XClarity Essentials Utility tools on the host, the IPMI-over-KCS interface to the XClarity Controller is required. It is still recommended that you disable the IPMI-over-KCS interface and only re-enable it when you need to use XClarity Essentials Utility tools on the host then disable it after you've finished using XClarity Essentials.

The parameter can be set in the following ways:

XCC WebUI

BMC Configuration –> **Security** –> **IPMI over KCS Access**

Disable Bluetooth Button on Front Panel

ThinkEge SE360 V2 server can be activated with ThinkShield Mobile App with bluetooth connection. And there's a button on the front panel where users can press to turn on / off support for Bluetooth connection. Disable this setting if you're not going to use ThinkShield Mobile App to activate the server with Bluetooth connection.

The parameter can be set in the following ways:

XCC WebUI

BMC Configuration –> **Security** –> **Bluetooth Button on Front Panel**

Prevent System Firmware Down-Level

The Enable Prevent System Firmware Down-level option prevents all system firmware including XCC, UEFI, and LXPM from being downgraded to an older revision. Enabling this setting prevents an attacker from installing a previous version of firmware that contains known vulnerabilities that can then be exploited. This option should be enabled unless for some reason there is an organizational requirement to allow firmware to be downgraded to an older version.

The parameter can be set in the following ways:
XCC WebUI:

BMC Configuration –> **Security** –> **Prevent System Firmware Down-Level**

System Lockdown Mode

ThinkEdge server is shipped with security sensors for tamper detection. ThinkEdge server will be locked down in the event of tamper detection if security sensor are enabled, which are configured under under *System Lockdown Mode* in XClarity Controller Web Console.

There are two type of security sensors:

- Motion detection: for unexpected movement of the server
- Chassis intrusion detection: trigger the system lockdown when the top cover is opened

It's highly recommended to enable these two options for Edge server deployed in Far Edge site,

Another configuration option under System Lockdown Mode is to determine whether Host OS will be shutdown as part of system lockdown. It is recommended to leave this option as default.

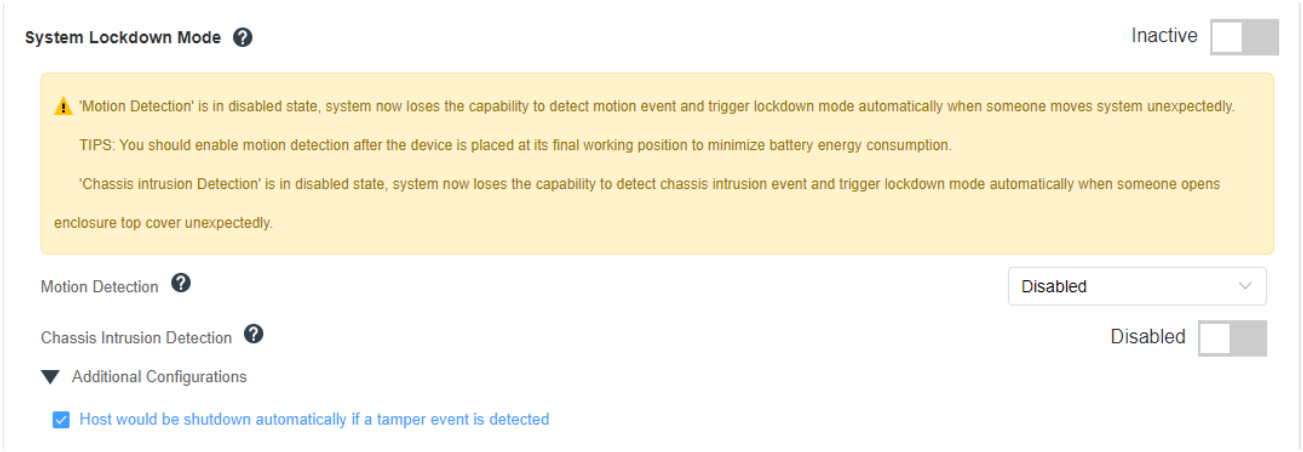


Figure 5.1 System Lockdown Mode in XCC

SED AK Management

As discussed in previous chapters, ThinkEdge SE350 V2 and SE360 V2 are shipped with SED drives. But data will not be encrypted unless SED Encryption is enabled.

When SED Encryption is enabled, SED AK (Authentication Key) is used to manage the access to DEK (Data Encryption Key) in SED drives. SED AK can be generated from a passphrase or randomly by XClarity Controller. If you want to share the SED drives between multiple ThinkEdge servers, generating SED AK from a passphrase is recommended.

It's highly recommended to backup SED AK when SED encryption is enabled, in particular when the AK is generated randomly. SED AK will be exported to an external file during SED AK backup. In case of system failure, or after replacement of motherboard, users may need to restore the SED AK to obtain access to the data stored in the SED drive. If SED AK is lost, user will not be able to read the encrypted data in SED drive.

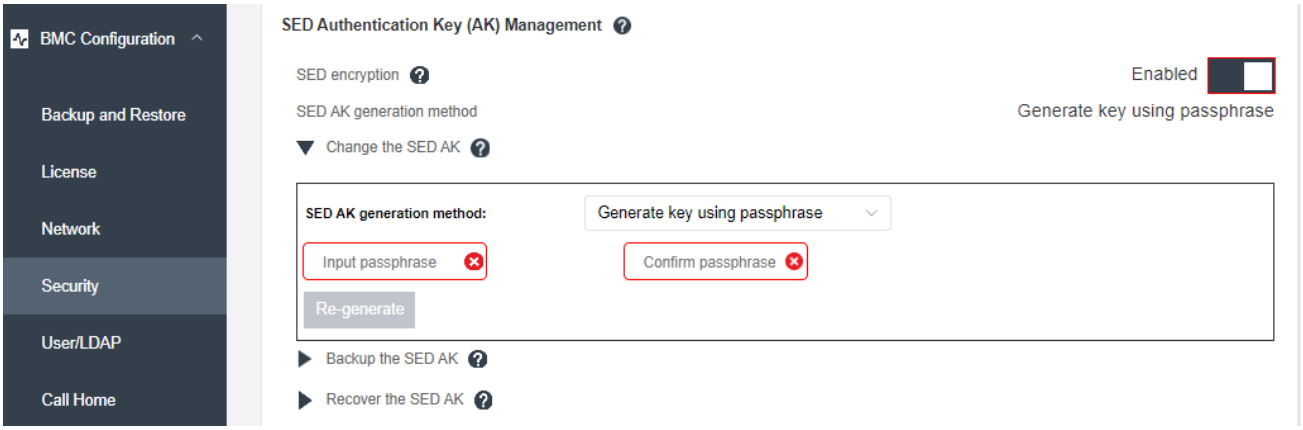


Figure 5.2 SED Authentication Key Management in XClarity Controller

5.3 Security Hardening of SUSE SLE Micro and K3S

In today's dynamic cybersecurity landscape, protecting sensitive data and maintaining system integrity is crucial. This authoritative operating system hardening guide from SuSE provides a comprehensive roadmap for securing SUSE Linux Enterprise Micro Operating System, empowering system administrators and security professionals to effectively safeguard their systems against potential threats. Through a structured approach, this guide delves into essential security measures, ensuring that your SUSE Linux Enterprise Micro environment remains robust and resilient in the face of cyberattacks.

In the ever-expanding realm of cloud-native computing, Kubernetes has emerged as a leading container orchestration platform. Its ability to automate the deployment, management, and scaling of containerized applications has made it a popular choice for organizations of all sizes. However, with increased adoption comes the need for heightened security measures. This Kubernetes hardening guide provides a comprehensive approach to securing a K3s cluster, ensuring that your containerized applications remain safe and protected from potential threats. By implementing the recommended security controls, you can effectively safeguard your K3s environment, minimizing vulnerabilities and maximizing resilience.

6 Far Edge Deployment Best Practice

6.1 Provision in staging environment

For Far Edge deployment, it is difficult to configure and provision bare-metal server in the remote Edge site due to the lack of IT expertise on-site. Generally, customers tend to get the Edge server provisioned in corporate IT room by IT engineers, or by 3rd party system integrator in a staging environment before shipping the server to remote Edge sites for operation.

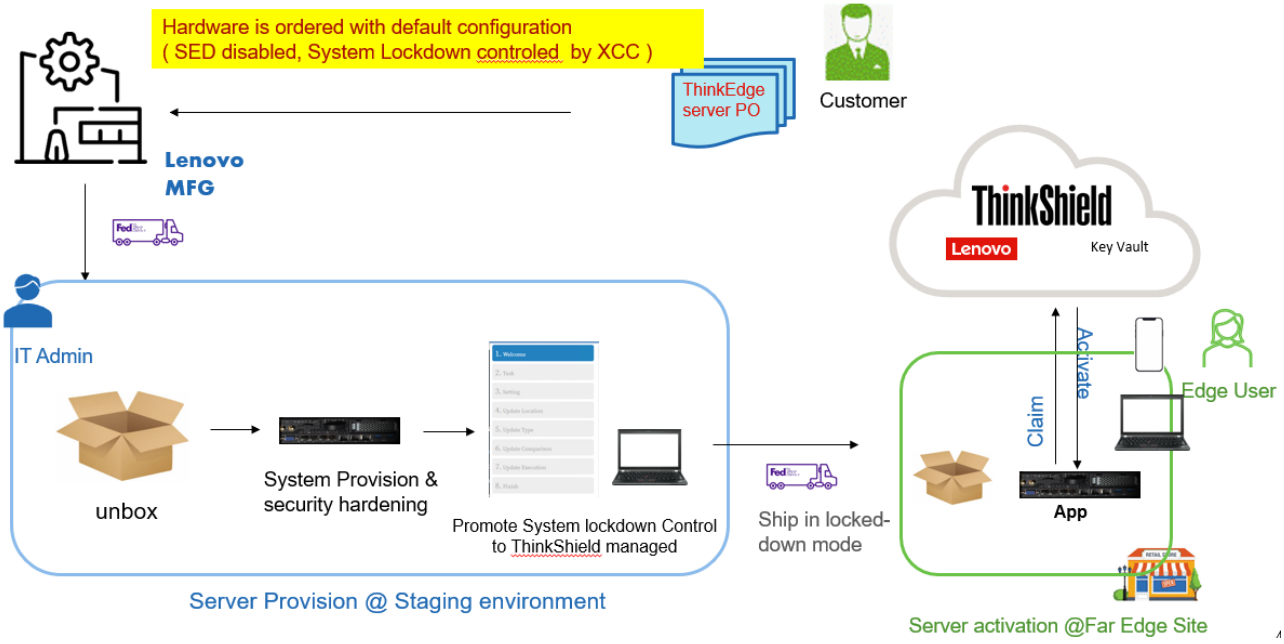


Figure 7.1 Server Provision in Staging Environment

Hardware Ordering

ThinkEdge server can be ordered with default configuration if customers plan to provision the server in a central IT room or staging environment. By default, system lockdown control is *XClarity Controller Managed*, and SED Encryption is disabled. Security settings will be configured in the staging environment as part of security hardening.

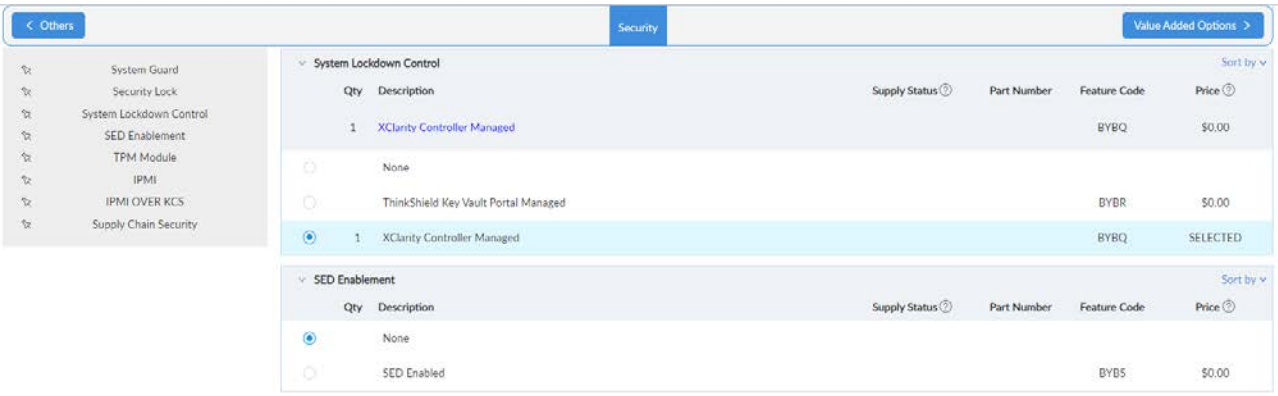


Figure 7.2 Default Security Setting in Hardware Ordering

Server Provisioning at Staging Environment

In this section, we outlined some high-level procedures to provision ThinkEdge servers in staging environment based on the best practice:

1. Change default Password of XClarity Controller

   This can be done directly in XClarity Controller Web GUI, or with LXCE OneCLI command line tool. It's highly recommended to save password of XClairty Controller in an enterprise password manager.

2. Upgrade firmware to latest version

   Get the latest firmware of Lenovo ThinkEdge SE350 V2 and SE360 V2 from Lenovo support website:

   https://datacentersupport.lenovo.com/us/en/products/servers/thinkedge/se350v2/downloads/driver-list/
   https://datacentersupport.lenovo.com/us/en/products/servers/thinkedge/se360v2/downloads/driver-list/

   Firmware update can be done in XClarity Controller Web GUI, or with LXCE OneCLI command-line tool.

3. Set up M.2 boot drive

   As best practice, it is recommended to install the operating system on a mirrored (RAID 1) pair of M.2 bootable drives. RAID configuration of M.2 bootable drive in ThinkEdge SE350 V2 and SE360 V2 is provided by Intel VROC (Virtual RAID on CPU) which can be ordered with following feature code:

Part number	Feature code	Description
4L47A39164	B96G / BS7N	Intel VROC (VMD NVMe RAID) Premium
4L47A83669	BR9B / BS7M	Intel VROC (VMD NVMe RAID) Standard

Intel VROC can be fulfilled as Feature on Demand (FoD) license and activated via XClarity Controller management console as well. Intel VROC Standard is required if only RAID 0,1 or 10 will be used for NVMe drives.

In order to enable Intel VROC for M.2 bootable drive, reboot the system and press F1, go to **System settings** > **Devices and I/O Ports** > **Intel® VMD technology** > **Enable/Disable Intel® VMD** and enable the option.

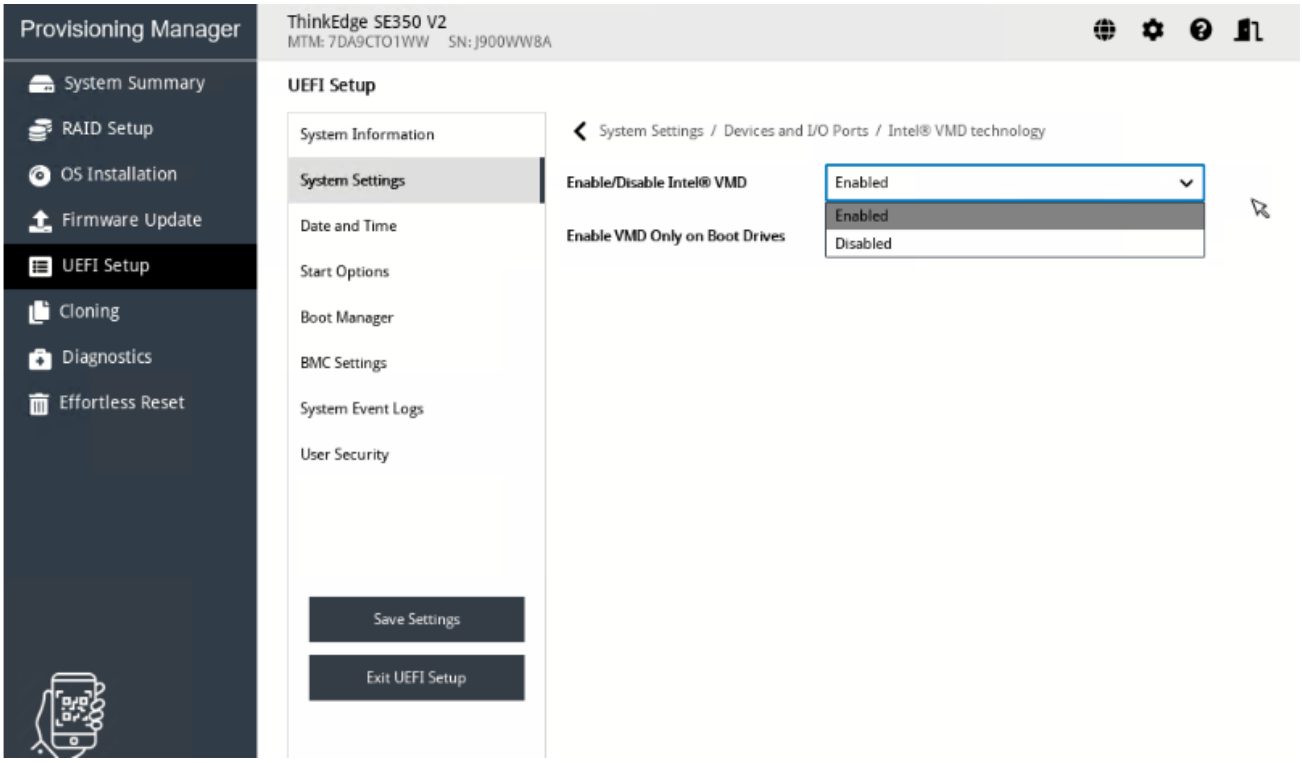


Figure 7.3 Enable Intel VMD in System setting

After Intel VROC is enabled, reboot the system and you should be able to configure RAID under XClarity Provision Manager (press F1 after the system is rebooted) under RAID Setup:

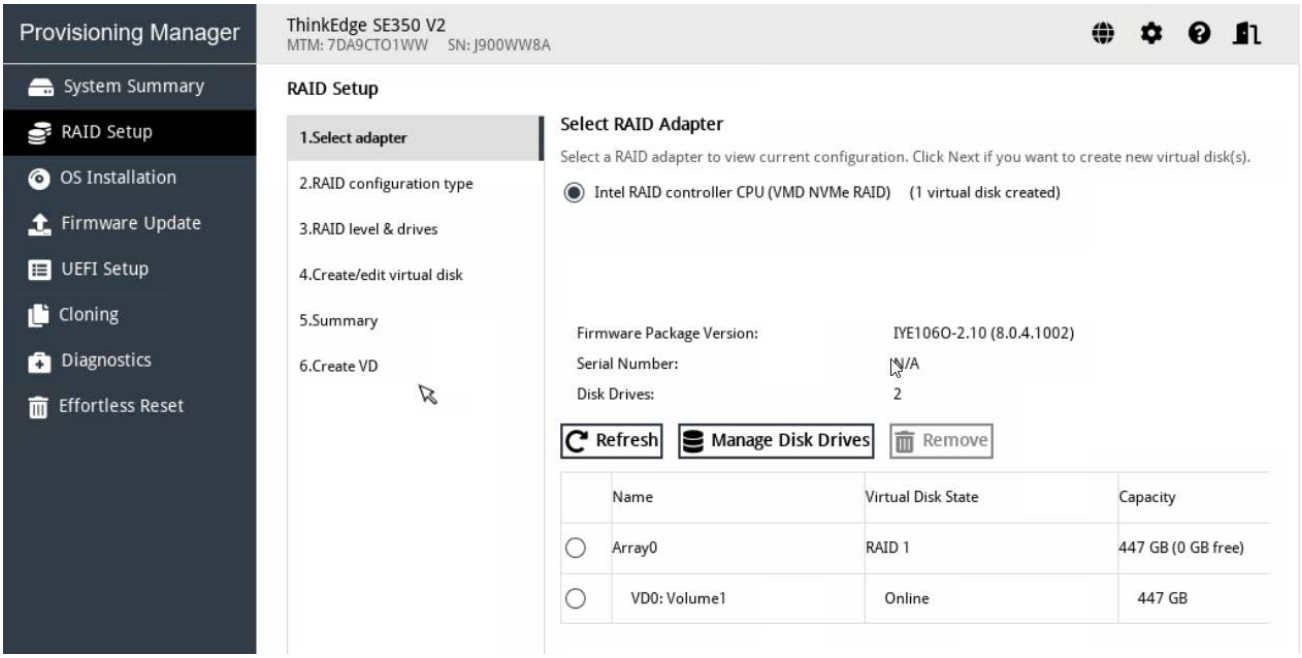


Figure 7.4 RAID Set up in System Setting

4. Install SUSE SLE Micro on M.2 bootable devices

   Lenovo XClarity Controller is designed for secure local and remote serve management. After upgrading XClarity license to “Platinum Upgrade”, users should be able to access remote console, and use virtual media to install operating systems.

   To install the SUSE operating system, download the latest version of SUSE Linux Enterprise Micro from https://www.suse.com/download/sle-micro/ as ISO image, and mount it using virtual media in the remote console. Reboot the server and follow steps from https://documentation.suse.com/sle-micro/5.5/html/SLE-Micro-all/cha-install.html to install SUSE Linux Enterprise Micro operating system on mirrored M.2 bootable drives configured in previous steps. As default configuration of SUSE SLE Micro, the root partition should be formatted to Btrfs file system to support snapshot and rolling upgrade.

5. Install K3S

   Specify the version of K3S to be installed in an environment variable, and install K3S server with embedded etcd enabled

```
# K3s_VERSION=""
# curl -sfL https://get.k3s.io | \
INSTALL_K3S_VERSION=${K3s_VERSION} \
INSTALL_K3S_EXEC='server --cluster-init --write-kubeconfig-mode=644' \
sh -s -
```

6. Security Hardening

Follow the instructions provided in chapter 6 for security hardening of system firmware, and SLE Micro operating system.

7. Turn-on SED Encryption

   After OS provisioned, it is highly recommended to enable SED encryption to protect the data stored in the SED drive.

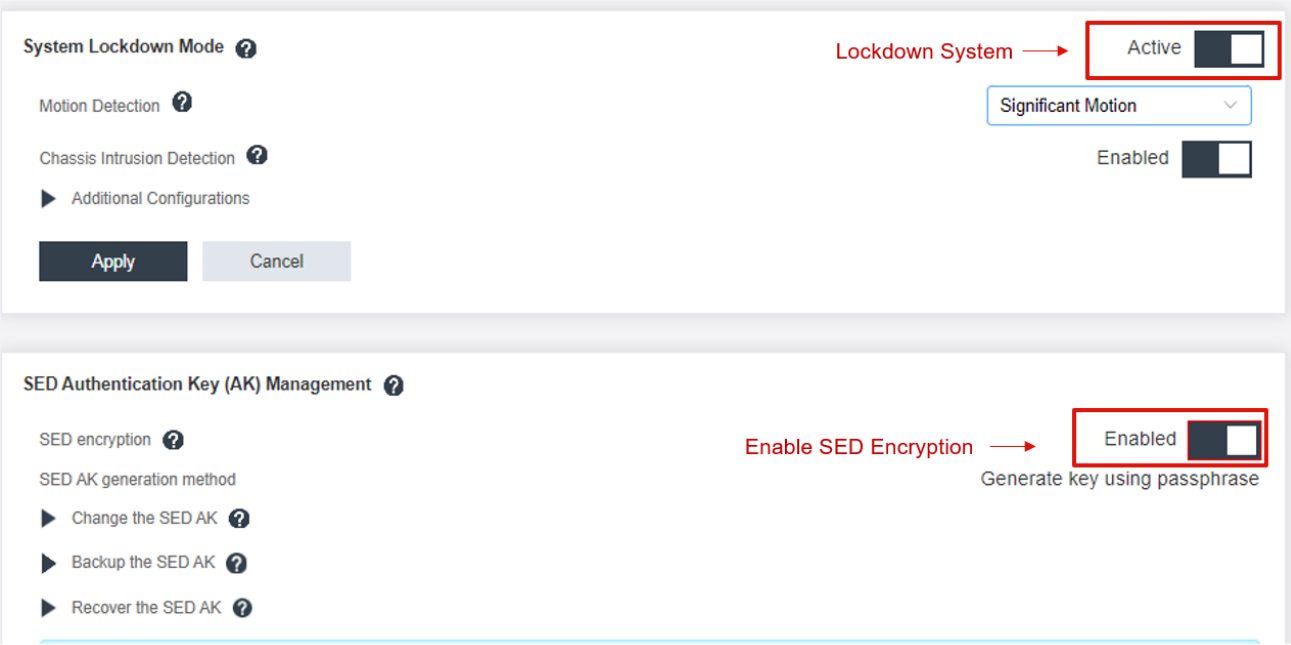


Figure 7.5 Enable SED Encryption in XClarity Controller

8. [Optional] Promote System Lockdown Control to ThinkShield Portal Managed.

   If the system will be deployed in an open space where remote access is not possible, it is recommended to promote system's Lockdown Control from XClarity Controller Managed to ThinkShield Key Vault Portal Managed. Therefore, when the system is locked down in the event of tamper detection, it can only be activated by on-site user who is authorized as owner of the system by ThinkShield Key Vault Portal.

   Promotion of the system's lockdown control to Thinkshield Key Vault Portal Managed need to be done with LXCE UpdateXpress tool on a Windows PC under Configure Security Features of ThinkEdge server. Please refer to Upgrading lockdown control mode | LXCE-UX | Lenovo Docs for details

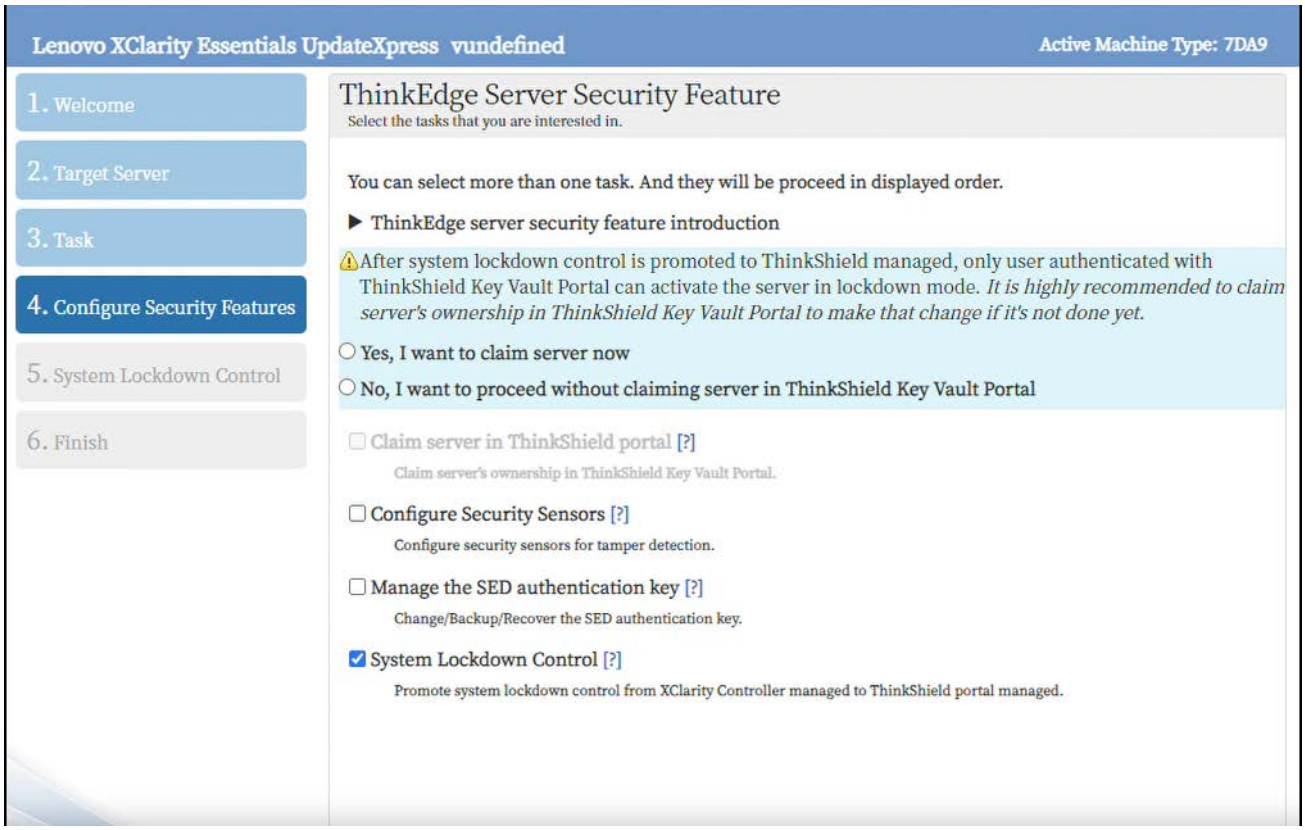


Figure 7.6 Promote System Lockdown Control in LXCE UpdateXpress

9. Lock down the server before shipping to Edge site

   Server is under unsecure environment during shipment. It is highly recommended to put the server in lockdown mode during the shipment to protected unauthorized access to the system, especially to protect the user data loaded in the system.

Receiving ThinkEdge Server at Far Edge Site

1. Activate ThinkEdge server

   As ThinkEdge server is shipped in lockdown mode, the first thing to do after the ThinkEdge server arrives at Edge site is to activate the server. Depending on how the system lockdown control is managed, the ThinkEdge server can be activated directly by administrators in the XClarity Controller Web Console, or by users authenticated with ThinkShield Key Vault Portal. Please refer to section 4.4 for details about activation of server in lockdown mode.

2. Connect the Server to customer's network at Edge site

3. Change the Network Setting of XClarity Controller if needed.

Network setting of XClarity Controller can be changed in XClarity Controller Web Console. It can also be changed with ThinkShield Mobile App. Please refer to following link for details:

https://support.lenovo.com/us/en/solutions/ht510111-how-to-modify-the-network-configuration-using-the-thinkshield-android-mobile-app

6.2 Provision in Far Edge site

As an alternative approach of Edge server provisioning, on-site user without strong IT skills can leverage Lenovo LXCE utilities and provisioning tools provided from SUSE to provision bare-metal server in Far Edge site with the configuration files and pre-built OS images provided by IT admins.

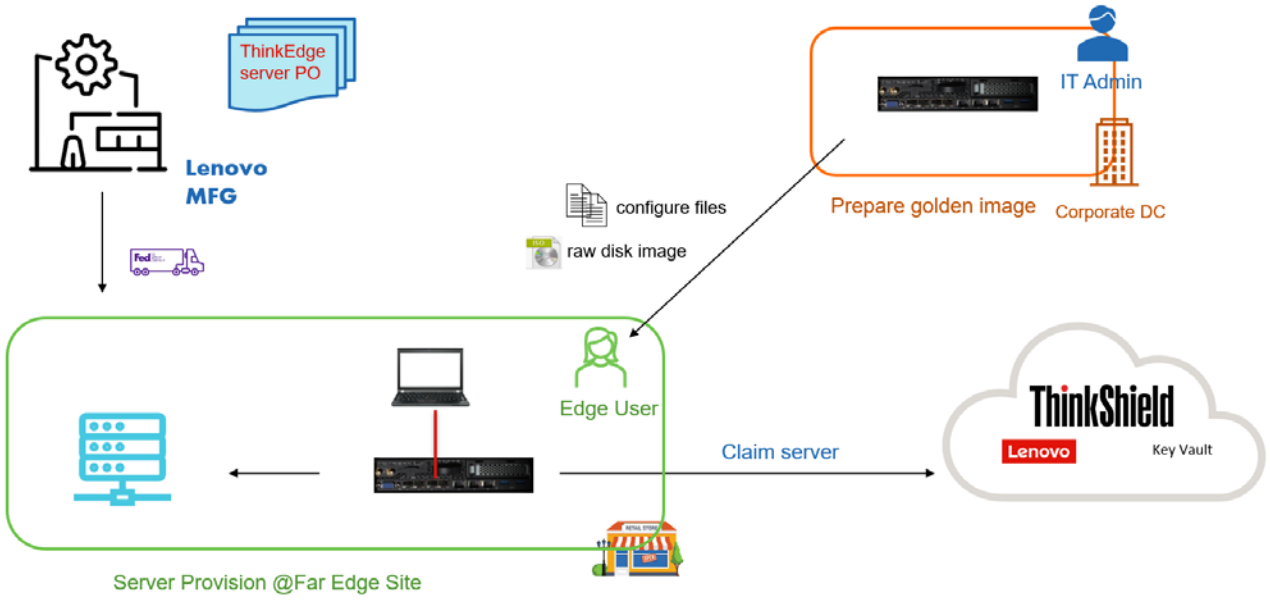


Figure 7.6 Server Provision in Staging Environment

Preparation in the IT room

In this approach, IT administrators need to prepare instructions or guidance which will be used by on-site Edge user to provision the Edge server. These instructions or guidance will be delivered to Edge user as configuration files or raw disk image.

So at first, IT administrator should provision an Edge server based on the best practice for Far Edge deployment following similar process described above:

- Upgrade Firmware to latest version
- Install SLE Micro on M.2 bootable drive
- Security hardening server's firmware and SLE Micro

Once the server is fully provisioned, it can be used as a “seed server” which can be used to generated configuration template for Edge server provisioning at remote Far Edge site. Firmware configuration can be exported to an external file with LXCE OneCLI utility tool. This file can be used as template to configure firmware of ThinkEdge server at Fat Edge site.

```
OneCli.exe config save --file fm-config.txt --bmc userid:password@host
```

In addition, IT admin also need to prepare pre-built OS image of SuSE SLE Micro operating system, as well as configuration file required to customize OS installation at Far Edge site:

- Prepare the pre-built OS image

  SUSE SLE Micro operating system can be installed using pre-built images. Currently, there are two types of images available: raw disk images and self-install ISOs. Download pre-build images from https://www.suse.com/download/sle-micro/

- Prepare OS configuration files

  Prepare Ignition and Combustin scripts to customize OS installation (like disk partition, user credentials) following instruction at https://documentation.suse.com/sle-micro/5.5/html/SLE-Micro-all/cha-images-ignition.html and https://documentation.suse.com/sle-micro/5.5/html/SLE-Micro-all/cha-images-combustion.html

OS configuration files (Ignition and Comustin scripts) are expected to be loaded from a particular location in a configuration medium. Usually configuration medium is a USB flash disk, or an ISO file which can be mounted as virtual media in the Edge server. The details of deployment of SLE Micro with pre-built image and preparation of configuration medium can be found at https://documentation.suse.com/sle-micro/5.5/html/SLE-Micro-all/cha-images-procedure.html. Firmware configuration file exported with OneCli command in the previous step can also be copied to that configuration medium and sent to Edge user at Far Edge site.

Hardware Ordering

ThinkEdge server ordered for Far Edge site deployment should have exactly same hardware BOM as the server used by IT administrator to prepare the configuration template in IT rooms. Otherwise, the configuration file prepared by IT administrator might not work for the Edge server deployed at Far Edge site.

As the Edge server will be shipped directly to Edge site for deployment, it is recommended to enable Intel VROC and configure RAID 1 volume for M.2 bootable drive in the manufactory to reduce the configuration complexity at edge site:

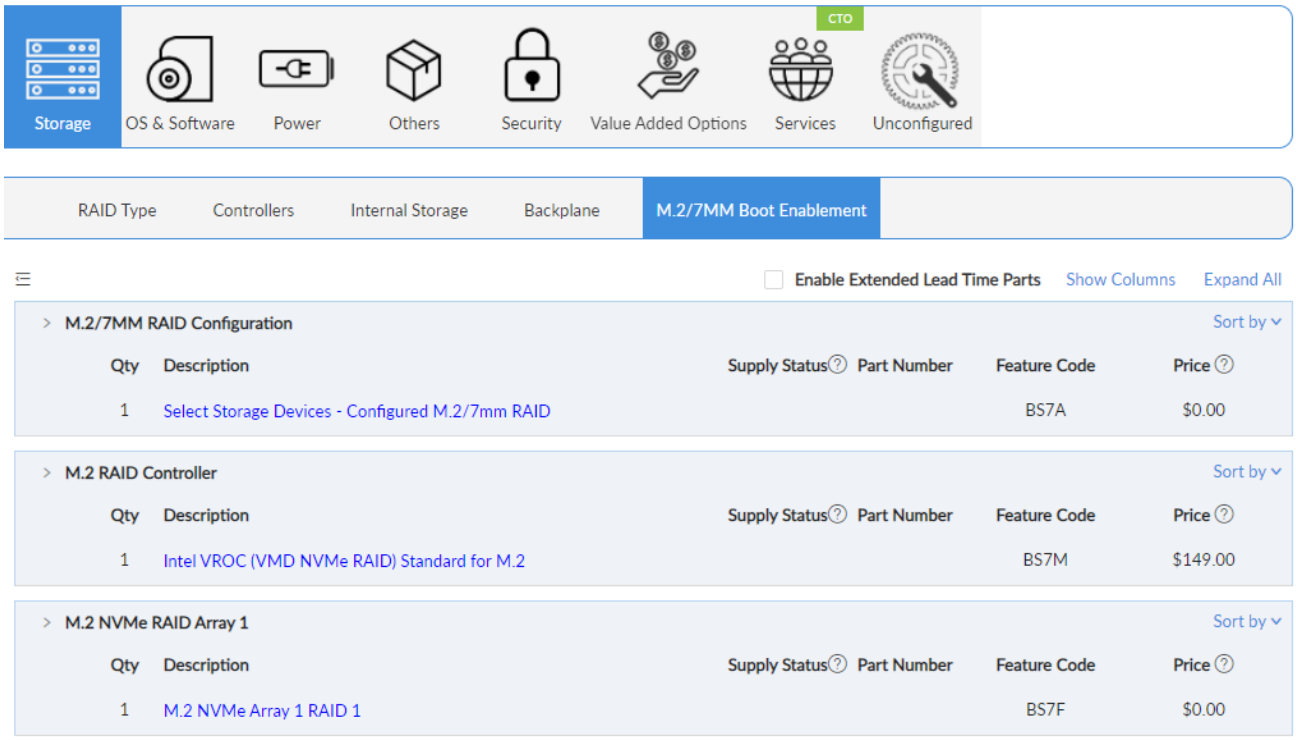


Figure 7.7 Enable RAID1 Configuration for bootable drives

Server Provision at Far Edge Site

Edge user at Far Edge site is expected to receive configuration medium (USB Flash disk or ISO file) and raw images from organization's IT admin. Upon receiving the ThinkEdge server shipped from manufacturing, Edge user can follow steps outlined below to provision the bare-metal server in Far Edge site

1. Change XCC default Password of XClarity Controller

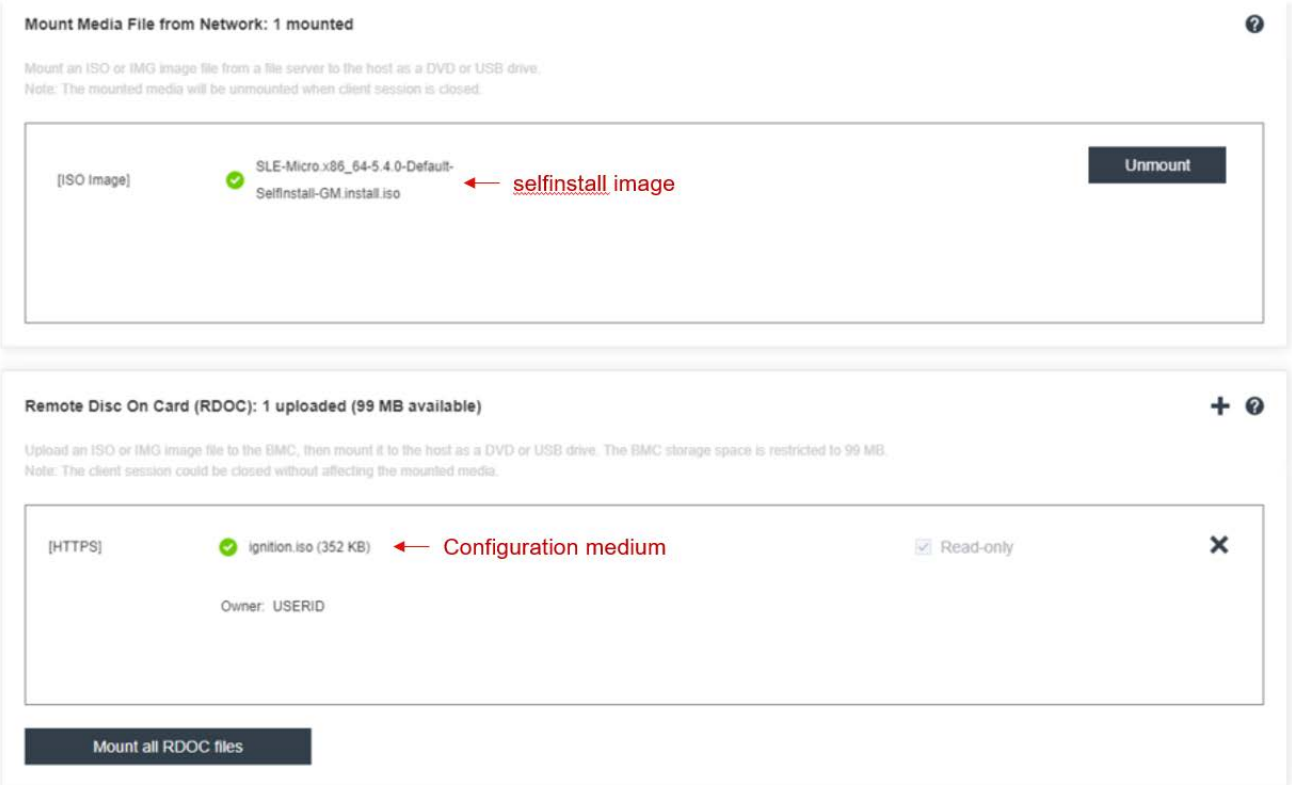
   This can be done either in XClarity Controller Web Console or with LXCE OneCli command-line tool.

2. Hardware & Firmware Configuration

   Import the firmware configuration template file using LXCE OneCli replicate command:

   ```
   OneCli.exe config replicate --file fm-config.txt --bmc userid:password@host
   ```

3. Mount SUSE SLE Micro self-install OS image and configuration medium (ISO file which contains Ignition and Combustin scripts for OS customization) as virtual media in remote console:



4. Reboot the server and OS installation will be done automatically.

   During OS installation, user only needs to specify where the OS will be installed (normally it's M.2 bootable drive). All other setting will be configured by Ignition file or Combustion script.

5. Install K3S cluster

   Specify the version of K3S to be installed in an environment variable, and install K3S server with embedded etcd enabled

```
# K3s_VERSION=""
# curl -sfL https://get.k3s.io | \
INSTALL_K3S_VERSION=${K3s_VERSION} \
INSTALL_K3S_EXEC='server --cluster-init --write-kubeconfig-mode=644' \
sh -s -
```

6. Promote System to ThinkShield Portal Managed for high security.

   It is highly suggested to promote system lockdown control from XClarity Controller Managed to ThinkShield Portal Managed if the system will be deployed in an open space where no security control is available to prevent physical access to the system. Using LXCE UpdateXpress to do promotion following the procedures documented in Upgrading lockdown control mode | LXCE-UX | Lenovo Docs.

7 Appendix A: Lenovo bill of materials

This appendix contains the bill of materials (BOMs) of ThinkEdge SE350V2 and SE360V2 server for deploying a single-node of K3S cluster on SUSE SLE Micro OS.

Lenovo ThinkEdge SE350 V2

Part #	Description	Qty
BS3S	ThinkEdge SE350 V2 Chassis	1
BS3U	ThinkEdge SE350 V2 4x 1Gb, 2x 2.5Gb(TSN) I/O Module	1
BFYE	Operating mode selection for: "Efficiency - Favoring Performance Mode"	1
BW2H	System Operational Temperature 5C to 40C / 41F to 104F	1
BS41	ThinkEdge SE350 V2/SE360 V2 Planar with Intel Xeon D-2733NT 8C 80W 2.1 GHz	1
B964	ThinkSystem 32GB TruDDR4 3200 MHz (2Rx4 1.2V) RDIMM	2
5977	Select Storage devices - no configured RAID required	1
BC4V	Non RAID NVMe	1
BS45	ThinkSystem 7mm U.3 7450 MAX 800GB Mixed Use NVMe PCIe 4.0 x4 HS SSD	2
BM8E	ThinkSystem 7mm S4520 1.92TB Read Intensive SATA 6Gb HS SSD	2
BNWP	ThinkSystem MicroSD 32GB Class 10 Flash Memory Card	1
BS48	ThinkEdge SE350 V2 7mm SSD Module	1
BS7A	Select Storage Devices - Configured M.2/7mm RAID	1
BS7M	Intel VROC (VMD NVMe RAID) Standard for M.2	1
BS7F	M.2 NVMe Array 1 RAID 1	1
BS46	ThinkSystem M.2 7450 PRO 480GB Read Intensive NVMe PCIe 4.0 x4 NHS SSD (with Heatsink)	2
BW2G	AC Power Cord to external 300W adapter mode	1
BS4A	ThinkEdge SE350 V2 DC Power Input Board	1
BU98	ThinkEdge SE350 V2 12-48V DC Power Module Board	1
BW2K	ThinkEdge 300W 230V/115V External Power Supply	2
BW2I	ThinkEdge SE350 V2 External 300W Bridge Cable	2
6201	1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	2
BS4E	ThinkEdge 130mm USB-C to VGA Display Cable	1
B755	Desktop Mode	1
B6Q3	ThinkEdge Rubber Feet	1
BYBQ	XClarity Controller Managed	1
B0MK	Enable TPM 2.0	1
B7XZ	Disable IPMI-over-LAN	1
BB98	Disable IPMI-over-KCS	1
A2N7	Planar Not Integrated With Chassis	1
B0ML	Feature Enable TPM on MB	1
2302	RAID Configuration	1
BRPJ	XCC Platinum	1
BS7J	M.2 NVMe Array 1 HDDs	2

B8KY	Thinksystem WW Lenovo LPK	1
BS4W	ThinkEdge SE350 V2 Front IO Bezel (1G) Assembly	1
BS4Z	ThinkEdge SE350 V2 MB to IO Board Power Cable	1
BS55	ThinkEdge SE350 V2 HDD Backplane Power Cable	1
BSF5	ThinkEdge SE350 V2 7mm HDD Cage Label	1
BS52	ThinkEdge SE350 V2 HDD Backplane1 PCIe Cable	1
BS53	ThinkEdge SE350 V2 HDD Backplane2 PCIe Cable	1
BS54	ThinkEdge SE350 V2 HDD Backplane1 SATA Cable	1
BVE3	ThinkEdge SE350 V2 Node WW Packaging	1
BTPQ	ThinkEdge SE350 V2 DC Power Input Board to DC Power Module Board Cable	1
BS4K	ThinkEdge SE350 V2 Top Cover	1
BS4L	ThinkEdge SE350 V2 Bridge Board	1
BS4M	ThinkEdge SE350 V2 Operational Panel Module	1
BS4X	ThinkEdge SE350 V2 MB to Operational Panel Cable	1
BS4Y	ThinkEdge SE350 V2/SE360 V2 Intrusion Cable	1
BTPN	ThinkEdge SE350 V2 REGID	1
BVE5	ThinkEdge SE350 V2/SE360 V2 Dust Cover Kit for I/O Ports	1
BSF0	ThinkEdge SE350 V2 Node Label GBM	1
BSF1	ThinkEdge SE350 V2 Node SSL_LI	1

Lenovo ThinkEdge SE360 V2

Part#	Description	Qty
BS56	ThinkEdge SE360 V2 Chassis	1
BS58	ThinkEdge SE360 V2 4x 1Gb, 2x 2.5Gb(TSN) I/O Module	1
BW2H	System Operational Temperature 5C to 40C / 41F to 104F	1
BFYE	Operating mode selection for: "Efficiency - Favoring Performance Mode"	1
BS41	ThinkEdge SE350 V2/SE360 V2 Planar with Intel Xeon D-2733NT 8C 80W 2.1 GHz	1
B964	ThinkSystem 32GB TruDDR4 3200 MHz (2Rx4 1.2V) RDIMM	2
5978	Select Storage devices - configured RAID	1
AVV0	On Board SATA Software RAID Mode	1
BC4V	Non RAID NVMe	1
B9XB	Controller 1 No RAID Array	1
BBP4	Controller 2 SW RAID Array 1 RAID 1	1
BM8E	ThinkSystem 7mm S4520 1.92TB Read Intensive SATA 6Gb HS SSD	2
BNWP	ThinkSystem MicroSD 32GB Class 10 Flash Memory Card	1
BS7A	Select Storage Devices - Configured M.2/7mm RAID	1
BS7M	Intel VROC (VMD NVMe RAID) Standard for M.2	1
BS7F	M.2 NVMe Array 1 RAID 1	1
BS46	ThinkSystem M.2 7450 PRO 480GB Read Intensive NVMe PCIe 4.0 x4 NHS SSD (with Heatsink)	2
BS5J	ThinkEdge SE360 V2 Riser Assembly (PCIe Riser + 7mm Backplane)	1

BW2G	AC Power Cord to external 300W adapter mode	1
BS4B	ThinkEdge SE360 V2 12-48V DC Power Module Board	1
BS5N	ThinkEdge SE360 V2 DC Power Input Board	1
BW2K	ThinkEdge 300W 230V/115V External Power Supply	2
BW2J	ThinkEdge SE360 V2 External 300W Bridge Cable	2
6313	2.8m, 10A/120V, C13 to NEMA 5-15P (US) Line Cord	2
BS5W	ThinkEdge SE360 V2 Fan Assembly (Front to Rear)	1
BS4E	ThinkEdge 130mm USB-C to VGA Display Cable	1
B755	Desktop Mode	1
B6Q3	ThinkEdge Rubber Feet	1
BS5S	ThinkEdge SE360 V2 Kensington Lock Kit	1
BYBQ	XClarity Controller Managed	1
B0MK	Enable TPM 2.0	1
B7XZ	Disable IPMI-over-LAN	1
BB98	Disable IPMI-over-KCS	1
A2N7	Planar Not Integrated With Chassis	1
2302	RAID Configuration	1
B0ML	Feature Enable TPM on MB	1
BRPJ	XCC Platinum	1
BBMA	Controller 2 SW RAID Array 1 HDDs	2
BS7J	M.2 NVMe Array 1 HDDs	2
B8KY	Thinksystem WW Lenovo LPK	1
BS6P	ThinkEdge SE360 V2 HDD Backplane PCIe Cable	1
BS6Q	ThinkEdge SE360 V2 HDD Backplane SATA Cable	1
BS6V	ThinkEdge SE360 V2 HDD Backplane Power Cable	1
BS5X	ThinkEdge SE360 V2 WW Packaging	1
BS69	ThinkEdge SE360 V2 Top Cover	1
BSFU	ThinkEdge SE360 V2 Riser Label LI (PCIe + 7mm)	1
BTJK	ThinkEdge SE360 V2 Air Baffle for Processor	1
BULN	ThinkEdge SE360 V2 PCIe Dummy Filler Low Profile	1
BS66	ThinkEdge SE360 V2 IO Cover Assembly for 1GbE I/O Module	1
BS6G	ThinkEdge SE360 V2 IO Board to MB Cable	1
BS6H	ThinkEdge SE360 V2 MB IO Board Power Cable	1
BS63	ThinkEdge SE360 V2 Operational Panel Module	1
BS64	ThinkEdge SE360 V2 Rear Operational Panel Module	1
BS6D	ThinkEdge SE360 V2 OP Panel Cable	1
BS6E	ThinkEdge SE360 V2 Operational Panel to Rear Operational Cable	1
BT93	ThinkEdge SE360 V2 DIMM Pen Tool	1
BTPP	ThinkEdge SE360 V2 REGID	1
BTPS	ThinkEdge SE360 V2 Chassis Intrusion Cable	2
BVE5	ThinkEdge SE350 V2/SE360 V2 Dust Cover Kit for I/O Ports	1
BTJM	ThinkEdge SE360 V2 DC Power Module Board Air Baffle	1
BS50	ThinkEdge SE360 V2 DC Power Input Board to DC Power Module Board Cable	1

BSFK	ThinkEdge SE360 V2 Node Label GBM	1
BT8Z	ThinkEdge SE360 V2 Node Bottom SSL_LI	1
BSFL	ThinkEdge SE360 V2 Node SSL_LI	1
BSN2	ThinkEdge SE360 V2 Enclosure SMA Filler	2

Document History

Version 1.0	20 Jan 2024	• Initial version