Lenovo XClarity Controller 3 (XCC3)
Product Guide

Most of the Lenovo ThinkSystem V4 servers contain an integrated service processor, XClarity Controller 3 (XCC3), which provides advanced service-processor control, monitoring, and alerting functions. XCC3 consolidates the service processor functionality, super I/O, video controller, and remote presence capabilities into a single chip on the server system board.

XCC3 is based on an OpenBMC design, using the AST2600 baseboard management controller (BMC) with a dual-core ARM Cortex A7 32-bit RISC service processor running at 1.2 GHz.
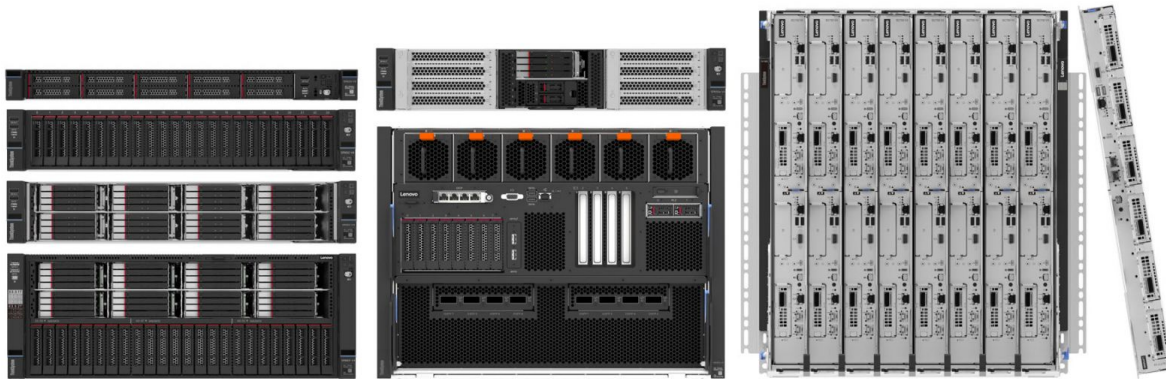

Figure 1. ThinkSystem V4 servers include the XCC3 integrated service processor

Did you know?

You can reduce the Ethernet connections needed for remote management by implementing ThinkSystem OCP 4 to 1 Management Port Consolidation Adapter. For more information see the Management Port Consolidation Adapter section.

XCC3 has the capability to manage and configure multiple XCC3-based servers from the one console. For more information see the Neighbor Group section.

With the System Guard feature, you can monitor hardware inventory for unexpected component changes, and simply log the event, or if needed, you can prevent the servers from booting. For more information, see the System Guard section.

Management Port Consolidation Adapter

The XClarity Controller uses two network controllers. One network controller is connected to the dedicated management port and the other network controller is connected to the shared port.

If using the Shared port option, there is an adapter that installs in the OCP slot that allows four servers to share the one Ethernet connection providing the possibility to reduce the number of Ethernet connections needed for remote management on some ThinkSystem V3 and ThinkSystem V4 servers. The adapter implements a 5-port Gigabit switch based on the Microchip KSZ9896 switch chip.

Ordering information is listed in the following table.

Table 1. 4-to-1 Management Port Consolidation Adapter supported in SD550 V3, SD530 V3, SD535 V3, SR650a V4, SR630 V4 and SR650 V4 servers

Part number	Feature code	Description
4XC7A90299	BZGE	ThinkSystem OCP 4 to 1 Management Port Consolidation Adapter Contains: ● 1x OCP adapter ● 2x 0.45m blue Cat5e cable ● 1x 0.25m blue Cat5e cable

The adapter is installed in the OCP slot of one server, as shown in the figure below. The adapter connects to the remote management port of up to three other servers via the included (or other) Ethernet cables. The OCP slot in the other three servers can be used for network connectivity, if desired.
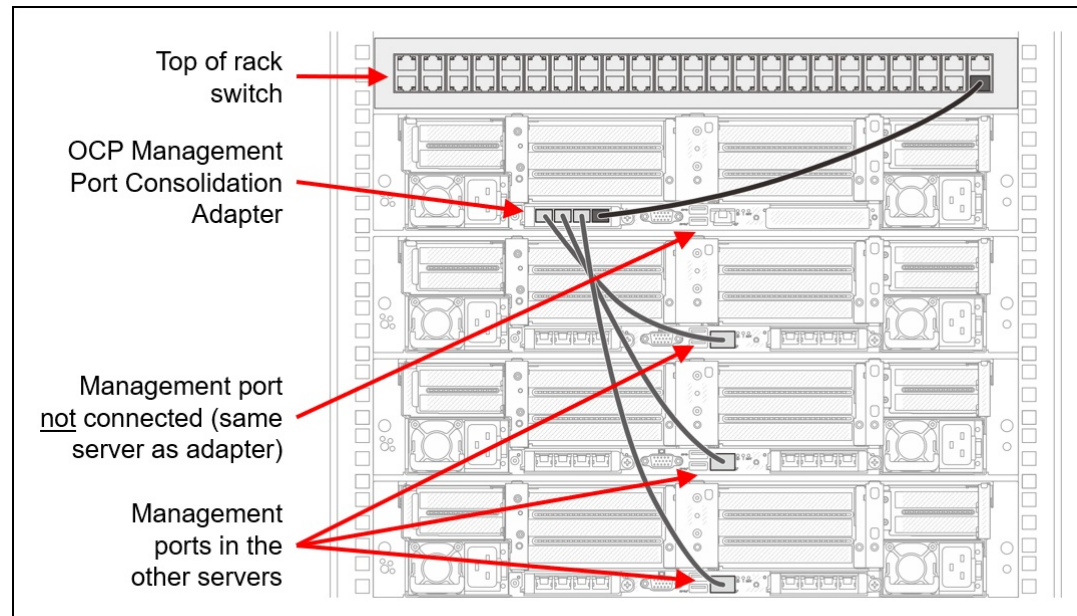

Figure 2. Connections to the ThinkSystem OCP 4 to 1 Management Port Consolidation Adapter

The adapter has four RJ45 ports. One port of the adapter connects to the local remote management port and the other three adapter ports connect to the remote management ports of three nearby servers. Either the included short Cat5e cables can be used or customer-supplied Cat5e Ethernet cables can be used.

Configuration notes:

● The adapter is only supported in OCP slot 1

- When the adapter is installed in slot 1, OCP slot 2 is disabled and cannot be used
- The OCP slot in the other three servers can be used for network connectivity, if desired.
- On the server with the adapter installed, in System Setup (F1 at boot), change **BMC settings > Network Settings > Network Interface port** to **Uplink MAC**.
- The connected servers can be any mix of servers that support the adapter. For example, they do not all have to be SR630 V4 servers.

For more information on the ThinkSystem OCP 4 to 1 Management Port Consolidation Adapter, see the relevant product guides for the servers supporting this adapter .

Comparing XCC3 to XCC2

The main difference between XCC2 and XCC3 is that XCC3 is OpenBMC-based. OpenBMC is an open-source server management stack that enhances security and frees you from vendor lock-in, all with flexible, modern infrastructure control. XCC3's adoption of OpenBMC, with full Redfish alignment, enables seamless integration with Lenovo or third-party software, which provides a consistent, standardized approach.

Redfish provides the standardized, programmatic interface that makes automation possible and OpenBMC provides a secure, transparent, and flexible open-source platform on which the Redfish interface runs.

Together, OpenBMC and Redfish create a powerful and secure foundation for automating a wide range of IT tasks at the hardware level, from zero touch deployment and configuration to monitoring and firmware updates. This is a fundamental shift towards more efficient, reliable, and secure data center and edge operations.

There are advantages to both Lenovo and customers in the following areas:

- Innovation and Agility
  - Faster adoption of new features from open-source Development
  - Community-driven innovation cycle

- Security and Transparency
  - Transparent development – easier to audit and validate
  - Regular security updates from a global developer community

- Interoperability
  - Standards-based (Redfish, IPMI) for broad compatibility
  - Easier integration into existing management tools

- Scalability
  - Scales from single servers to large fleets
  - Scales for both cloud-native and traditional data center environments

Features

There are two levels of features of XCC3: Standard and Premier.

XCC3 Standard

XClarity Controller 3 Standard level offers the features and capabilities detailed below, and more. For a full list of all features and capabilities, see the following link:
https://pubs.lenovo.com/xcc3/nn1ia_c_standardlevelfeatures

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware

- Configuring server settings and devices
- Real-time power and thermal utilization monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected
- FIPS 140-2 compliant encryption
- REST API interface
- Blue Screen Capture (OS Failure, in FFDC)
- Embedded Diagnostic Tools
- Call home capability

XCC3 Premier

XClarity Controller 3 Premier adds the following functionality to the Standard features:

- **Event Logs**
  - Component Replacement Log

- **RAS**
  - Boot Capture
  - Crash Video Capture

- **Alerts**
  - Syslog

- **Remote Presence**
  - Remote KVM
  - Mounting of local client IO/IMG files
  - Quality/Bandwidth Control
  - Virtual Console Collaboration (6 users)
  - Virtual Console Chat
  - Video Record/Replay
  - Virtual Media mounting of remote ISO/IMG files http, Samba & NFS
  - Remote Console Java Client

- **Serial Redirection**
  - Serial Redirection via SSH-CLI

- **Security**
  - Single Sign-On
  - Security Key Lifecycle Manager (SKLM/KMIP)
  - IP address blocking
  - Enterprise Strict Security mode (CNSA compliant) (new feature)
  - System Guard

- **Power Management**
  - Power Capping
  - OOB Performance Monitoring — System Performance metrics
  - Real time Power Graphics
  - Historical Power Counters
  - Temperature Graphics

- **Deployment & Configuration**
  - Remote OS Deployment

- **Firmware Updates**
  - Sync with Repository
  - Firmware bundle update
  - Firmware rollback from the local repository in MicroSD card

- **Additional management functions**
  - Neighbor group management

For details on each of the features, please refer to the various sections in the XCC3 Online User Guide Documentation:
https://pubs.lenovo.com/xcc3/

Management interfaces

XCC3 can be accessed remotely via these methods:

- **Command-line interface.** To access the CLI interface, use SSH to log in to the management processor.

- **Web-based interface.** Web browser - HTML 5-based browser interface (Java and ActiveX not required) using a responsive design (content optimized for device being used - laptop, tablet, phone) with NLS support. To access the web-based interface, point your browser to the IP address for the management processor. The new intuitive interface includes at-a-glance visualizations and simple access to common system actions. The dashboard is shown in the following figure.
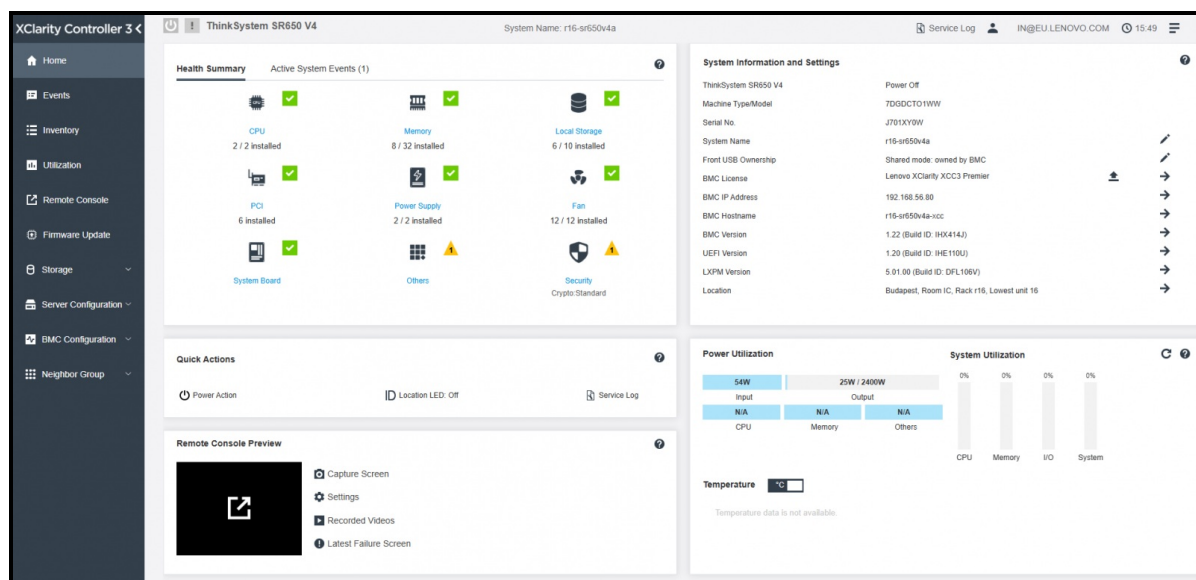

Figure 3. XClarity Controller 3 Web interface dashboard

XCC3 can also be accessed remotely through industry-standard interfaces:

- Representational State Transfer (REST) support

- Redfish support (DMTF compliant) currently with specification v1.17.0 -schema bundle is 2024.3

- Intelligent Platform Management Interface (IPMI) Version 2.0

- Simple Network Management Protocol (SNMP)
    - Version 3 supported (no SET commands)
    - Version 1 supported, traps only

- Common Information Model (CIM-XML)

- Data Center Manageability Interface (DCMI) Version 1.5

Access via the XClarity Mobile app

XCC3 can also be managed locally from the XClarity Mobile app on a phone or table. The mobile device is physically attached to the server via a USB cable connected to a front USB port with XClarity Controller access.

The steps to enable this tethering function are as follows:

1. If you haven't done so already, install the XClarity Mobile app on your mobile device.
2. Enable USB Management on the server, by holding down the ID button for 3 seconds (or pressing the dedicated USB management button if one is present)
3. Connect the mobile device via a USB cable to the server's USB port with the management symbol

4. In iOS or Android settings, enable Personal Hotspot or USB Tethering
5. Launch the XClarity Mobile app

Once connected you can see the following information via a Virtual Operator Panel:

- System status, firmware, network, health, and alerts information (read only, no login required)
- Server management functions including configuring systems management and network settings, and controlling system power (power on, power off, restart) (XClarity login credentials required)

For more information on the XClarity Mobile App see the following page:
https://pubs.lenovo.com/lxca/lxca_usemobileapp

Part numbers

Models of the ThinkSystem V4 server family come with either XCC3 Standard or XCC3 Premier, depending on the server type and the model, as described in the Server support section.

Important considerations:

- If you will be using XClarity One, XClarity Administrator, or XClarity Orchestrator for tasks such as remote control and Bare Metal Operating System Deployment then the XCC3 Premier level must be installed on the server.
- XCC3 Premier license includes hardware license for Lenovo XClarity Energy Manager (LXEM), a power and temperature management solution for data centers.

The following table shows the field upgrades available for models that come with XCC3 Standard.

Table 2. XCC3 field upgrades

Part number	Description
7S0X000XWW	Lenovo XClarity Controller 3 (XCC3) Premier

For configure-to-order (CTO) models, the XCC3 Premier Upgrade feature code listed in the following table is usually selected and included by default in the order. If desired, you can remove this feature code if only the Standard level is required.

Table 3. XCC3 upgrades for configure-to-order

Feature code	Description
SCY0	Lenovo XClarity Controller 3 (XCC3) Premier

Server support

The following table shows what level of XCC3 is included with each ThinkSystem V4 server. Supported servers are also detailed at the Lenovo XClarity Controller overview page, https://pubs.lenovo.com/lxcc-overview/.

Table 4. Server support

Server	XCC3 Standard	XCC3 Premier	
		CTO orders	Preconfigured models
SR630 V4	Included	Included (customizable)*	Varies**
SR650 V4	Included	Included (customizable)*	Varies**
SR650a V4	Included	Included (customizable)*	Varies**
SR680a V4	Included	Included (customizable)*	Not applicable
SR850 V4	Included	Included	Included
SR860 V4	Included	Included	Included
SC750 V4	Included	Included (customizable)*	Not applicable
SC777 V4	Included	Included	Not applicable

* XCC3 Premier is included in CTO orders by default, but can be deselected in Lenovo Data Center Solution Configurator (DCSC) if desired, however please ensure to refer to the Premier License feature list to see what would not be included.

** Some preconfigured models of the server have XCC3 Premier included. See the Models section of the product guide for specifics.

Security dashboard

XCC3 provides a security dashboard which shows an overall security assessment and status of the system. Providing status on:

- **BMC Security Events** report events asserted by security issues, such as chassis intrusion, PFR detected corruption, System Guard detected hardware inconsistency, security jumper open on planar, etc.
- **BMC Security mode** provides an overall status of Security Mode compliance.
- **BMC Services & Ports** enumerate all insecure services/ports enabled but non-compliant with the current Security Mode.
- **BMC Certificates** list all non-compliant certificates used by XCC3.
- **BMC User Accounts** provide general suggestions on how to make the account and password management more secure.

The dashboard shows a warning icon if there is any risk in these security areas scanned by XCC3. The detail link under each category also brings the user to the setup page to solve the issues.
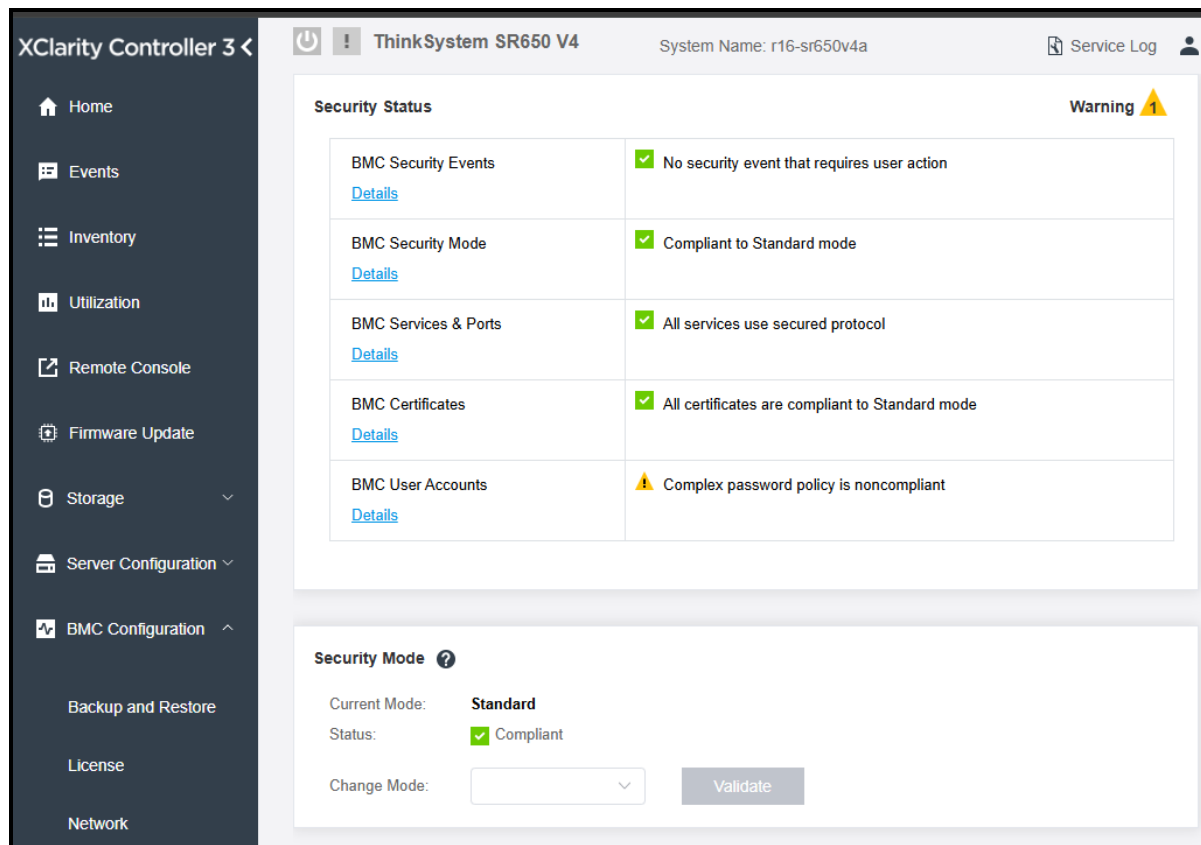

Figure 4. XCC3 Security Status dashboard, highlighting a warning on User Accounts

Service and support

With XCC3-based servers, customers can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using the Call Home function.

Figure 5. XCC3 Call Home

When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure.

Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later.

Lenovo is committed to the security of customer data : Customer business data is never transmitted and access to service data in the Lenovo Support Center is restricted to authorized service personnel.

If the customer is managing their servers with XClarity One, XClarity Administrator or XClarity Orchestrator they can choose to configure centralized Call Home via XClarity One, XClarity Administrator or XClarity Orchestrator, rather than at each XCC3 instance. these XClarity Solutions will additionally provide the capability to view information about service tickets that were manually and automatically submitted to the Lenovo Support Center using Call Home, including the current status and associated service files that were transferred to the Lenovo Support Center, and service tickets that were generated by support services other than Call Home.

For full details see more information at the appropriate links below depending on the XClarity Solution being used for Call home:

- XClarity One (LXC1) working with service and support
- XClarity Administrator (LXCA) working with service and support
- XClarity Orchestrator (LXCO) working with service and support

For details on which events per system will automatically notify support, go to Events and alerts for servers page in the LXCA User Guide, click the link for the specific server, then select submenu entry for **XCC events that automatically notify Support**.

Enhancements included with XCC3 Premier

XCC3 Premier license adds the same features as the XCC 2 Platinum License, as detailed in Features section.

The XCC3 also includes key features which were introduced with the release of XCC2 Platinum, as follows:

- System Guard – Monitor hardware inventory for unexpected component changes, and simply log the event or prevent booting.
- Enterprise Strict Security mode – Enforces FIPS 140-3 level security and enhanced NIST 800-193
- Neighbor Group Feature Group – Enables administrators to manage and synchronize configurations and firmware level across multiple servers.
- XCC3 Service Log – Service tool that provides XCC3 first-failure logs in HTML and JSON format.

For details, see the following sections:

- System Guard
- Enhanced Security Modes
- Neighbor Group
- Service Log

System Guard

To ensure your server arrives as it left Lenovo manufacturing, and confirm nothing has changed along the way, with the XCC3-based servers, customers can request to have the System Guard feature enabled before shipment of their Server. System Guard feature takes a snapshot of the hardware component inventory as trusted reference, then monitors for any deviation from the reference snapshot. When deviation occurs, it can report an event to the user, optionally, can also prevent the server from booting into the OS and prompt the user for response.
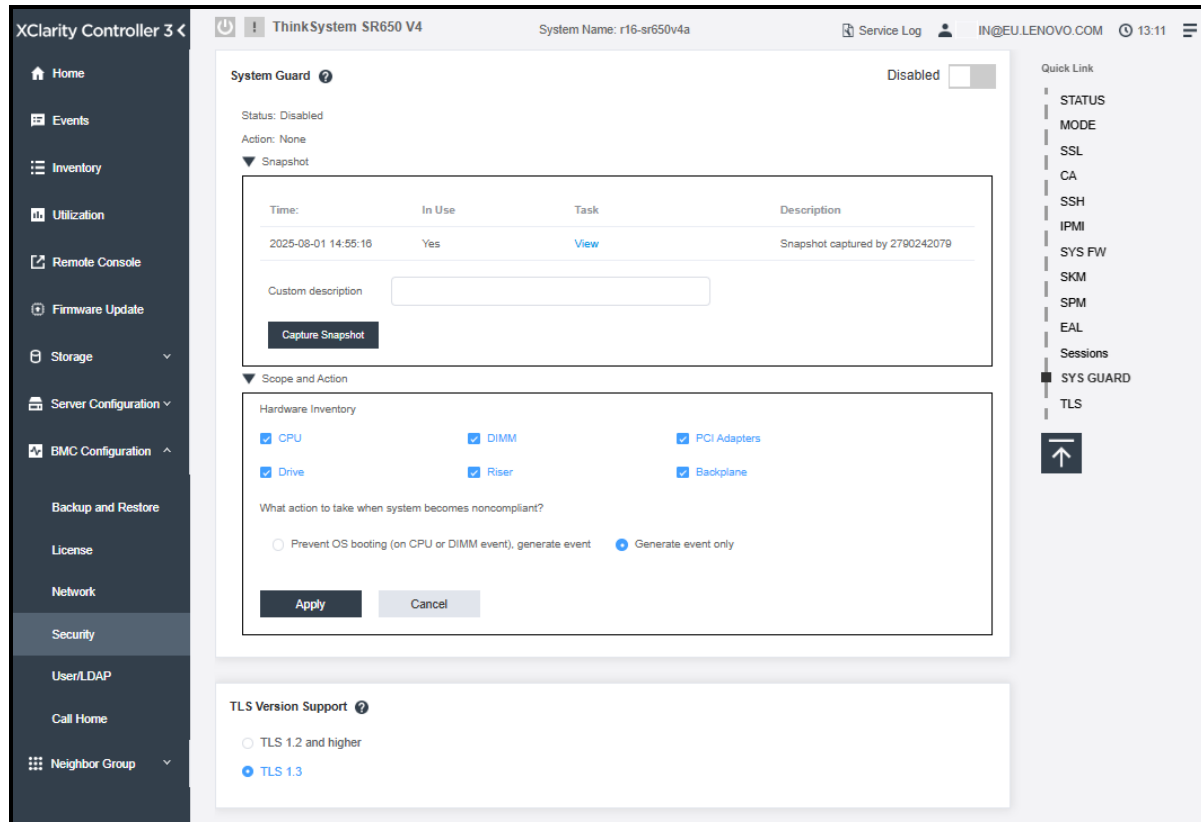
Figure 6. System Guard

User can also take a snapshot at any time even while the feature is disabled. The generation of snapshot takes around one minute. User can select a subset of hardware components to enforce and select a corresponding action to take when deviation is detected.

Deviation detection is executed at server power on (POST) or system reboot. For example, while the OS is still running, if a disk drive is being pulled out and then plugged back in a moment later, System Guard is not going to record the event or take any action. If the extracted disk drive remains absent until next reboot, then System Guard would get in action.

For more information on working with System Guard see System Guard in the XCC3 User Guide.

Enhanced Security Modes

Like XCC2, XCC3 Enhanced Security Modes are also configurable.

- The XCC3 Standard license enables the users to configure their servers in one of the two Security Modes: Standard Mode and Compatibility Mode. These are available in all XCC3-based servers.
- The XCC3 Premier license comes with a third Security Mode: Enterprise Strict Mode. This mode is most suitable for high-level security requirements.
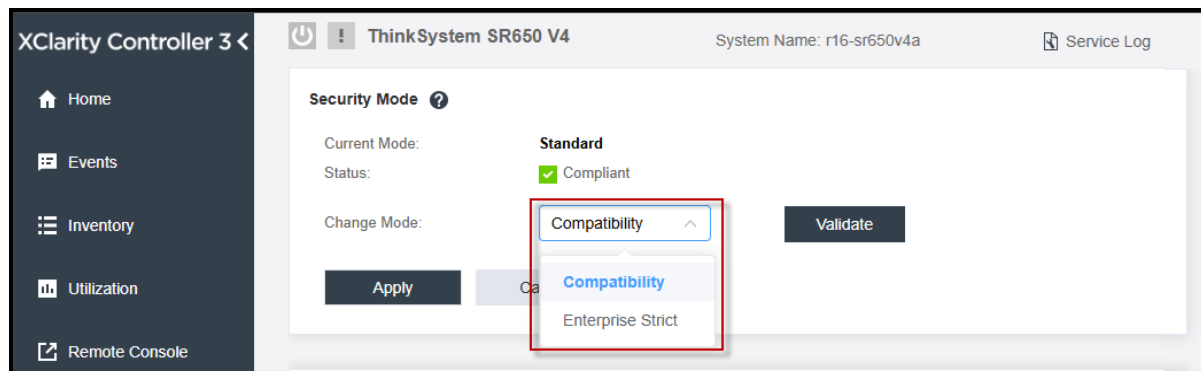
Figure 7. Security Mode in XCC3

Each of the security modes has defined characteristics, as follows:

- **Enterprise Strict Security Mode**
  - Enterprise Strict Security Mode is the most secure mode.
  - Commercial National Security Algorithm Suite (CNSA) compliant.
  - NIST Compliant.
  - PFS-compliant (Perfect Forward Secrecy).
  - All cryptography algorithms used by BMC are enterprise strict compliant.
  - BMC operates in standard validated mode.
  - Requires enterprise strict grade certificates.
  - Only services that support enterprise strict level cryptography are allowed.
  - Requires Feature on Demand Key to enable.

- **Standard Security Mode**
  - Standard Mode is the default security mode.
  - NIST Compliant.
  - PFS-compliant (Perfect Forward Secrecy).
  - All cryptography algorithms used by BMC are standard compliant.
  - BMC operates in standard validated mode.
  - Requires standard grade certificates.
  - Services that require cryptography that do not support standard level cryptography are disabled by default.

- **Compatibility Security Mode**
  - Compatibility Mode is the mode to use when services and clients require cryptography that is not enterprise strict/standard compliant.
  - Non NIST and PFS (Perfect Forward Secrecy) compliant
  - A wider range of cryptography algorithms are supported.
  - When this mode is enabled, BMC is NOT operating in standard-validated mode.
  - Allows all services to be enabled.

For more information on configuring security modes refer to Security Mode in the XCC3 User Guide.

Neighbor Group

XCC3 Neighbor Group Management is a virtual management group among XCC3-based servers, which allows the management of up to 200 XCC3-based servers from a single XCC3 management interface.

Typically, in the past, XCC could only manage a single server and XClarity Administrator (LXCA) facilitated scalability management to multiple servers. However, if LXC1, LXCA, or LXCO are not deployed in the field, especially for SMB users, each node has to be configured one by one which is an inefficient process.

To counter this scenario, the XCC3 neighbor group feature provides a flexible way of initiating speedy deployment for multiple servers within a local network segment.
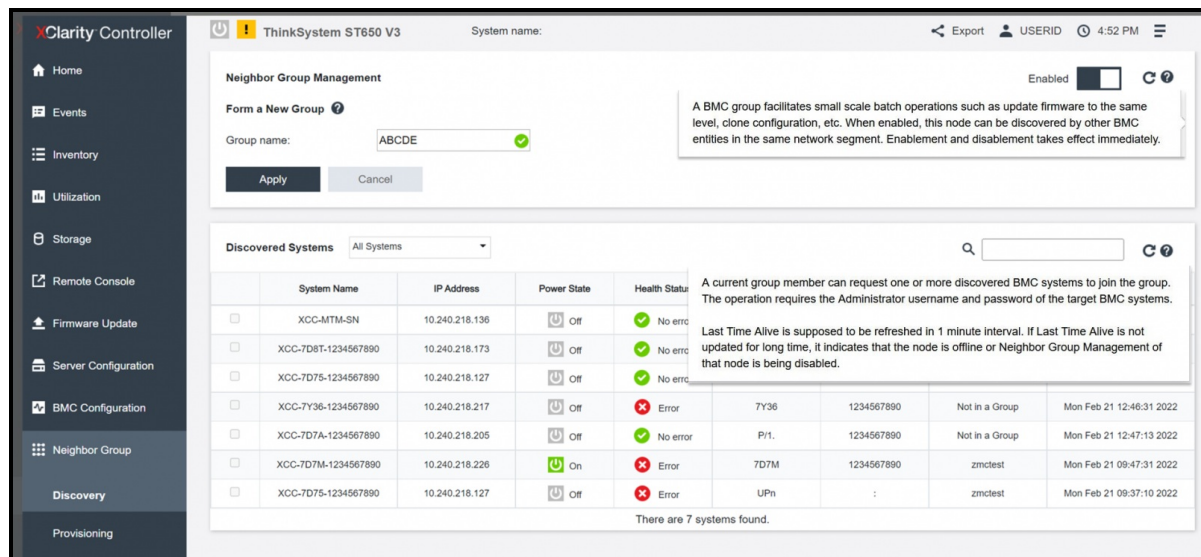
Figure 8. XCC2 Neighbor Group (XCC3 has the same content)

The XCC3 neighbor group provides the following capabilities:

- Discover the neighbor nodes located in the same local network segment using Simple Service Discovery Protocol (SSDP) multicast message.
- Monitor the system health, and power status of the neighbor nodes.
- Configure neighbor group in leader node.
- Clone system configuration to multiple members of the neighbor group.
- Initiate concurrent firmware updates to multiple members of the neighbor group.
- The Leader node XCC3 supports a maximum of 200 nodes.

Mixing XCC2 and XCC3: Although both XCC3-based servers and XCC2-based servers both have the Neighbor Groups capability, the guideline is to ensure groups are made up with servers with the same baseboard management controller. That is, you should not include a mix of XCC3 based and XCC2 based servers in any group.

For more information on XCC3 Neighbor Group Management see Neighbor Group Management in the XCC3 User Guide.

Service Log

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. XCC3 Service data log is a service tool that provides XCC3 first-failure logs in HTML and JSON formats.
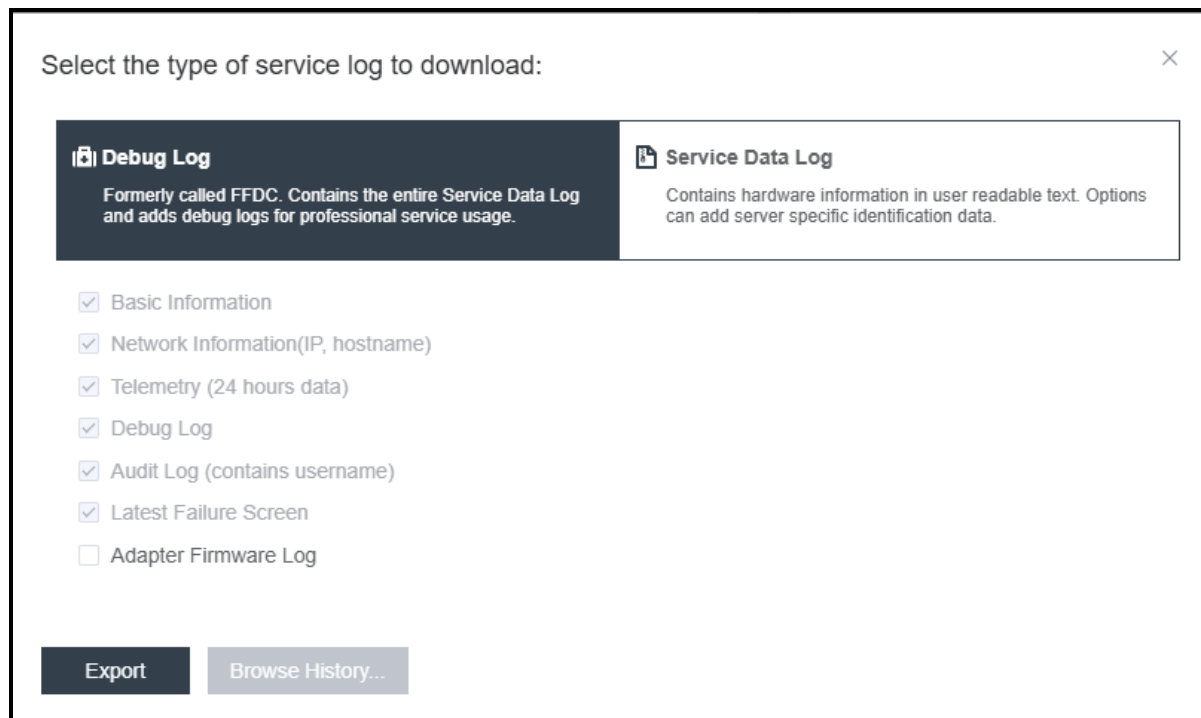
Figure 9. Service log

By default, the service log will contains the following data: system information, system inventory, system utilization, SMBIOS table, sensors reading, events log, FOD key, SLP key, UEFI configuration and XCC3 configuration.

User can also mouse over the Basic Information option and click on the floating window to see some actual data to be exported, as shown in the following figure.
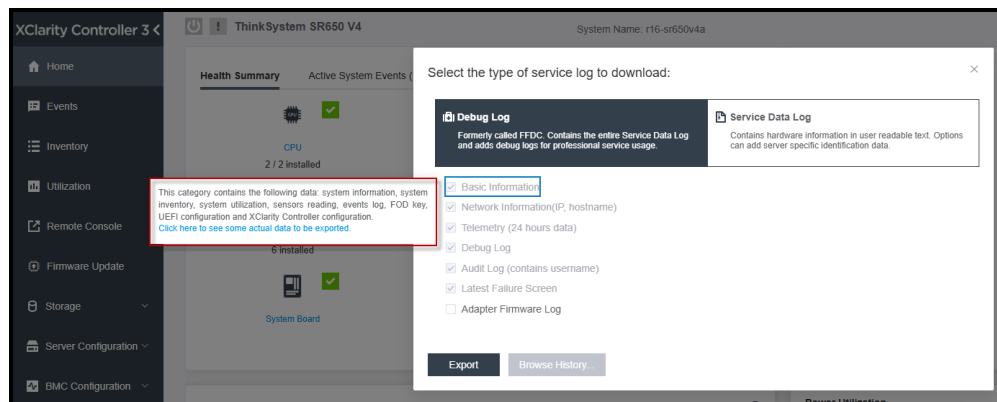

Figure 10. Mouse over additional information option

By clicking to see some actual data provides the user will be presented with a similar view to the following figure.

System Information

machine_name	ThinkSystem SR650 V4
machine_typemodel	7DGDCTO1WW
serial_number	J701XY0W
uuid	4CF9EDFE329A11F09B64C4EFBB1FA8F5
manufactureid	LNVO
hw_revision	5
power_state	Off
server_state	Off
system_name	r16-sr650v4a
location	Budapest
lowest_u	16
rack_id	r16
room_id	IC
ipv4_address	
hostname	
current_time	2025-08-04 14:27:44+00:00

Figure 11. Example of actual data being exported for SR650 V4 via XCC3

While Basic Information is mandatory, user has the option to additionally export the following information:

- Network information (IP, hostname)
- Telemetry (24 hours data)
- Audit log (contains username)
- Latest failure screen

REST API interface

XCC3 provides support for the industry standard Redfish Scalable Platforms Management API. The Redfish API can be used to access XCC3 data and services from applications running outside of XCC3. This allows for easy integration of XCC3 capabilities into Lenovo or 3rd party software. Redfish uses RESTful interface semantics and JSON resource payload to perform system management via the HTTPS protocol.

XClarity Controller 3 currently supports Redfish Specification 1.17.0 and Redfish Schema bundle 2024.3.

Lenovo additionally provides some Python and PowerShell sample scripts to use Redfish. These are available as open-source code on Lenovo's Github page http://github.com/lenovo/

- **Lenovo Python Redfish Scripts**: https://github.com/lenovo/python-redfish-lenovo
- **Lenovo PowerShell Redfish Scripts**: https://github.com/lenovo/powershell-redfish-lenovo

These scripts utilize Redfish API to manage Lenovo ThinkSystem servers. Currently, the scripts support hardware/firmware inventory, basic management of configuration and control, firmware updates, and alerts/eventing. The scripts can be used both remotely (out-of-band to the XCC3 Network) and locally (in-band on the ThinkSystem server, connecting to the XCC3 local host Network interface).

Other open-source tools that support Redfish include Ansible, which added support for Redfish starting with version 2.7, in the form of three modules for Remote Hardware Management. These modules are tested on Lenovo ThinkSystem servers:

- **redfish_facts**: https://docs.ansible.com/ansible/latest/modules/redfish_facts_module.html
- **redfish_command**: https://docs.ansible.com/ansible/latest/modules/redfish_command_module.html
- **redfish_config**: https://docs.ansible.com/ansible/latest/modules/redfish_config_module.html

See the Lenovo publications site for more information on XCC3 REST API:
https://pubs.lenovo.com/xcc3-restapi/

Seller training courses

The following sales training courses are offered for employees and partners (login required). Courses are listed in date order.

1. **Understanding Lenovo XClarity**
   2025-06-11 | 8 minutes | Employees and Partners

   This course is designed to give Lenovo sales and partner representatives an understanding of Lenovo XClarity.

   Learning Objectives:

   •Identify the different components of XClarity
   •Describe the primary benefits to customers
   •Define its core features

   Tags: XClarity

   Published: 2025-06-11
   Length: 8 minutes

   > **Start the training:**
   > Employee link: Grow@Lenovo
   > Partner link: Lenovo 360 Learning Center

   Course code: SXXW2118r2

Additional information

For more information, consult these resources:

- XClarity product web page
- XClarity Controller 3 online documentation
- Service Enablement and Port Assignment
- XCC3 Redfish REST API documentation
- XCC Overview videos:
    - Playlist item 6: Lenovo XClarity Mobile App demo
    - Playlist item 10: Lenovo XClarity Controller Overview
- XClarity One Online Documentation
- XClarity Administrator Online Documentation
- XClarity Orchestrator Online Documentation
- XClarity Systems Management Documentation
- Lenovo Online Documentation

Related product families

Product families related to this document are the following:

- Lenovo XClarity

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, LP2273, was created or updated on August 15, 2025.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2273
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2273.

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®
ThinkSystem®
XClarity®

The following terms are trademarks of other companies:

ActiveX® and PowerShell are trademarks of Microsoft Corporation in the United States, other countries, or both.

Initiate® is a trademark of IBM in the United States, other countries, or both.

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