Lenovo XClarity Controller 2 (XCC2)
Product Guide

Most of the latest Lenovo ThinkSystem, ThinkAgile and ThinkEdge servers contain an integrated service processor, XClarity Controller2 (XCC2), which provides advanced service-processor control, monitoring, and alerting functions. The XCC2 consolidates the service processor functionality, super I/O, video controller, and remote presence capabilities into a single chip on the server system board.

XCC2 is based on the AST2600 baseboard management controller (BMC) using a dual-core ARM Cortex A7 32-bit RISC service processor running at 1.2 GHz. XCC2 integrates four 10/100/1000 Mbps Fast Ethernet MACs compliant with IEEE802.3 and IEEE802.3z specification.

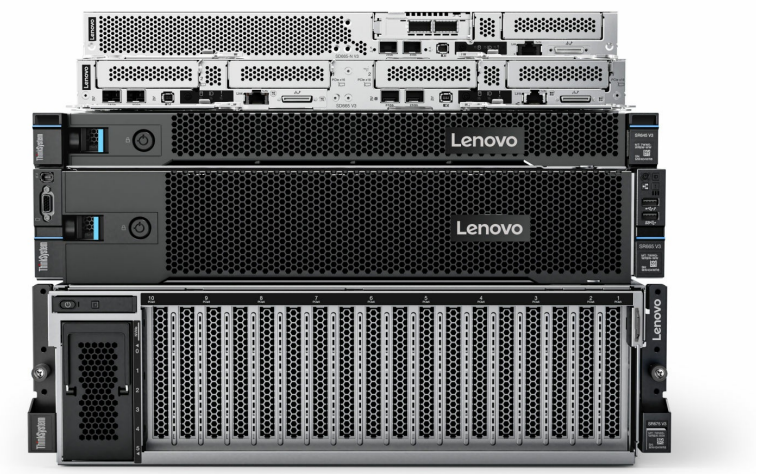


Figure 1. ThinkSystem V3 servers include the XClarity Controller2 integrated service processor

Did you know?

XCC2 has the capability to manage and configure multiple XCC2s 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.

Features

There are two levels of features of XCC2: Standard and Platinum. Compared to the XCC functions of ThinkSystem V2 and earlier systems, XCC2 Platinum adds the same features as Enterprise and Advanced levels in XCC, plus additional and new features.

XCC2 Standard

XClarity Controller2 Standard offers the following capabilities:

- 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 usage 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

For more information, see the following page:
https://pubs.lenovo.com/xcc2/NN1ia_c_standardlevelfeatures

XCC2 Platinum

XClarity Controller2 Platinum 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 Telnet / SSH
- **Security**
  - Single Sign-On
  - Security Key Lifecycle Manager (SKLM)
  - IP address blocking
  - Enterprise Strict Security mode (CNSA compliant) (new feature)
  - System Guard (new feature)

- **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
- **Other Management Functions**
  - Neighbor group management (new feature)

For details, see the following page:
https://pubs.lenovo.com/xcc2/NN1ia_c_platinumlevelfeatures

Management interfaces

The XCC 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.** 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.

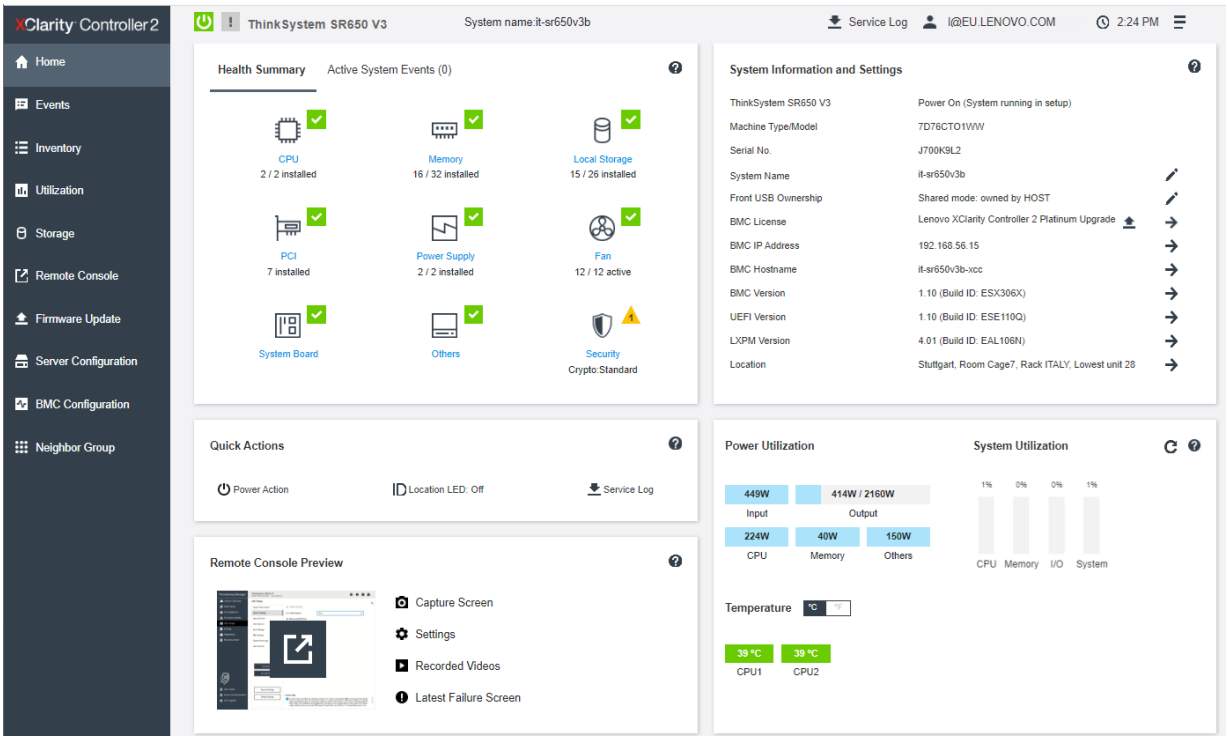


Figure 2. XClarity Controller2 Web interface dashboard

XCC2 can also be accessed remotely through industry-standard interfaces:

- 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
- Representational State Transfer (REST) support
- Redfish support (DMTF compliant) currently with specification v1.15.0 -schema bundle is 2021.4
- 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

Access via the XClarity Mobile app

XCC2 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)

Part numbers

Models of ThinkSystem V3 servers come with either XCC2 Standard or XCC2 Platinum, depending on the server type and the model, as described in the Server support section.

Important considerations:

- If you will be using XClarity Administrator for tasks such as remote control and Bare Metal Operating System Deployment then the XCC Platinum level must be installed on the server.
- XClarity Controller 2 Platinum 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 XCC Standard.

Table 1. XCC2 field upgrades

Part number	Description
7S0X000KWW	Lenovo XClarity Controller 2 (XCC2) Platinum Upgrade

For configure-to-order (CTO) models, you can specify the XCC2 level you require by selecting the appropriate XCC2 feature code as listed in the following table.

Table 2. XCC2 upgrades for configure-to-order

Feature code	Description
SBCV	Lenovo XClarity Controller 2 (XCC2) Platinum Upgrade

Server support

The following table shows what level of XCC2 is included with each ThinkSystem V3 server.

Table 3. Server support

Server	XCC2 Standard	XCC2 Platinum	
		CTO orders	Preconfigured models
Lenovo ThinkSystem servers with Intel Xeon D processors			
SE350 V2	Included	Available upgrade	Varies*
SE360 V2	Included	Available upgrade	Varies*
Lenovo ThinkSystem servers with 4th Gen Intel Xeon Scalable processors			
ST650 V3	Included	Available upgrade	Varies*
SR630 V3	Included	Available upgrade	Varies*
SR650 V3	Included	Available upgrade	Varies*
SR850 V3	Included	Included	Included
SR860 V3	Included	Included	Included
SR950 V3	Included	Included	Included
SD650-I V3	Included	Available upgrade	Not applicable
SD650 V3	Included	Available upgrade	Not applicable
Lenovo ThinkSystem Servers with 4th Gen AMD EPYC processors			
SE455 V3	Included	Available upgrade	Varies*
SR635 V3	Included	Available upgrade	Varies*
SR645 V3	Included	Available upgrade	Varies*
SR655 V3	Included	Available upgrade	Varies*
SR665 V3	Included	Available upgrade	Varies*
SR675 V3	Included	Included	Included
SD665 V3	Included	Available upgrade	Not applicable
SD665-N V3	Included	Available upgrade	Not applicable

* Some preconfigured models of the server have XCC2 Platinum included. See the Models section of the product guide for specifics.

Security dashboard

The XCC2 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 XCC.
- **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 XCC. The detail link under each category also brings the user to the setup page to solve the issues.

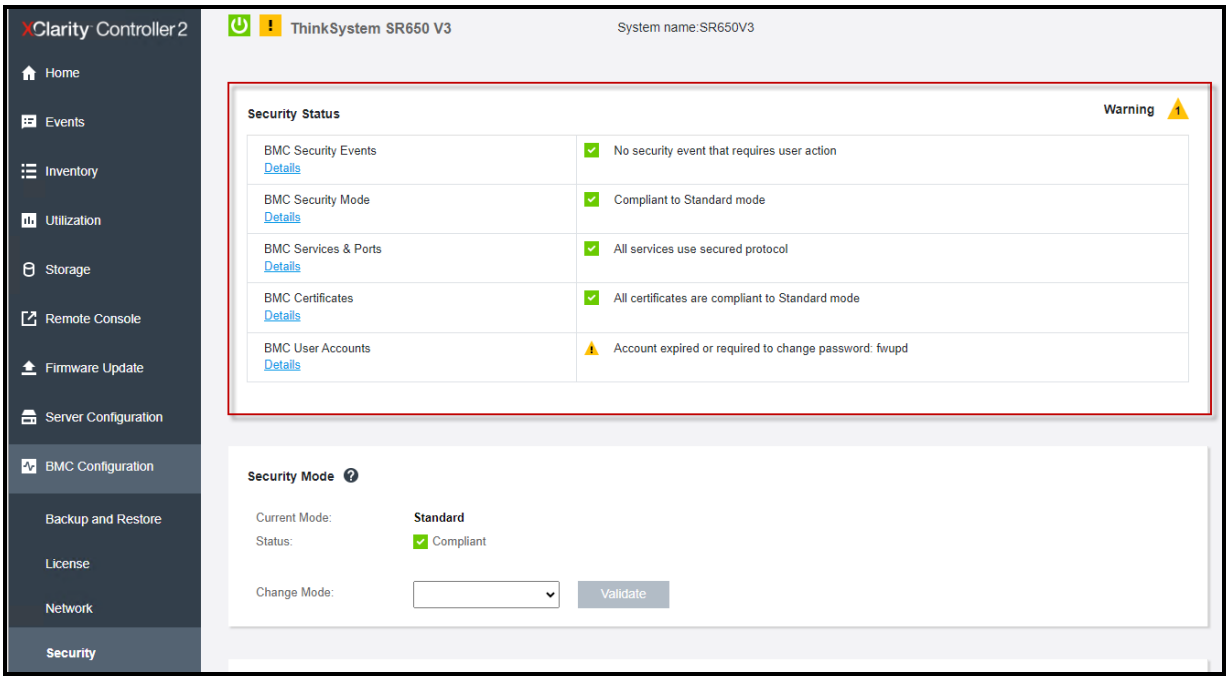


Figure 3. XCC2 Security Status dashboard, highlighting a warning on User Accounts

Service and support

With XCC2-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.

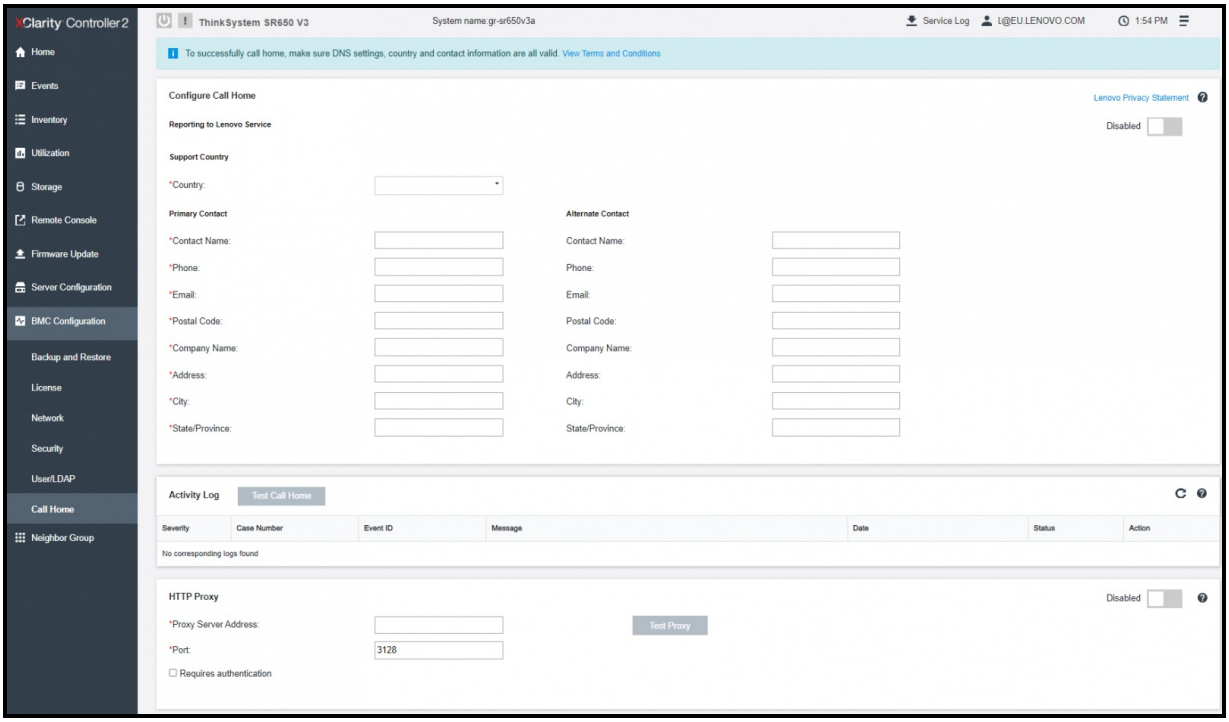


Figure 4. XCC2 Call Home

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 Administrator they can choose to configure centralized Call Home via XClarity Administrator, rather than at each XCC or XCC2 instance. XClarity Administrator 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 XClarity Administrator (LXCA) 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 XCC2 Platinum

Compared to the XCC, XCC2 Platinum license adds the same features as Advanced and Enterprise levels combined in XCC, plus additional features.

The new features included with XCC2 Platinum are 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.
- XCC2 Service Log – New service tool that provides XCC first-failure logs in HTML and JSON format.

For details, see the following sections:

System Guard

To ensure your server arrives as it left Lenovo manufacturing, and confirm nothing has changed along the way, with the XCC2-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.

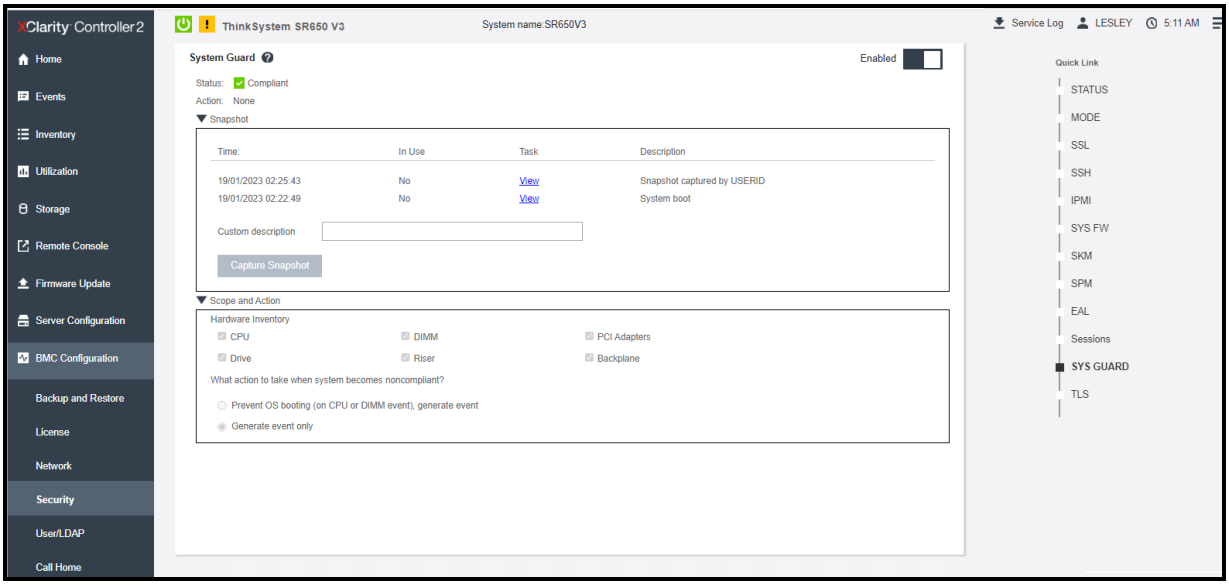


Figure 5. System Guard in XCC2

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 XCC2 User Guide.

Enhanced Security Modes

With XCC2, Enhanced Security Modes are now configurable.

- The XCC2 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 XCC2-based servers.
- The XCC2 Platinum license comes with a third Security Mode: Enterprise Strict Mode. This mode is most suitable for high-level security requirements.

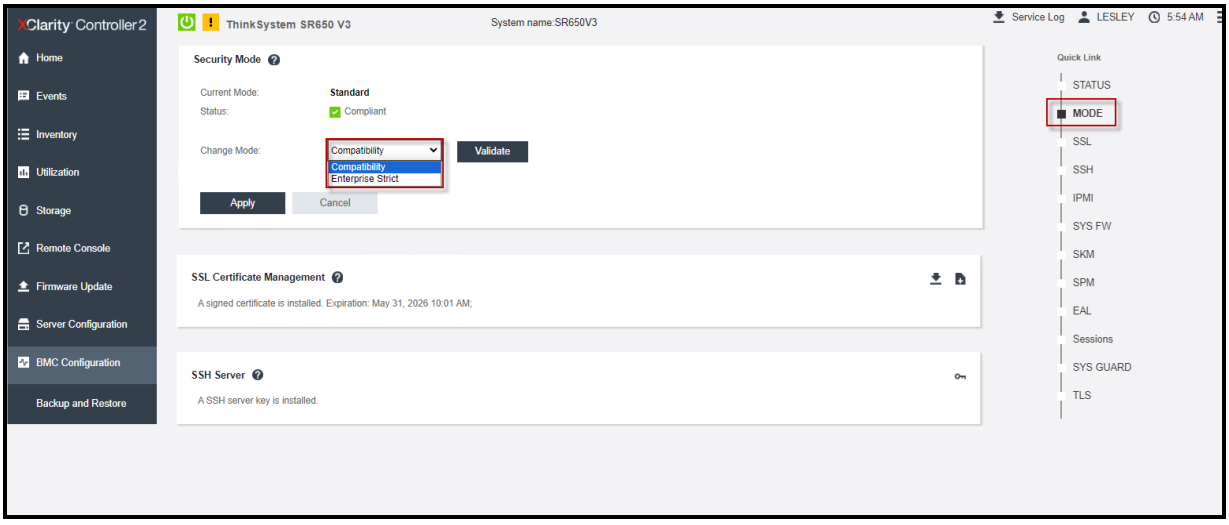


Figure 6. Security Mode in XCC2

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

- **Enterprise Strict Security Mode**
  - Enterprise Strict Security Mode is the most secure mode.
  - 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 XCC2 User Guide.

Neighbor Group

XCC2 Neighbor Group Management is a virtual management group among XCC2-based servers, which allows the management of up to 200 XCC2-based servers from a single XCC2 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 LXCA is 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 XCC2 neighbor group feature provides a flexible way of initiating speedy deployment for multiple servers within a local network segment.

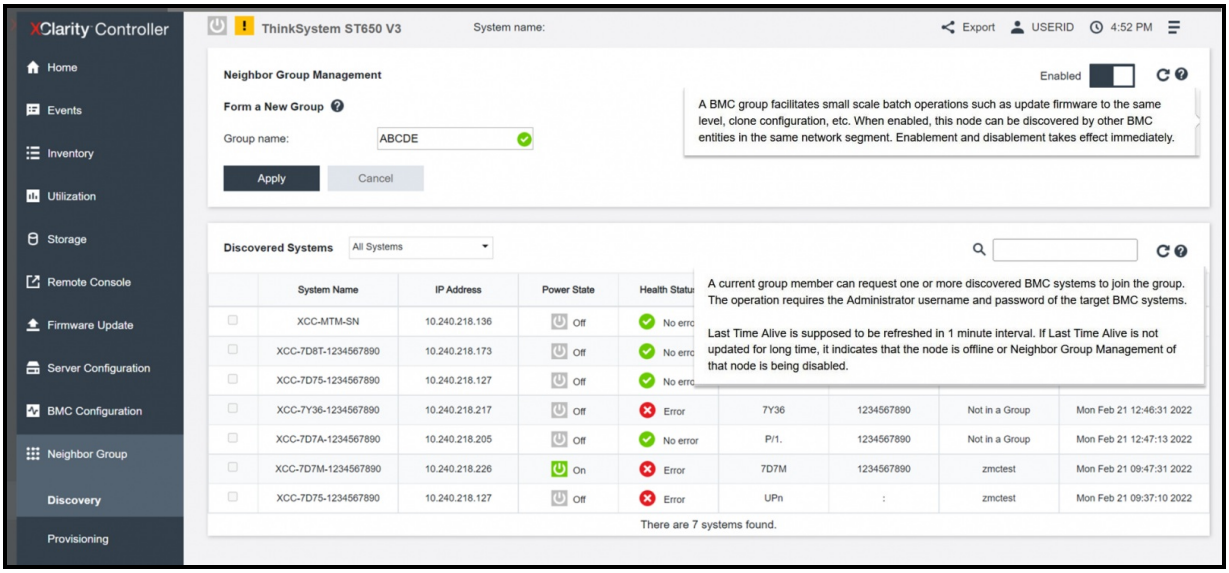


Figure 7. XCC2 Neighbor Group

The XCC 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 XCC supports a maximum of 200 nodes.

For more information on XCC Neighbor Group Management see Neighbor Group Management in the XCC2 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. XCC2 Service data log is a new service tool that provides XCC2 first-failure logs in HTML and JSON formats.

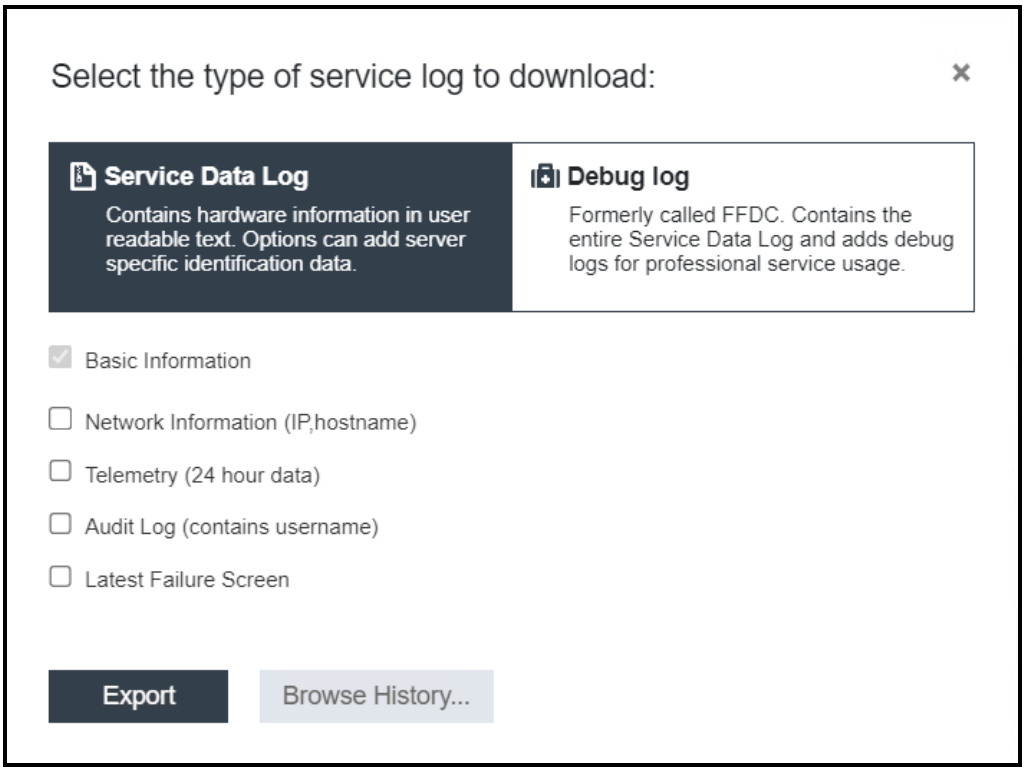


Figure 8. Service log

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 XCC2 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.

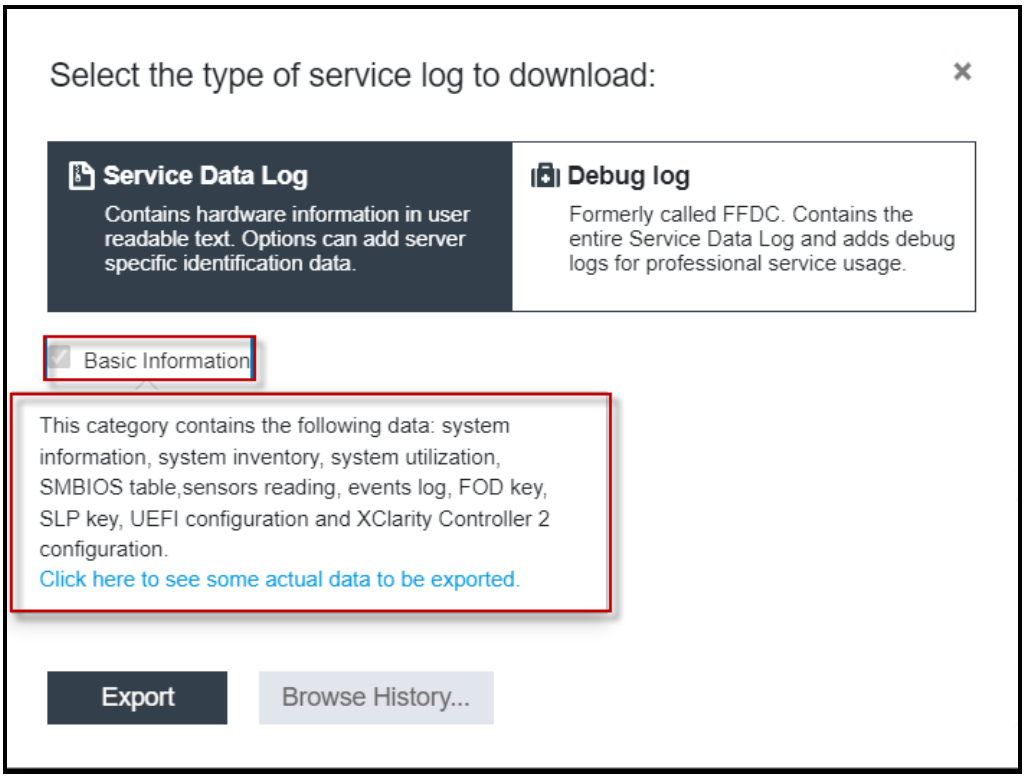
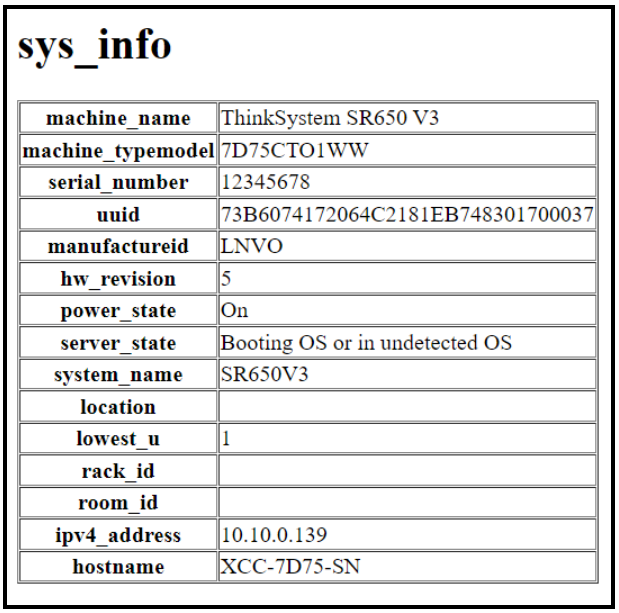


Figure 9. Mouse over additional information option

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



sys_info

machine_name	ThinkSystem SR650 V3
machine_typemodel	7D75CTO1WW
serial_number	12345678
uuid	73B6074172064C2181EB748301700037
manufactureid	LNVO
hw_revision	5
power_state	On
server_state	Booting OS or in undetected OS
system_name	SR650V3
location	
lowest_u	1
rack_id	
room_id	
ipv4_address	10.10.0.139
hostname	XCC-7D75-SN

Figure 10. Example of Actual Data being exported

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

XCC2 provides support for the industry standard Redfish Scalable Platforms Management API. The Redfish API can be used to access XCC2 data and services from applications running outside of the XCC2. This allows for easy integration of Lenovo XCC2 capabilities into Lenovo or 3rd party software. Redfish uses RESTful interface semantics and JSON resource payload to perform system management via the HTTPS protocol.

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 XCC2 Network) and locally (in-band on the ThinkSystem server, connecting to the XCC2 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 XCC2 REST API:
https://pubs.lenovo.com/xcc2-restapi/

Additional information

For more information, consult these resources:

- XClarity product web page
- TCP/IP Ports Used by XCC2
- XClarity Controller online documentation
- XCC2 Redfish REST API documentation
- XCC Overview videos:
  - Playlist item 6: Lenovo XClarity Mobile App demo
  - Playlist item 10: Lenovo XClarity Controller Overview
- XClarity Administrator 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, LP1800, was created or updated on November 24, 2023.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1800
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1800.

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®
ThinkAgile®
ThinkEdge®
ThinkSystem®
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

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

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