

Lenovo XClarity Controller 2 on ThinkSystem V3 servers

New features and enhancements

The Lenovo logo is positioned in the top right corner of the slide. It consists of the word "Lenovo" written vertically in white, set against a rectangular background with a vertical color gradient from green at the top to blue at the bottom.

Lenovo

Tool overview

XCC2 has the following new features and enhancements:

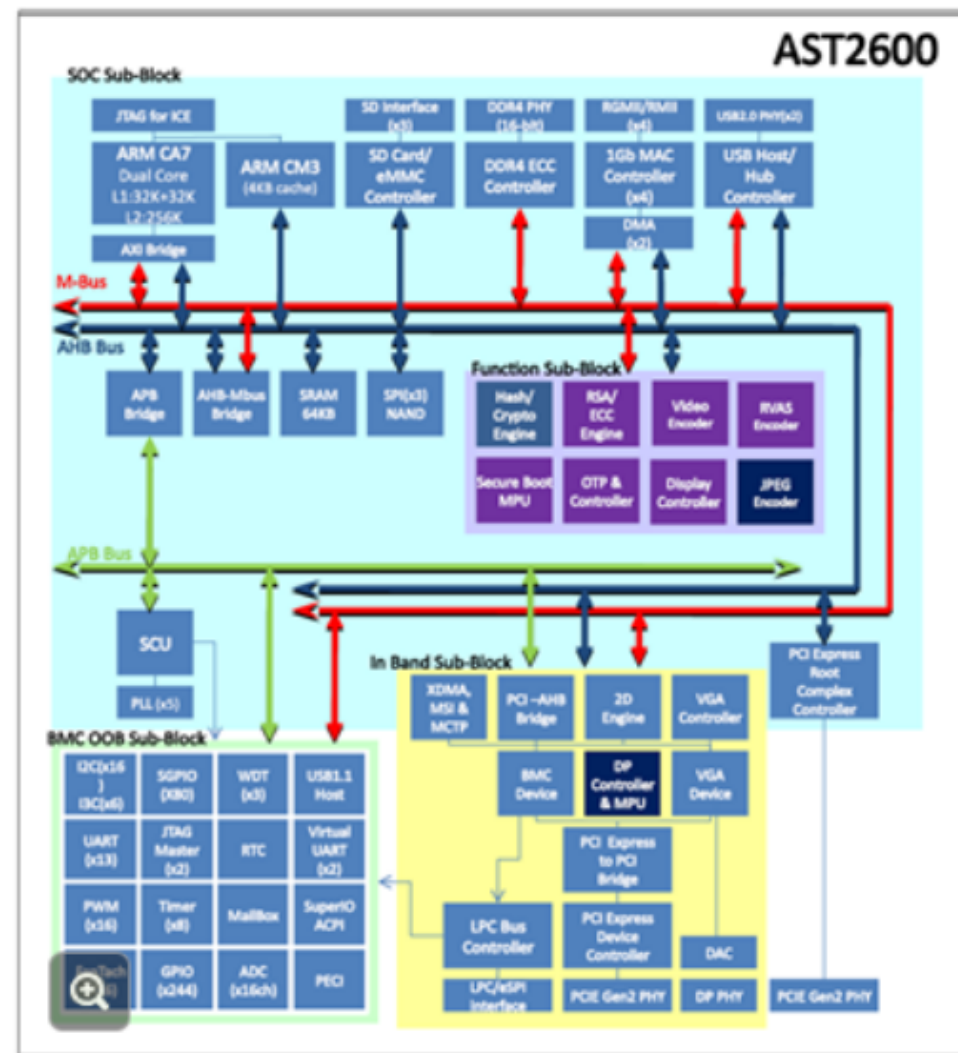
- New XCC chip with enhanced performance and security
 - ASPEED AST2600
- Advanced security enhancements
 - Enhanced security modes
 - Enterprise Strict Security Mode, Standard Security Mode, and Compatibility Security Mode
 - Enhanced NIST 800-193 (PFR) support
 - System Guard to protect against supply chain attacks
- New features to extend the manageability and serviceability functions
 - Redfish standard-based firmware update enhancement
 - Support for an SD card option to extend XCC storage
 - XCC federated group support
 - Enhanced LDAP configuration to support complex hierarchies
 - Customer-configurable thermal fan speed profile
 - Customer-selectable Service Data Log (Mini-Log)

Note: XCC2 is only available on the ThinkSystem V3 platform.

New XCC chip – ASPEED AST2600

The ASPEED AST2600 is the main XCC chipset, and it's installed on the system I/O board. This chip has the following improvements:

- Embedded dual-core ARM Cortex A7 32-bit RISC CPU, maximum running frequency: 1.2 GHz
- Integrated quad ports 10/100/1000 Mbps Fast Ethernet MACs compliant with IEEE802.3 and IEEE802.3z specification
- Integrated 16 multi-function I2C/SMBus bus controllers and six sets of MIPI I3C controllers
- Support for 13 UART controllers and 13 UART I/O interfaces
- Hardware hash and crypto engine
- Improved security for protection
 - Hardware secure boot, support for hardware boot image measurement and decryption
 - Hardware secure vault



Security modes

Three new security modes are available for selection by going to the **XCC** page and selecting **BMC Configuration → Security**.

- Enterprise Strict Security Mode
 - Strict Security Mode is the most secure mode
 - Enablement requires an XCC Platinum license key
 - All cryptography algorithms used by XCC are CNSA compliant
 - XCC operates in FIPS 140-2/140-3 validated mode
 - Requires CNSA grade certificates
 - Only services that support CNSA-level cryptography are allowed
- Standard Security Mode
 - Standard Mode is the default security mode
 - Requires FIPs grade certificates
 - All cryptography algorithms used by XCC are FIPS 140-3/FIPS 140-2 compliant
 - XCC operates in FIPS 140-2/140-3 validated mode
 - Services that require cryptography that do not support FIPS 140-2/FIPS 140-3-level cryptography are disabled by default

Security modes - continued

- Compatibility Security Mode
 - Used when services and clients require cryptography that is not CNSA/FIPS compliant
 - A wider range of cryptography algorithms are supported
 - When this mode is enabled, XCC is NOT operating in FIPS-validated mode
 - Allows all services to be enabled

The screenshot displays the BMC Configuration web interface. On the left is a dark sidebar with navigation options: BMC Configuration, Backup and Restore, License, Network, Security (highlighted), User/LDAP, Call Home, and Neighbor Group. The main content area shows a 'Details' section for 'BMC User Accounts' with a green checkmark and the text 'All settings of user accounts are compliant to Compatibility mode'. Below this, a 'Security Mode' section is highlighted with a red box. It shows 'Current Mode: Compatibility', 'Status: Compliant' with a green checkmark, and a 'Change Mode' dropdown menu currently set to 'Select'. A 'Validate' button is located to the right of the dropdown.

Security modes – show details

Click **show details** to check the security mode status and to validate mode compliance and switch modes.

The screenshot displays the 'Security Mode' configuration page in the XClarity Controller interface. The page is titled 'Security Mode' with a help icon. The current mode is 'Standard'. The status is 'Noncompliant due to user override', indicated by a yellow warning icon. A 'show details' link is highlighted with a red box and an arrow pointing to it. Below the status, there is a 'Change Mode' dropdown menu with options 'Compatibility' and 'Enterprise Strict'. A 'Validate' button is also present. The left sidebar shows navigation options: Server Configuration, BMC Configuration, Backup and Restore, License, Network, Security, and User/LDAP. The bottom of the page shows 'SSL Certificate Management' with a help icon.

Security modes – Security Status

Use this feature to manage overall XCC security.

System name: ThinkSystem

Warning 2

Item	Status
BMC Security Events Details	✔ No security event that requires user action
BMC Security Mode Details	⚠ Noncompliant to Standard Security mode
BMC Services & Ports Details	✔ All services use secured protocol
BMC Certificates Details	✔ All certificates are valid in the next 90 days All certificates in use were uniquely generated
BMC User Accounts Details	⚠ 1 user password expired 61 days ago

Quick Link

- STATUS
- CRYPTO
- IPMI
- SYS FW
- TPM/TCM
- SKLM
- SPM

Certified for FIPS 140-3

XCC2 has passed the FIPS 140-3 validation through the CMVP (Cryptographic Module Validation Program) program and has received FIPS 140-3 certification.

- Federal Information Processing Standard (140-3/140-2) specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments.
- FIPS 140-3 supersedes FIPS 140-2 and outlines updated federal security requirements for cryptographic modules

Enhanced NIST 800-193 (PFR) support

The NIST SP 800-193 specification provides a set of high-level guidelines for implementing platform firmware resilience (PFR).

- A “platform” in this context is a collection of fundamental hardware and firmware components needed to boot and operate a server system.
- The key items of interest here are the CPU and PCH (southbridge), which run UEFI, and the BMC chip, which runs the BMC firmware.
- For more information, refer to the [Platform Firmware Resiliency Guidelines](#).

These guidelines are based on the following three principles:

- Protection: Ensure that the platform firmware and updates are protected from corruption
- Detection: Detect corruption of platform firmware
- Recovery: Restore platform firmware to a state of integrity in the event of corruption

PFR on Lenovo servers

PFR operates on the following server components:

- UEFI image – This is the low-level server firmware that connects the OS to the server hardware
- XCC image – This is the management “engine” software that controls and reports on the server status separate from the server OS
- FPGA image – This is the code that runs the server’s lowest level hardware controller on the system board

ThinkSystem V3 platform Root of Trust hardware complies with the following PFR guidelines:

- Detection – Measures the firmware and updates for authenticity
- Recovery – Recovers a corrupted image to a known safe image
- Protection – Monitors the system to ensure that known, good firmware is not maliciously written over or erased

System Guard

This feature monitors hardware including CPUs, DIMMs, PCI adapters, and HDDs for unexpected changes and can then log events or prevent booting.

To open this section, go to the **XCC** page and select **BMC Configuration** → **Security** → **SYS GUARD**.

The screenshot displays the XClarity Controller 2 web interface. On the left is a dark sidebar with navigation options: Utilization, Remote Console, Firmware Update, Storage, Server Configuration, BMC Configuration, Backup and Restore, License, Network, and Security. A red arrow points to the Security option. The main content area is divided into two sections. The top section, titled 'System Guard', is enclosed in a red border and shows a toggle switch set to 'Disabled'. Below the title, it indicates 'Status: Disabled', 'Action: None', and two expandable options: 'Snapshot' and 'Scope and Action'. The bottom section, titled 'TLS Version Support', shows two radio button options: 'TLS 1.2 and higher' (selected) and 'TLS 1.3'. On the right side, a 'Quick Link' menu lists various system settings: STATUS, MODE, SSL, SSH, IPMI, SLW, SYS FW, SKM, SPM, EAL, Sessions, SYS GUARD, and TLS. A red arrow points to the 'SYS GUARD' link in this menu. At the bottom of the sidebar, the 'Lenovo' logo is visible.

System Guard behavior examples

The following screen capture shows the different types of System Guard behavior.

The image displays three screenshots of the System Guard configuration interface, each showing a different status and action.

- Top Left Screenshot:** System Guard is Disabled. The status is "Disabled" and the action is "None". A toggle switch is in the "Off" position. A blue link "System Guard disabled" is visible.
- Top Right Screenshot:** System Guard is Enabled and Compliant. The status is "Compliant" (indicated by a green checkmark) and the action is "None". A toggle switch is in the "On" position. A blue link "System Guard enabled" is visible.
- Bottom Screenshot:** System Guard is Enabled but Noncompliant. The status is "Noncompliant due to configuration mismatch" (indicated by a yellow warning triangle) and the action is "OS booting is prevented, event asserted". A toggle switch is in the "On" position. A blue link "System Guard enabled but with a warning status" is visible.

System Guard – more features

Select **Snapshot** and **Scope and Action** to expand the sections and see more System Guard features for configuration.

In **Scope and Action**, select the hardware to be monitored for unexpected changes, and then select **Prevent OS booting** or **Generate event only**.

The screenshot displays the System Guard configuration page. At the top right, the status is 'Disabled' with a toggle switch. Below this, the status is 'Status: Disabled' and 'Action: None'. The 'Snapshot' section is expanded, showing a table of snapshots and a 'Capture Snapshot' button. The 'Scope and Action' section is also expanded, showing hardware inventory options and action settings.

System Guard ? Disabled

Status: Disabled
Action: None

▼ Snapshot

Time:	In Use	Task	Description
21/02/2022 06:38:21	Yes	View	Enforced by USERID
10/02/2022 04:04:29	No	View	Enforced by USERID
10/02/2022 04:03:29	No	View	System boot

Custom description

Capture Snapshot

▼ Scope and Action

Hardware Inventory

- CPU
- DIMM
- PCI Adapters
- Drive
- Riser
- Backplane

What action to take when system becomes noncompliant?

- Prevent OS booting (on CPU or DIMM event), generate event
- Generate event only

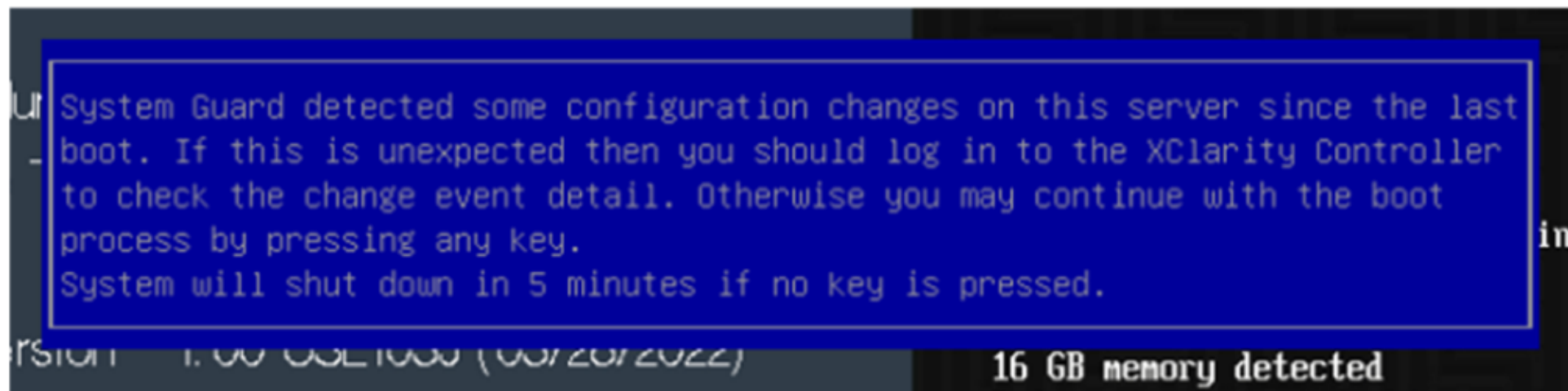
System Guard – scenario study

Question:

If **Prevent OS booting** is enabled, how will this feature impact field replacements and customer upgrades? For example, even if a system suffers a DIMM or disk failure that changes the inventory, they can often still operate. Would System Guard stop the system from booting?

Answer:

If **Prevent OS booting** has been enabled, the OS boot will be impacted and a pop-up UEFI message (as shown below) will be displayed. Users can continue the boot by pressing any key. It is recommended to disable this feature before replacing hardware component.



Redfish standard-based firmware update enhancements

- Follow the new DSP2062 standard to support the standard Redfish update methods
- Support for single firmware as well as firmware bundle updates
- Support for Redfish Job to monitor the update progress/status

```
"FirmwareInventory": {
  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"
},
"MultipartHttpPushUri": "/#fwupdate",
"ServiceEnabled": true,
"Actions": {
  "Oem": { ...
  },
  "#UpdateService.SimpleUpdate": {
    "target": "/redfish/v1/UpdateService/Actions/UpdateService.SimpleUpdate",
    "@Redfish.OperationApplyTimeSupport": {
      "@odata.type": "#Settings.v1_3_3.OperationApplyTimeSupport",
      "SupportedValues": [
        "Immediate",
        "OnReset",
        "OnStartUpdateRequest"
      ]
    },
    "@Redfish.ActionInfo": "/redfish/v1/UpdateService/SimpleUpdateActionInfo",
    "Targets@Redfish.AllowableValues": [
      "/redfish/v1/UpdateService/FirmwareInventory/BMC-Backup"
    ],
    "TransferProtocol@Redfish.AllowableValues": [
      "TFTP",
      "SFTP",
      "HTTPS",
      "HTTP"
    ]
  },
  "title": "SimpleUpdate"
},
  "#UpdateService.StartUpdate": {
    "@Redfish.ActionInfo": "/redfish/v1/UpdateService/StartUpdateActionInfo",
    "target": "/redfish/v1/UpdateService/Actions/UpdateService.StartUpdate",
```

Support for an SD card option to extend XCC storage

- With an SD card (micro SD format) installed, the virtual media of the Remote Disc On Card (RDOC) can be extended
 - With the previous ThinkSystem platform, RDOC space cannot be extended. For more information, refer to the following Knowledge Base article: [HT507561](https://www.lenovo.com/knowledgebase/HT507561).
- Support for the saving of N-1 firmware history for rollback in the SD card

The screenshot displays the XClarity Controller web interface. On the left is a dark sidebar with navigation options: Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Neighbor Group. The main content area is divided into several sections:

- Retimer Information:** A table showing the status of various retimers.
- PSU Firmware:** A table listing PSU units and their firmware versions.
- Update from Repository:** A form for selecting a storage source and mounting options.

Bay No.	Version	Manufacturer
1	14.11	ACBE
2	4.50	ACBE

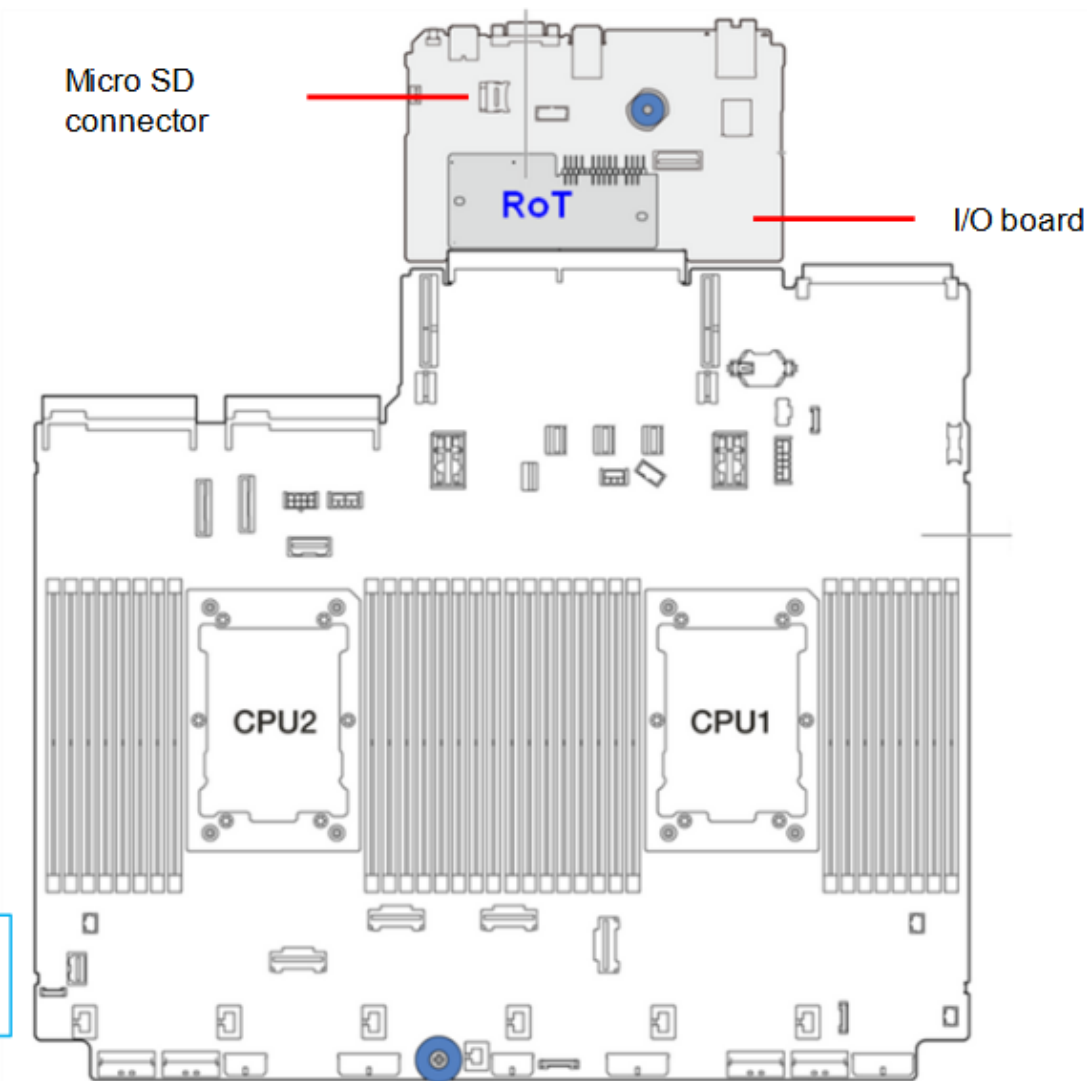
In the 'Update from Repository' section, a dropdown menu is open, showing options: CIFS, NFS, HTTP, HTTPS, Internal Storage, and Onboard Firmware History. The 'Internal Storage' and 'Onboard Firmware History' options are highlighted with a red box. Below the dropdown are input fields for 'Share Path', 'User Name', 'Password', 'Mount Options', and 'Domain', along with 'Update System' and 'Mount' buttons.

Locating an SD card

This example uses the SR650 V3 system board.

The SD card connector is located on the I/O board. To locate the SD card connector on a specific V3 server, refer to that server's individual course.

SR650 V3



SD card option - scenario study

Question 1: Will the SD card need to be formatted in a specific way, such as FAT32/EXT4?

Answer: If a card is not formatted before installation, XCC will format it to EXT4.

Question 2: If data is transferred to an SD card after it has been removed from a system, will the data be accessible after the SD card has been reinstalled?

Answer: No.

Question 3: Is it possible to move an ISO locally or from a network to the local SD card and use that local image to present the ISO to LXPM for guided OS installation?

Answer: Yes, the SD card can be used to extend the RDOC space, so you can transfer the image to the SD card and mount it to the host.

Question 4: Will the SD card be presented to the OS, allowing tools such as ONECLI and BOMC to write log data to the SD card, enabling the remote collection of logs without the need to install a USB drive?

Answer: It is not currently supported.

Neighbor Group

Neighbor Group is a new feature of XCC2, and it gives users the ability to see multiple peer instances of XCC from their XCC web UI. After creating a neighbor group, users can monitor the health status of group members. A maximum of 200 peer XCCs are allowed in a group.

The screenshot displays the XClarity Controller web interface. The top navigation bar includes a power icon, a warning icon, the system name 'ThinkSystem ST650 V3', and a 'System name:' field. On the right, there are links for 'Export', 'USERID', and a clock showing '4:52 PM'. A left-hand sidebar contains navigation options: Home, Events, Inventory, Utilization, Storage, Remote Console, Firmware Update, Server Configuration, BMC Configuration, Neighbor Group (highlighted), Discovery, and Provisioning.

The main content area is titled 'Neighbor Group Management'. It features a toggle switch set to 'Enabled' and a 'Form a New Group' section. The 'Form a New Group' section includes a 'Group name:' field with the value 'ABCDE' and a green checkmark, along with 'Apply' and 'Cancel' buttons.

A callout box on the right contains the text: 'A current group member can request one or more discovered BMC systems to join the group. The operation requires the Administrator username and password of the target BMC systems.'

Below the management section is a 'Discovered Systems' table with a search bar and a refresh icon. The table lists 7 systems with columns for System Name, IP Address, Power State, Health Status, Machine Type, Serial Number, Group, and Last Time Alive.

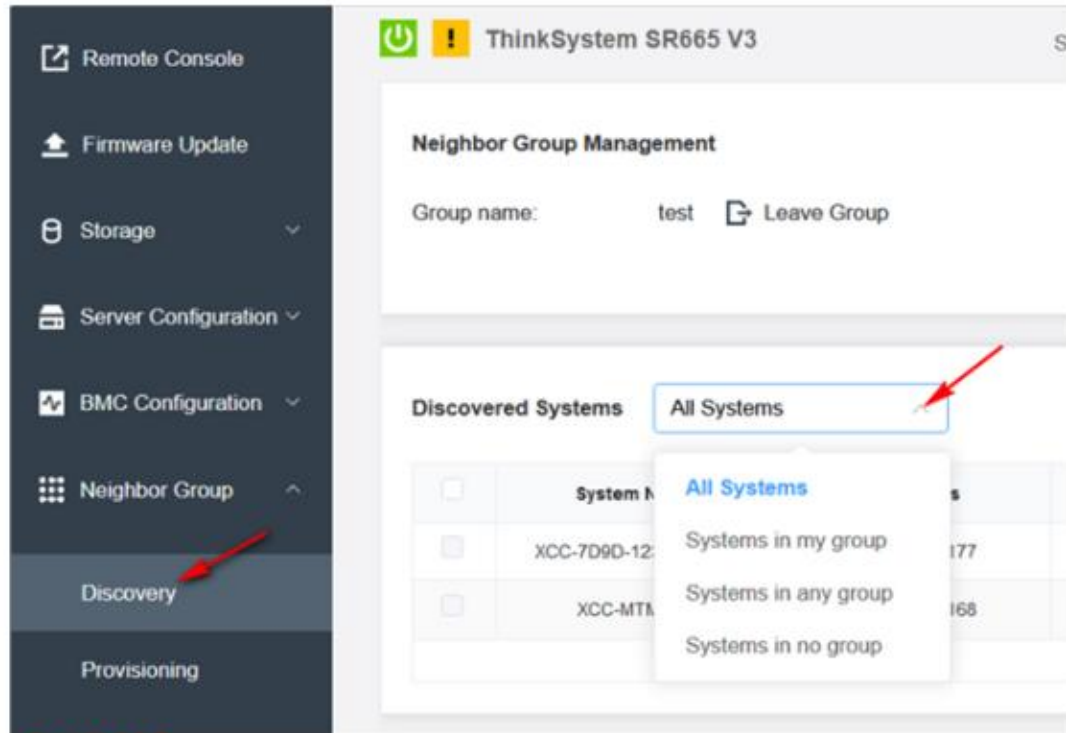
	System Name	IP Address	Power State	Health Status	Machine Type	Serial Number	Group	Last Time Alive
<input type="checkbox"/>	XCC-MTM-SN	10.240.218.136	Off	No error	7D72	1234567890	ggg	Fri Feb 18 08:13:44 2022
<input type="checkbox"/>	XCC-7D8T-1234567890	10.240.218.173	Off	No error	7D8T	1234567890	testZMC	Mon Feb 21 16:50:54 2022
<input type="checkbox"/>	XCC-7D75-1234567890	10.240.218.127	Off	No error	7D75	1234567890	zmctest	Mon Feb 21 08:59:53 2022
<input type="checkbox"/>	XCC-7Y36-1234567890	10.240.218.217	Off	Error	7Y36	1234567890	Not in a Group	Mon Feb 21 12:46:31 2022
<input type="checkbox"/>	XCC-7D7A-1234567890	10.240.218.205	Off	No error	PI1.	1234567890	Not in a Group	Mon Feb 21 12:47:13 2022
<input type="checkbox"/>	XCC-7D7M-1234567890	10.240.218.226	On	Error	7D7M	1234567890	zmctest	Mon Feb 21 09:47:31 2022
<input type="checkbox"/>	XCC-7D75-1234567890	10.240.218.127	Off	Error	UPn	:	zmctest	Mon Feb 21 09:37:10 2022

There are 7 systems found.

Neighbor Group – Discovery

Select **Discovered Systems**, and a drop-down menu will be displayed with the following items:

- All Systems
- Systems in my group
- Systems in any group
- Systems in no group



Example: All systems

The screenshot shows the 'Discovered Systems' table with the dropdown menu set to 'All Systems'. The table contains 7 rows of system data. A search bar and a refresh icon are visible at the top right. Below the table, it says 'There are 7 systems found.'

	System Name	IP Address	Power State	Health Status	Machine Type	Serial Number	Group	Last Time Alive
<input type="checkbox"/>	XCC-MTM-SN	10.240.218.136	Off	No error	TD72	1234567890	g00	Fri Feb 18 06:13:44 2022
<input type="checkbox"/>	XCC-TD8T-1234567890	10.240.218.173	Off	No error	TD8T	1234567890	testZMC	Mon Feb 21 16:50:54 2022
<input type="checkbox"/>	XCC-TD75-1234567890	10.240.218.127	Off	No error	TD75	1234567890	zmcctest	Mon Feb 21 08:59:53 2022
<input type="checkbox"/>	XCC-FY36-1234567890	10.240.218.217	Off	Error	FY36	1234567890	Not in a Group	Mon Feb 21 12:46:31 2022
<input type="checkbox"/>	XCC-TD7A-1234567890	10.240.218.205	Off	No error	PI1	1234567890	Not in a Group	Mon Feb 21 12:47:13 2022
<input type="checkbox"/>	XCC-TD7M-1234567890	10.240.218.226	On	Error	TD7M	1234567890	zmcctest	Mon Feb 21 09:47:31 2022
<input type="checkbox"/>	XCC-TD75-1234567890	10.240.218.127	Off	Error	UPh		zmcctest	Mon Feb 21 09:37:10 2022

Example: System in my group

The screenshot shows the 'Discovered Systems' table with the dropdown menu set to 'Systems in my group'. The table contains 3 rows of system data. A search bar and a refresh icon are visible at the top right. Below the table, it says 'There are 3 systems found.'

	System Name	IP Address	Power State	Health Status	Machine Type	Serial Number	Group	Last Time Alive
<input type="checkbox"/>	XCC-TD75-1234567890	10.240.218.127	Off	No error	TD75	1234567890	zmcctest	Mon Feb 21 08:59:53 2022
<input type="checkbox"/>	XCC-TD7M-1234567890	10.240.218.226	On	Error	TD7M	1234567890	zmcctest	Mon Feb 21 09:47:31 2022
<input type="checkbox"/>	XCC-TD75-1234567890	10.240.218.127	Off	Error	UPh		zmcctest	Mon Feb 21 09:37:10 2022

Neighbor Group - Provisioning

- The group master XCC configuration can be cloned to all group member XCCs
- The firmware of all servers in the group can be updated from the group master
- The provisioning feature is not available on group member nodes

Group master view:

The screenshot shows the Group Master view for a ThinkSystem ST650 V3 server. The left sidebar contains navigation options: BMC Configuration, Neighbor Group (highlighted with a red box), Discovery, and Provisioning. The main content area is titled "Provisioning" and includes three action buttons: Clone Configuration, Update Firmware From Repository, and Remove, all of which are highlighted with a red box. A dropdown menu on the right is set to "Same MT with Leader Node". Below the buttons is a table with the following columns: System Name, IP Address, Power State, Health Status, Machine Type, Serial Number, Group, and Last Time Alive.

Group member view:

The screenshot shows the Group Member view for a ThinkSystem SR665 V3 MB, Genoa, Kauai, DDR... server. The left sidebar contains navigation options: Neighbor Group (highlighted with a red box), Discovery, and Provisioning. The main content area is titled "Provisioning" and displays a light blue informational message: "Provisioning feature is not available on member node, please access the leader node to perform the operations".

Enhanced LDAP configuration – from the group master

This feature supports the configuration of the domain controller for each group from the group master XCC, and also an enhanced auto search of users and groups from domain controller catalogs.

To go to this page, select **BMC Configuration** → **User/LDAP** on the **XCC** page.

Local User **LDAP** Allow logons from: []

LDAP Server Information

Use LDAP server for Authentication only (with local authoriz...
Use Pre-Configured Servers []

Hostname or IPv4, IPv6 address Port
1: [0.0.0.0] [389] +

Enable Secure LDAP []

Trusted certificate [] Trusted Cert #1 is installed. Expires: 1900-01-00T00:00:00 [] []

▼ Additional Parameters

Binding method: [No Credentials Required] []
Root DN: [] []
User's Login Name Search Attribute: [sAMAccountName] []
Group Filter: [] []
Group Membership Search Attribute: [memberOf] []
Login Permission attribute: [] []

Groups for Local Authorization:

	Group Name	Group Domain	Role	
01.	[test]	[]	[Administrator]	[+]

Specify the attribute used for displaying user name
[cn/name]

[Apply] [Reset]

Enhanced LDAP configuration – from a group member

The domain controller configuration field is not available in group member XCCs.

The screenshot displays the XClarity Controller 2 web interface for a ThinkSystem SR665 V3 server. The left sidebar shows the navigation menu with 'User/LDAP' highlighted by a red arrow. The main content area is titled 'LDAP' and includes a dropdown for 'Allow logons from:' set to 'Local only'. The 'LDAP Server Information' section contains several configuration options: 'Use LDAP server for Authentication and Authorization' (dropdown), 'Use Pre-Configured Servers' (dropdown), a table for server entries (hostname and port), 'Enable Secure LDAP' (checkbox), and 'Trusted certificate' (status: No trusted certificates are installed). The 'Additional Parameters' section includes fields for 'Binding method', 'Root DN', 'User's Login Name Search Attribute', 'Group Filter', 'Group Membership Search Attribute', and 'Login Permission attribute'. A red dashed box highlights a 'Not available' message, indicating that the domain controller configuration field is not accessible in this context. A tooltip at the bottom right suggests clicking the '?' icon for more details.

Customer-configurable thermal fan speed profile

With this new feature, users can configure an additional cooling boost that goes beyond normal, automatic cooling. It provides the flexibility to cool custom hardware or add additional cooling for specific environments.

The screenshot displays the XClarity Controller interface. On the left is a navigation sidebar with options: Utilization, Storage, Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Neighbor Group. The main area shows system utilization bars for CPU, Memory, I/O, and System, all at 0%. Below this is a 'Fan Speed (RPM)' section with a gear icon for configuration. Three fan tachometers are shown: 1 Front Tach (14022 RPM), 2 Front Tach (13858 RPM), and 3 Front Tach (14022 RPM). A red arrow points from the gear icon to a 'Fan Speed Boost' configuration dialog box. The dialog box contains the following text and options:

Fan Speed Boost [X]

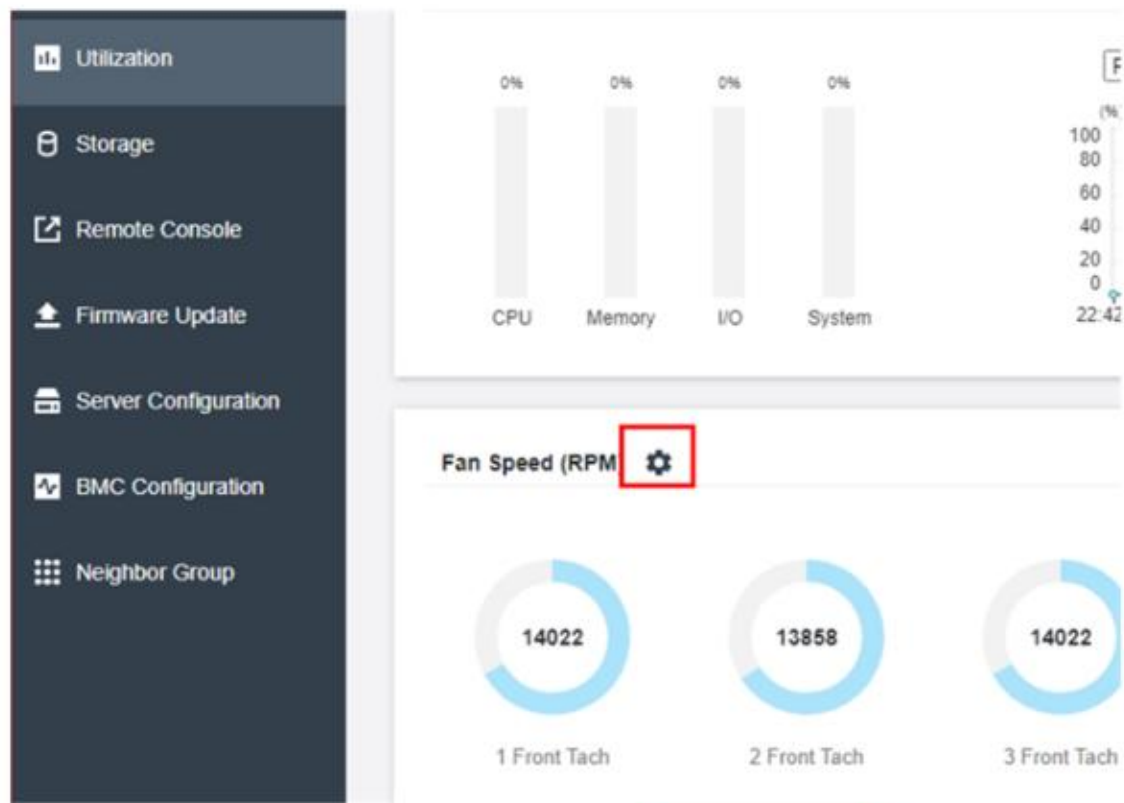
This setting allows additional cooling to the server based on ambient temperature. It can increase the fan over normal speed by controlled thermal algorithm. There will be no change if fan already running at full speed.

- Normal (No fan speed boost)
- Low (Slight boost in fan speed)
- Medium (Moderate boost in fan speed)
- High (Large boost in fan speed)

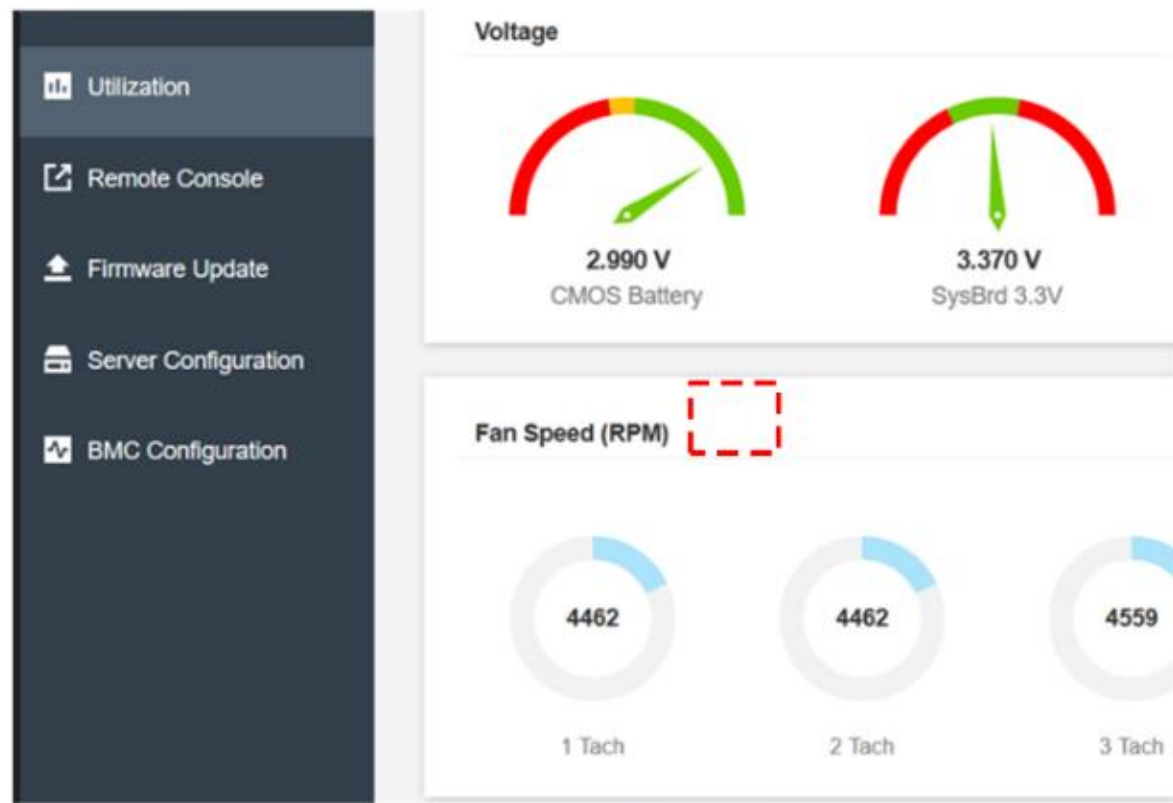
Buttons: Apply, Cancel

Fan speed configuration on XCC and XCC2

The fan speed configuration feature is not available on the previous version of XCC.



XCC2



XCC

Service logs

There are two types of XCC2 service logs:

- Service Data Log: Customer-selectable content categories – the content is user readable and contains basic system information and optional identification data
- Debug log: Formerly called FFDC, it contains the entire service data log and debug log for professional servicing – It was named Service Data in the previous version of XCC

The screenshot displays the XClarity Controller 2 web interface for a ThinkSystem SR650 V3 server. The top navigation bar includes a 'Service Log' button, a user profile icon labeled 'USERID', and a clock showing '7:55 PM'. The main content area is divided into several sections:

- Health Summary:** A grid of system components with status indicators. CPU (2/2 installed), Memory (2/32 installed), Local Storage (8/16 installed), PCI (7 installed), Power Supply (1/2 installed), Fan (4/12 active), System Board, Others, and Security (Crypto Compatibility).
- System Information and Settings:** A list of system details including Machine Type, Serial No., System Name, Front USB Ownership, BMC License, BMC IP Address, BMC Hostname, BMC Version, UEFI Version, LXP Version, and Location.
- Quick Actions:** Includes 'Power Action' and 'Location LED: Off'. A 'Service Log' button is highlighted with a red box.
- Power Utilization:** Shows a bar chart for 'Input' (34W) and 'Output' (17W / 1100W).
- System Utilization:** Shows four vertical bars representing different utilization metrics, all at 0%.

A modal dialog titled 'Select the type of service log to download:' is open over the System Information and Settings section. It offers two main options:

- Service Data Log:** Described as containing 'basic system information and optional identification data, content is user readable'. This option is selected and highlighted with a red box.
- Debug log:** Described as containing 'the entire service data log and debug log for professional service usage, formerly called FFDC'.

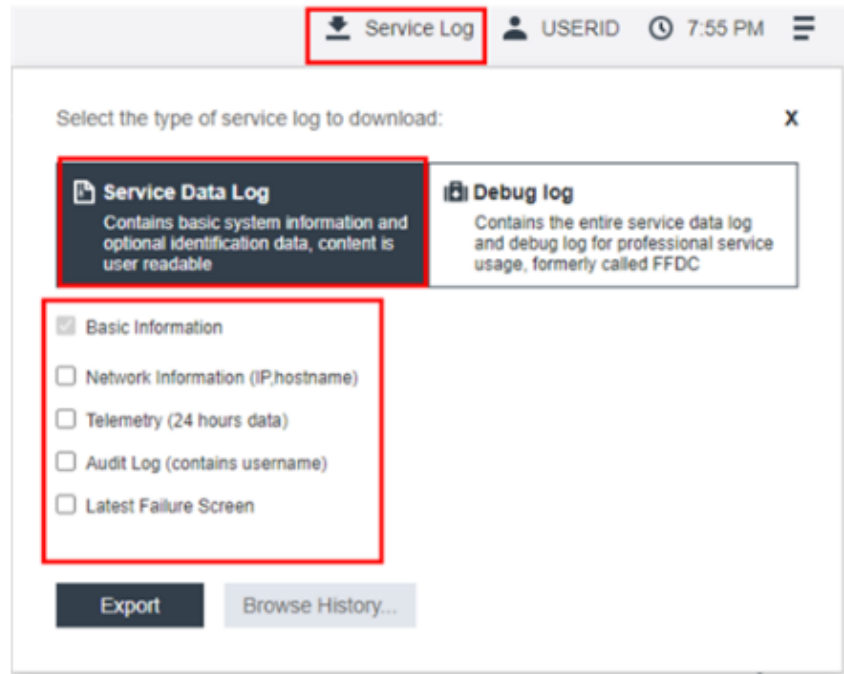
Below these options, a list of checkboxes allows for selecting specific content categories for the Service Data Log:

- Basic Information
- Network Information (IP/hostname)
- Telemetry (24 hours data)
- Audit Log (contains username)
- Latest Failure Screen

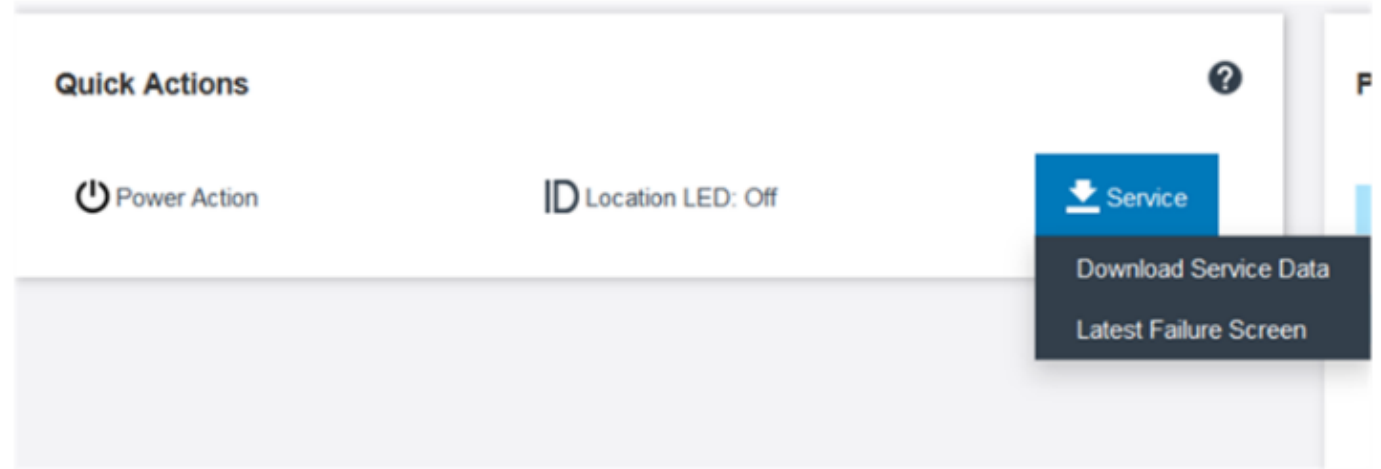
Buttons for 'Export' and 'Browse History...' are located at the bottom of the dialog.

Service logs on XCC and XCC2

With XCC2, users can download the Service Data Log or the Debug log (FFDC), while with XCC, users can only download Service Data (FFDC).



XCC2



XCC

Service Data Log – Browse History

Select **Browse History** to access the entire Service Data Log (mini-log) and the corresponding full FFDC. It is possible to download the full FFDC if a customer case is escalated to PE or development.

The screenshot displays the XClarity Controller interface. At the top right, there is a 'Service Log' button with a download icon, highlighted with a red box. Below it, a modal window titled 'Select the type of service log to download:' is open. This modal contains two main options: 'Service Data Log' and 'Debug log'. The 'Service Data Log' option is highlighted with a red box and includes a list of sub-options: 'Basic Information' (checked), 'Network Information (IP,hostname)', 'Telemetry (24 hours data)', 'Audit Log (contains username)', and 'Latest Failure Screen'. Below the modal, there are 'Export' and 'Browse History...' buttons, with the latter highlighted by a red box and a red arrow pointing to it. In the background, another modal window titled 'Select the file to download:' is visible, showing two file names: '7D75CTO0WW_1234567890_xcc_mini-log_20220316-133658.tgz' and '7D75CTO0WW_1234567890_xcc_20220316-133658.tzz', both highlighted with a red box. The interface also shows a 'System name:' field, user information (USERID), and a clock (8:00 PM). At the bottom left, the Lenovo logo is visible.

XCC Platinum license key for new XCC2 features

The following new XCC2 features require an XCC Platinum license:

- System Guard – Monitors hardware inventory for unexpected component changes and then logs events or prevents booting
- Enterprise Strict Security mode – Enforces FIPS 140-3 level security and enhanced NIST 800-193 support
- Neighbor Group – Enables administrators to manage and synchronize configurations and firmware levels across multiple servers
- Mini-Log – New service tool that provides XCC first-failure logs in HTML and JSON format

Refer to [Lenovo Press](#) for more details about XCC Platinum.

XCC2 – scenario study

Question 1: Which server system boards will be equipped with the XCC2 chip?

Answer: Depending on the machine type, the XCC2 chip will be on the system board or I/O board.

Question 2: Will the service logs (Service Data Log and Debug log) be identical on both AMD-based servers and Intel-based servers?

Answer: The design is the same, but the content will differ due to the differences between AMD and Intel processor/chipset architecture.

Question 3: To update XCC2, does USB over LAN need to be enabled?

Answer: USB over LAN only has to be enabled for in-band updates.

Question 4: Do different security levels – for example: Enterprise Strict Security Mode or Standard Security Mode – influence XCC FFDC log collection?

Ans: No. All security levels support FFDC log collection.

XCC tool for XCC2

The XCC tool is a CLI-based tool for XCC2 on the ThinkSystem V3 platform, and it can be used to back up and restore FoD keys, XCC2 configuration, and VPD.

This tool is only available for service engineers - do not share it with customers.

For more information about XCC tool, refer to the following GLOSSE tip page:

[TOOL_XCC tool for XCC2](#)

Description↵

-----↵

↵

This project includes a set of sample Python scripts that utilize the Redfish API to replace Lenovo ThinkSystem servers.↵

↵

Installing↵

-----↵

*To install the python, download for windows from

<<https://www.python.org/downloads/>>↵

↵

Manually add environment variables: My Computer -> Properties -> Advanced System Settings -> Environment Variables -> PATH -> Edit->Add our Python installation path at the end:

C:\Users\APP_Server\AppData\Local\Programs\Python\Python39\ -> OK.↵