

System management tool, security, and Edge networking

Security settings and Edge networking in XCC

The Lenovo logo is positioned on the right side of the slide. It consists of the word "Lenovo" in a white, sans-serif font, oriented vertically. The background behind the text is a vertical gradient bar that transitions from green at the top to blue at the bottom.

Server management tool

As with other Lenovo ThinkSystem products, the SE350 uses the XCC as a system management tool, but it also has the following specific features:

- ThinkShield Key Vault security settings:
 - System lockdown mode
 - Self Encryption Drive (SED) Authentication Key (AK) Manager
- Edge networking (Wireless-enabled LOM package only)
 - Edge device network topology
 - Wi-Fi connectivity
 - LTE connectivity
 - Edge network board address
 - BMC network bridge
 - Edge network board troubleshooting

ThinkShield Key Vault security settings

Select **BMC configuration > Security**, and then scroll down the page until you see **System Lockdown Mode** and **SED Authentication Key (AK) Manager**.

The screenshot shows the BMC configuration > Security page with the following sections:

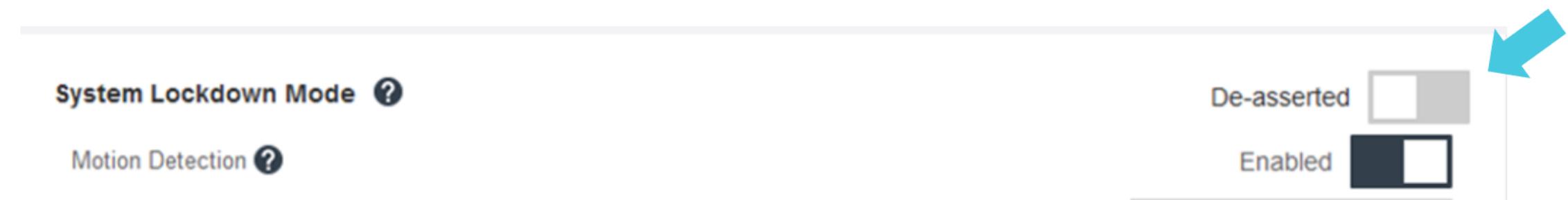
- System Lockdown Mode**: A warning message states: "'Motion Detection' is in disabled state, system now loses the capability to detect motion event and trigger lockdown mode automatically when someone moves system unexpectedly. 'Chassis intrusion Detection' is in disabled state, system now loses the capability to detect chassis intrusion event and trigger lockdown mode automatically when someone opens enclosure top cover or front bezel unexpectedly." The "De-asserted" checkbox is checked.
- Motion Detection**: The "Disabled" checkbox is checked.
- Chassis Intrusion Detection**: The "Disabled" checkbox is checked.
- Additional Configurations**: A checkbox for "Host would be shutdown automatically if a tamper event is detected" is checked. A "Reset Device Internal Counter" section contains a "Yes I would like to reset counter" checkbox and a "Reset Counter" button. The ThinkShield Key Vault logo is present.
- SED Authentication Key (AK) Manager**: A list of options: "Change the SED AK", "Backup the SED AK", and "Recover the SED AK". A search icon is also present.

System lockdown mode

System Lockdown Mode is triggered either as a result of a tamper event (either chassis intrusion or motion detection) or because it was selected through the external BMC interface. One of the following things would have happened for system lockdown mode to be asserted:

- A chassis intrusion event was detected because the top cover or front bezel was opened.
- A motion event was detected by the accelerometer because the machine was moved a significant distance.
- The user manually asserted lockdown mode using the toggle button shown below.

When system lockdown mode is asserted, access to the system is denied. When the system is locked, activation is required for it to be unlocked. Refer to the [Web manual activation](#) section in this course for details of how to unlock the system.



Motion detection

When motion detection is enabled, the BMC is able to detect motion events and protect the system by automatically triggering lockdown mode when someone moves the system. Users need to set up **Sensitivity Level** and **Orientation** when they enable motion detection.

- **Sensitivity Level:** This field allows users to configure accelerometer sensitivity.
 - Low: Shaking, falling, or rolling – 500 Gal / 100 ms
 - Medium: Stealing or significant movement – 250 Gal / 300 ms
 - High: Vibrations or a magnitude 5 earthquake – 250 Gal / 100 ms
- **Orientation:** This is set according to chassis mount type.

The screenshot shows the Motion Detection configuration page. On the left, there are several configuration options: Motion Detection (Enabled), Sensitivity Level (Low), Orientation (Stand Desktop), Chassis Intrusion Detection, and Additional Configurations (Host would be shutdown automatically if a tamper event is detected). The Additional Configurations section has a note: "Host would be shutdown automatically if a tamper event is detected". On the right, there is a note: "Please ensure to select 'Orientation' according to chassis mount type exactly before enabling Motion Detection." Below this note, five orientation options are listed with corresponding diagrams: 1. Stand Desktop (horizontal), 2. Wall Mount (Horizontal), 3. Wall Mount (Vertical), 4. Bookshelf, and 5. Ceiling Mount.

Motion Detection

Enabled

Sensitivity Level

Orientation

Chassis Intrusion Detection

Additional Configurations

Host would be shutdown automatically if a tamper event is detected

Enabled

Low

Stand Desktop

Stand Desktop

Wall Mount (Horizontal)

Wall Mount (Vertical)

Bookshelf

Ceiling Mount

Please ensure to select "Orientation" according to chassis mount type exactly before enabling Motion Detection.

1. Stand Desktop

2. Wall Mount (Horizontal)

3. Wall Mount (Vertical)

4. Bookshelf

5. Ceiling Mount

Chassis intrusion detection

When chassis intrusion detection is enabled, the BMC is able to detect chassis intrusion events and protect the system by automatically triggering lockdown mode when someone opens the enclosure top cover or front bezel.

⚠ 'Motion Detection' is in disabled state, system now loses the capability to detect motion event and trigger lockdown mode automatically when someone moves system unexpectedly.

'Chassis intrusion Detection' is in disabled state, system now loses the capability to detect chassis intrusion event and trigger lockdown mode automatically when someone opens enclosure top cover or front bezel unexpectedly.

Motion Detection ?

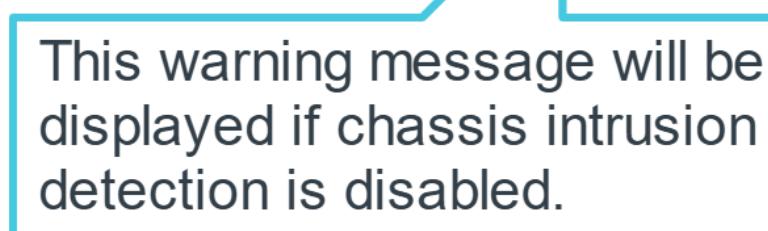
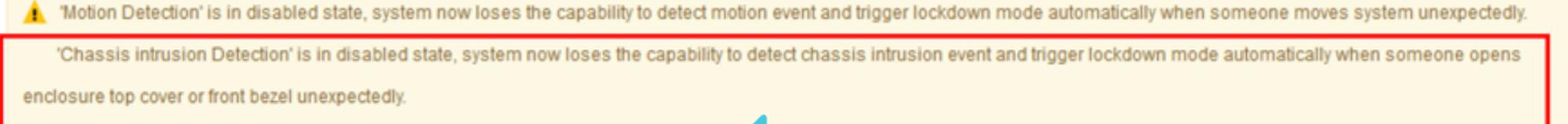
Chassis Intrusion Detection ?

► Additional Configurations

Disabled

Disabled

This warning message will be displayed if chassis intrusion detection is disabled.



ThinkShield
Key Vault

Additional configurations

Users can choose to select or deselect the following settings in the **Additional Configurations** section.

- Host would be shut down automatically if a tamper event is detected
- BMC network bridge through Up Link Ports would be disabled automatically if a tamper event is detected
- BMC network bridge through Wi-Fi Ports would be disabled automatically if a tamper event is detected

Chassis Intrusion Detection 

Disabled 

▼ Additional Configurations

Host would be shutdown automatically if a tamper event is detected

BMC network bridge through Up Link Ports would be disabled automatically if a tamper event is detected

BMC network bridge through Wi-Fi Ports would be disabled automatically if a tamper event is detected

Reset Device Internal Counter

Yes I would like to reset counter

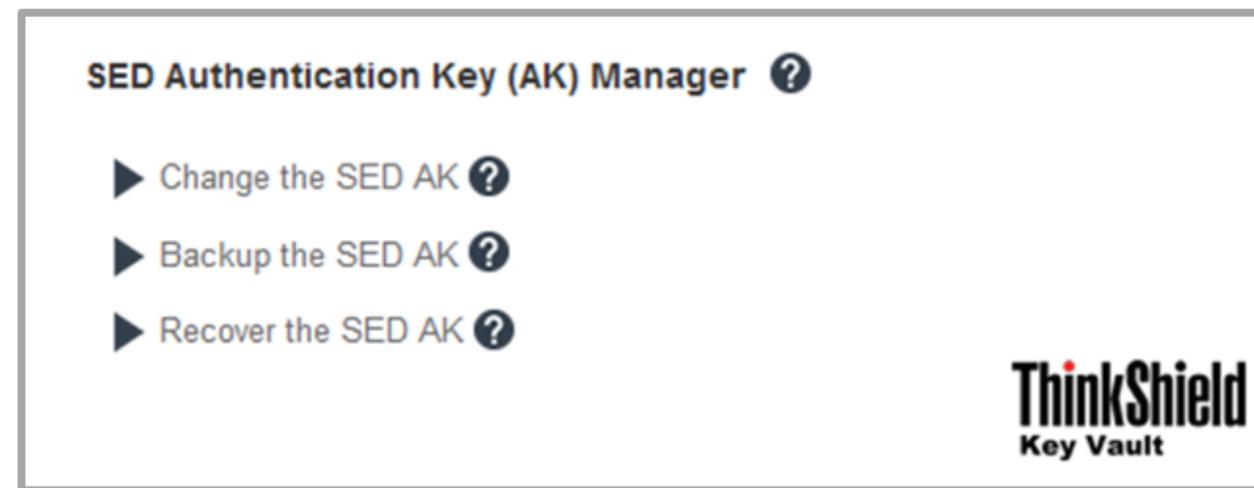




SED Authentication Key (AK) Manager

This feature allows the BMC to deploy the SED key. The SED key is designed for encryption of both boot and data drives, and it should be stored securely in the BMC to allow the system to boot without manual intervention. The SED AK Manager includes the following features:

- Change the SED AK
- Backup the SED AK
- Recover the SED AK



Note: This operation is not allowed when the system is not activated (lockdown mode has been asserted) or when the current user does not have the authority to manage the SED key.

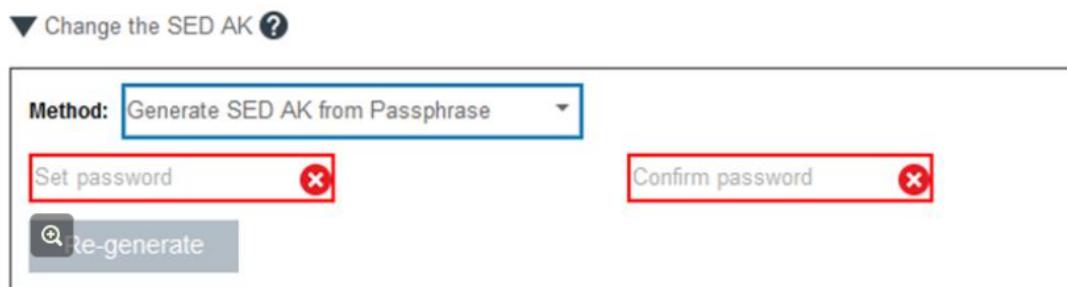
Change the SED AK

This option allows users to renew the SED AK. If users select **Generate a Random SED AK**, it is highly recommended that they back up the SED AK. Users can also select **Generate SED AK from Passphrase**.

- Generate SED AK from Passphrase:
 - XCC generates an SED AK based on the given passphrase, and the user is then able to restore the SED AK without having an SED AK backup file.
 - Generate a Random SED AK:
 - XCC generates a random SED AK, and the user then needs to back up the AK file.
- After a customer changes the SED AK, the security chip will keep two SED AKs (new and old). At the next system restart, UEFI will replace the old SED AK with the new AK. After completion, XCC will replace the AK in the security chip.

▼ Change the SED AK ?

Method:



▼ Change the SED AK ?

Method:



Backup the SED AK

It is the customer's responsibility to maintain the SED AK. To be fully prepared for a hardware failure, a user backup of the SED AK is required. For customer security, Lenovo does not keep a copy of the SED AK. Data loss could occur if the SED AK backup is not available after hardware repair.

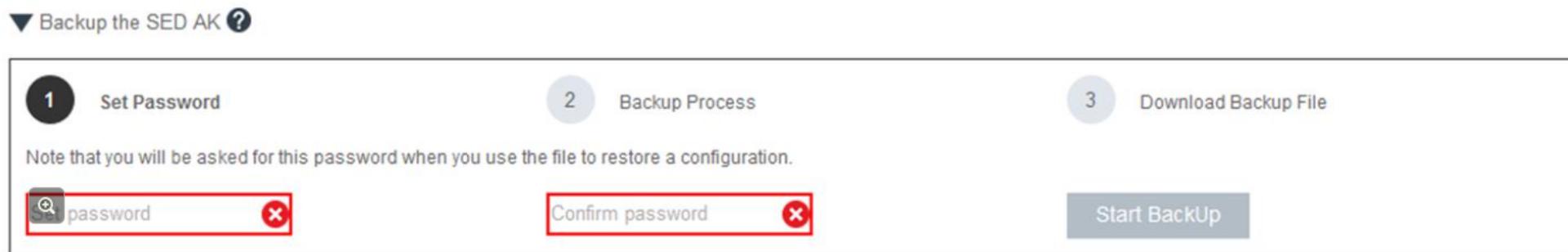
Customers have to assign a unique password to the SED AK backup file; the password needs at least nine characters.

▼ Backup the SED AK ?

1 Set Password 2 Backup Process 3 Download Backup File

Note that you will be asked for this password when you use the file to restore a configuration.

password × Confirm password × Start BackUp



Recover the SED AK

The SED authentication key can be imported from an external file. Select the file that contains the SED authentication key you wish to recover. You will need to provide the password you specified when the SED authentication key was exported.

▼ Recover the SED AK ?

Method: Recover SED AK from Backup file

1 Select File and Input 2 Verify File 3 Restore Process

Password

Note that you need to provide a BMC backup file and corresponding password.

Browse... Browse a back... **Next >**

Edge Networking setting

The Edge Networking setting in XCC is only available for the Wireless-enabled LOM package model. Users can set up their network topology and WiFi/LTE connection in this section.

The screenshot shows the Clarity Controller interface with the following details:

- Left Sidebar:** Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Server Configuration, BMC Configuration, Edge Networking (highlighted with an orange box).
- Header:** Clarity Controller, ThinkSystem SE350 Planner (2123IT C...), System name: (empty), A yellow warning bar: "The SED AK has changed, please make a backup of SED AK and store it safely".
- Edge Device Network Topology:** A diagram of a server board with ports 1-9. Ports 8 and 9 are labeled "Wi-Fi" and "LTE" respectively. Other ports are unlabeled.
- Current ports assignment:**

Port	Assignment
1	10 GbE SFP+
2	10 GbE SFP+
3	1 GbE SFP
4	1 GbE SFP
5	1 GbE RJ45
6	1 GbE RJ45
7	1 GbE RJ45
8	Wi-Fi
9	LTE
- Wi-Fi Connectivity:**

Hardware Level	Driver Version	MAC Address	Enabled
rti68x2be	v5.2.21.5_30361.20181019	105BAD084v5.2.21.5_30361.201810	<input type="checkbox"/>

Edge device network topology settings

A network topology is the arrangement of nodes and their connections within a network. The system will reset the network settings of ports to default after a user changes their network topology.

Several network topology presets have been defined to facilitate port assignments on this device for operation as a standalone system or as a cluster with another local peer device. Five types of network topology are available. Click the preset buttons for more details.

Preset 1

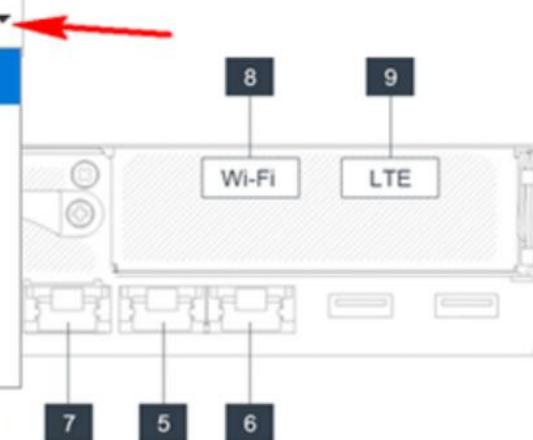
Edge Device Network Topology

Several network topology presets have been defined to facilitate port assignments on this device for

Note: changing the topology might disrupt the communication on this device.

Preset 2

- Network Topology Preset 1
- Network Topology Preset 1
- Network Topology Preset 2
- Network Topology Preset 3
- Network Topology Preset 4
- Network Topology Preset 5
- Custom Configuration



Preset 3

Preset 4

Preset 5

Edge deployment

A network topology system will have several network devices for connection. Five types of

Preset 1

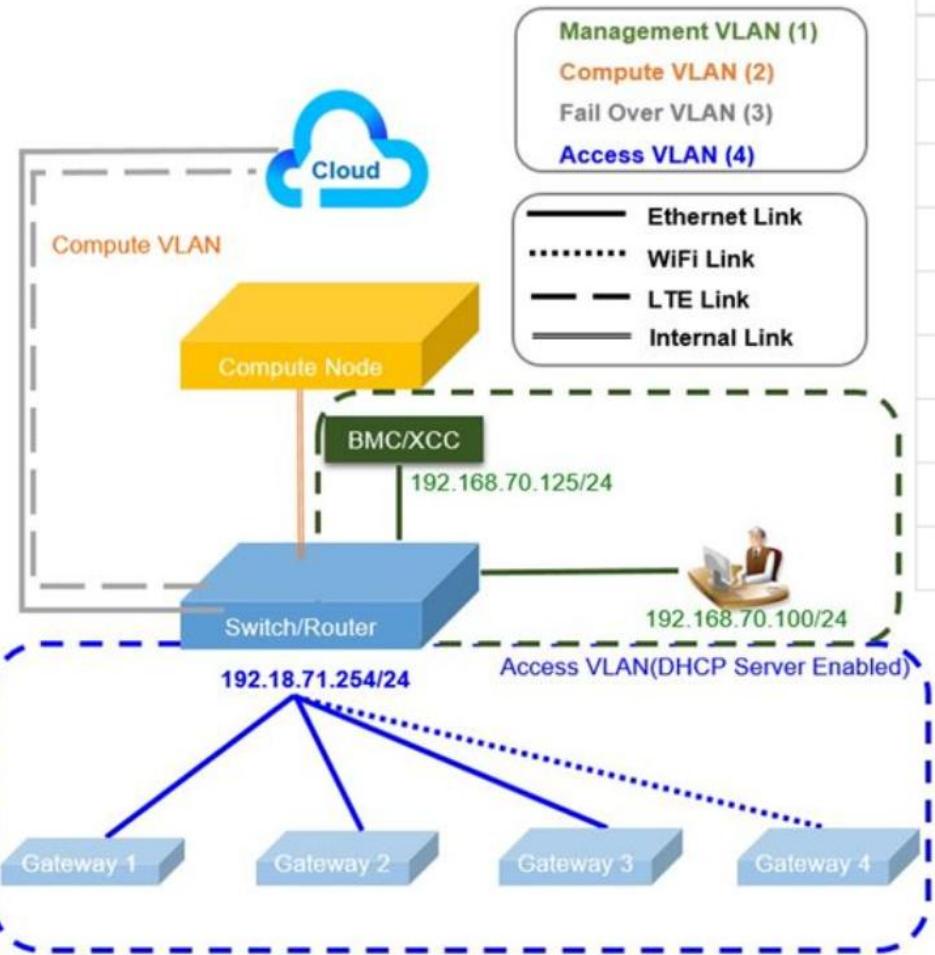
Preset 2

Preset 3

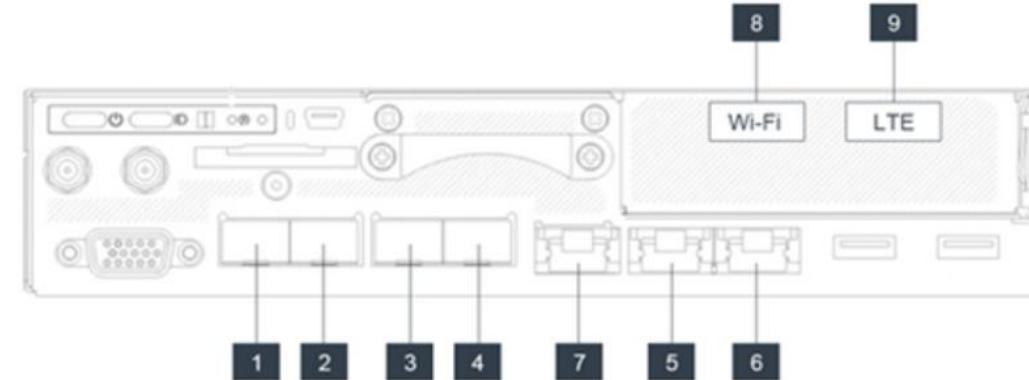
Preset 4

Preset 5

Preset 1 is the default configuration, and it provides maximum access links to the IoT gateway.



	Port	Assignment
1	10 GbE SFP+	Host OS Managed Link
2	10 GbE SFP+	Host OS Managed Link
3	1 GbE SFP	Down Link (Individual)
4	1 GbE SFP	Down Link (Individual)
5	1 GbE RJ45	Down Link (Individual)
6	1 GbE RJ45	Up Link (Failover pair master or slave)
7	1 GbE RJ45	XClarity Controller Management Link
8	Wi-Fi	Down Link (Individual)
9	LTE	Up Link (Failover pair master or slave)



Edge devices

A network topology is the way a system will connect to the Internet. Several network topologies exist. A network device for connecting to the Internet. Five types of network topologies exist.

Preset 1

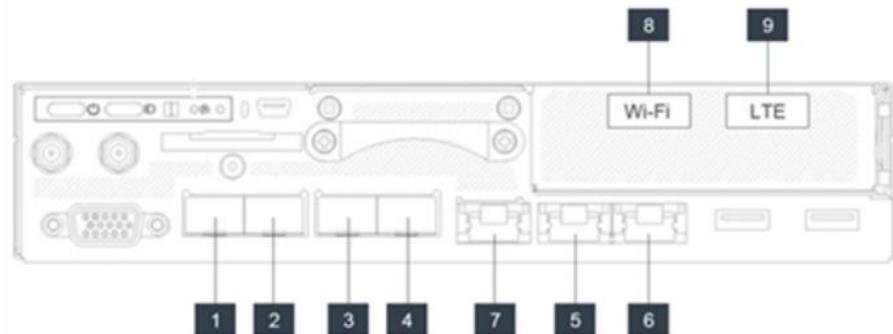
Preset 2

Preset 3

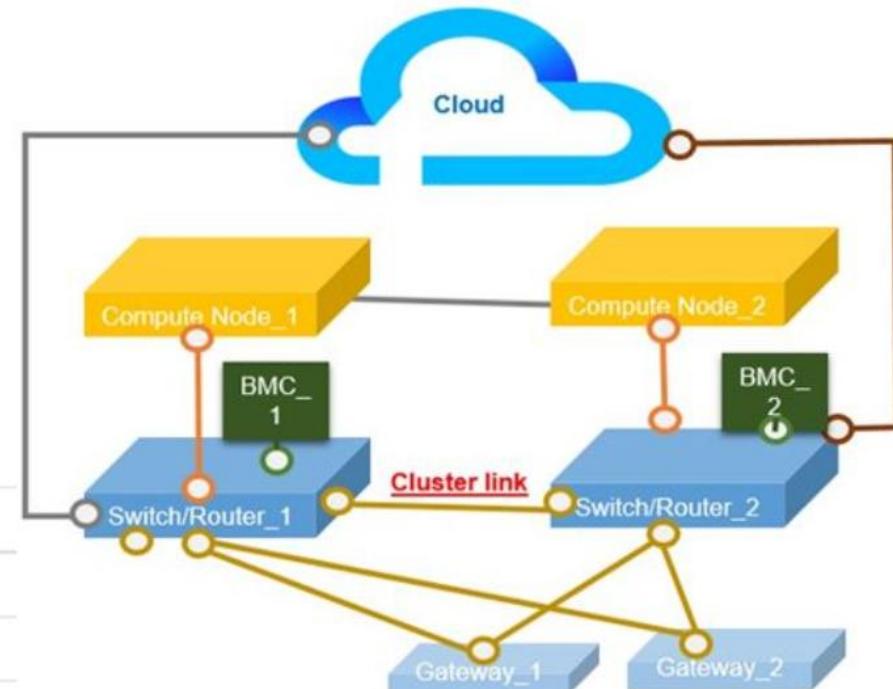
Preset 4

Preset 5

Preset 2 is used when two SE350s are connected for redundancy in cluster mode. Note that Port 3 is assigned as the cluster port in this setting.



VLAN_Cloud_1
VLAN_Cloud_2
VLAN_BMC
VLAN_X86
VLAN_Edge



	Port	Assignment
1	10 GbE SFP+	Host OS Managed Link
2	10 GbE SFP+	Host OS Managed Link
3	1 GbE SFP	Cluster Port
4	1 GbE SFP	Down Link (Individual)
5	1 GbE RJ45	Down Link (Individual)
6	1 GbE RJ45	Up Link (Failover pair master or slave)
7	1 GbE RJ45	XClarity Controller Management Link
8	Wi-Fi	Down Link (Individual)
9	LTE	Up Link (Failover pair master or slave)

Edge deployment

A network topology is the way a system will be connected. There are several network topologies. A network topology is the way a system will be connected. Several network topologies are possible. A network topology is the way a system will be connected. Several network topologies are possible. Five types of network topologies are possible.

Preset 1

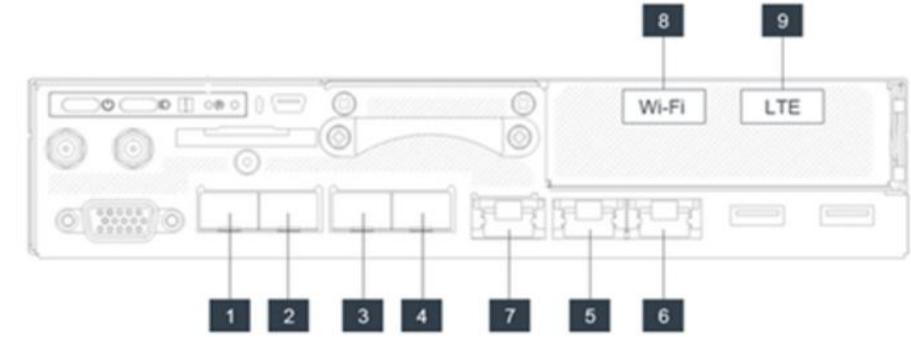
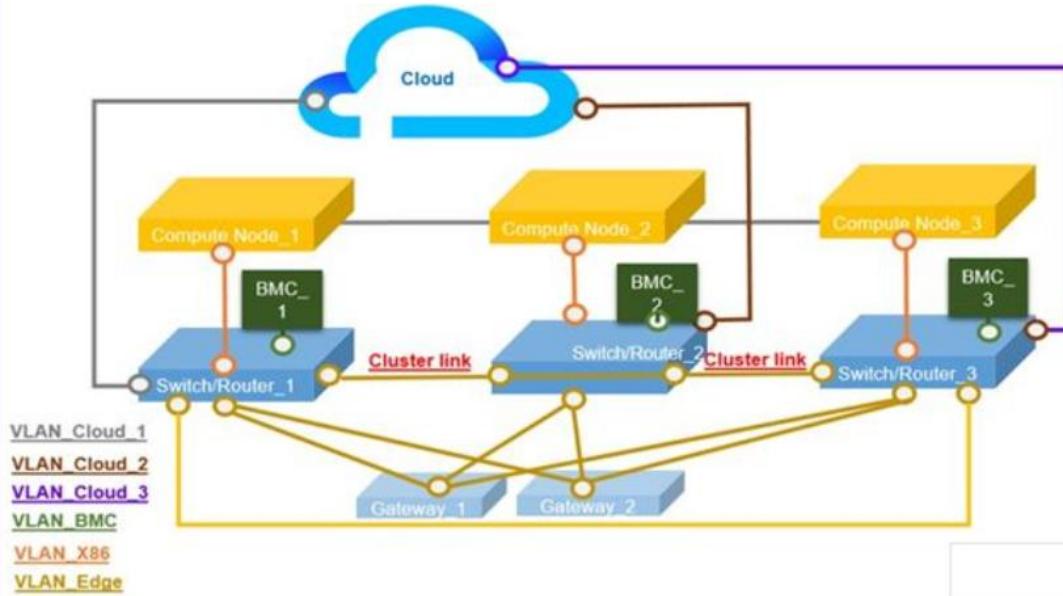
Preset 2

Preset 3

Preset 4

Preset 5

Preset 3 is used when three SE350s are connected for redundancy in cluster mode. Note that Ports 3 and 4 are assigned as cluster ports in this setting.



	Port	Assignment
1	10 GbE SFP+	Host OS Managed Link
2	10 GbE SFP+	Host OS Managed Link
3	1 GbE SFP	Cluster Port
4	1 GbE SFP	Cluster Port
5	1 GbE RJ45	Down Link (Individual)
6	1 GbE RJ45	Up Link (Failover pair master or slave)
7	1 GbE RJ45	XClarity Controller Management Link
8	Wi-Fi	Down Link (Individual)
9	LTE	Up Link (Failover pair master or slave)

Edge devices

A network topology system will have several network devices for connection. Five types of

Preset 1

Preset 2

Preset 3

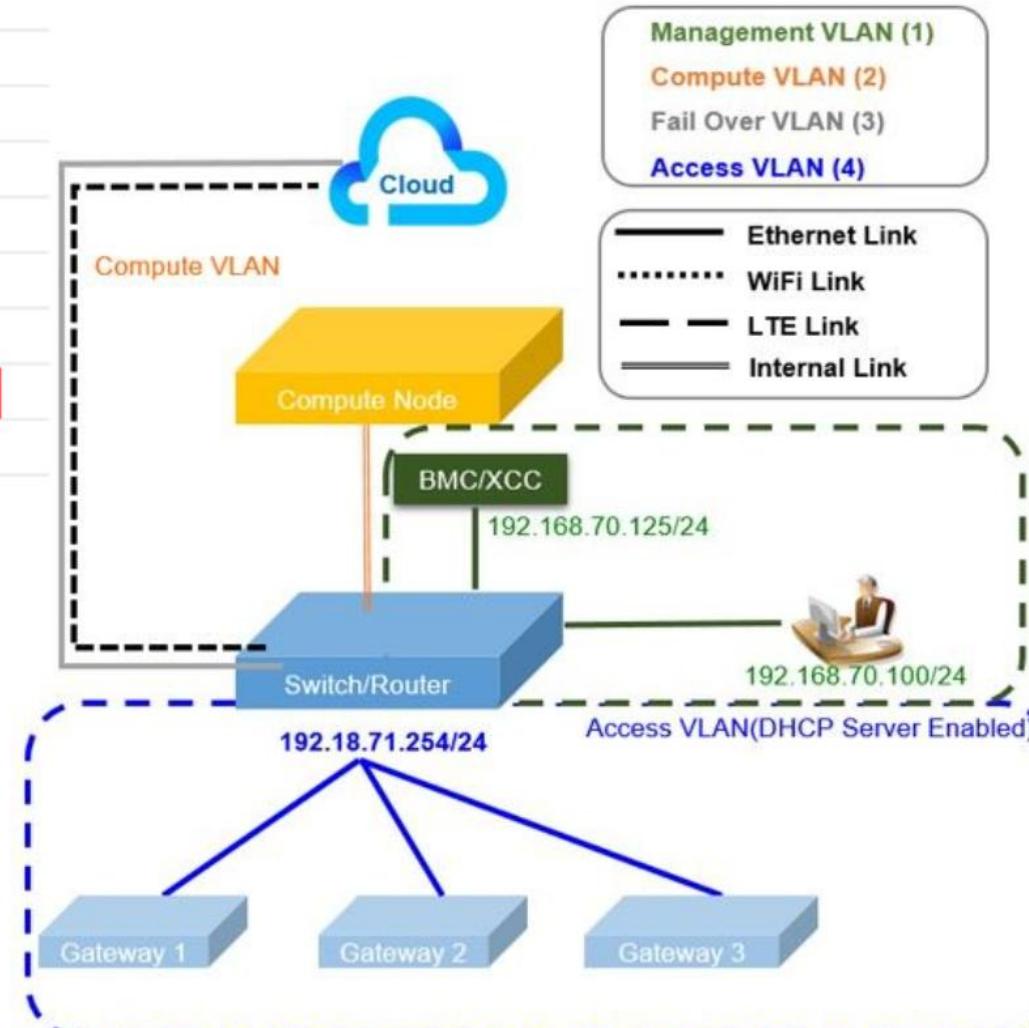
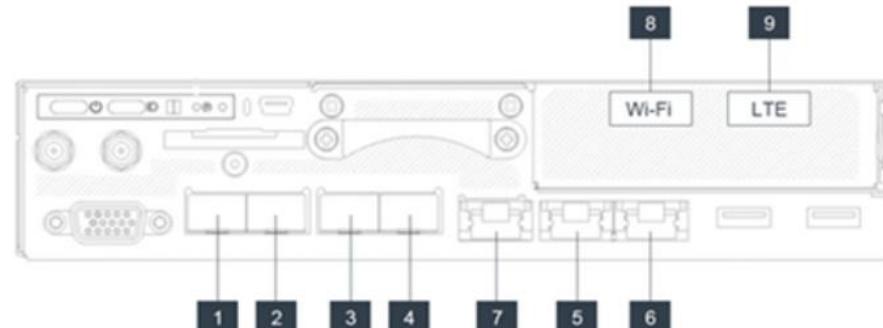
Preset 4

Preset 5

With Preset 4, Port 8 is configured as an uplink failover.



	Port	Assignment
1	10 GbE SFP+	Host OS Managed Link
2	10 GbE SFP+	Host OS Managed Link
3	1 GbE SFP	Down Link (Individual)
4	1 GbE SFP	Down Link (Individual)
5	1 GbE RJ45	Down Link (Individual)
6	1 GbE RJ45	Up Link (Failover pair master or slave)
7	1 GbE RJ45	XClarity Controller Management Link
8	Wi-Fi	Up Link (Failover pair master or slave)
9	LTE	Up Link (Failover pair master or slave)



Edge devices

A network topology is a system that defines the way data travels through a system. Several network topologies exist, each device for different purposes. Five types of network topologies are:

Preset 1

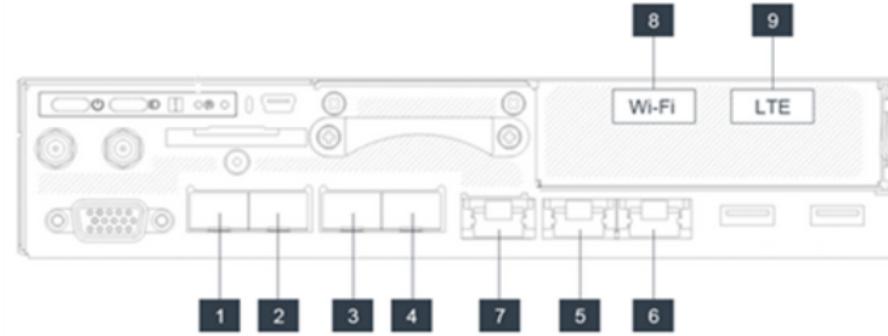
Preset 2

Preset 3

Preset 4

Preset 5

Preset 5 is used to change the assignment of Ports 3 to 6 and Port 8. Ports 3 to 6 are given the Plate assignment (like a layer 2 switch that only forwards frames in a LAN). 



	Port	Assignment
1	10 GbE SFP+	Host OS Managed Link
2	10 GbE SFP+	Host OS Managed Link
3	1 GbE SFP	Plate
4	1 GbE SFP	Plate
5	1 GbE RJ45	Plate
6	1 GbE RJ45	Plate
7	1 GbE RJ45	XClarity Controller Management Link
8	Wi-Fi	User Configuration
9	LTE	Up Link (Failover pair master or slave)

Wi-Fi connectivity

This feature uses the BMC to configure Wi-Fi credentials for the Edge network board. Users can choose between Access Point and Client methods, and they must also enter the SSID and WPA password. The information is stored securely in the BMC.

Wi-Fi Connectivity ?		
Hardware Level	Driver Version	MAC Address
rtl88x2be	v5.2.21.1_27105.20180315_COEX20180112-5959	
Method:	<input type="button" value="▼"/>	
SSID:	<input type="text" value=""/> ✖	
Encryption:	WPA2	
Password:	<input type="text" value=""/> ✖	
<input type="button" value="🔍 Apply"/>		<input type="button" value="Reset"/>

LTE connectivity

This feature allows users to enable or disable LTE connectivity for the Edge network board.

LTE Connectivity [?](#)

Hardware Level	Firmware Version	IMEI Code

Enabled

[Apply](#) [Reset](#)

Edge network board address

This feature allows users to configure the IPv4 and IPv6 addresses of the Edge network board.

Edge Network Board Address

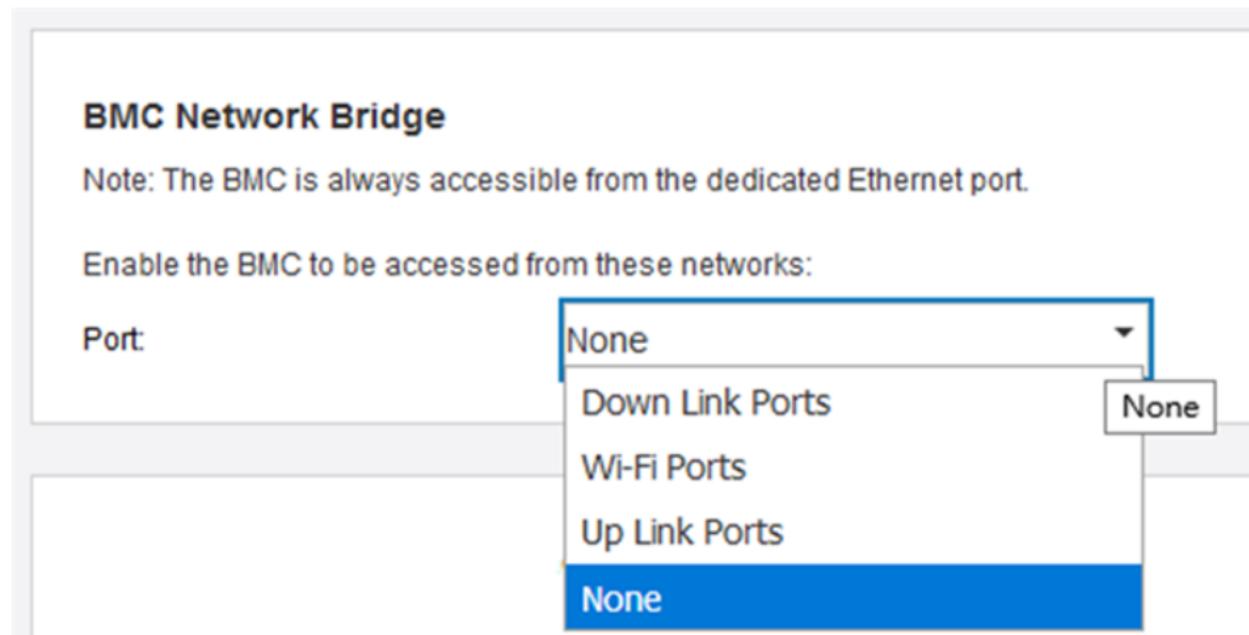
This IP address would be accessed through the BMC dedicated port as well as any bridged network as configured.

IPv4	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
DHCP Server 	<input type="checkbox"/> Disabled	
Method:	<input type="button" value="Use static IP address"/>	
IPv4 address:	192.168.70.254	
Network mask:	255.255.255.0	

IPv6	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled
DHCP Server 	<input type="checkbox"/> Enabled	
Method:	<input type="button" value="Obtain IP from DHCP"/>	
IPv6 address:	::	
Prefix length:	0	

BMC network bridge

The BMC network bridge allows users to select the outbound interface to access the BMC management port. There are four options as shown below. The default option is **None**, which means that only the dedicated RJ45 port can access the XCC interface.



BMC network bridge configuration – example

The following steps show you how to configure BMC access through the Wi-Fi network.

Click each number in turn to see the procedure.

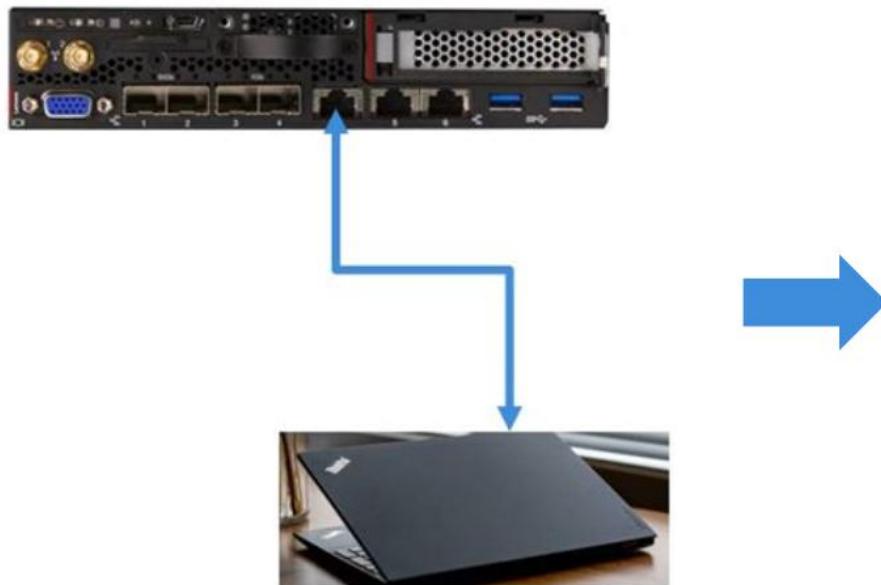
Step



BMC network bridge configuration – example

Assuming it is a new SE350, leave all the configurations in their default settings.

- Connect the RJ45 network cable to the SE350 XCC MGMT port and to your laptop.
- Open the XCC Web page in a Web browser and log in with the default XCC IP address and credentials:
 - Default XCC IP: 192.168.70.125
 - Username: USERID
 - Password: PASSW0RD (0 = Zero)

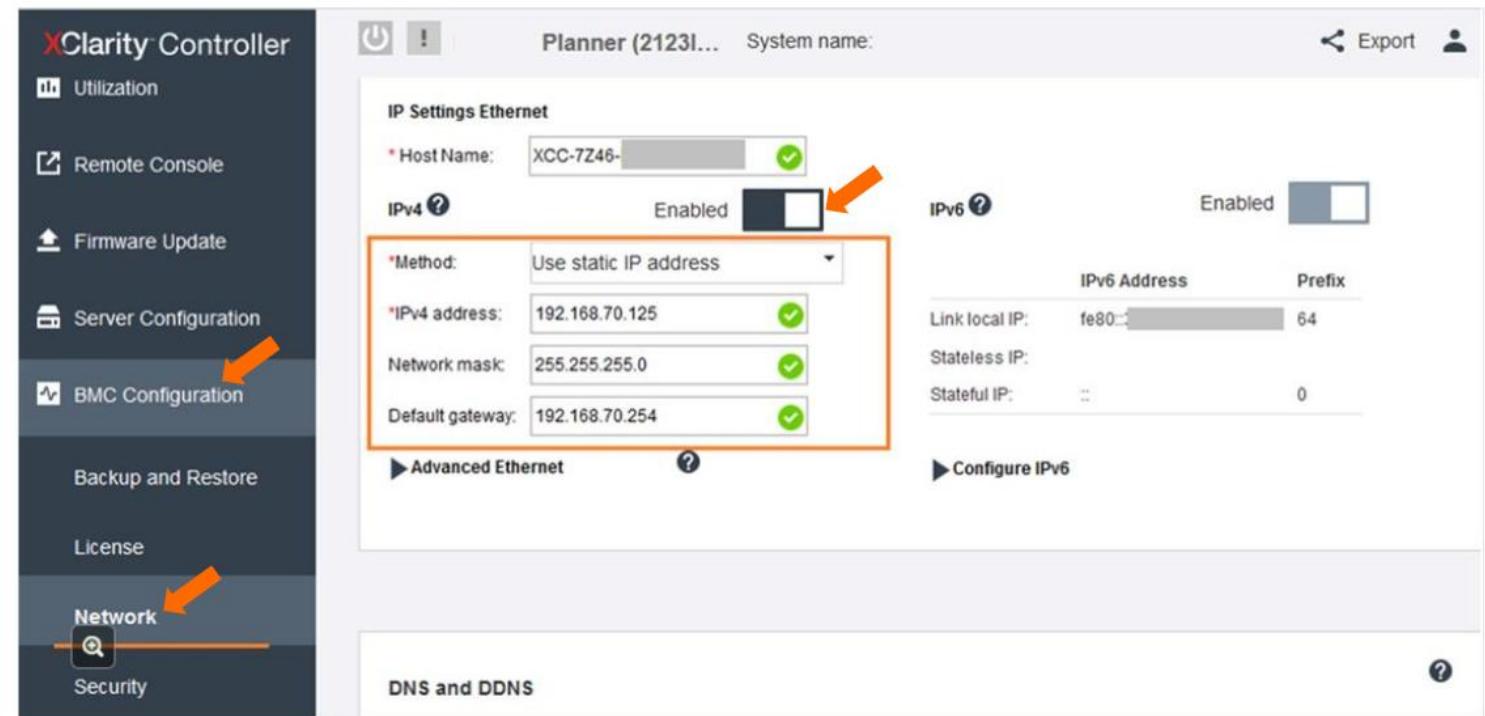


Note: You will be asked to change the default BMC password after logging in for the first time.



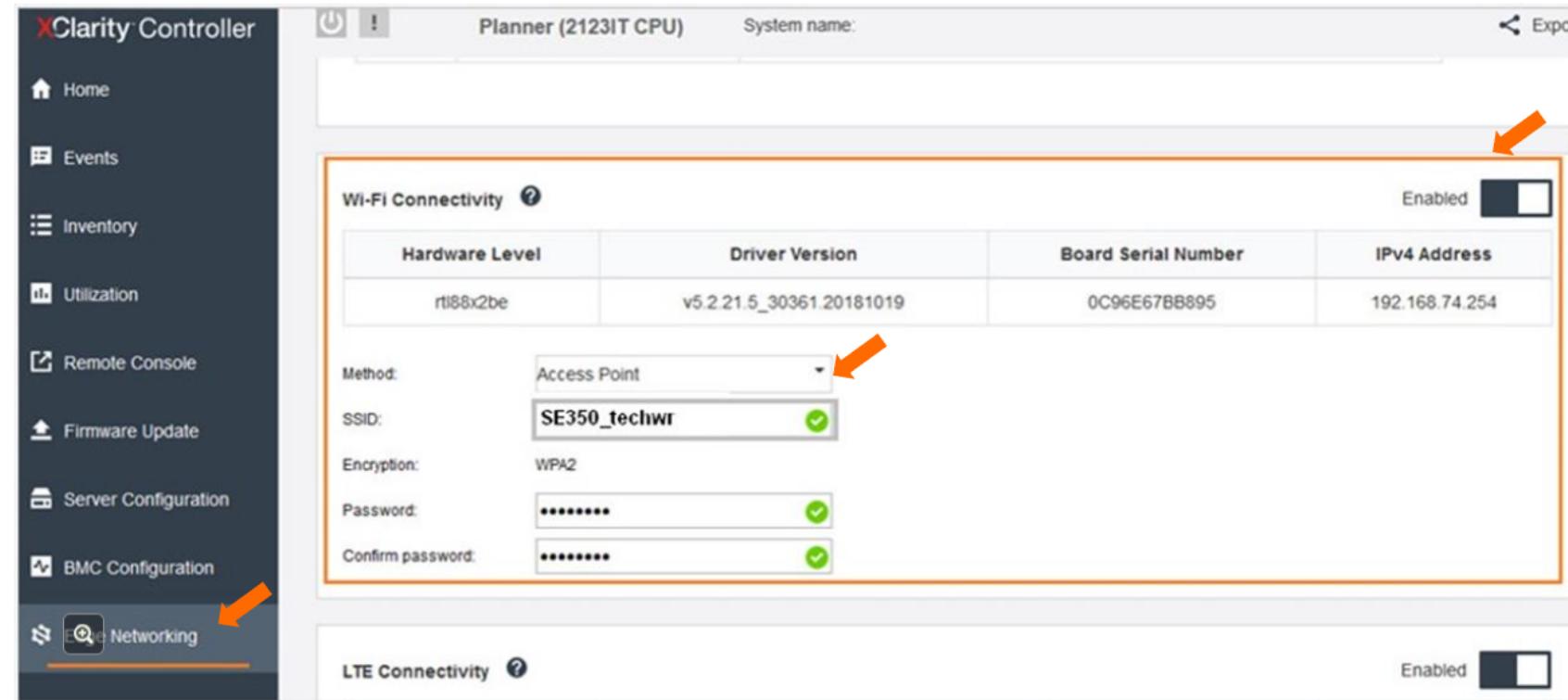
BMC network bridge configuration – example

- Set up the XCC IPv4 configuration.
- From the XCC Web GUI, select **BMC Configuration** → **Network**.
 - **Method:** select **Use static IP address**
 - **Network mask:** customer preferences
 - **Default gateway:** customer preferences



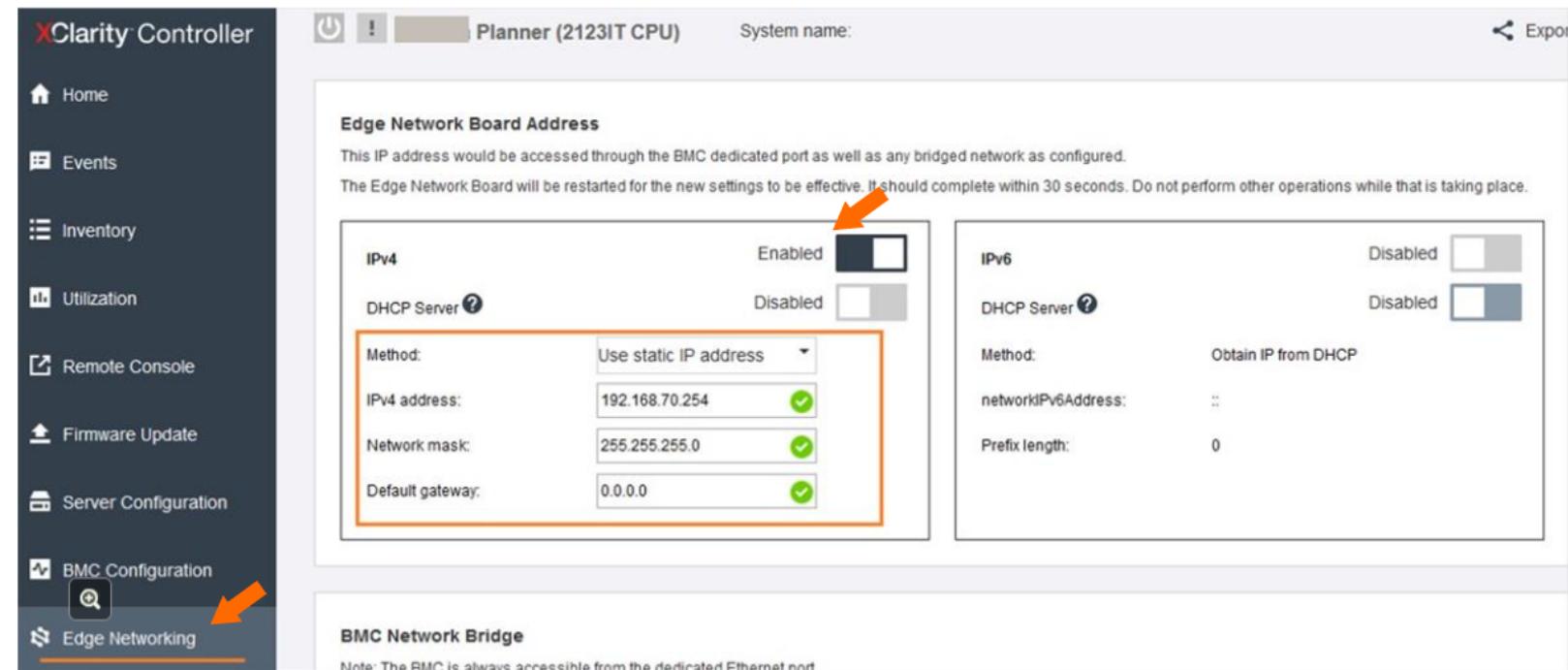
BMC network bridge configuration – example

- Set up the Wi-Fi connectivity configuration.
- From the XCC Web GUI, select **Edge Networking** → **Wi-Fi Connectivity**.
 - Select **Enabled**
 - **Method:** select **Access Point**
 - **SSID:** your own SSID
 - **Password:** your own password



BMC network bridge configuration – example

- Set up the Edge network board address.
- From the XCC Web GUI, select **Edge Networking → Edge Network Board Address**.
 - **IPv4**: select **Enabled**
 - **Method**: select **Use static IP address**
 - **IPv4 address**: your own
 - **Network mask**: your own
 - **Default gateway**: your own



The screenshot shows the XClarity Controller (XCC) Web GUI interface. The left sidebar has the following menu items: Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Edge Networking. The Edge Networking item is highlighted with an orange arrow. The main content area is titled 'Edge Network Board Address' and contains the following configuration:

Edge Network Board Address
This IP address would be accessed through the BMC dedicated port as well as any bridged network as configured.
The Edge Network Board will be restarted for the new settings to be effective. It should complete within 30 seconds. Do not perform other operations while that is taking place.

IPv4 Enabled Disabled

DHCP Server Enabled Disabled

Method: Use static IP address

IPv4 address: 192.168.70.254

Network mask: 255.255.255.0

Default gateway: 0.0.0.0

IPv6 Enabled Disabled

DHCP Server Enabled Disabled

Method: Obtain IP from DHCP

networkIPv6Address:

Prefix length: 0

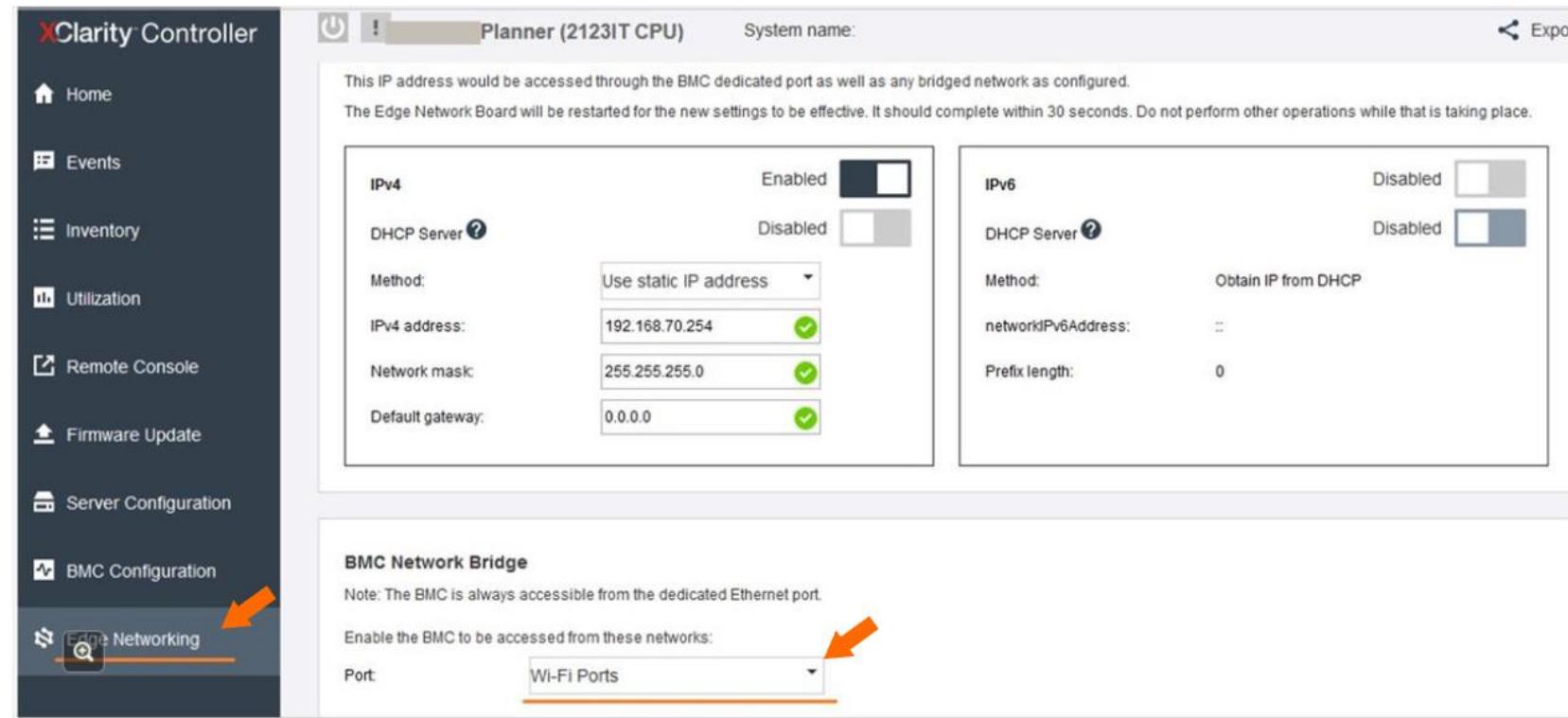
BMC Network Bridge
Note: The BMC is always accessible from the dedicated Ethernet port

Step



BMC network bridge configuration – example

- Set up the BMC network bridge configuration.
- From the XCC Web GUI, select **Edge Networking** → **BMC Network Bride**.
 - **Port: Wi-Fi Ports**



The screenshot shows the XClarity Controller (XCC) Web GUI interface. The left sidebar menu includes: Home, Events, Inventory, Utilization, Remote Console, Firmware Update, Server Configuration, BMC Configuration, and Edge Networking (which is highlighted with an orange arrow). The main content area is titled 'Planner (2123IT CPU)' and shows the following configuration:

IPv4

- Enabled:
- Disabled:
- DHCP Server:
- Method: Use static IP address
- IPv4 address: 192.168.70.254
- Network mask: 255.255.255.0
- Default gateway: 0.0.0.0

IPv6

- Enabled:
- Disabled:
- DHCP Server:
- Method: Obtain IP from DHCP
- networkPv6Address: ::
- Prefix length: 0

BMC Network Bridge

Note: The BMC is always accessible from the dedicated Ethernet port.

Enable the BMC to be accessed from these networks:

Port:

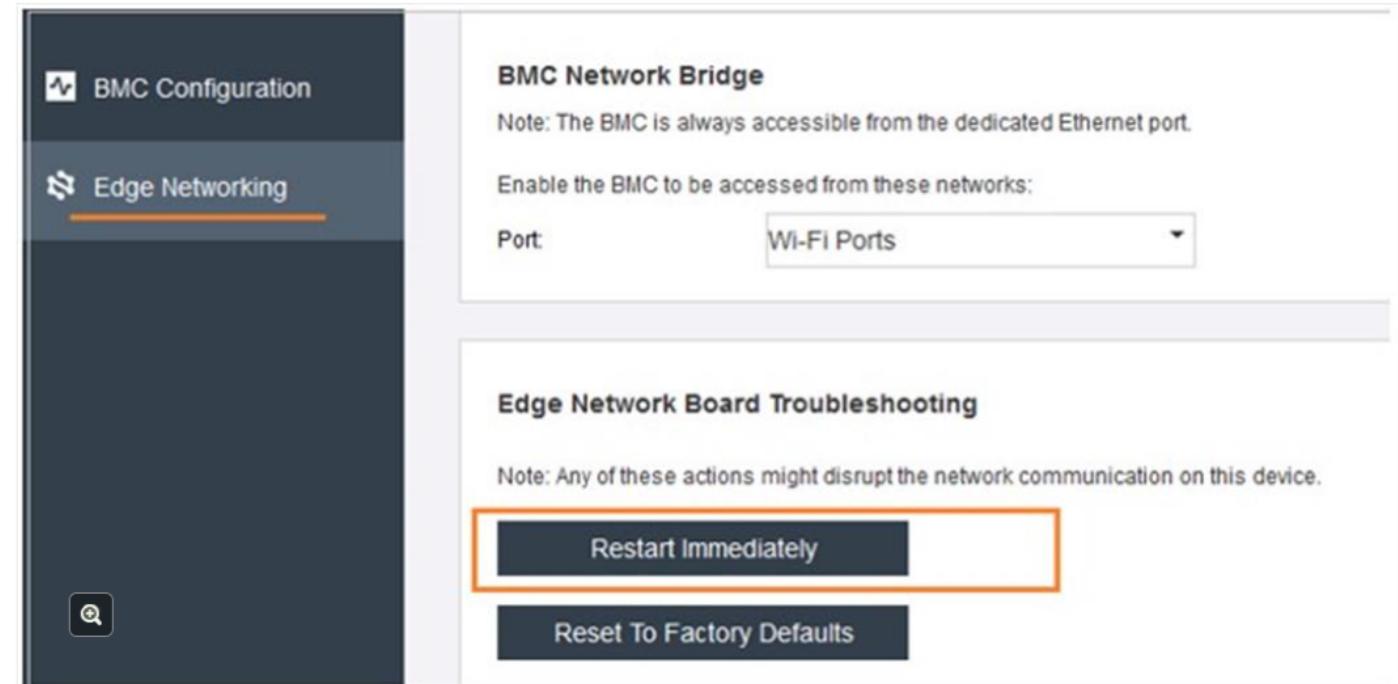
Step



BMC network bridge configuration – example

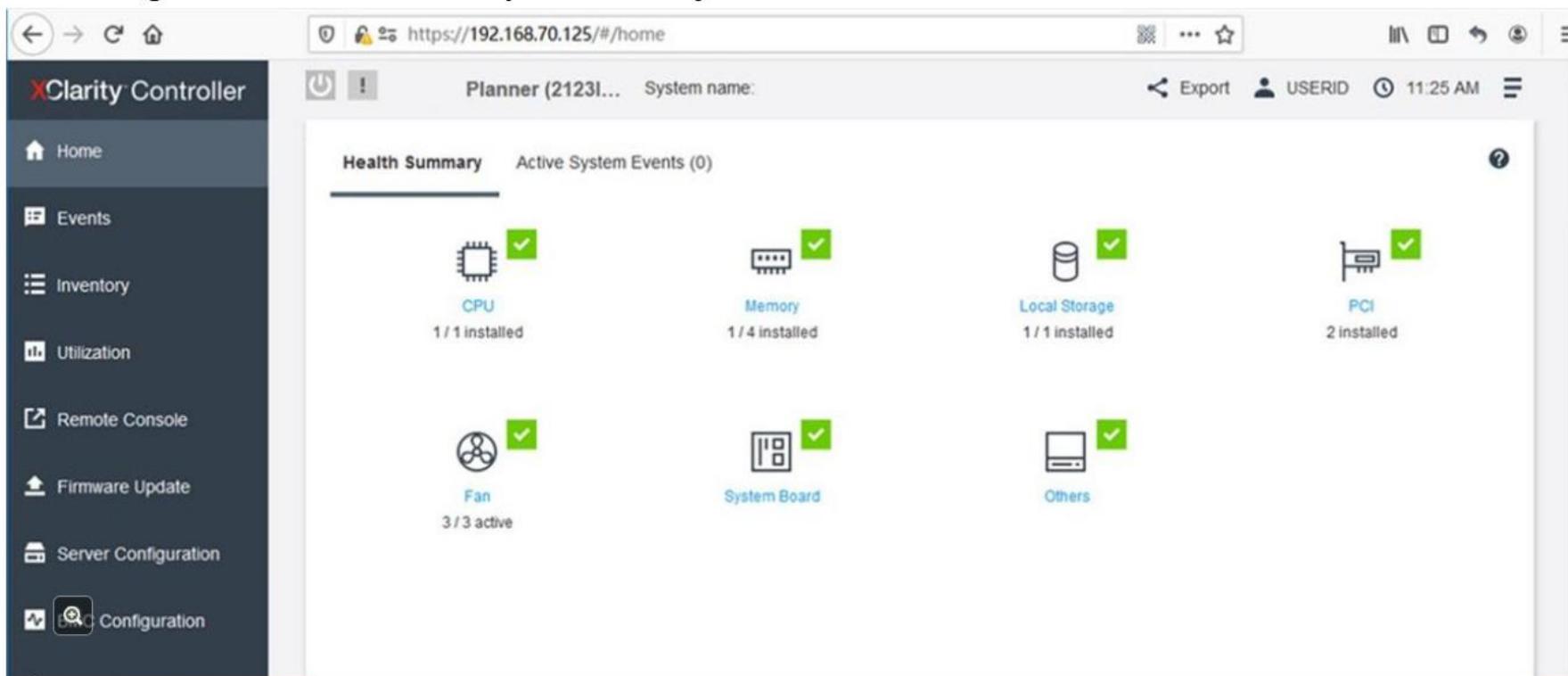
Activate the new settings.

- From the XCC Web GUI, select **Edge Networking** → **Edge Network** **Board Troubleshooting** → **Restart Immediately**
- Wait for one to two minutes and then connect to the SE350's Wi-Fi access point. The SSID should have the name entered during step 3.



BMC network bridge configuration – example

Using the PC or laptop connected to the SE350 Wi-Fi access point, open the XCC Web page in a Web browser with the correct XCC IP address. (In this example, it's 192.168.70.125.) The XCC home page will open if the configuration was set up correctly.



Step



Edge network board troubleshooting

Users can restart or reset the Edge network board when an error occurs.

Edge Network Board Troubleshooting

Note: Any of these actions might disrupt the network communication on this device.

Restart Immediately

Reset To Factory Defaults

Note: For more information about the edge network setting on the ThinkSystem SE350 edge server, refer to the **WLAN client Configuration** section on the [Lenovo Info Center](#).