CCG-1500 Series User Manual

Version 1.3, April 2026

www.moxa.com/products

CCG-1500 Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

Overview

The CCG-1500 Series is designed for media and protocol conversion, including 5G-to-Ethernet and 5G-to-serial and is suitable for private networks. The CCG-1500 Series acts as a protocol converter for Modbus TCP/RTU communications and supports 5G-based wireless communications. Equipped with a Cortex-A7 processor built for media conversion, the CCG-1500 Series is suitable for a wide range of industrial applications. The wide-temperature design also makes the CCG-1500 Series ideal for applications in harsh environments.

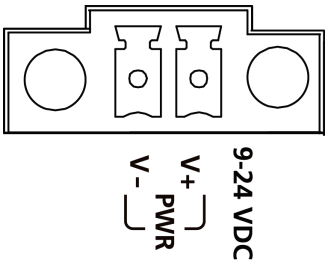
LED Indicator Overview

The LED indicators are located on the front panel of the CCG-1500. The behavior of each LED is described in the following table below.

LED	Color	Behavior	Description
Signal Strength (Strong)	Green	On	Indicates a strong 4G/5G signal.
Signal Strength (Medium)	Green	On	Indicates a medium 4G/5G signal.
Signal Strength (Weak)	Green	On	Indicates a weak 4G/5G signal.
P/S (Power/System Status)	Red	On	The system is booting up or is not ready yet.
	Green	On	The system is powered on and ready.
	Off	Off	The system is powered off.
SIM 1/2	Amber	On	A SIM card is inserted in slot 1.
	Green	On	A SIM card is inserted in slot 2.
	Off	Off	No SIM card is inserted.
4G/5G	Amber	On	A cellular connection is established to a 4G network.
	Green	On	A cellular connection is established to a 5G network.
	Off	Off	No cellular network signal.
LAN1, LAN 2	Green	On	The port is active, and a link is established at 1000 Mbps.
	Green	Blinking	Data is being transmitted at 1000 Mbps.
	Amber	On	The port is active, and a link is established at 10/100 Mbps.
	Amber	Blinking	Data is being transmitted at 10/100 Mbps.
	Off	Off	The port is inactive, or the link is down.

Connecting the Power

The CCG Series device is powered by connecting a power source to the terminal block. Refer to the power terminal block pin assignments below:



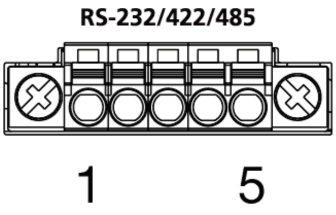
1. Loosen or remove the screws on the terminal block.
2. Turn off the power source and then connect a 9–24 VDC power line to the terminal block.
3. Tighten the connections, using the screws on the terminal block.
4. Turn on the power source.

NOTE

The unit does not have an on/off switch. The device will automatically turn on when it receives power. When the system is ready, the SYS LED will light up green.

Connecting the Serial Devices

The CCG-1500 Series supports connections to Modbus serial devices through the DB9 male serial port. The serials port can be configured for the RS-232, RS-422, or RS-485 mode using serial software. Refer to the serial port pin assignment below:



Pin	Definition
1	RS-232TXD/RS-422T+/RS-485T+
2	RS-232RXD/RS-422T-/RS-485T-
3	RS-232RTS/RS-422R+/RS-485R+
4	RS-232CTS/RS-422R-/RS-485R-
5	GND

Connecting to a Network

Connect one end of an Ethernet cable to one of the CCG-1500 Series device's 10/100/1000 Mbps Ethernet ports. Connect the other end of the cable to your Ethernet network. If a connection is established, the corresponding LAN LED will turn solid green.

Accessing the Web Interface

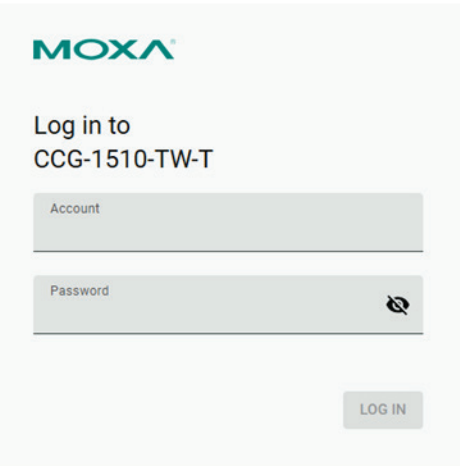
NOTE

Make sure the host and the CCG device are on the same subnet. The CCG device's default subnet is **255.255.255.0**.

1. Connect the CCG device's LAN1 or LAN2 port to your network.
2. Open a web browser and enter the CCG device's IP address into the address bar.
   The default IP address is **https://192.168.225.1:443.**
3. Log in using your user account and password. If this is the first time logging in, use the default login credentials.

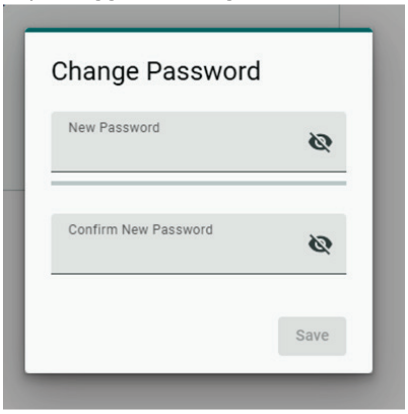
   Account: **admin**

   Password: **moxa**

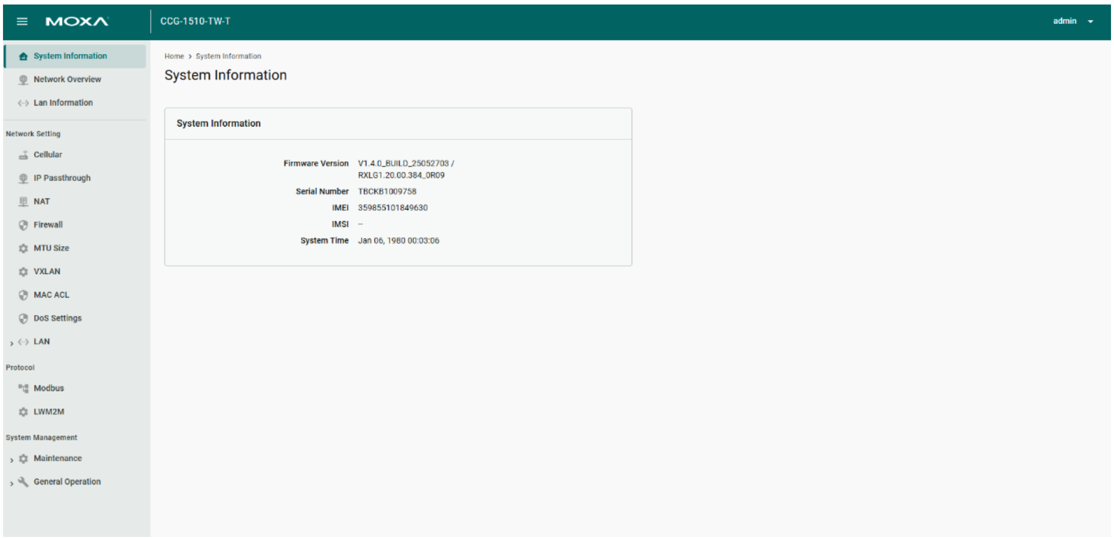
   

4. Click **LOG IN**.

5. If you logged in using the default credentials, the password change window will appear.



6. Enter your new password and click **Save**. You will be redirected to the login page. Log in using your new password.
7. When logged in, the System Information screen will appear by default.



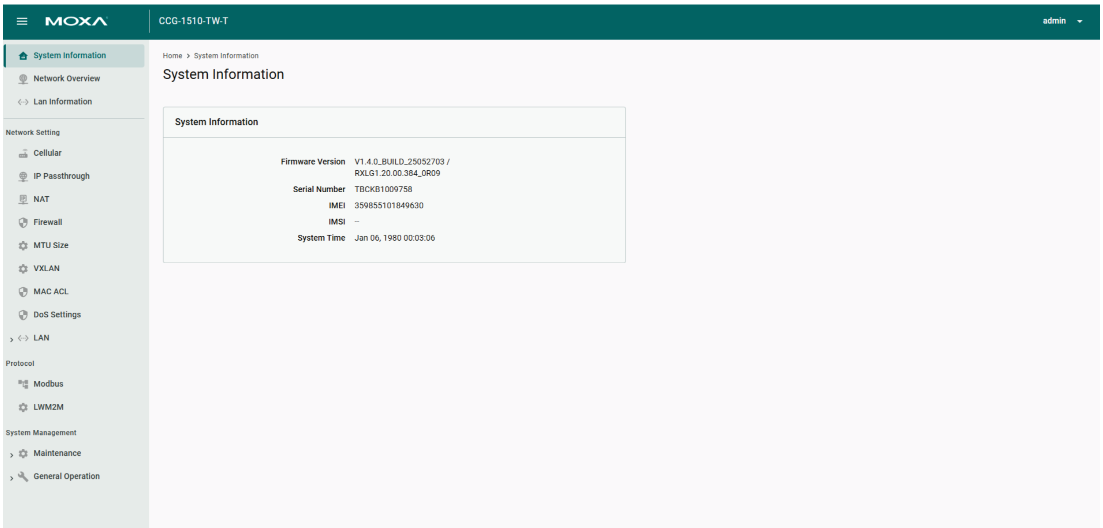
3. Web Interface

Overview

System Information

Menu path: System Information

The **System Information** page shows basic details about the device, including the firmware version and serial number. From this screen, you can also check the device's physical location and GPS coordinates.



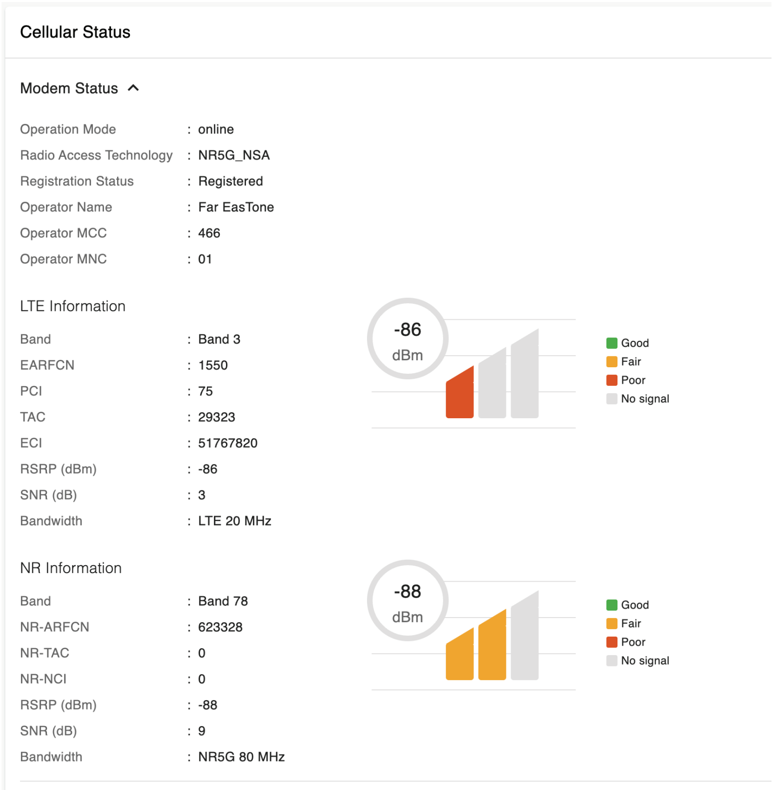
Network Overview

Menu path: Network Overview

The **Network Overview** dashboard displays information about the device's cellular status (if a SIM card is inserted), WWAN statistics, WWAN IP configuration, and SIM card status. Refer to the following segments for more details about each section.

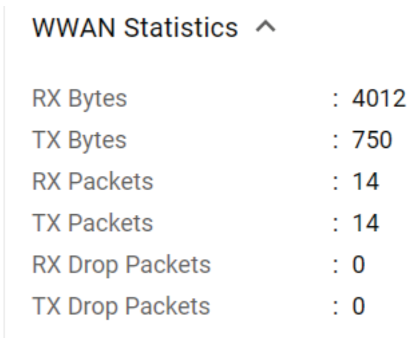
Cellular Status

The **Cellular Status** section displays the current modem status, LTE and NR information, and cellular signal strength. A SIM card must be installed to view this information.



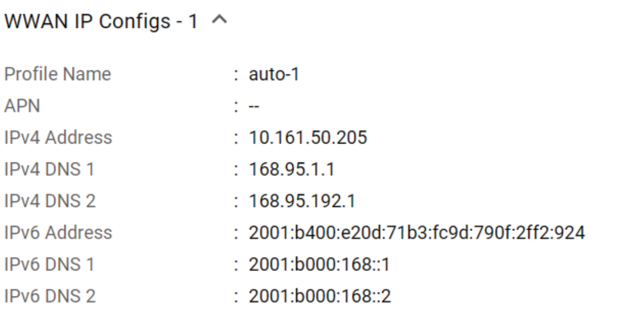
WWAN Statistics

The **WWAN Statistics** section displays information about the data sent and received through the WAN interface. The WWAN information automatically refreshes every 10 seconds.



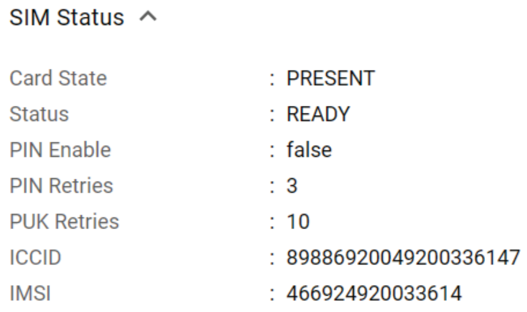
WWAN IP Configs-1

The **WWAN IP Config** section displays WWAN IP configuration details, including the IPv4/v6 address and IPv4/v6 DNS server name.



SIM Status

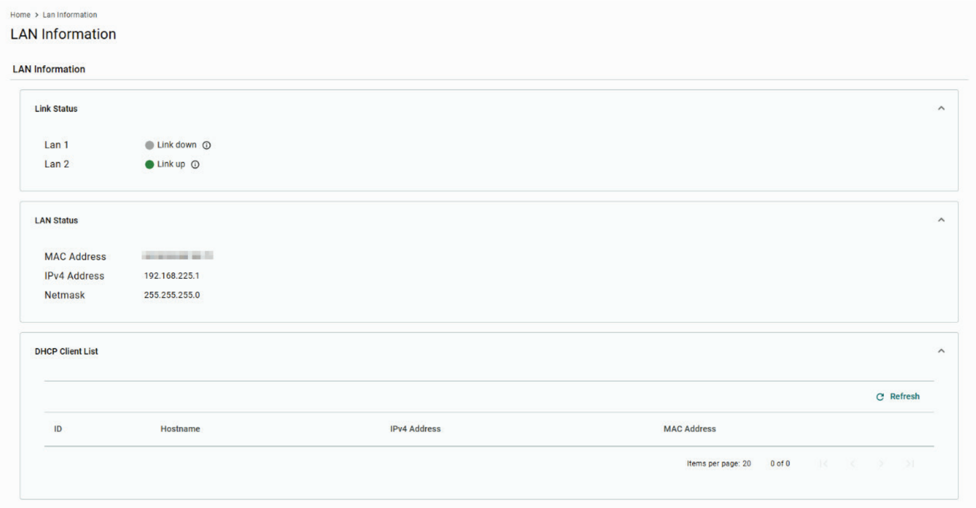
The **SIM Status** section displays information about the installed SIM card including the PIN code, ICCID, and IMS.



LAN Information

Menu path: LAN Information

The **LAN Information** page is used to view the link status, LAN status, and the DHCP Client list.

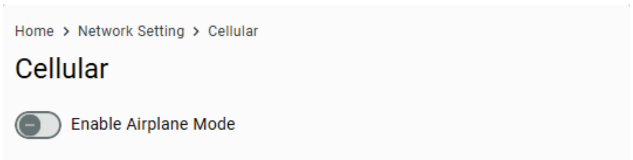


Network Settings

Cellular

Menu path: Cellular

The **Cellular** page is used to configure cellular connection health, profiles, bands, and SIM settings.



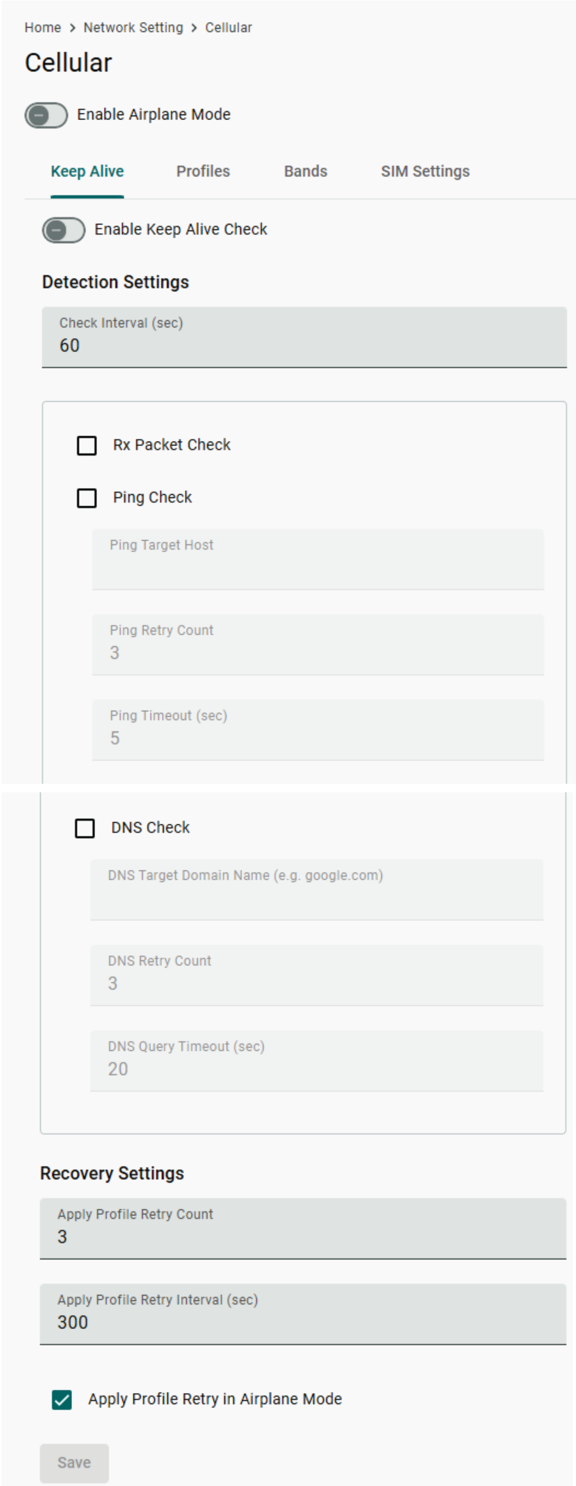
Enable Airplane Mode

Setting	Description	Factory Default
Toggle	Enable or disable Airplane Mode. If enabled, cellular functionality will be disabled.	Off

Keep Alive

Menu path: Cellular > Keep Alive

The CCG-1500 Series device supports Keep Alive checks to monitor the health of the cellular connection and cellular connection recovery functionality.



Enable Keep Alive Check

Setting	Description	Factory Default
Toggle	Enable or disable Keep Alive packets to monitor the health of the cellular connection.	Off

Check Interval

Setting	Description	Factory Default
1 to 3600	Specify the interval (in seconds) at which Keep Alive packets are sent.	60

Rx Packet Check

Setting	Description	Factory Default
Checkbox	Enable or disable Rx packets. If enabled, the system will check for incoming Keep Alive packets as a means to monitor connection health. This function is useful for scenarios where the network does not permit devices to send out ping packets.	Unchecked

Ping Check

Setting	Description	Factory Default
Checkbox	Enable or disable ping checks. If enabled, the system will ping the specified host to determine the health of the connection.	Unchecked

Ping Target Host

Setting	Description	Factory Default
Domain Name or IP Address	Specify the domain name or IP address of the host to ping.	N/A

Ping Retry Count

Setting	Description	Factory Default
1 to 10	Specify the number of times the system will attempt to ping an unresponsive host.	3

Ping Timeout (sec)

Setting	Description	Factory Default
1 to 300	Specify the duration (in seconds) before the host is considered unresponsive.	5

DNS Check

Setting	Description	Factory Default
Checkbox	Enable or disable DNS checks. If enabled, the system will ping the specified DNS server to determine the health of the connection.	Unchecked

DNS Target

Setting	Description	Factory Default
Domain Name	Specify the domain name of the DNS server.	N/A

DNS Retry Count

Setting	Description	Factory Default
1 to 5	Specify the number of times the system will attempt to ping an unresponsive DNS server.	3

DNS Query Timeout (sec)

Setting	Description	Factory Default
1 to 300	Specify the duration (in seconds) before the DNS server is considered unresponsive.	20

Apply Profile Retry Count

Setting	Description	Factory Default
1 to 10	Specify the number of times the system will attempt to apply the assigned cellular profile.	3

Apply Profile Retry Interval (sec)

Setting	Description	Factory Default
0 to 3600	Specify the duration (in seconds) for the system to consider the attempt failed before trying to apply the assigned cellular profile again.	300

Apply Profile Retry in Airplane Mode

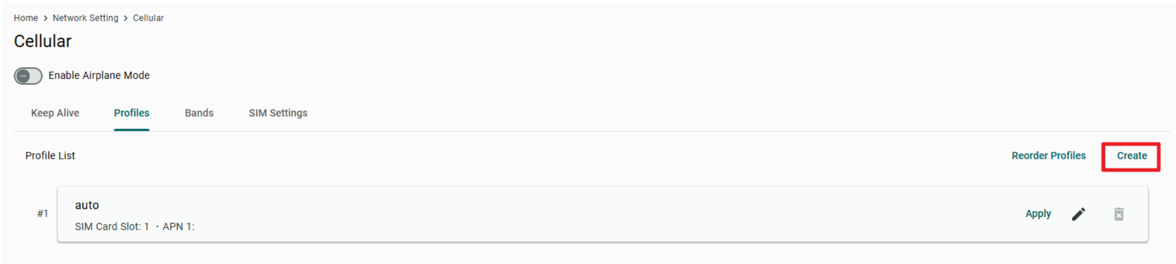
Setting	Description	Factory Default
Checkbox	Enable or disable profile retries if Airplane Mode is enabled. For more information about cellular profiles, refer to the Profiles section.	Checked

When finished, click **Save**.

Profiles

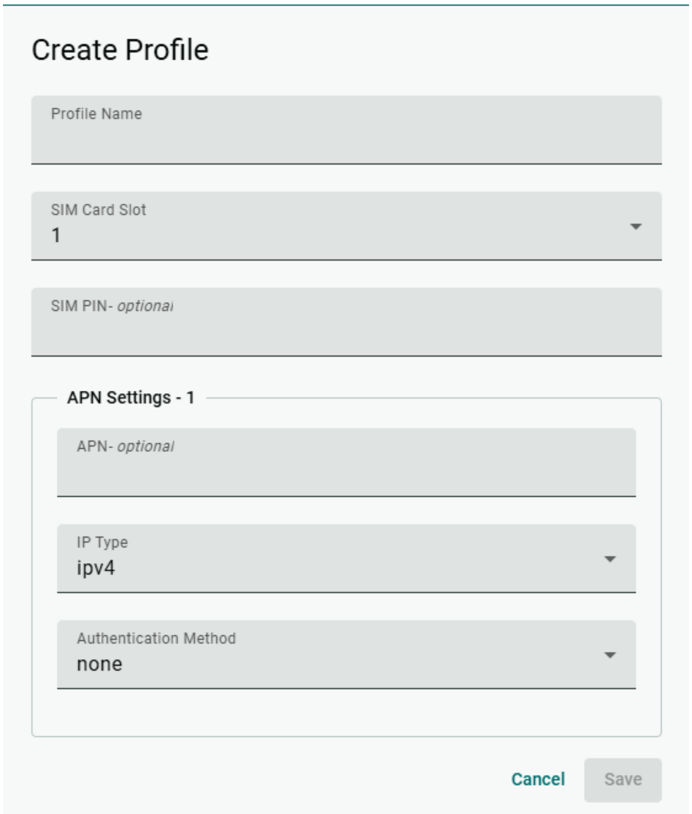
Menu path: Cellular > Profiles

From the **Profiles** screen, you can create multiple customized cellular profiles with specific configuration settings. The CCG device will always deploy the cellular settings of the profile with the highest priority.



Adding a Profile

To create a new profile, click **Create** in the Profile List.



Profile Name

Setting	Description	Factory Default
Name	Enter a name for the profile	N/A

SIM Slot

Setting	Description	Factory Default
1 or 2	Select the SIM slot of the profile.	1

SIM PIN - optional

Setting	Description	Factory Default
PIN number	If the inserted SIM card has a PIN code configured, specify the PIN code.	N/A

APN

Setting	Description	Factory Default
APN	Specify the Access Point Name (APN), if available.	N/A

IP Type

Setting	Description	Factory Default
IPv4, IPv6, IPv4v6	Select the IP type.	IPv4

Authentication Method

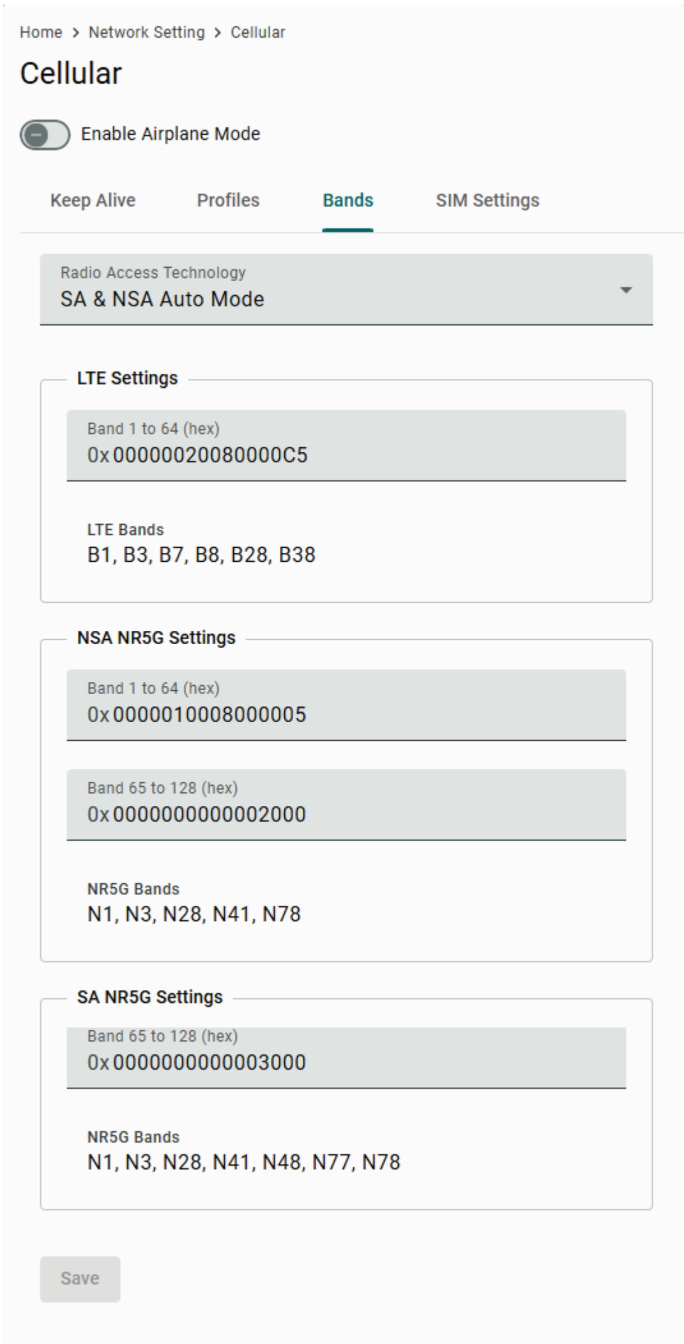
Setting	Description	Factory Default
None, PAP, CHAP, PAP-CHAP	Select the authentication mechanism.	None

When finished, click **Save**.

Bands

Menu path: Cellular > Bands

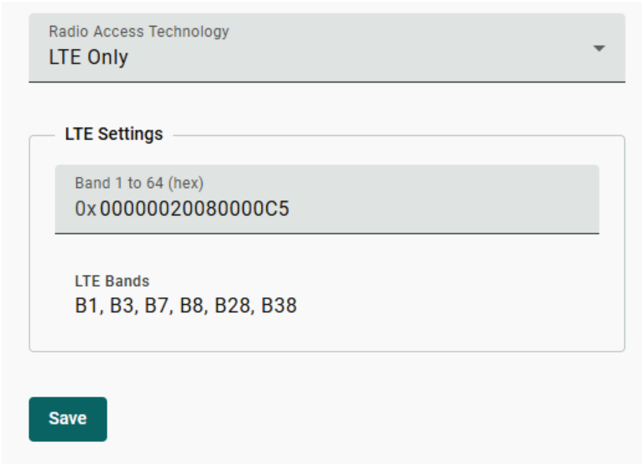
From the **Bands** screen, you can configure specific bands for different radio technologies.



Radio Access Technology

Setting	Description	Factory Default
LTE Only, NSA NR5G, SA NR5G, SA & NSA Auto Mode	Select the radio access technology (RAT) from the list. Available settings depend on the selected type. Refer to the following sections for more information: LTE Only NSA NR5G SA NR5G SA & NSA Auto Mode	SA & NSA Auto Mode

LTE Only



Band 1 to 64 (hex)

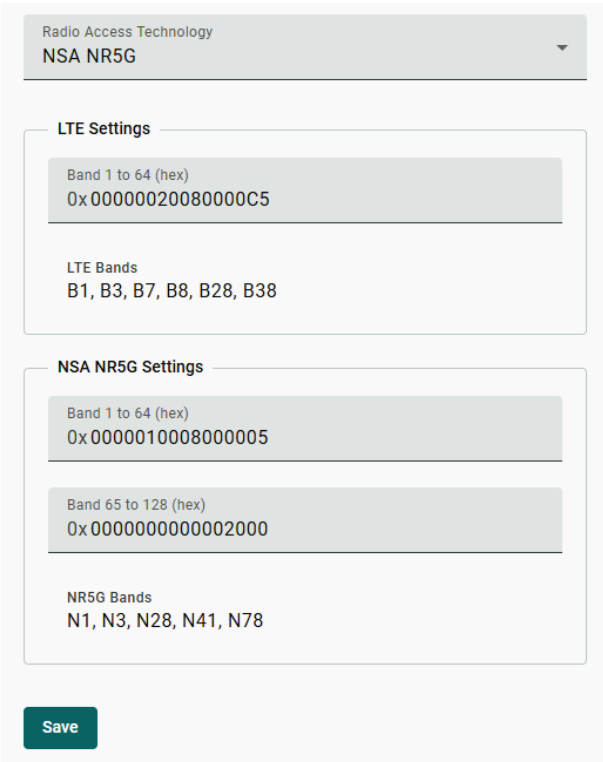
Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

LTE Bands

Setting	Description	Factory Default
Read Only	This shows the supported LTE bands.	N/A

When finished, click **Save**.

NSA NR5G



Band 1 to 64 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

Band 65 to 128 (hex)

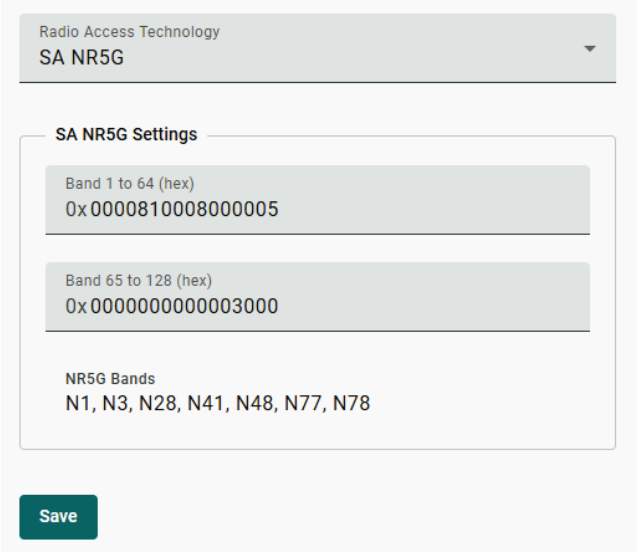
Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

NR5G Bands

Setting	Description	Factory Default
Read Only	This shows the supported NSA NR5G bands.	N/A

When finished, click **Save**.

SA NR5G



Band 1 to 64 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

Band 65 to 128 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

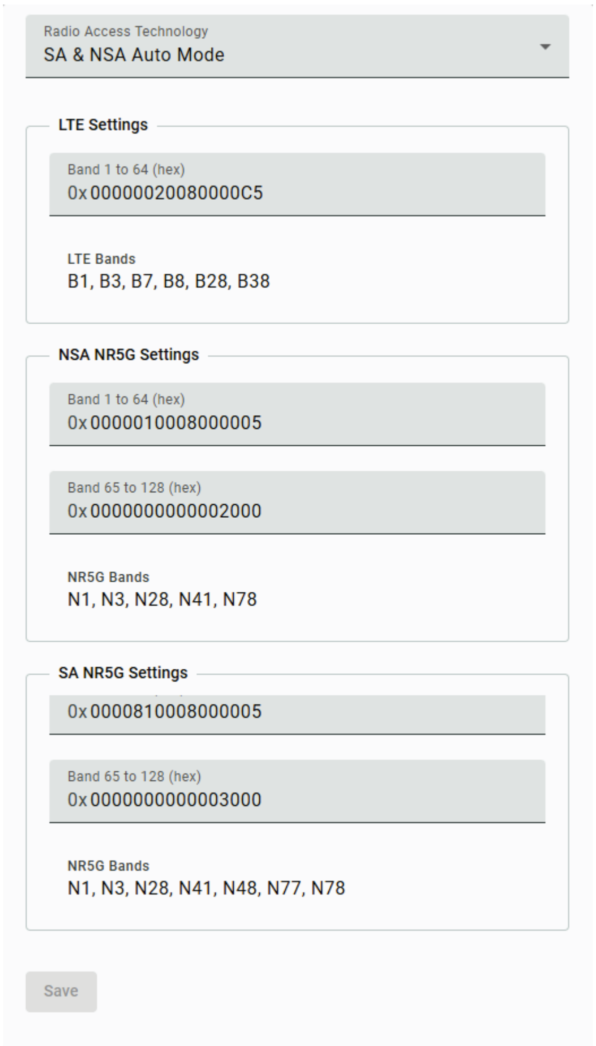
NR5G Bands

Setting	Description	Factory Default
Read Only	This shows the supported SA NR5G bands.	N/A

When finished, click **Save**.

SA & NSA Auto Mode

In SA & NSA Auto mode, the system will automatically switch between SA and NSA NR5G mode.



NSA NR5G Settings

Band 1 to 64 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

Band 65 to 128 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

NR5G Bands

Setting	Description	Factory Default
Read Only	This shows the supported NSA NR5G bands.	N/A

SA NR5G Settings

Band 1 to 64 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

Band 65 to 128 (hex)

Setting	Description	Factory Default
Hex Number	Specify the cellular band number in hex format.	N/A

NR5G Bands

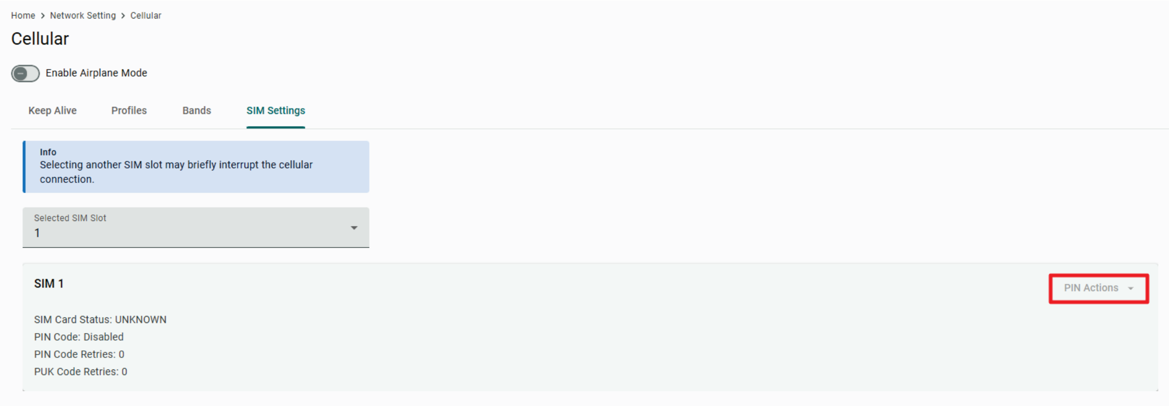
Setting	Description	Factory Default
Read Only	This shows the supported SA NR5G bands.	N/A

When finished, click **Save**.

SIM Settings

Menu path: Cellular > SIM Settings

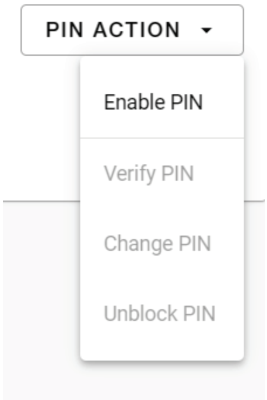
From the SIM Settings screen, you can select the active SIM slot and perform basic SIM card actions.



Selected SIM Slot

Setting	Description	Factory Default
1 or 2	Select the active slot. If changed, the cellular connection will be temporarily uninterrupted.	1

From the **PIN Actions** menu, you can perform the following actions:



PIN ACTION

Action	Description
Enable PIN	Enable or disable SIM card PIN code verification. If enabled, users will be required to enter the PIN code to unlock and use the SIM card. Every time the device is rebooted, users will be required to re-enter the PIN code using the Verify PIN function. If disabled, the SIM card will be unlocked without the need to enter a PIN code.
Verify PIN	If PIN code verification is enabled, enter the PIN code to verify and unlock the SIM card.
Change PIN	Change the current PIN code.
Unblock PIN	If the PIN code of the SIM card was entered incorrectly multiple times in a row, the SIM card will be blocked. Use the unblock PIN function to unblock the SIM card.

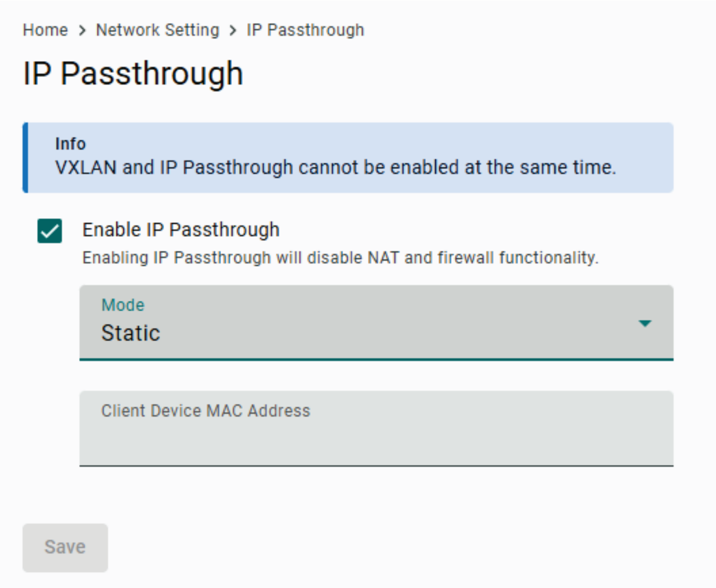
IP Passthrough

Menu path: IP Passthrough

The **IP Passthrough** page is used to enable or disable the IP Passthrough function.

WARNING

Enabling IP Passthrough will disable all NAT and firewall settings, and may impact DoS protection.



Enable IP Passthrough

Setting	Description	Factory Default
Checkbox	Enable or disable the IP Passthrough function.	Unchecked

If enabled, also configure the following settings:

Mode

Setting	Description	Factory Default
Static	Manually specify the MAC address of the client device for IP Passthrough.	Static
Dynamic (LAN 1)	The MAC address is automatically configured based on the client device connected to the LAN 1 port.	
Dynamic (LAN 2)	The MAC address is automatically configured based on the client device connected to the LAN 2 port.	

Client Device MAC Address

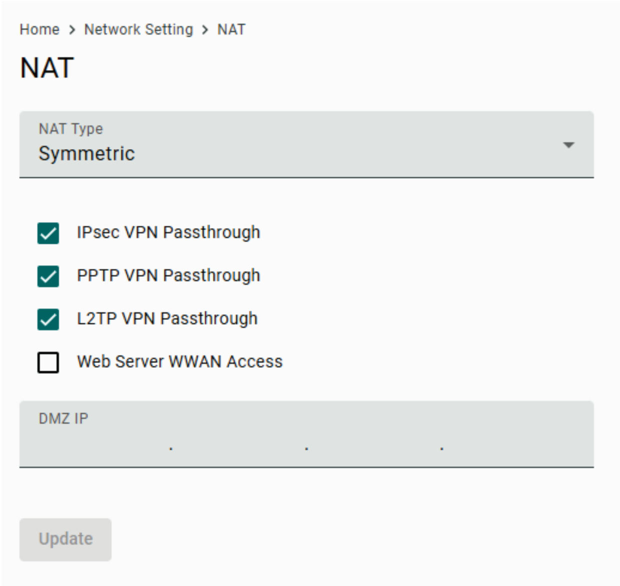
Setting	Description	Factory Default
MAC Address	If the Mode is set to Static, specify the client device MAC address. In Dynamic mode, this field is automatically configured and read-only.	N/A

When finished, click **Save**.

NAT Settings

Menu path: **NAT**

The **NAT** page is used to set the NAT mode and configure relevant NAT and port forwarding settings. Configurable settings depend on which NAT mode is selected.



NAT Type

Setting	Description	Factory Default
Symmetric	Set the NAT mode to Symmetric.	Symmetric
Port Restricted Cone	Set the NAT mode to Port Restricted Cone.	
Full Cone	Set the NAT mode to Full Cone.	
Access Restricted	Set the NAT mode to Access Restricted.	

IPSEC VPN Pass-Through

Setting	Description	Factory Default
Checkbox	Enable or disable IPsec VPN passthrough functionality.	Checked

PPTP VPN Pass-Through

Setting	Description	Factory Default
Checkbox	Enable or disable PPTP VPN passthrough functionality.	Checked

L2TP VPN Pass-Through

Setting	Description	Factory Default
Checkbox	Enable or disable L2TP VPN passthrough functionality.	Checked

Webserver WWAN Access

Setting	Description	Factory Default
Checkbox	Enable or disable Webserver WWAN Access functionality. If enabled, the web interface can be accessed via the WWAN interface.	Unchecked

DMZ IP

Setting	Description	Factory Default
IP Address	Specify the NAT DMZ IP address.	N/A

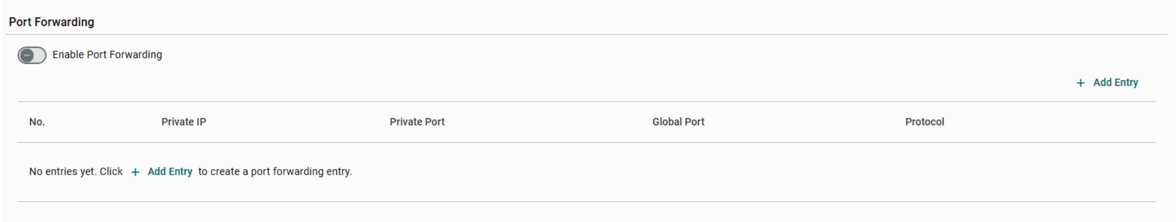
When finished, click **Update**.

Port Forwarding

Menu path: NAT

The **Port Forwarding** section on the NAT page is used to enable or disable the port forwarding function and to manage port forwarding rules.

> **WARNING**
>
> Enabling Port Forwarding may impact DoS protection.

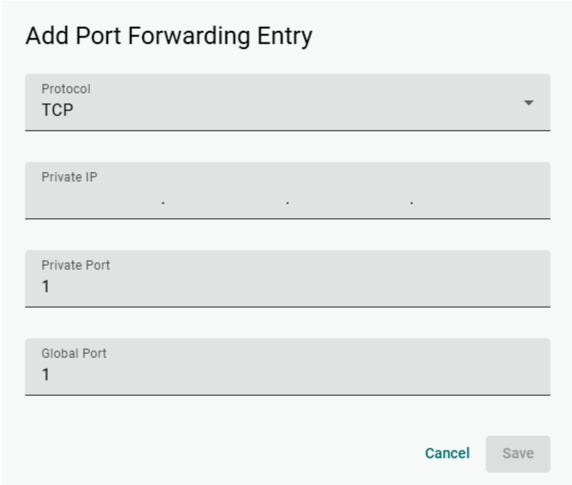


Enable Port Forwarding

Setting	Description	Factory Default
Toggle	Use the toggle button to enable or disable the port forwarding function.	Disabled

Adding a Port Forwarding Entry

In the Port Forwarding section, click **+ Add Entry** to create a port forwarding entry.



Protocol

Setting	Description	Factory Default
ICMP, TCP, UDP, TCP & UDP	Select the port forwarding protocol.	TCP

Private IP

Setting	Description	Factory Default
IP Address	Specify the private IP address.	N/A

Private Port

Setting	Description	Factory Default
1 to 65535	Specify the private port number.	1

Global Port

Setting	Description	Factory Default
1 to 65535	Specify the global port number.	1

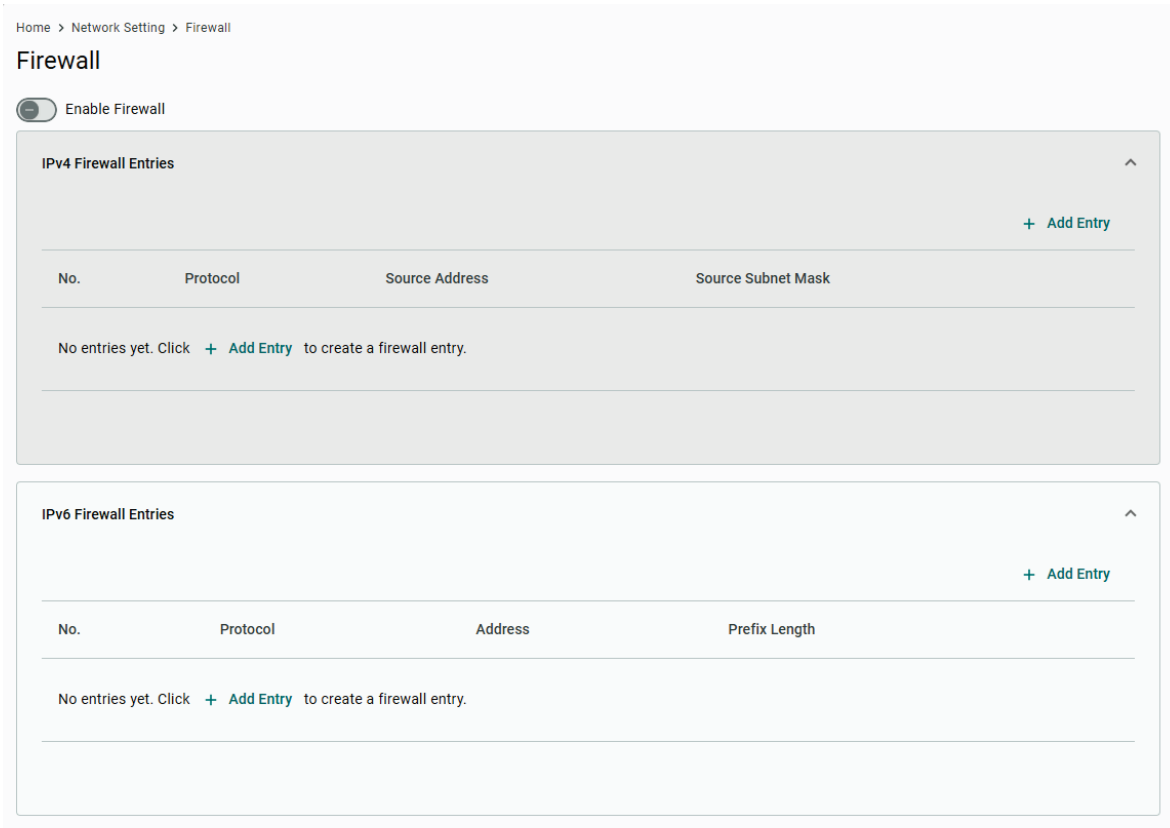
When finished, click **Save**.

Firewall Settings

Menu path: Firewall

The **Firewall** page is used to enable or disable the IPv4 firewall function and to manage IPv4 and IPv6 firewall rules. The firewall will drop any packets that match the configured policy rules.

> **NOTE**
>
> To enhance network security, it is recommended to enable firewall functionality.

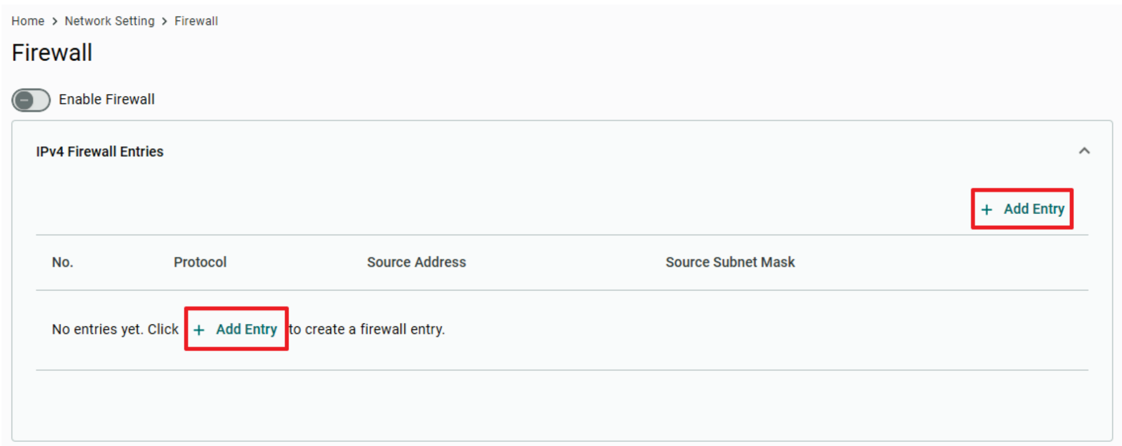


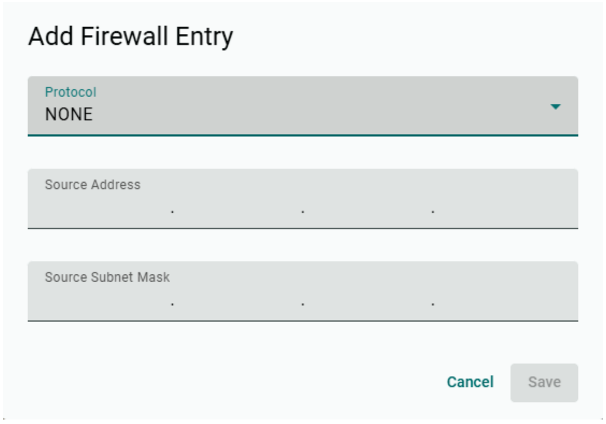
Enable Firewall

Setting	Description	Factory Default
Toggle	Use the toggle button to enable or disable the firewall function.	Disabled

Adding an IPv4 Firewall Entry

In the IPv4 Firewall Entries section on the Firewall Settings screen, click **+ Add Entry** to create a new IPv4 firewall entry.





Protocol

Setting	Description	Factory Default
None, ICMP, TCP, UDP, TCP & UDP	Select the protocol for the firewall rule.	None

Source Address

Setting	Description	Factory Default
IP Address	Specify the source IP address.	N/A

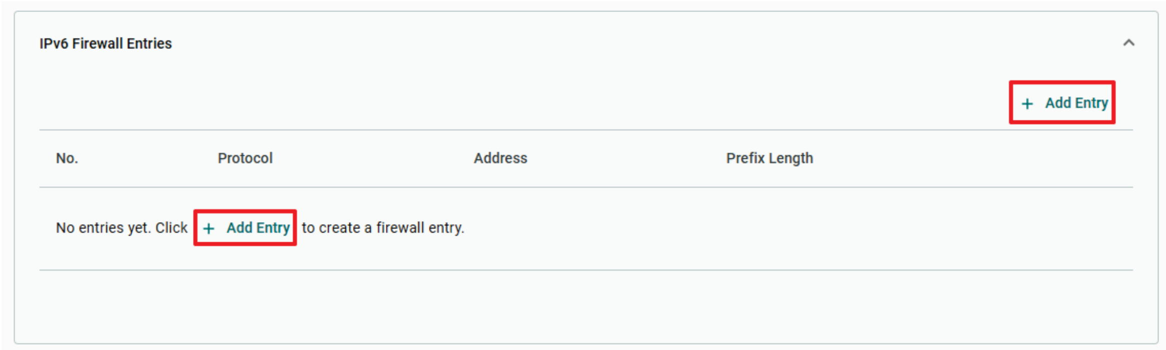
Source Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the source subnet mask.	N/A

When finished, click **Save**.

Adding an IPv6 Firewall Entry

In the IPv6 Firewall Entries section on the Firewall Settings screen, click **+ Add Entry** to create a new IPv6 firewall entry.



Protocol

Setting	Description	Factory Default
None, ICMP6, TCP, UDP, TCP & UDP	Select the protocol for the firewall rule.	None

Address

Setting	Description	Factory Default
IPv6 Address	Specify the IPv6 address.	N/A

Prefix Length

Setting	Description	Factory Default
IPv6 Prefix Length	Specify the prefix length for the IPv6 address.	0

When finished, click **Save**.

MTU Size

Menu path: MTU Size

The **MTU Size** page is used to configure the largest packet size that can be transmitted over the network.

Enable MTU Size

Setting	Description	Factory Default
Checkbox	Enable or disable MTU size settings.	Unchecked

MTU Size

Setting	Description	Factory Default
1200 to 1500	Specify the MTU size (in bytes).	1500

When finished, click **Apply**.

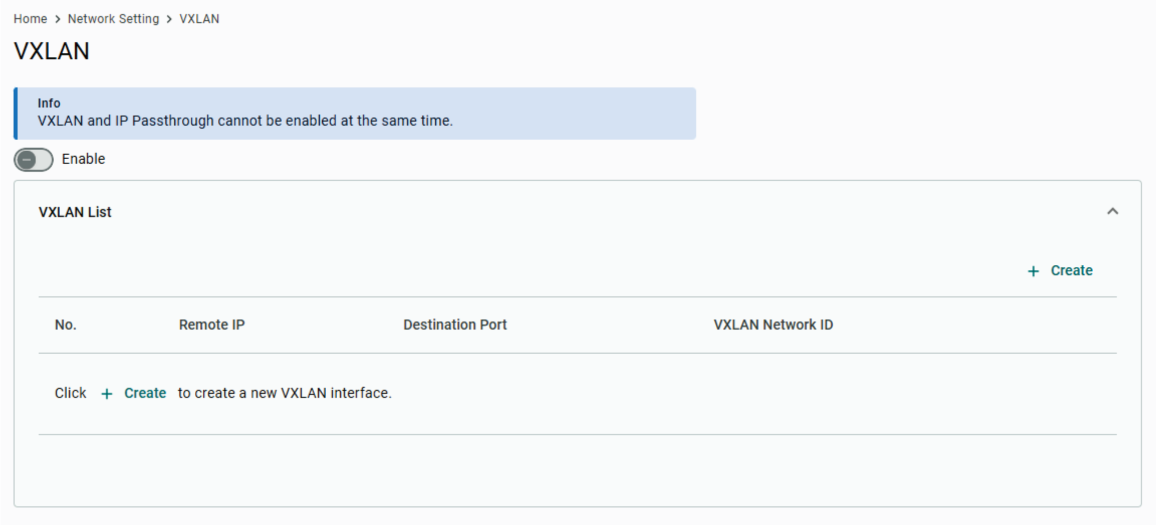
VXLAN

Menu path: VXLAN

The **VXLAN** page is used to configure the Virtual Extensible LAN (VXLAN) function that enables CCG-1500 Series gateway to push Layer 2 or Layer 3 packets through a VXLAN tunnel.

NOTE

To enhance network security, it is recommended to enable VXLAN in private network environments.

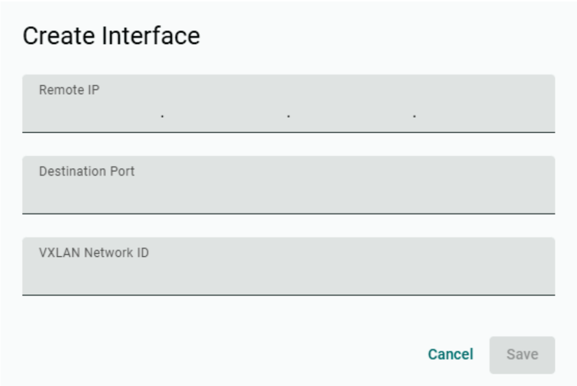


Enable

Setting	Description	Factory Default
Enable or Disable	Use the toggle to enable or disable VXLAN functionality.	Disabled

Adding a VXLAN

In the VXLAN List section on the VXLAN screen, click **+ Create** to create a new VXLAN.



Remote IP

Setting	Description	Factory Default
IP Address	Specify the remote IP of this VXLAN.	N/A

Destination Port

Setting	Description	Factory Default
1 to 65535	Specify the destination port of this VXLAN.	N/A

VXLAN Network ID

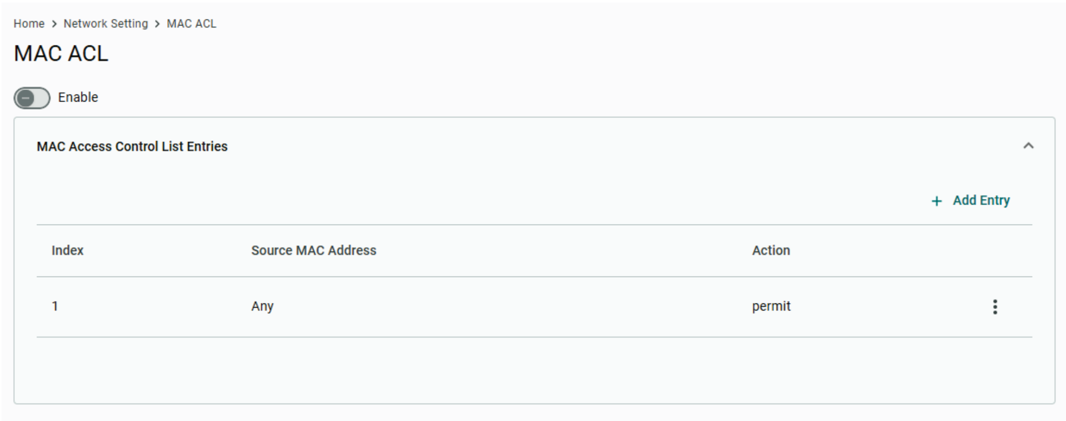
Setting	Description	Factory Default
0 to 16777215	Specify the network ID for this VXLAN.	N/A

When finished, click **Save**.

MAC ACL

Menu path: MAC ACL

The **MAC ACL** page is used to enable or disable the MAC-based Access Control List, which allows you to configure access to the device based on specific MAC addresses.

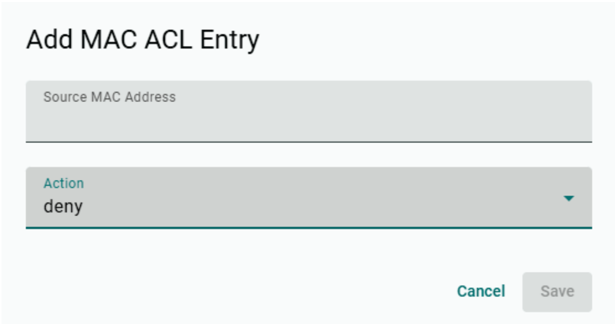


Enable

Setting	Description	Factory Default
Enable or Disable	Use the toggle to enable or disable MAC ACL functionality.	Disabled

Adding a MAC ACL Entry

In the MAC Access Control List Entries section on the MAC ACL screen, click **+ Add Entry** to create a new MAC ACL entry.



Source MAC Address

Setting	Description	Factory Default
MAC Address	Specify the source MAC address.	N/A

Action

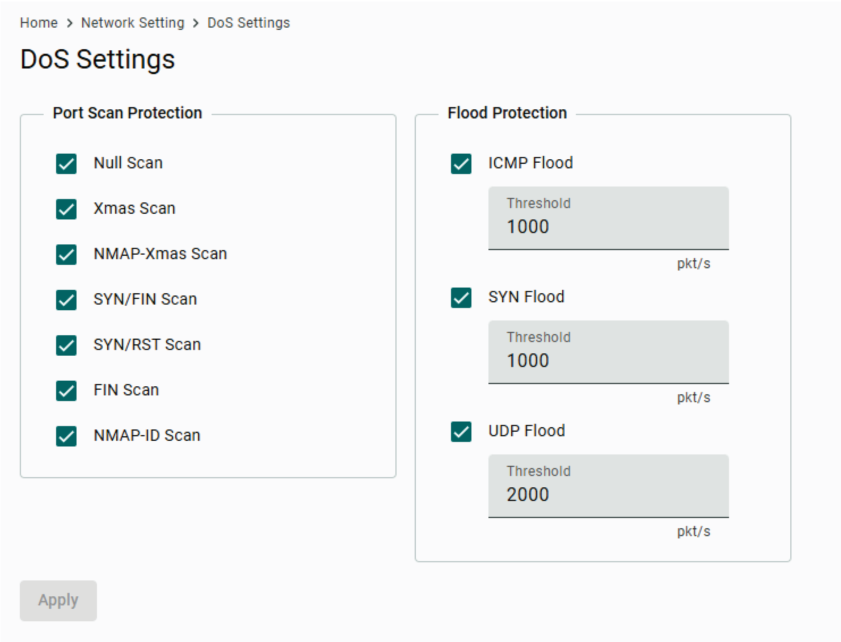
Setting	Description	Factory Default
Deny, Permit	Choose to deny or permit access to the device for the specified MAC address.	Deny

When finished, click **Save**.

DoS Settings

Menu path: DoS Settings

The **DoS Settings** page is used to configure Denial of Service (DoS) protection measures, divided into two main types: Port Scan Protection and Flood Protection.



Port Scan Protection

Setting	Description	Factory Default
Checkbox	Enable or disable the corresponding port scan protection measure.	Checked (all)

Flood Protection

Setting	Description	Factory Default
Checkbox	Enable or disable the corresponding flood protection measure.	Checkbox
Threshold	Specify the threshold (in pkt/s) to determine when the corresponding flood protection measure is triggered.	1000

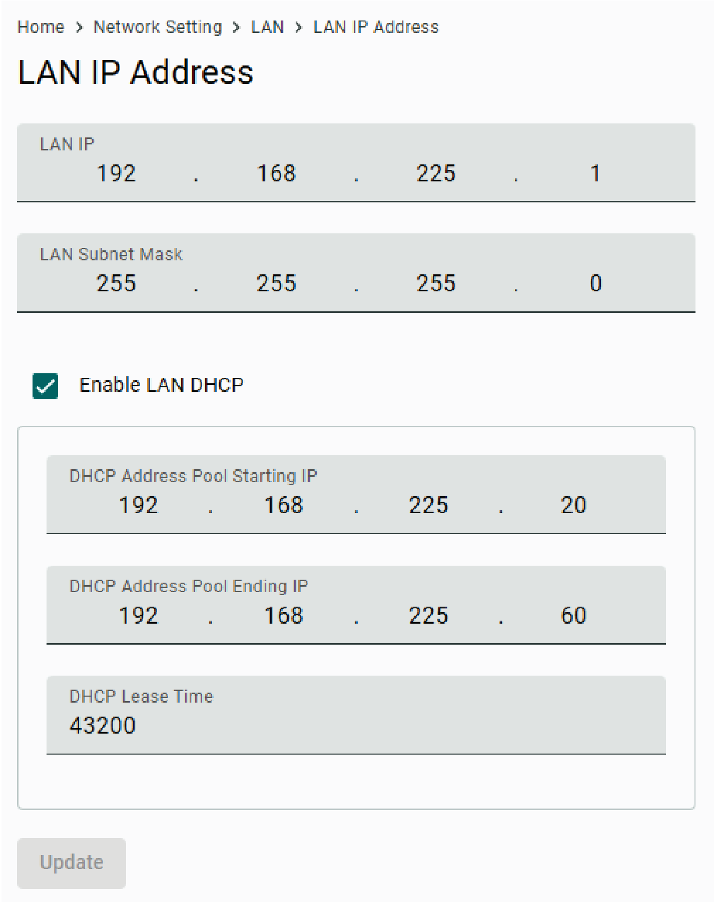
When finished, click **Apply**.

LAN Settings

IP Address

Menu path: LAN > IP Address

The **IP Address** page is used to configure the device's access IP address and specify the LAN DHCP IP pool range.



LAN IP

Setting	Description	Factory Default
IP Address	Specify the device's LAN IP address.	192.168.225.1:443

LAN Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the device's LAN subnet mask.	255.255.255.0

Enable LAN DHCP

Setting	Description	Factory Default
Checkbox	Enable or disable the LAN DHCP server.	Checked

LAN DHCP Start IP

Setting	Description	Factory Default
IP Address	Specify the starting IP address of the LAN DHCP IP address pool.	192.168.225.20

LAN DHCP End IP

Setting	Description	Factory Default
IP Address	Specify the ending IP address of the LAN DHCP IP address pool.	192.168.225.60

LAN DHCP Lease Time

Setting	Description	Factory Default
120 to 86400	Specify the IP address lease time (in seconds).	43200

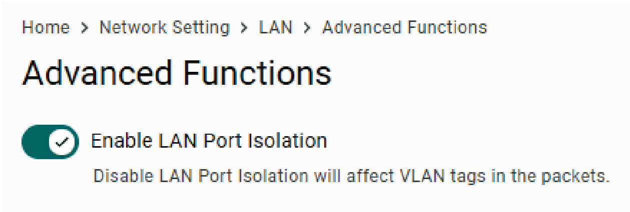
When finished, click **Update**.

> **NOTE**
>
> To enhance security and performance, DNS Proxy is enabled and set to the LAN IP by default. These settings cannot be modified. This design ensures that all devices connected to the LAN rely on a controlled, trusted DNS server for name resolution, mitigating risks such as DNS spoofing and man-in-the-middle attacks. Additionally, DNS Proxy uses caching to speed up domain name resolution, improving network efficiency.

Advanced Functions

Menu path: LAN > Advanced Functions

The **Advanced Functions** page is used to manage the device's advanced functions.



Enable LAN Port Isolation

Setting	Description	Factory Default
Toggle	Enable or disable the LAN port isolation function. Enabling this function will isolate devices connected to the CCG Series device's LAN ports from each other.	Enabled

Protocol Management

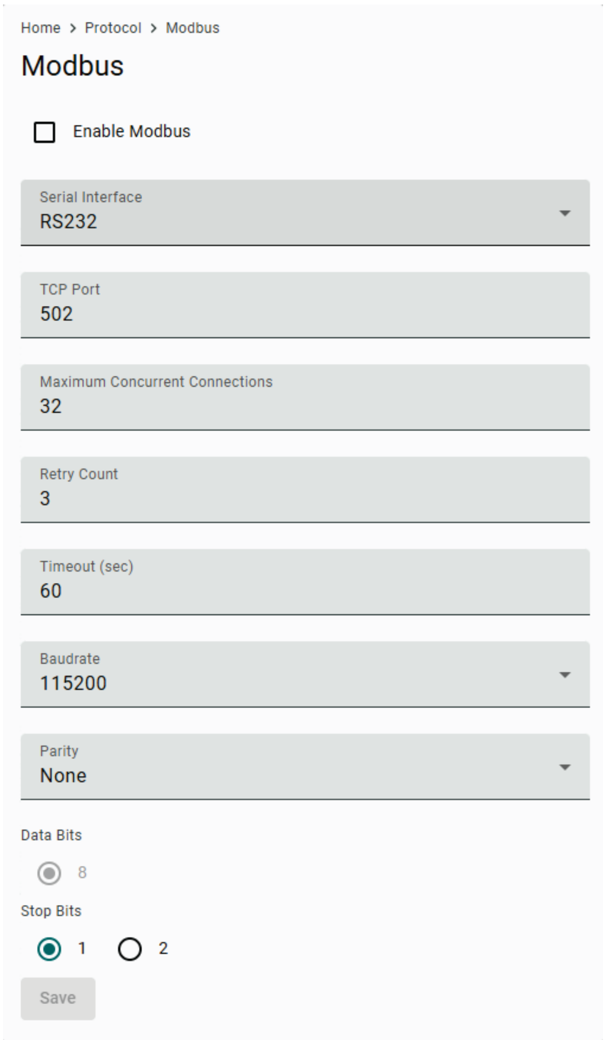
Modbus

Menu path: Modbus

The **Modbus** page is used to enable Modbus protocol support and configure relevant protocol settings.

NOTE

To enhance network security, it is recommended to enable Modbus in private network environments.



Enable

Setting	Description	Factory Default
Checkbox	Enable or disable Modbus protocol support.	Unchecked

Interface

Setting	Description	Factory Default
RS232, RS422, RS485	Select the interface used for Modbus communication.	RS232

TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the Modbus TCP port.	502

Maximum Connections

Setting	Description	Factory Default
1 to 32	Specify the maximum number of concurrent connections allowed.	32

Retry Count

Setting	Description	Factory Default
0 to 15	Specify the number of times the system will attempt to re-establish the Modbus connection.	3

Timeout (sec)

Setting	Description	Factory Default
0 to 1000	Specify the duration of inactivity (in seconds) after which the connection will time out.	60

Serial Baud Rate

Setting	Description	Factory Default
9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600	Specify the serial baudrate value.	115200

Parity

Setting	Description	Factory Default
None, Even, Odd	Select the parity mode.	None

Data Bits

Setting	Description	Factory Default
8	Select the number of data bits.	8

Stop Bits

Setting	Description	Factory Default
1, 2	Select the number of stop bits.	1

When finished, click **Save**.

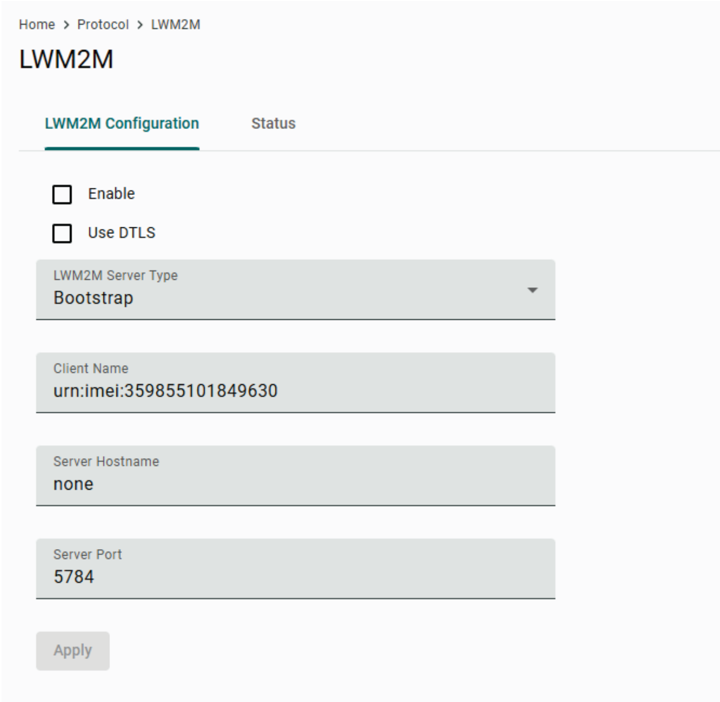
LWM2M

The CCG-1500 Series device supports Lightweight M2M (LWM2M) communication protocol by the Open Mobile Alliance, which enables links between devices equipped with a LWM2M agent and LWM2M-enabled servers.

LWM2M Configuration

Menu path: LWM2M > LWM2M Configuration

From the LWM2M Configuration page, you can enable LWM2M functionality and configure relevant connection parameters.



Enable

Setting	Description	Factory Default
Checkbox	Enable or disable LWM2M connections. If enabled, the system will connect to the specified LWM2M server.	Unchecked

Use DTLS

Setting	Description	Factory Default
Checkbox	Enable or disable Datagram Transport Layer Security (DTLS). The LWM2M client connects to the server using the CoAP protocol. For secure connections it uses DTLS with the Pre-Shared Key (PSK). If DTLS is enabled, you have to enter the PSK information manually.	Unchecked

NOTE

To enhance network security, it is recommended to enable DTLS when using LWM2M.

LWM2M Server Type

Setting	Description	Factory Default
Bootstrap, LWM2M	Select the server type. Bootstrap is recommended for deployments that require enhanced security and management of multiple LWM2M servers. LWM2M is suitable for single-server deployments with end-to-end authentication.	Bootstrap

Client Name

Setting	Description	Factory Default
Client Name	Enter a LWM2M client name for the CCG device.	IMEI

Server Hostname

Setting	Description	Factory Default
Server Hostname	Enter the LWM2M server hostname. This information is provided by the LWM2M server.	None

Server Port

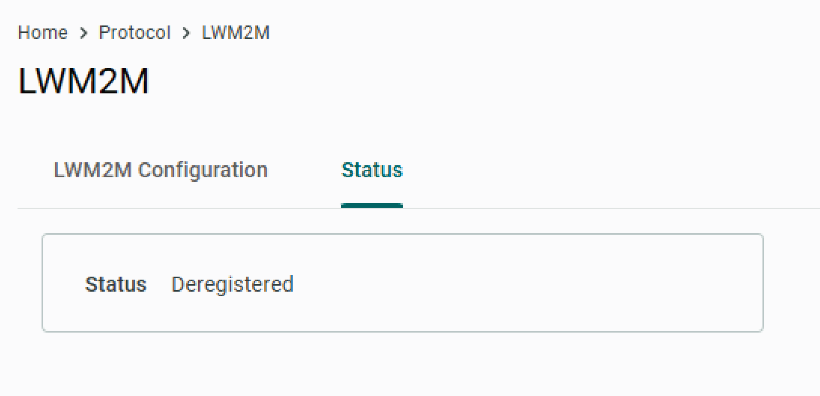
Setting	Description	Factory Default
1 to 65535	Specify the LWM2M server port. This information is provided by the LWM2M server.	5784

When finished, click **APPLY**.

Status

Menu path: LWM2M > Status

From the **Status** page, you can check the LWM2M server connection status.



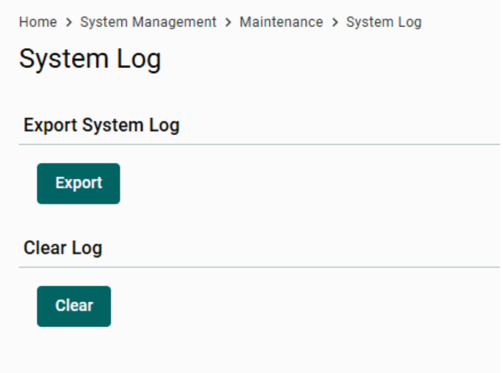
Maintenance

The **Maintenance** section covers the event log, configuration backup and import, and diagnostics functions.

System Log

Menu path: Maintenance > System Log

The **System Log** page is used to export the device's event log to a specified location.



Click **Export** to save the event log to your local host.

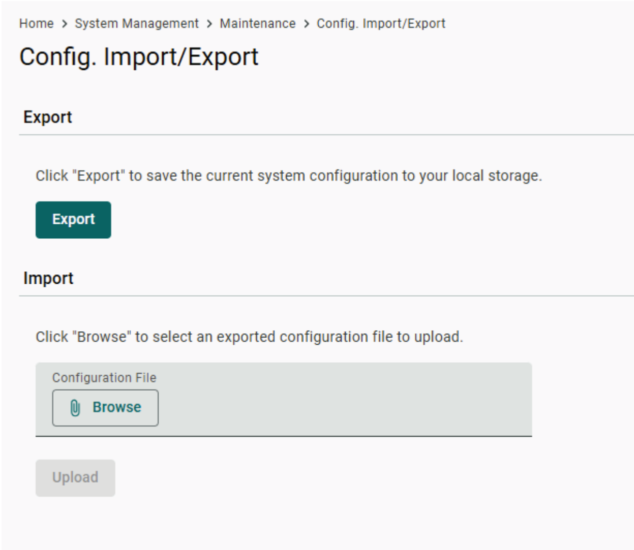
Click **Clear** to clear the event log.

Configuration Import/Export

Menu path: Maintenance > Config. Import/Export

From the **Config. Import/Export** page, you can export the current configuration or import a previously exported configuration file.

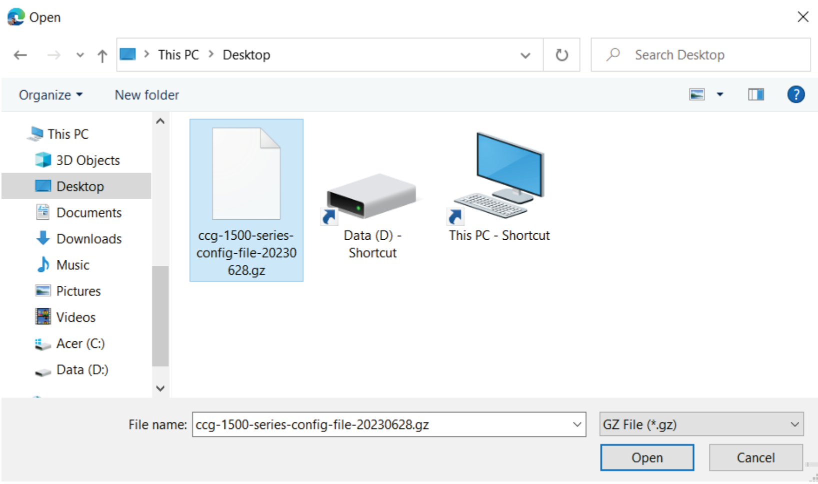
Exporting the Device Configuration



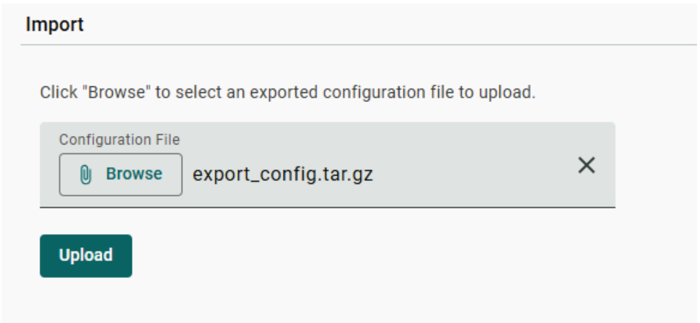
Click **Export** to export the configuration file of the CCG Series device to the local host machine. The configuration file will be compressed and exported to the specified location in **.gz** format.

Importing a Device Configuration Backup

Click **Browse** and navigate to the configuration backup file (in .gz format) on the local machine. Select the file and click **Open**.



Click **Upload** to import the selected configuration file to the CCG Series device. A prompt will appear to reboot the device. Once rebooted, the system will apply the imported configuration settings.

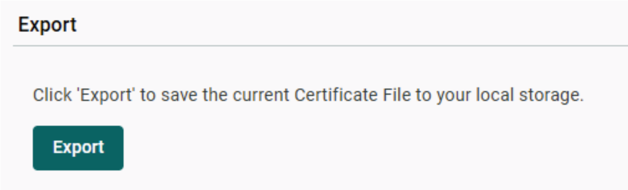


Web SSL Certificate

Menu path: Maintenance > Web SSL Certificate

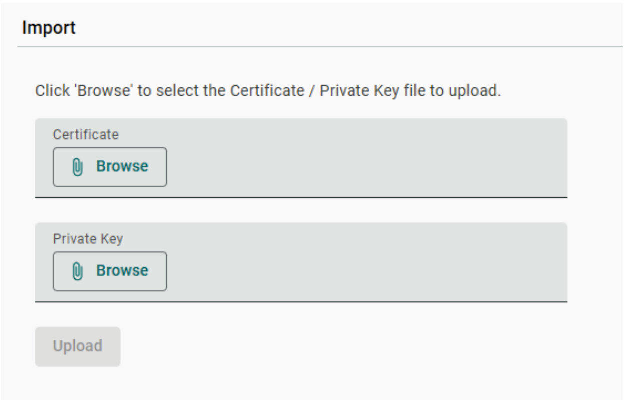
From the **Web SSL Certificate** page, you can export the web SSL certificate or upload a third-party SSL certificate and key file.

Exporting the Certificate



Click **Export** to export the web SSL certificate of the CCG Series device to the local host machine. The certificate file will be exported to the specified location in **.crt** format.

Importing a Certificate



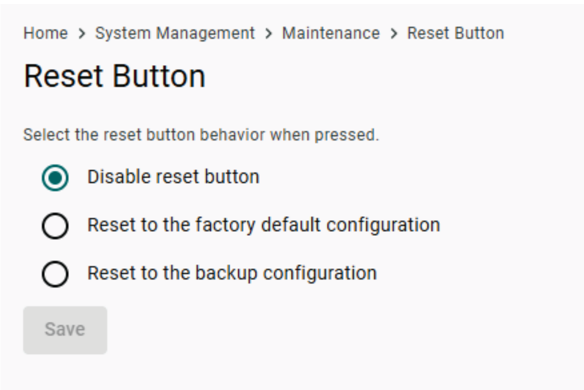
Click **Browse** and navigate to the certificate file (in .crt format) and key file (in .pem, .pk, .key format) on the local machine. Select the file and click **Open**.

Click **Upload** to import the selected certificate and key file to the CCG Series device. A prompt will appear to reboot the device. Once rebooted, the system will apply the imported certificate.

Reset Button

Menu path: Maintenance > Reset Button

The **Reset Button** page is used to configure the behavior of the physical reset button when pressed.



When pressing the reset button for less than 4 seconds, the device will reboot.

When pressing the reset button for longer than 4 seconds, the reset button will behave based on the selected behavior.

Reset Button

Setting	Description	Factory Default
Disable reset button	Disable the reset button. If disabled, the following behavior will still apply: • Pressing the reset button for less than 4 seconds will still reboot the device. • Pressing and holding the button for more than 4 seconds within 120 seconds after the P/S LED turns green will still reset the device to the factory default configuration.	Disable reset button
Reset to factory default configuration	When pressed for longer than 4 seconds, the device will be reset to the Moxa factory default settings.	
Reset to backup configuration	When pressed longer than 4 seconds, the device will be reset to the most-recent configuration backup. If no configuration backup exists, click **Back Up Now**.	

When finished, click **Save**.

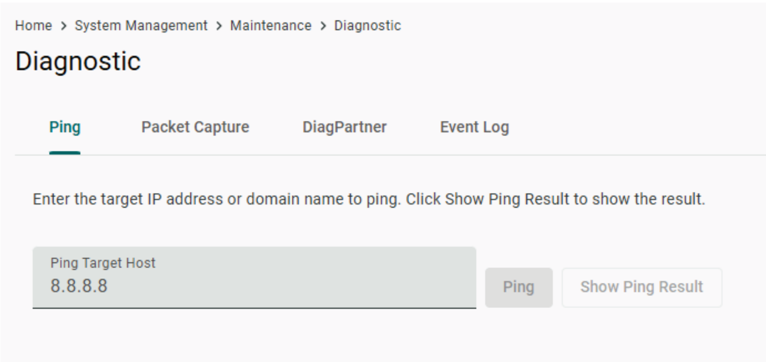
Diagnostic

The **Diagnostic** page is used to perform connection checks and monitor network activity.

Ping

Menu path: Maintenance > Diagnostic > Ping

The **Ping** page is used to ping a target host to check the connection status.



Ping Target Host

Setting	Description	Factory Default
IP Address or Domain Name	Specify the target IP address or domain to ping.	N/A

Click **Ping** to start pinging the specified target host.

Click **Show Ping Result** to view the result of the ping test.

Packet Capture

Menu path: Maintenance > Diagnostic > Packet Capture

The **Packet Capture** page is used to configure packet capturing for traffic analysis. If enabled, the device will run a tcpdump on its cellular interface and stream the raw capture to a PC running a packet analyzer tool connected to the LAN port.

Enable

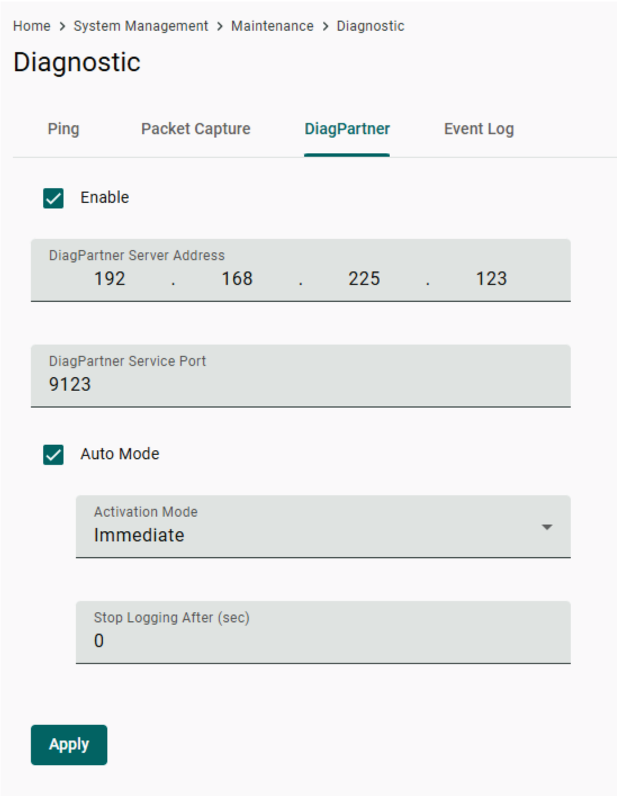
Setting	Description	Factory Default
Checkbox	Enable or disable cellular packet capturing.	Unchecked

When finished, click **Apply**.

DiagPartner

Menu path: Maintenance > Diagnostic > DiagPartner

The **DiagPartner** page allows you to enable or disable the DiagPartner cellular modem debug mode. This function is mainly used by Moxa technical support engineers to troubleshoot the connection of the cellular modem to the cellular base station and core network.



Enable

Setting	Description	Factory Default
Checkbox	Enable or disable the DiagPartner debug mode.	Unchecked

DiagPartner Server Address

Setting	Description	Factory Default
IP Address	Specify the DiagPartner server address.	192.168.225.123

DiagPartner Service Port

Setting	Description	Factory Default
1 to 65535	Specify the DiagPartner service port.	9123

Auto Mode

Setting	Description	Factory Default
Checkbox	Enable or disable the Auto Mode. If checked, DiagPartner will automatically start depending on the selected Activation Mode and will stop after the specified duration.	Unchecked

Activation Mode

Setting	Description	Factory Default
Immediate	The DiagPartner service will start logging immediately once click **Apply**.	Immediate
Event	The DiagPartner service will start logging when the device is disconnected or when a network issue is detected.	

Stop Logging After (sec)

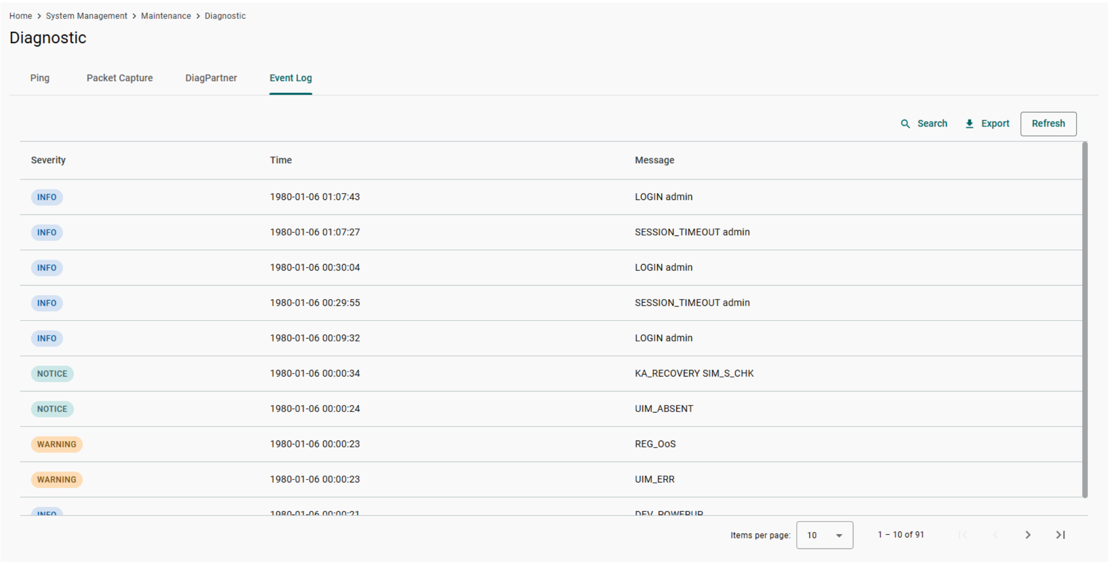
Setting	Description	Factory Default
1 to 9999999	Specify the duration (in sec) DiagPartner will run for after being activated. If set to 0, the service will keep running until manually stopped.	Unchecked

When finished, click **Apply**.

Event Log

Menu path: Maintenance > Diagnostic > Event Log

The **Event Log** page is used to view and export device event logs. The device supports up to 1,000 logs. When exceeded, the oldest logs will be overwritten first.



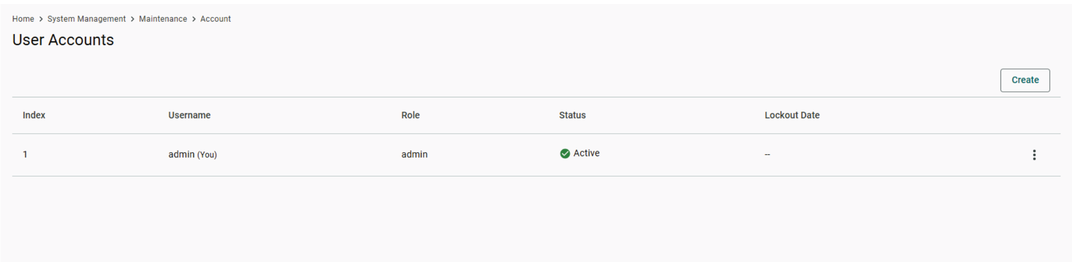
Click **Export** to export the event logs to the local host in Excel format.

Click **Refresh** to renew the information in the event log.

Account

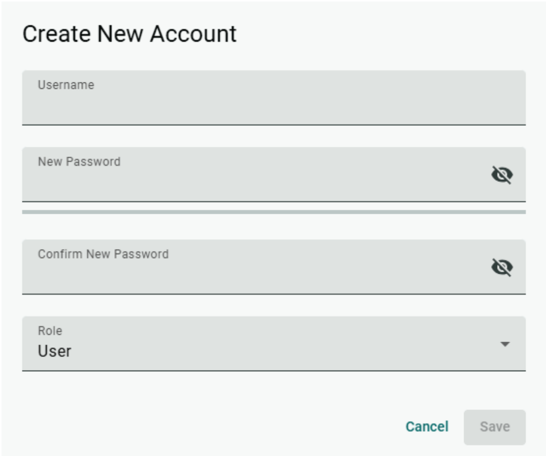
Menu path: Maintenance > Account

The **Account** page is used to manage user accounts on the device. Permissions can be configured for each user account to determine which functions the account can view and modify. Three user roles are available: Admin, Engineer, and User.



Adding an Account

On the User Accounts screen, click **Create** to create a new user account.



Username

Setting	Description	Factory Default
4 to 63 Characters	Enter the username of the account.	N/A

New Password

Setting	Description	Factory Default
8 to 64 Characters	Enter the password of the account.	N/A

Confirm New Password

Setting	Description	Factory Default
8 to 64 Characters	Enter the password of the account again for confirmation.	N/A

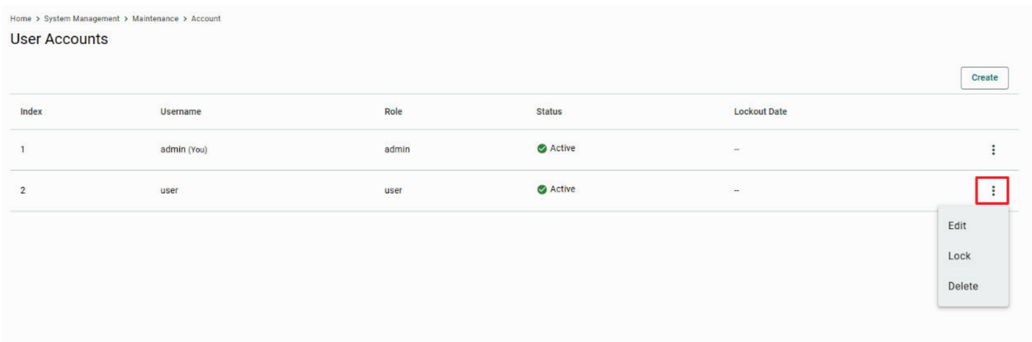
Role

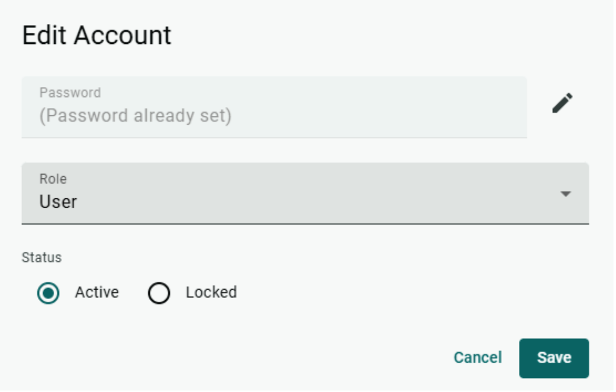
Setting	Description	Factory Default
Admin	Set the user role to Admin. This role has full access to all device settings.	User
Engineer	Set the user role to Engineer. This role has full access to all device settings except the Reset Button and Account settings.	
User	Set the user role to User. This role has view-only access to the System, Network, and LAN information pages.	

When finished, click **Save**.

Editing an Account

In the account list, click the **Menu** (⋮) icon of the account you want to modify and click **Edit**. The username of an account cannot be modified.





Password

Click the **Pencil** icon to modify the password.

Setting	Description	Factory Default
8 to 64 Characters	Enter the password of the account.	N/A

Role

Setting	Description	Factory Default
Admin	Set the user role to Admin. This role has full access to all device settings.	User
Engineer	Set the user role to Engineer. This role has full access to all device settings except the Reset Button and Account settings.	
User	Set the user role to User. This role has view-only access to the System, Network, and LAN information pages.	

Status

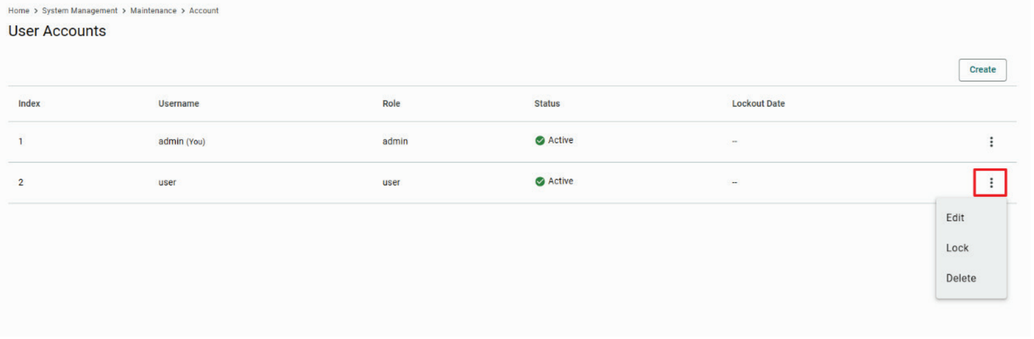
Setting	Description	Factory Default
Active	Select Active to enable this account.	Active
Locked	Select Locked to lock the account and prevent this account from logging in. Set the status to Active to unlock the account.	

When finished, click **Save**.

Locking an Account

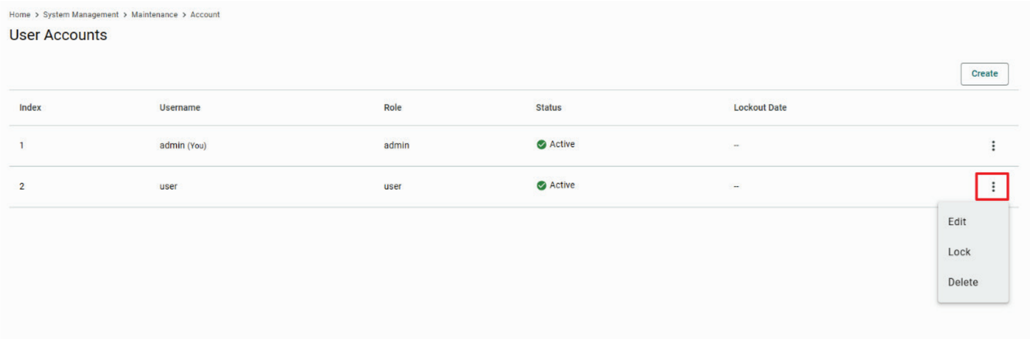
In the account list, click the **Menu** (⋮) icon of the account you want to lock and click **Lock**. Locking an account will prevent it from logging in to the system.

To unlock the device, click the **Menu** (⋮) icon of the account you want to unlock and click **Unlock**.



Deleting an Account

In the account list, click the **Menu** ( ) icon of the account you want to delete and click **Delete**. When prompted to confirm, click **Delete**.



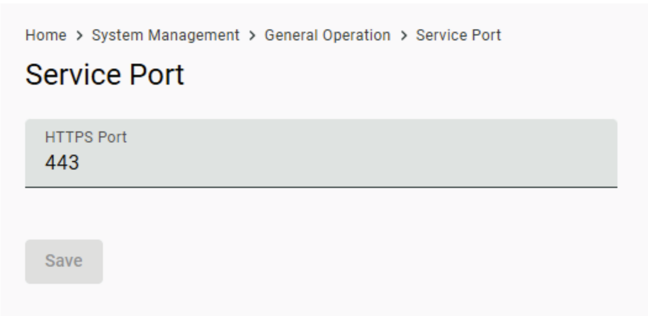
General Operation

The **General Operation** section covers service port and time settings. You can also restart or reset the device from this section.

Service Port Settings

Menu path: General Operation > Service Port

From the **Service Port** page, you can configure the protocol access ports to connect to the device.



HTTPS

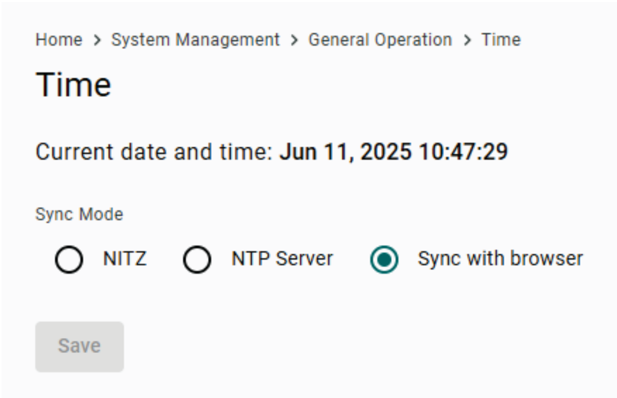
Setting	Description	Factory Default
1 to 65535	Specify the HTTPS port number. The following ports are reserved and cannot be used: 53, 80, 500, 502, 1701, 1723, 4500, 5037, 7777.	443

When finished, click **Save**.

Time

Menu path: General Operation > Time

From the **Time** page, you can configure the system time.

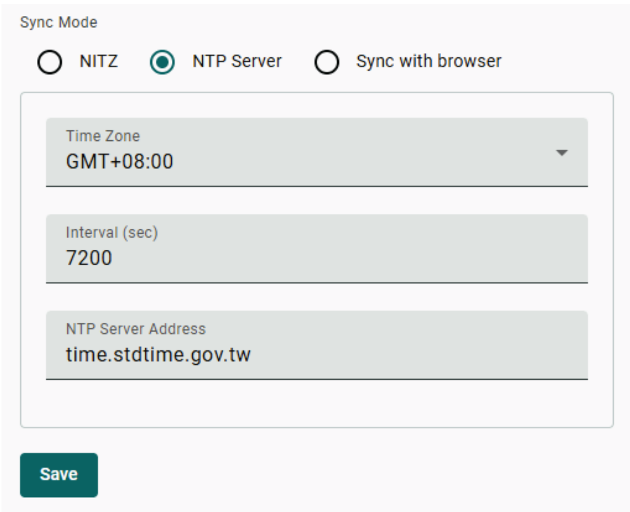


Sync Mode

Setting	Description	Factory Default
NITZ	Synchronize the system time using NITZ.	NITZ
NTP Server	Synchronize the system time with the specified NTP server. Additional configuration options will be available.	
Sync with browser	Synchronize the system time with the browser time.	

When finished, click **Save**.

If you selected **NTP Server**, configure the following settings.



Time Zone

Setting	Description	Factory Default
Time Zone	Select the NTP server's time zone.	GMT +08:00

Interval (sec)

Setting	Description	Factory Default
60 to 604800	Specify the interval (in seconds) at which the device will sync the system time with the NTP server.	7200

NTP Server Address

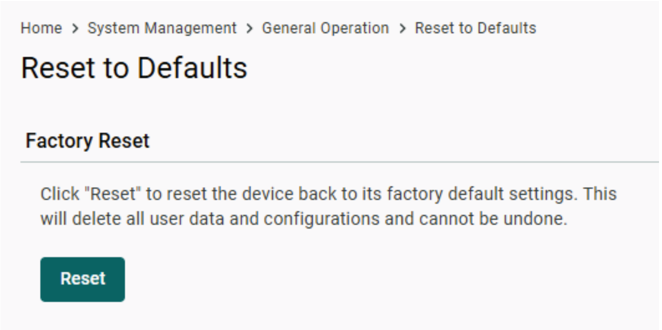
Setting	Description	Factory Default
Server Address	Specify the NTP server address.	time.stdtime.gov.tw

When finished, click **Save**.

Reset to Defaults

Menu path: General Operation > Reset to Defaults

From the **Reset to Defaults** page, you can restore the CCG device to its factory default settings. Resetting the configuration is permanent and cannot be undone.

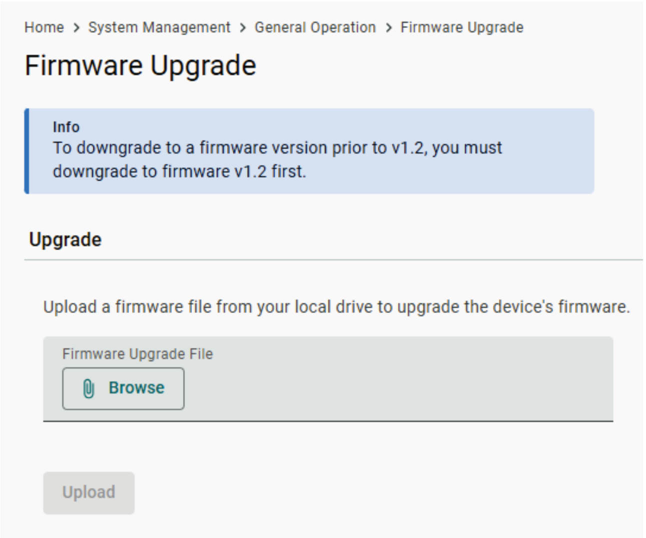


Click **Reset** to reset the device to its default factory settings.

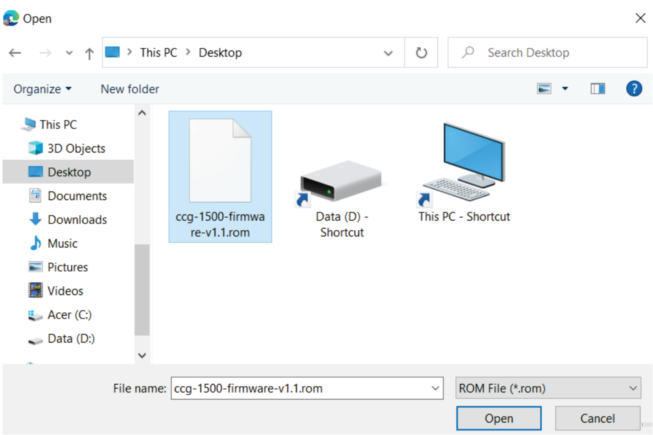
Firmware Upgrade

Menu path: General Operation > Firmware Upgrade

From the **Firmware Upgrade** page, you can upload new firmware versions to the device.



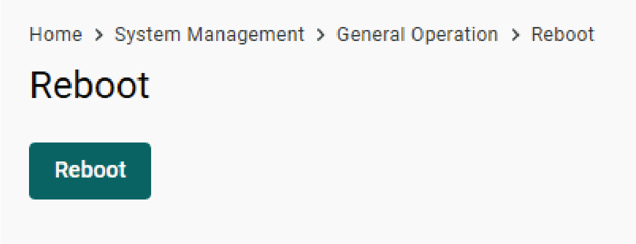
Click **Browse** and navigate to the firmware file (in .rom format) on the local machine. Select the file and click **Open**.



Click **Upload** to import the selected firmware file to the CCG Series device.

Reboot

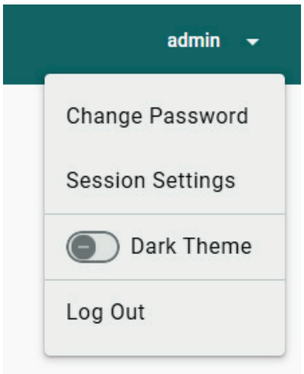
Menu path: General Operation > Reboot



Click **Reboot** to restart the device.

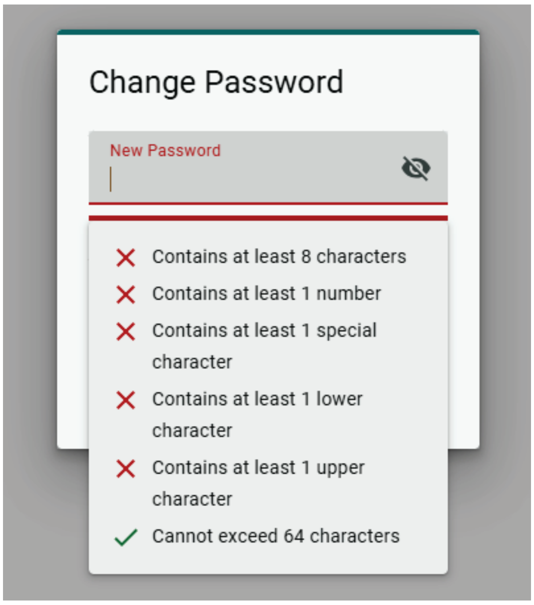
Administration Management

Click **Admin** in the upper-right corner of the page to open the user management menu. You can perform several basic functions from this menu.



Change Password

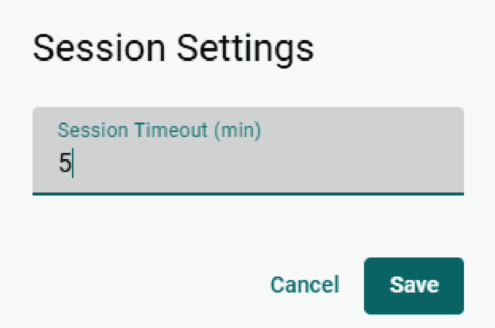
From the user management menu, click **Change Password** to update your user password. The password is subject to certain limitations and requirements.



When finished, click **Save**.

Session Settings

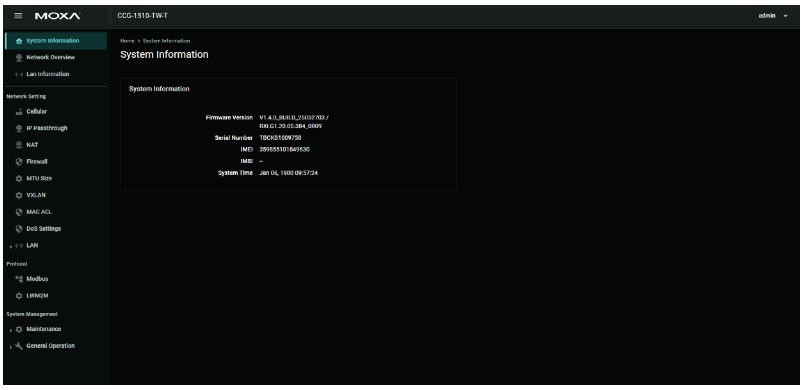
From the user management menu, click **Session Settings** to specify the duration of inactivity before the login session is terminated.



When finished, click **Save**.

Dark Theme

From the user management menu, click the **Dark Theme** toggle to enable or disable the dark UI theme.



Log Out

From the user management menu, click **Log Out** to immediately log out from the device. You will be automatically redirected to the login page.