Moxa Remote Connect (MRC)

User Manual

Version v1.1

August 2025

Table of Contents

Overview

This document includes the following sections:

- **Overview**: This section introduces the overall concept of the Moxa Remote Connect (MRC) service and the basic information you need to know before using it.

- **MRC Quick Link**: This section covers the UI and usage of the MRC Quick Link service.

- **MRC Gateway**: This section explains how to configure the MRC Gateway to use the MRC Quick Link service.

- **MRC Client**: This section introduces the UI and usage of the MRC Client.

- **Troubleshooting and Common Questions**: This section addresses common issues and questions.

Introduction

Welcome to the MRC Quick Link user manual. This comprehensive guide is designed to help you understand and navigate the UI features, technical concepts, and tasks you may encounter while using the MRC Quick Link service.

Moxa Remote Connect (MRC) is a convenient, secure, and versatile networking solution designed to seamlessly bridge field devices and engineers over the Internet for industrial applications.

Moxa Remote Connect Suite consists of three main components:

1. **MRC Quick Link:** A secure cloud-based remote access platform. This centralized connection management platform handles security levels, user privileges, and the configuration of the MRC gateway and MRC Client.

2. **MRC Gateway**: A Moxa device that supports MRC functionality, allowing secure remote access to local devices via the MRC Client.

3. **MRC Client:** Windows software enabling engineers to connect to remote devices from their PCs.
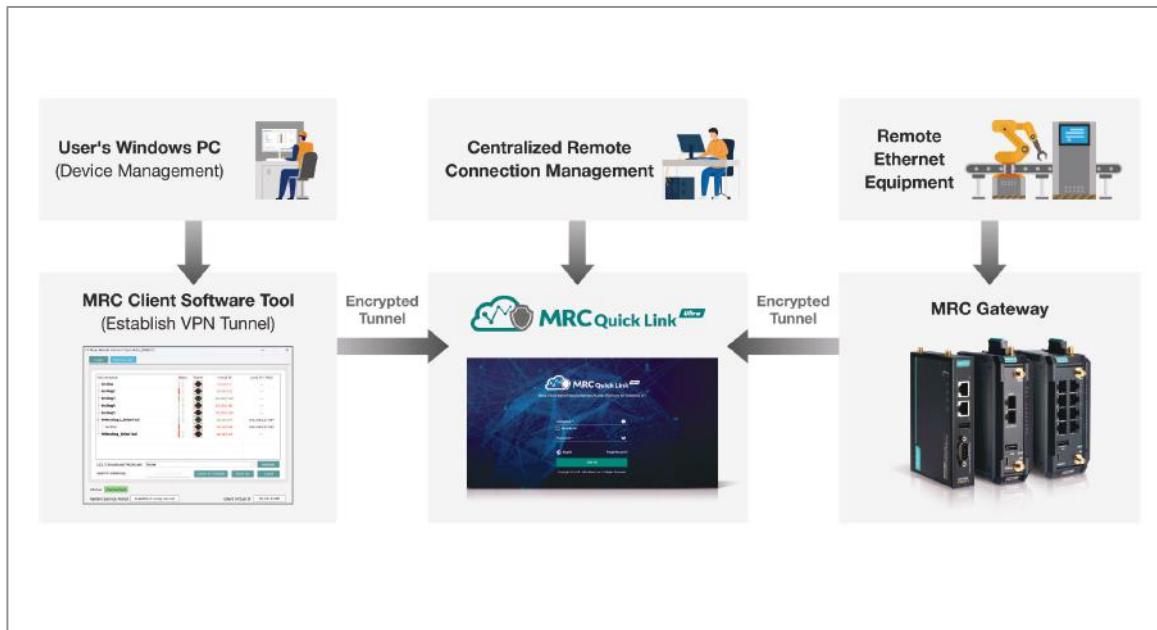
Supported Series and Software Versions

Supported Series and Firmware Versions

MRC Quick Link		MRC Client	MRC Gateway	
Version	URL	Version	Model	Version
MRC Quick Link **v3.3**	mrcasia.moxa.com mrcus.moxa.com mrceu.moxa.com mrcchina.moxa.com.cn	Software v3.3.0	MRC-1002 Series	v3.3.0 and earlier
MRC Quick Link Ultra **v4.1**	mrc.moxa.com	Software v4.1.0	OnCell G4302 Series	v3.18.0 and above
			OnCell G4308 Series	v3.18.0 and above
			OnCell 3120 Series (HW Rev 2.0.0 only)	v2.4.0 and above
			MRC-1002 Series	v4.1.0 and above

Checking the Version Information

MRC Quick Link

Click the triple dot (⋮) icon in the top-right to expand the drop-down menu and click **About**.
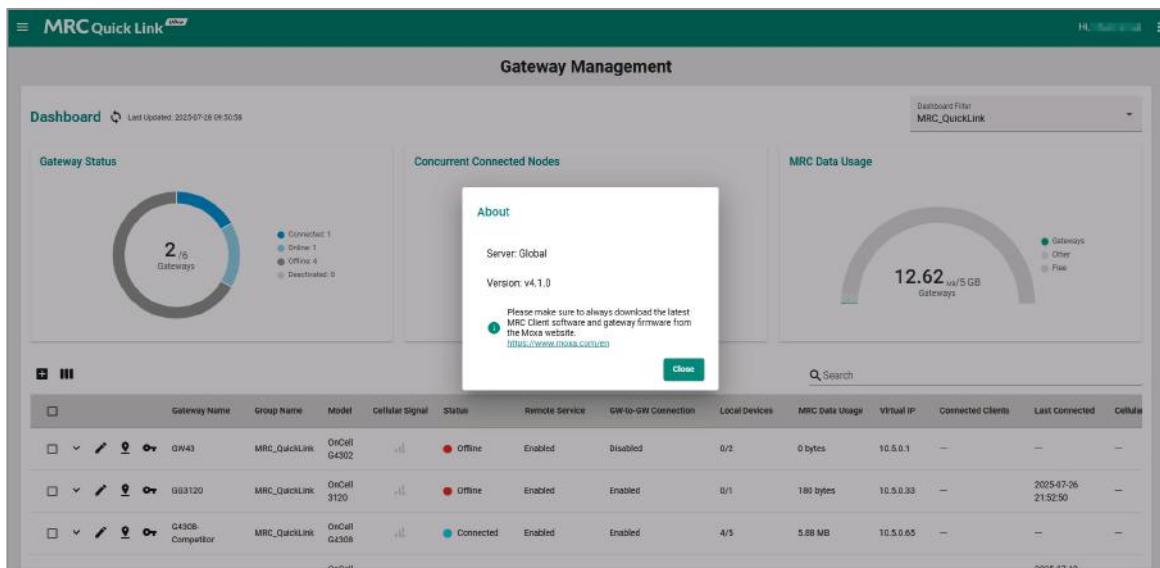
MRC Client

The version information is shown in the header bar of the MRC Client software.
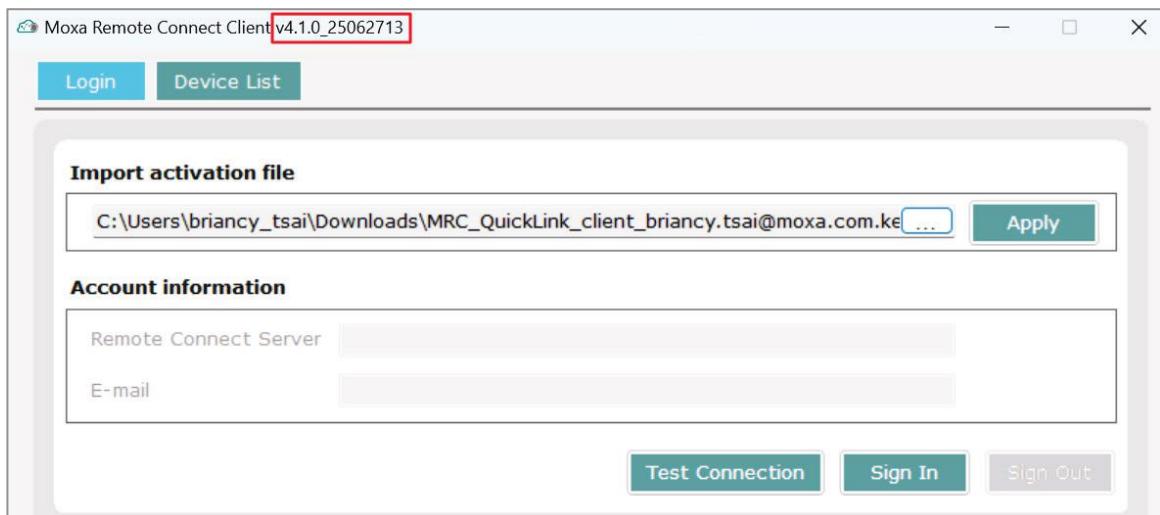
MRC Gateway

Log in to the gateway device and navigate to **Device Summary**.

Getting Started

This section will guide you step by step on how to activate the MRC Quick Link service.

Activating Your MRC Quick Link Account

> ✎ **Note**
>
> MRC can only be used on supported Moxa products. Refer to the Supported Series and Software Versions section for an overview of supported devices.

1. Log in to the Moxa license portal using your Moxa account.
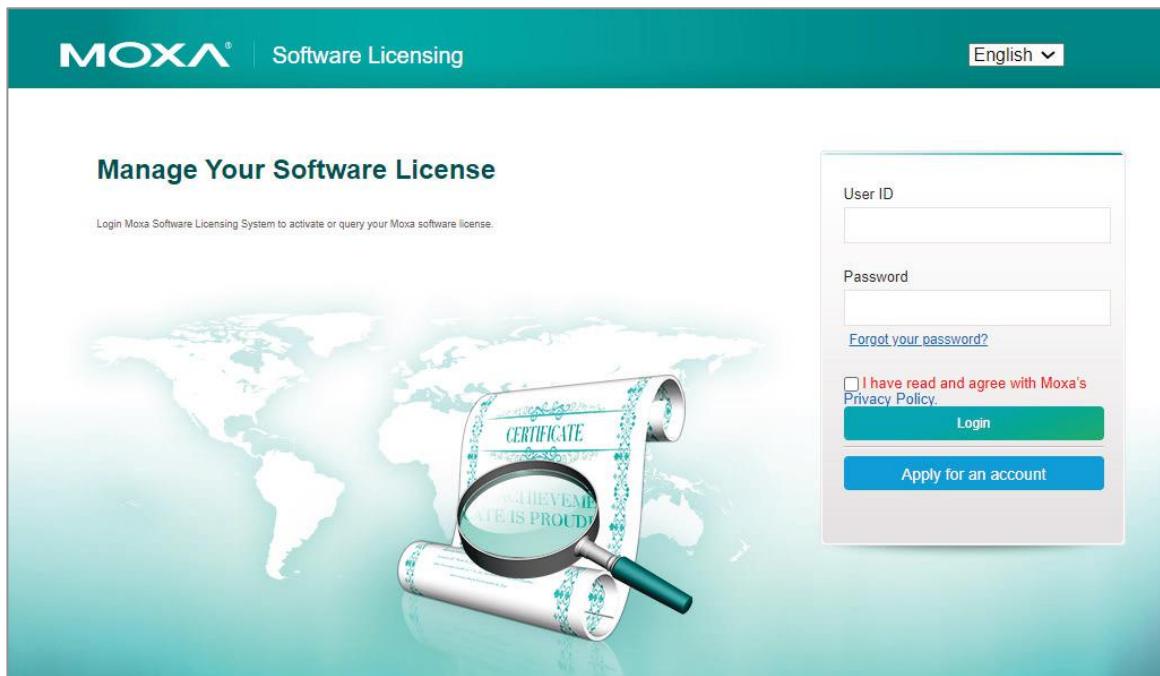
2. Navigate to **Products and Licenses > Activate a Product License**.

3. Select **MRC Quick Link** as the **Product Type**.

4. Enter the product serial number (S/N) and other required information, then click **Activate**.

5. You will receive an email confirming the successful registration of your MRC Quick Link account.

Dear Elizabeth Jackson,

Congratulations! You have successfully registered your MRC Quick Link.

Moxa will use this email address to contact you regarding your MRC Quick Link. Below are the details of your Quick Link service:

MRC Quick Link : https://mrcasia.moxa.com
MRC Quick Link Username: testUser_19807176
Password: u-6bd9f9a-2017-4176-aacd-3af5dfc023ed
Upon your first login to your MRC Quic Link, we strongly recommend changing the default password for security reasons. If you did not register for an MRC Quick Link, please contact Moxa and include the contents of this email.

_____

Note: Please do not reply to this email. This email address is not monitored, and replies to this message will not be read.

_____

Best regards,

MRC Quick Link Operation team

6. Follow the instructions in the email to log into MRC Quick Link.

7. Navigate to **Wizard** in the function column to get started with the MRC Quick Link service.
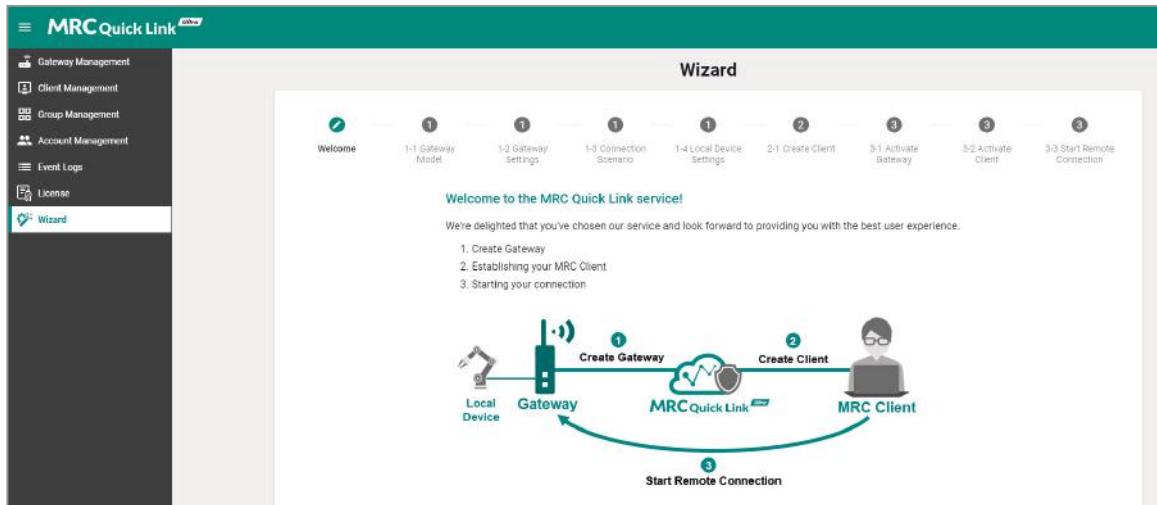
Activating an Add-on License

1. After purchasing an add-on license product, you will receive a product registration code via email.

Moxa trial license notification

Dear Customers,

Your trial registration code type (MRC QuickLink TRIAL) model name () is ▓▓▓▓▓▓▓▓▓▓. Please go to our activation portal to activate your purchased products.
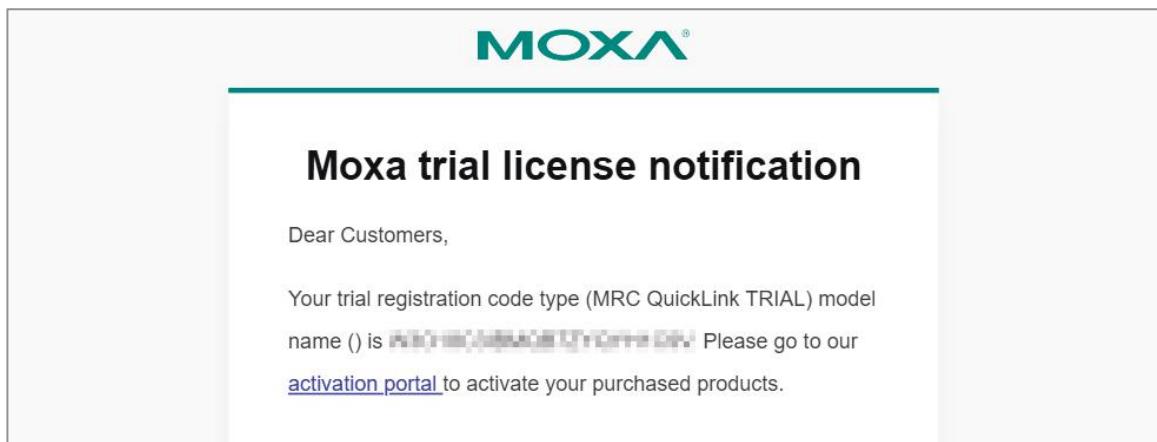
2. Log in to the Moxa license portal using your Moxa account.
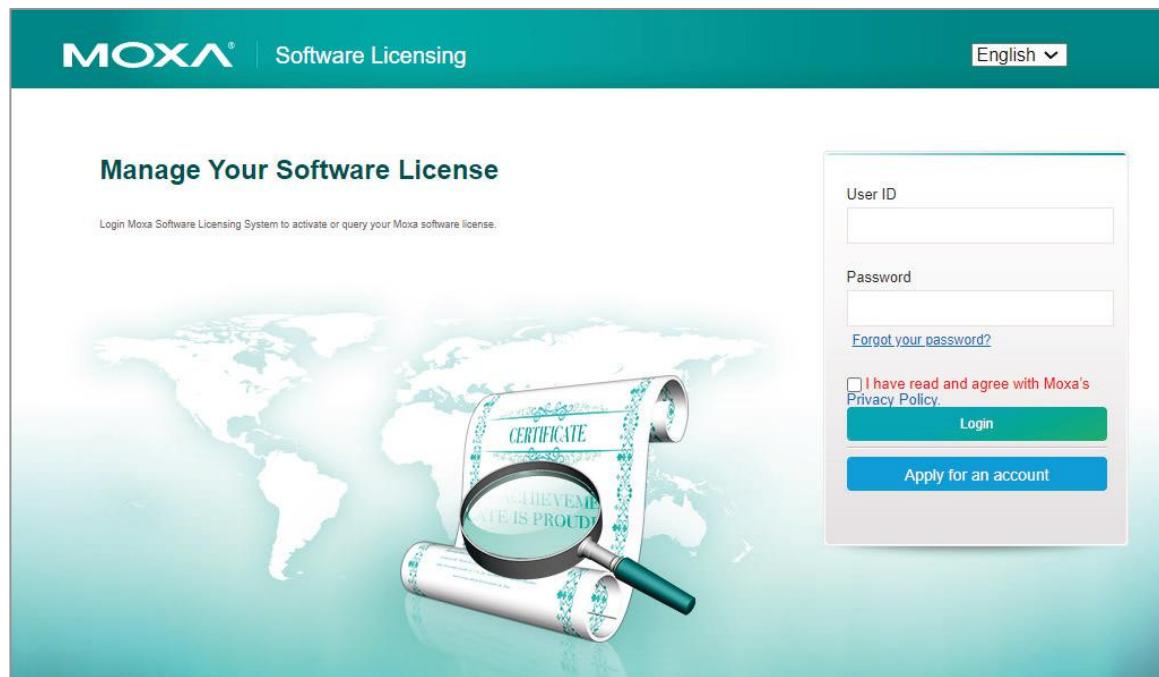
3. Navigate to **Products and Licenses > Activate an add-on or renewal license**.
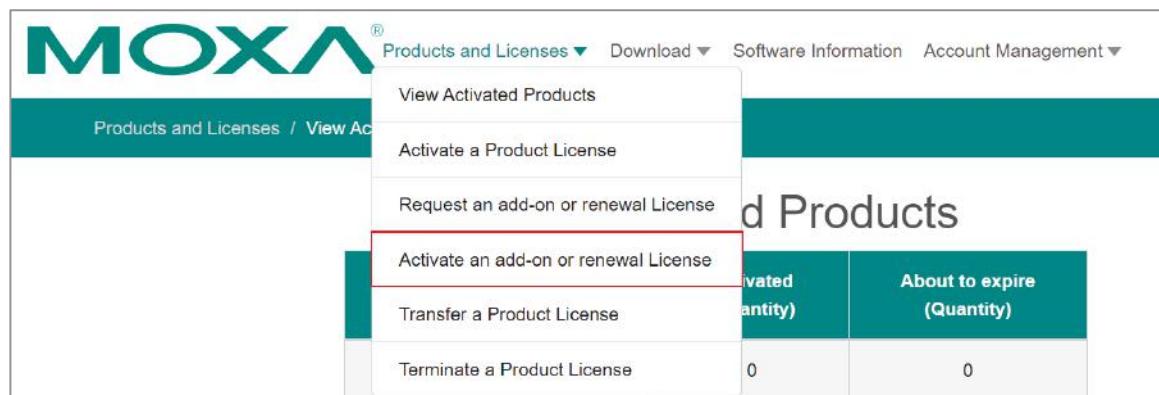
4. Enter the registration code and other required information, then click **Activate**.

5. Log in to MRC Quick Link.

6. Navigate to License in the function column to verify the status of the license.

Service Concepts and Architecture

This section provides some common scenarios for remote connections and introduces how MRC Quick Link establishes secure and efficient remote communication between MRC Gateways and MRC Clients. This page also provides the MRC Quick Link service architecture as a reference for users to deploy the MRC solution.

Scenarios for Remote Connections

In an increasingly connected world, the ability to remotely interact with devices not only saves time and human resources on physical visits, but also enhances operational efficiency and ensures the continuous performance and reliability of critical systems.

Remote connectivity has many purposes. Below are some important implementations of remote connectivity in industrial applications:

1. **Monitoring**: Engineers can remotely keep track of the operational status of devices and connections, and access device logs for analysis.

2. **Maintenance**: Maintenance staff can access devices remotely to perform diagnostics and repairs, firmware updates, or configurations.

3. **Control**: Control centers can leverage remote connectivity to issue commands to devices, enabling them to perform their daily tasks and operations.

Challenges for Remote Device Access

In the past, when setting up services, remote access and maintenance were often overlooked, making it very difficult to set up remote connections later on.

Below are common challenges related to remote device access:

1. **Security and Access Restrictions**: The network where the device is located may have security permissions that restrict external access, requiring the establishment of an independent connection.

2. **Closed Network Environments**: The device operates within a closed network without an available public IP for connection.

3. **Cellular Communication**: The device communicates via cellular networks and the SIM card used is assigned a private IP, which, unlike a public IP, cannot be directly accessed.

MRC Quick Link Service Concepts

MRC Quick Link is designed to facilitate a variety of remote access applications. Below is an overview of the key concepts of the solution.

- **Cloud Platform**: MRC Quick Link serves as a publicly accessible cloud platform to bridge connections between MRC Gateways and MRC Clients. MRC Quick Link facilitates the handshake process, establishing secure and efficient communication between MRC Gateways and MRC Clients.

- **Establishing Connections From an MRC Client**: When an MRC Client wishes to connect to an MRC Gateway, the connection request is initiated by the MRC Client. MRC Quick Link then verifies permissions and provides the path to the MRC Gateway to establish the connection.

- **Gateway-to-gateway Connectivity:** MRC Quick Link supports the gateway-to-gateway feature, allowing MRC Gateways within the same group to maintain continuous connections. When this feature is enabled, if a gateway connects to MRC Quick Link, it automatically establishes a connection to other gateways in the same group.

- **Point-to-point Connection:** All connections are started through MRC Quick Link, which acts as an intermediary interface which converts to point-to-point direct connections if possible. The possibility of converting to point-to-point connections is based on the specific environmental conditions with the purpose of enhancing transmission efficiency. When point-to-point connections are not feasible and MRC Quick Link is required as an intermediary, MRC Quick Link will instead switch to the most suitable regional server for the best connection quality.
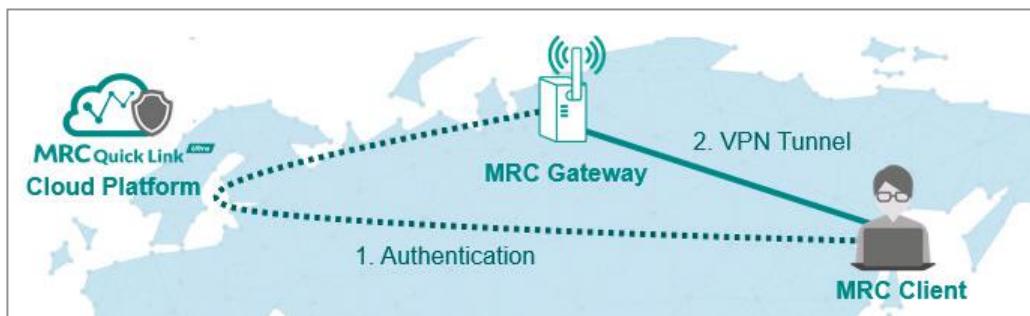
Service Concepts

Service Architecture
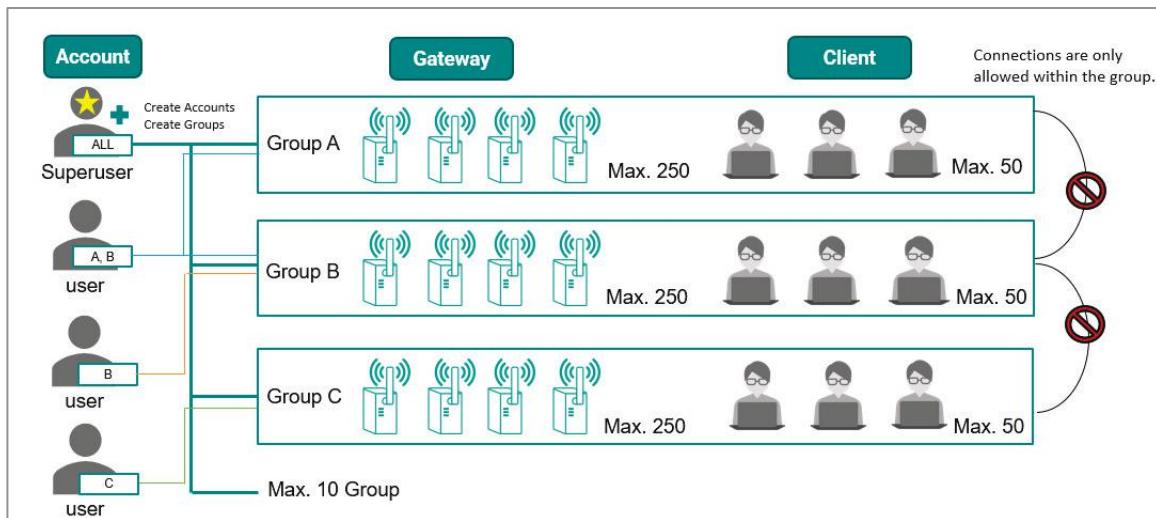
Superuser Role Permissions:

- Customers can obtain a superuser account from the Moxa License Site.

- A Superuser has the highest level of authority, capable of creating user accounts and managing groups.

- For a comparison of permissions, refer to the Account Management section.

Group Limitation and Access

- Each Superuser can create up to 10 user groups.

- Superusers define group access for users. Users can only interact with authorized groups.

- Communication between different groups is not allowed. Only Gateways and Clients within the same group can establish remote connections.

Gateway and Client Capacity

- Each group supports a maximum of 250 Gateways and 50 Clients.

- MRC supports a total maximum of 2500 Gateways and 500 Clients.

- Each gateway supports a maximum of 25 local devices connected to it.

License Usage
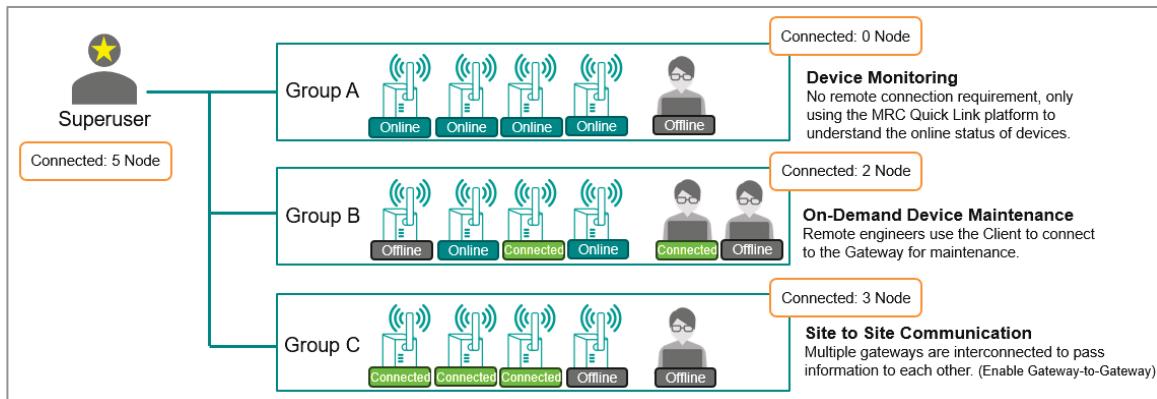
Shared Licenses Across Groups

- Licenses are shared across all groups managed by a Superuser.

- When a remote connection is established, each connected Gateway or Client consumes concurrent connection nodes and a data volume license.

- License usage works on a first-come-first-served basis.

Purchasing Additional Licenses

- MRC supports 2 types of licenses: concurrent connection nodes and data volume licenses.

  o Concurrent connection nodes: A maximum of 300 node licenses can be purchased.

  o Data usage: No upper limit on additional purchases.

- Licenses are added and activated via the Moxa License Site.

MRC Quick Link

Logging In

This section describes how to log in to the MRC Quick Link service.

Logging In

1. Open a web browser and navigate to https://mrc.moxa.com.

2. Enter your MRC account username and password. Refer to the Activating Your MRC Quick Link Account section.

3. Click **LOG IN**.
   The system will send a verification code to your registered email.

4. Enter the verification from the email.
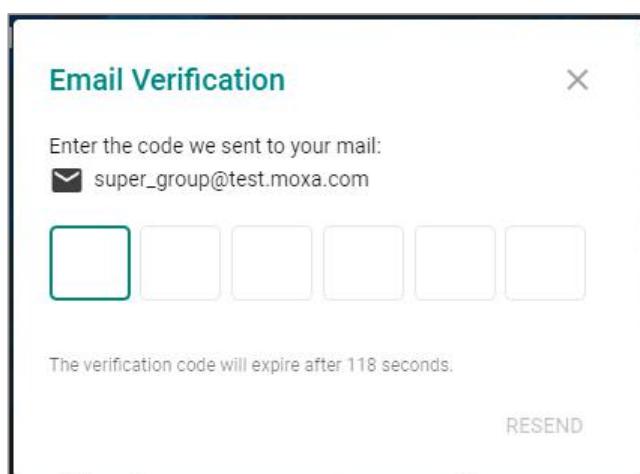
UI Setting	Description	Valid Range	Default Value
Username	Enter the account username.	Username	N/A
Remember Me	Check the checkbox to save the username in this browser.		Unchecked
Password	Enter the account password.		N/A

Change the Interface Language

Click the globe ( ) icon to change the interface language.

UI Setting	Description	Valid Range	Default Value
Language	Select the preferred interface language.	English 繁體中文 (Traditional Chinese) 简体中文 (Simplified Chinese) 日本語 (Japanese)	English

Forgot Password

Click **Forgot Password?** to reset your password. The system will send a verification email for resetting your password to your registered email.

UI Setting	Description	Valid Range	Default Value
Username	Enter the username for this account.	Username	N/A

Basic Functions

This section covers the following topics:

UI Interface Overview

Below is an overview of the MRC Quick Link user interface.
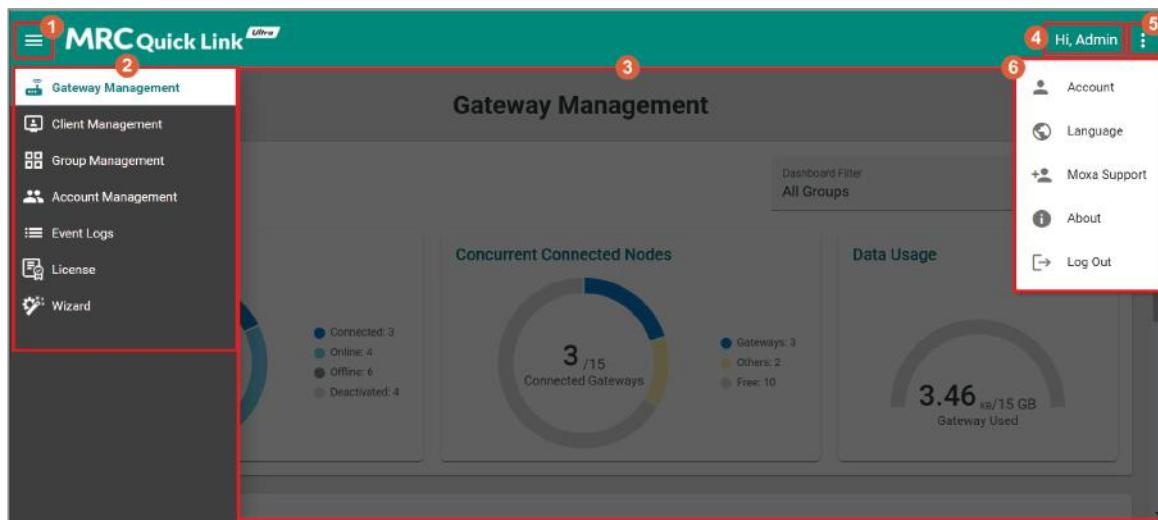
	Section	Description
1	Function menu	Click the menu (☰) icon in the top-left to show or hide the function menu.
2	Function pages	This menu contains all function-related configuration pages. Click on a function name in the function tree to go to the configuration screen for that function.
3	Configuration screen	Shows information and configuration options depending on the selected function page.
4	Username	Shows the username of the user that is currently logged in.
5	User account menu	Click the triple dot (⋮) icon to expand the basic functions menu.
6	Basic function menu	This menu contains all basic system functions.

Account

Edit Account

Click the triple dot ( ) icon to expand the basic functions menu and click **Account** to edit your account information. Information about transferring or deleting superuser accounts is only visible when logged in with a superuser account.

Edit Account

- To transfer a superuser account to a different administrator, contact Moxa for assistance.
- To delete a superuser account, log in to the Moxa license portal as the superuser and delete the account. 🖼

Username
PM_trans_Test_1225   **Change Password**
                                                18 / 64

Email *
▓▓▓ ▓▓@moxa.com

This email address will be used for two-factor authentication.

First Name (Given Name)   Last Name (Family Na...
                    0 / 64   0 / 64

Office Phone Number   Mobile Phone Number
                    0 / 64   0 / 64

Additional Information
                                                    0 / 254

Event Notifications
☐ Gateway status change

Cancel   **Apply**

UI Setting	Description	Valid Range	Default Value
Username	Shows the username for this account. The username cannot be changed.	N/A	N/A
Email	Enter the email address for this account. This email address will be used for two-factor authentication.	N/A	N/A
Secondary Email	Enter the backup email address for this account used for recovery purposes.	N/A	N/A
First Name	Enter the first name for this account user.	0 to 64 characters	N/A
Last Name	Enter the last name for this account user.	0 to 64 characters	N/A
Office Phone Number	Enter the office phone number for this account user.	0 to 64 characters	N/A
Mobile Phone Number	Enter the mobile phone number for this account user.	0 to 64 characters	N/A
Additional Information	Enter a description for this account.	0 to 254 characters	N/A
Event Notifications	Enable or disable the event notifications function. Enabled: The account user will receive email notifications if any gateway under their management changes status (online, offline, connected, disconnected). Disabled: The account user will not receive email notifications for gateway status changes.	N/A	Unchecked

Change Password

Click the triple dot (⋮) icon to expand the basic functions menu and click **Account**. In the **Edit This Account** screen, click **Change Password** to edit your account password.

UI Setting	Description	Valid Range	Default Value
New Password	Enter the new password for this account.	6 to 64 characters	N/A
Confirm Password	Enter the password again to confirm.	6 to 64 characters	N/A

Language

Click the triple dot (⋮) icon to expand the basic functions menu and click **Language** to change the interface language.

UI Setting	Description	Valid Range	Default Value
Language	Select the preferred language.	English 繁體中文 (Traditional Chinese) 简体中文 (Simplified Chinese) 日本語 (Japanese)	English

Moxa Support

Click the triple dot (:⋮) icon to expand the basic functions menu and click **Moxa Support** to create a temporary Moxa Support account for troubleshooting purposes. Repeating this process will create another Moxa Support account, up to a maximum of 3.

If you encounter any issues with MRC, you can use the Moxa Support function to create a temporary account for Moxa Support to access your MRC account and perform troubleshooting. Moxa Support accounts have elevated system privileges and can only be created by superusers.

> ✎ **Note**
>
> For security reasons, only 3 Moxa Support Accounts can be created at any given time. If necessary, you can manually terminate an active Moxa Support account from the Account Management section.
>
> Only 3 Moxa Support Accounts can be created. Please go to Account Management to remove any unnecessary Moxa support accounts. CLOSE

> ✎ **Note**
>
> The Moxa Support account username and password will disappear after closing this window. Please ensure that you have copied and provided the support account credentials to our technical support team before closing the window. You can find the Moxa Support account credentials in the Account Management section.
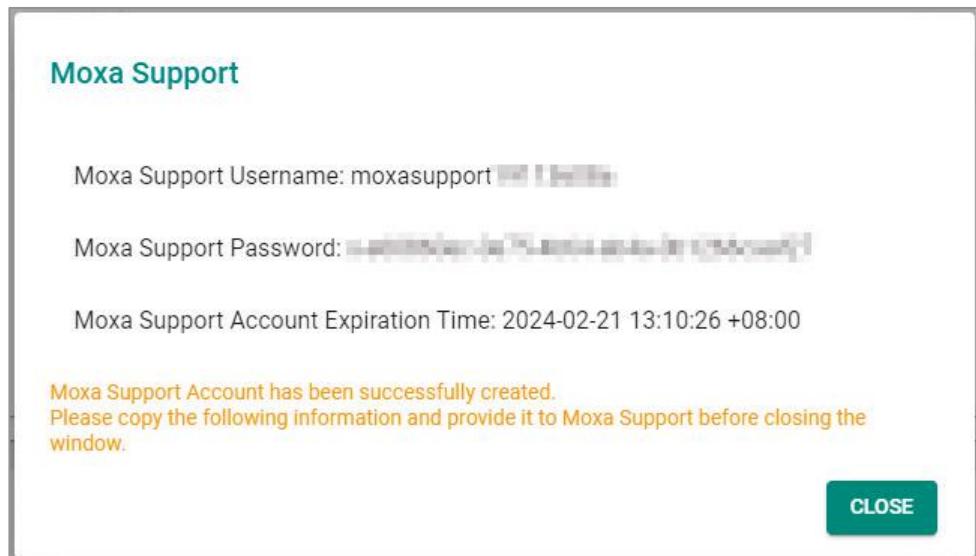
UI Setting	Description
Moxa Support Account	Shows the username of the Moxa Support account.
Moxa Support Password	Shows the password of the Moxa Support account.
Moxa Support Account Expiration Time	Shows the expiration time of the Moxa Support account. The Moxa Support Account has a validity period of one month and is automatically deleted when it expires. For security reasons, you can delete any accounts that are no longer needed from the **Account Management** section.

About

Click the triple dot ( ) icon to expand the basic functions menu and click **About** to check information about the MRC Quick Link instance.
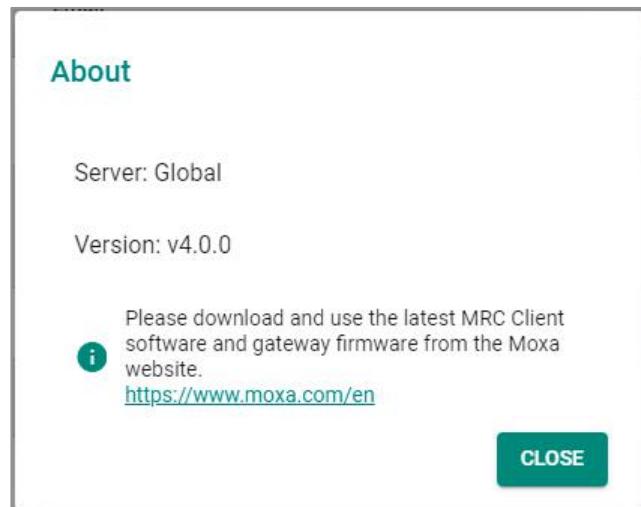
UI Setting	Description
Server	Shows the regional server information of your MRC Quick Link server.
Version	Shows the system version of the MRC Quick Link server.

Log Out

Click the triple dot ( ) icon to expand the basic functions menu and click **Log Out** to log out of MRC Quick Link.
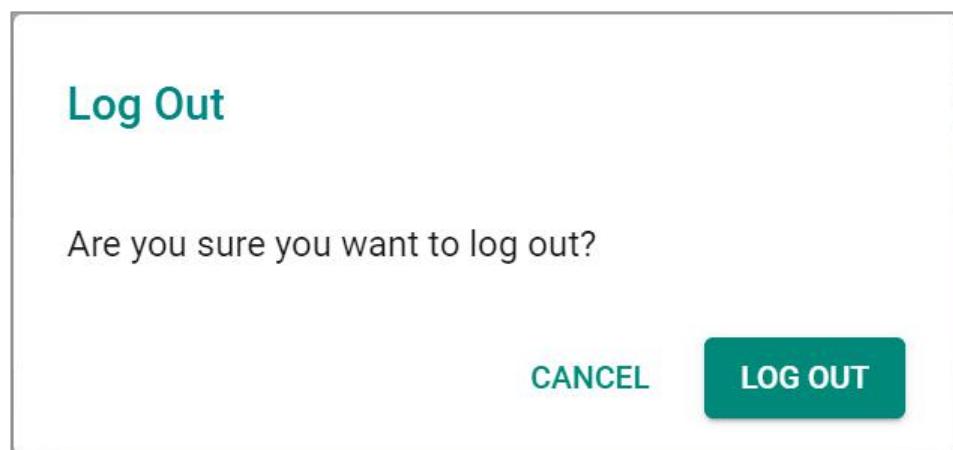
Gateway Management

From the **Gateway Management** section, you can check the gateway's status and configure gateway device settings.
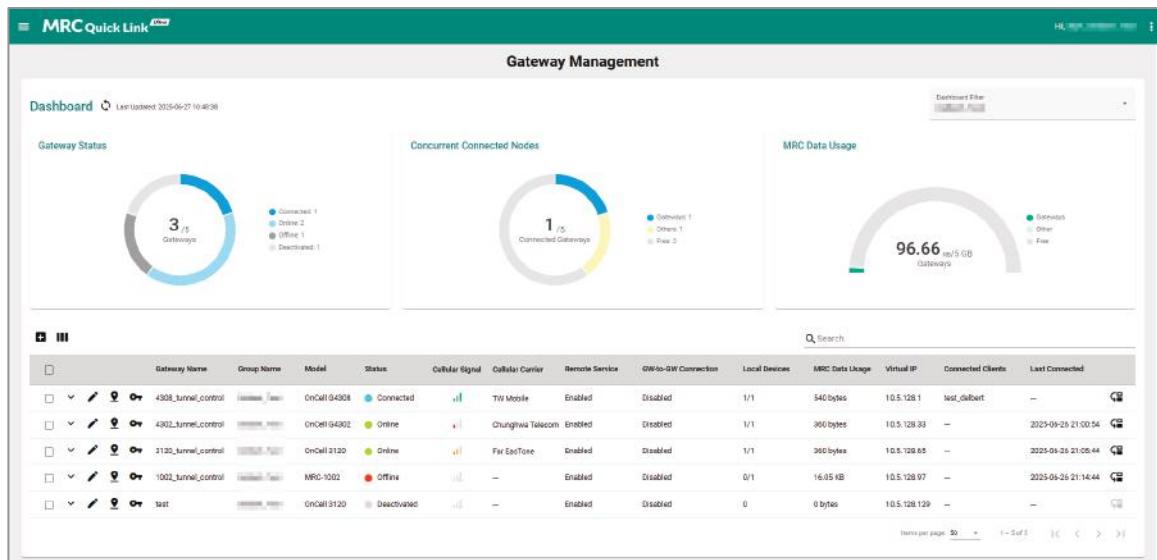
Dashboard

Menu Path: Gateway Management

The dashboard shows information about your gateways and licenses.
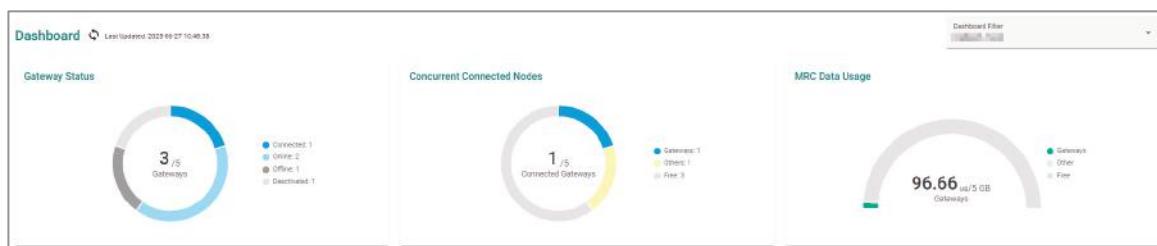
Auto Refresh

By default, the dashboard will automatically refresh the displayed information every 10 seconds. A timestamp will indicate the time the information was last updated.

You can enable or disable this function by clicking the **Auto Refresh** (⟳) icon in the top-left of the dashboard.

⟳ indicates Auto Refresh is enabled.

⟲ indicates Auto Refresh is disabled.

Dashboard Filter

The **Dashboard Filter** located in the top-right corner of the Dashboard lets you show information for specific groups.

Gateway Status

This widget shows the status of associated gateway devices.

UI Setting	Description
Available Gateways	The first number indicates the number of available gateways (Connected, Online). The number after the slash indicates the total number of gateways (Connected, Online, Offline, Deactivated gateways).
Connected	Shows the number of gateways that have successfully established a remote connection.
Online	Shows the number of gateways that are online but have not yet established a remote connection.
Offline	Shows the number of gateways that are offline or unable to connect to the MRC Quick Link server. ✎ **Note** When the gateway exhibits any of the following behaviors, it will appear as offline in MRC Quick Link: • Clicking **RESET KEY** on the MRC settings page in the gateway's web console. • Clicking **Reset to Defaults** in the gateway's web console. • Physically pressing the reset button on the hardware.
Deactivated	Shows the number of gateways that have been added but have not been successfully activated.

Concurrent Connected Nodes

This widget shows the status of the concurrent connected nodes.
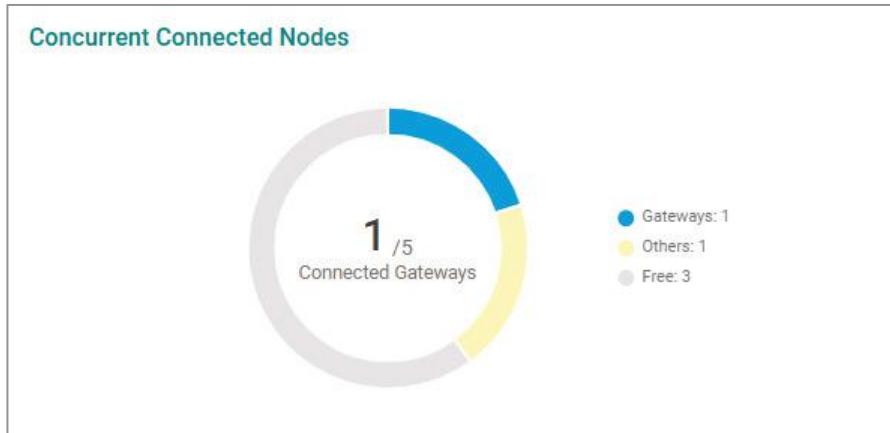
UI Setting	Description
Connected Gateways	The first number indicates the number of gateways that have successfully established a remote connection. The number after the slash indicates the total number of concurrent connected nodes in the license.
Gateways	Shows the number of gateways that have successfully established a remote connection within the specific group.
Others	Shows the number of the concurrent connected nodes used outside of the connected gateway, including connected clients and concurrent connected nodes used by other groups.
Free	Shows the number of remaining nodes on the license that can still be used to set up remote connections.

Data Usage

This widget shows the overall data usage of the gateways using the MRC Quick Link service.

MRC Data Usage

96.66 MB/5 GB
Gateways

- Gateways
- Other
- Free
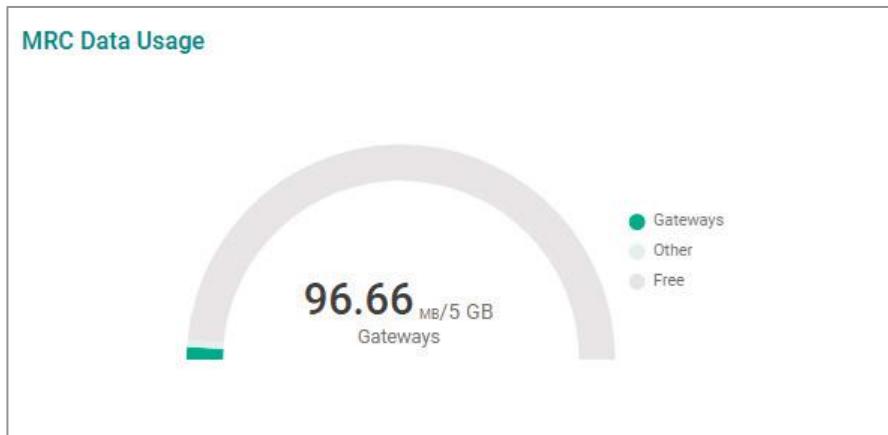
UI Setting	Description
Gateways	The first number indicates the data used by gateways in the specified group. The number after the slash indicates the total available data on the license.
Other	Shows the data usage of devices other than the gateways, including clients and data used by other groups.
Free	Shows the amount of available data left on the license.

Gateway List

Menu Path: Gateway Management

The **Gateway List** screen lets you view and configure gateway settings.

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

Edit Columns

The **Edit Columns** feature lets you reorder and hide columns in the gateway table.
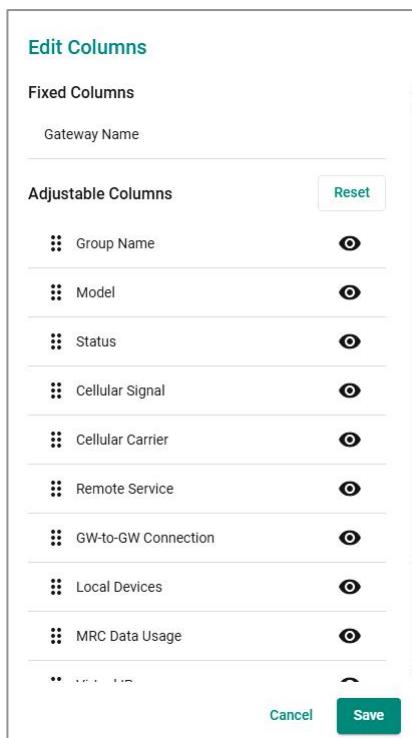
Click and hold the item (⣿) icon, then drag the column to the desired position.

Click the **Hide** (👁) icon to hide the column. If hidden, click the **Unhide** (👁̸) icon to unhide the column.

Click the **Reset** button to restore the default column display settings.

Gateway Table

UI Setting	Description
Gateway Name	Shows the name of the gateway.

UI Setting	Description
Group Name	Shows the name of the group the gateway belongs to.
Model	Shows the model name of the gateway.
Status	Shows the status of the gateway.

Connected: The gateway has successfully established a remote connection. When the gateway status is "Connected", it will consume one node of the assigned Concurrent Connected Node license.

Online: The gateway is online but has not yet established a remote connection.

Offline: The gateway is unable to connect to the MRC Quick Link server.

Deactivated: The gateway has been added but has not been activated yet.

Cellular Signal	Shows the cellular signal strength of the gateway. The strength of the cellular signal is a composite evaluation based on RSRP (Reference Signal Received Power), RSRQ (Reference Signal Received Quality), and SINR (Signal-to-interference-plus-noise Ratio).

: Good

: Fair

: Poor

: No Signal

> **✎ Note**
>
> If the gateway is using a wired network connection (Ethernet WAN), the cellular strength indicator will show as "No Signal".

Cellular Carrier	Shows the cellular carrier.
Remote Service	Shows the remote service status of the gateway.

Enabled: The gateway is allowed to establish a remote connection.

Disabled: The gateway is not allowed to establish a remote connection.

GW-to-GW Connection	Shows the status of the gateway-to-gateway connection feature.

Enabled: The gateway is allowed to establish a remote connection to other gateways in the same group that also have GW-to-GW Connection enabled. When an applicable gateway is online, it will automatically establish the remote connection and switch to the "Connected" status.

Disabled: The gateway is not allowed to establish a remote connection to other gateways.

UI Setting	Description
Local Devices	Shows the number of local devices associated with the gateway.
MRC Data Usage	Shows the MRC data usage of the gateway. When the gateway has established a remote connection, the outbound traffic transmitted from the gateway is calculated as data usage of the MRC service and consumes available data from the assigned Data Usage license.
Virtual IP	Shows the virtual IP of the gateway for remote connections.
Connected Clients	Shows the number of clients connected to the gateway.
Last Connected	Shows the time the gateway last established a remote connection. If the gateway has an active remote connection, this field will show as "---".
Replace Gateway	Replace the old gateway with a new one while retaining the existing MRC service settings. This provides a seamless way to switch gateways.

Add Gateway

Menu Path: Gateway Management

Click the **Add** ( ) icon in the top-left corner of the gateway list to add a new gateway.

Select a gateway model and click **Next**.

The available settings will vary depending on which **Model** is selected.

Add Gateway - MRC-1002

If **MRC-1002** is selected as the **Model**, configure the following settings:

1. Gateway Settings

UI Setting	Description	Valid Range	Default Value
Gateway Name	Enter a name for the gateway.	1 to 64 characters	N/A
Group	Select the group to assign the gateway to.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Remote Service	Enable or disable the remote connection service on the gateway. Enabled: The gateway is allowed to establish a remote connection. Disabled: The gateway is not allowed to establish a remote connection. ✎ **Note** If you do not require remote connections it is recommended to disable this function.	Enabled / Disabled	Enabled
Location	Enter the location information for the gateway.	0 to 64 characters	N/A
Map Coordinates - Latitude and Longitude	Enter the latitude and longitude coordinates for the gateway. ✎ **NOTE** The latitude and longitude information will be used to visualize the gateway on the interactive world map. Refer to the **Show Gateway Location** section for more information.	-90 to 90 / -180 to 180	N/A
Lock to MAC Address	Enter the MAC address of the gateway to bind the gateway to this MAC address. If it does not match the configured MAC, the gateway will not activate successfully. If left blank, the gateway will not be bound.	MAC Address	N/A
Broadcast Forwarding	Enable or disable the Broadcast Forwarding function of the gateway. Some applications may rely on broadcasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward broadcast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward broadcast network traffic to MRC Clients.	Enabled / Disabled	Disabled
Multicast Forwarding	Enable or disable the Multicast Forwarding function of the gateway. Some applications may rely on multicasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward multicast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward multicast network traffic to MRC Clients.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Auto IP Mapping	Enable or disable the Auto IP Mapping service. In distributed systems, it's common for multiple gateways and local devices to have the same IP settings. When there are multiple gateways with overlapping IP/subnet configurations in an application, enabling auto IP mapping is necessary to ensure a valid connection to the designated gateway. Enabled: The gateway will automatically assign an IP to use with the MRC service. Disabled: The gateway will use its original IP for the MRC service.	Enabled / Disabled	Enabled
Gateway-to-gateway	Enable or disable the Gateway-to-gateway function. Enabled: When connecting to MRC Quick Link, the gateway will automatically establish connections with other gateways in the same group that have this function enabled. Disabled: The gateway will only allow remote connections initiated from the MRC Client. ✎ **Note** When Gateway-to-gateway is enabled, the Broadcast Forwarding and Multicast Forwarding services will be disabled to avoid traffic storms. ✎ **Note** When Gateway-to-gateway is enabled, the Transparent Mode in the Connection Scenario step will be unavailable. ✎ **Note** When Gateway-to-gateway is enabled, the gateway will default to a Connected status and will consume one node of the associated Concurrent Connect Node license.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Tunnel Control	Select the VPN tunneling method for remote connections. Persistent Connection: The gateway will maintain a constant remote connection until manually disconnected. Controlled by key file from USB drive: A remote connection can be established only when a Moxa ABC-02 Series USB device or a USB drive with an activation key is inserted into the gateway. Once the USB drive is removed, the remote connection permission is disabled. Controlled by DI: A remote connection can be established only when a DI signal is received by the gateway. Once the signal is lost, the permission for remote connection is disabled.	Persistent Connection / Controlled by key file from USB drive / Controlled by DI	N/A

Click **Next** to move to the next step.

2. Connection Scenario
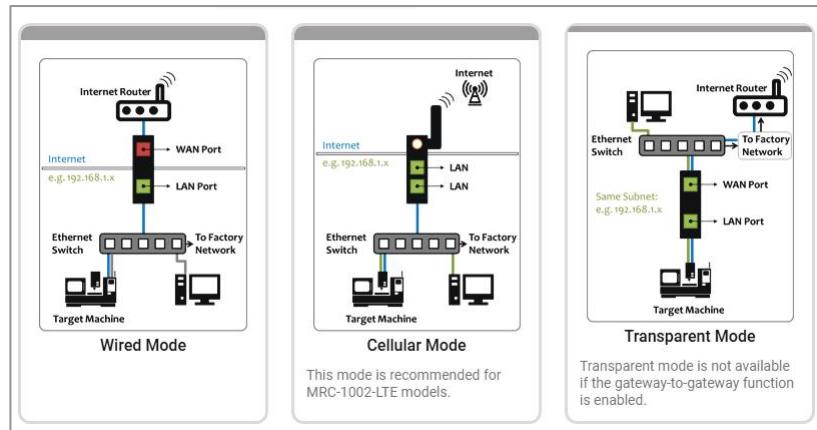
UI Setting	Description
Wired Mode	Connect an external router to access the Internet and establish remote access.
Cellular Mode	Use the cellular interface for Internet access. Both Ethernet ports function as LAN ports for connecting local devices.
Transparent Mode	Use the existing network to access the Internet and establish remote access. Ensure LAN device communication remains transparent to the network. ✎ **Note** Transparent mode is not available if the gateway-to-gateway function is enabled.

Wired Mode

UI Setting	Description	Valid Range	Default Value
LAN Settings			
IP Address	Enter the IP address of the device.	Valid IP address	N/A
Subnet Mask	Select the subnet mask of the device.	Valid Subnet Mask	N/A
WAN Settings			
IP Address Mode	Select the WAN IP address mode. DHCP: The gateway is assigned an IP address and subnet mask automatically by a DHCP server. Static: Manually specify the gateway's IP address and subnet mask.	Static / DHCP	Static
IP Address	Enter the IP address for the WAN port. This setting does not show in DHCP mode.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Subnet Mask	Select the subnet mask for the WAN port. This setting does not show in DHCP mode.	Valid subnet mask	N/A
Gateway	Enter the gateway address for the WAN port. This setting does not show in DHCP mode.	Valid IP address	N/A
Primary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Secondary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Tertiary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A

Click **Next** to move to the next step.

Cellular Mode

UI Setting	Description	Valid Range	Default Value
LAN Settings			
IP Address	Enter the IP address of the device.	Valid IP address	N/A
Subnet Mask	Select the subnet mask of the device.	Valid Subnet Mask	N/A
WAN Settings			
Carrier	Select the carrier to use with the SIM card.	Generic / AT&T / Verizon	Generic
APN	Specify the access point network (APN) information provided by your cellular carrier if they require it.	0 to 64 characters	N/A
PIN	Enter the PIN number to unlock the SIM card.	0 to 6 characters	N/A
Username	Enter username for Internet access. This is provided by your carrier.	0 to 64 characters	N/A
Password	Enter password for Internet access. This is provided by your carrier.	6 to 64 characters	N/A
Cellular Keep Alive	When the cellular connection loses Internet access, the device will automatically restart the cellular connection to the carrier.	Enabled / Disabled	Enabled
Cellular Watchdog	When the cellular system stops working, the device will restart the cellular hardware to reinitialize the connection.	Enabled / Disabled	Disabled
Primary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Secondary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Tertiary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A

Click **Next** to move to the next step.

Transparent Mode

UI Setting	Description	Valid Range	Default Value
WAN Settings			
IP Address Mode	Select the WAN IP address mode. DHCP: The gateway is assigned an IP address and subnet mask automatically by a DHCP server. Static: Manually specify the gateway's IP address and subnet mask.	Static / DHCP	Static
IP Address	Enter the IP address for the WAN port. This setting does not show in DHCP mode.	Valid IP address	N/A
Subnet Mask	Select the subnet mask for the WAN port. This setting does not show in DHCP mode.	Valid subnet mask	N/A

UI Setting	Description	Valid Range	Default Value
Gateway	Enter the gateway address for the WAN port. This setting does not show in DHCP mode.	Valid IP address	N/A
Primary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Secondary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A
Tertiary DNS Server	Enter the DNS server address.	Valid DNS Server address	N/A

Click **Next** to move to the next step.

3. Local Device List

Click the **Add** ( ) icon to add devices connected to the gateway to the local device list for monitoring and for establishing remote connections.

A single gateway supports up to 25 local devices.

Click **Apply** without adding devices to skip this step and add local devices later. Refer to the Add Local Device section for information on how to add local devices.
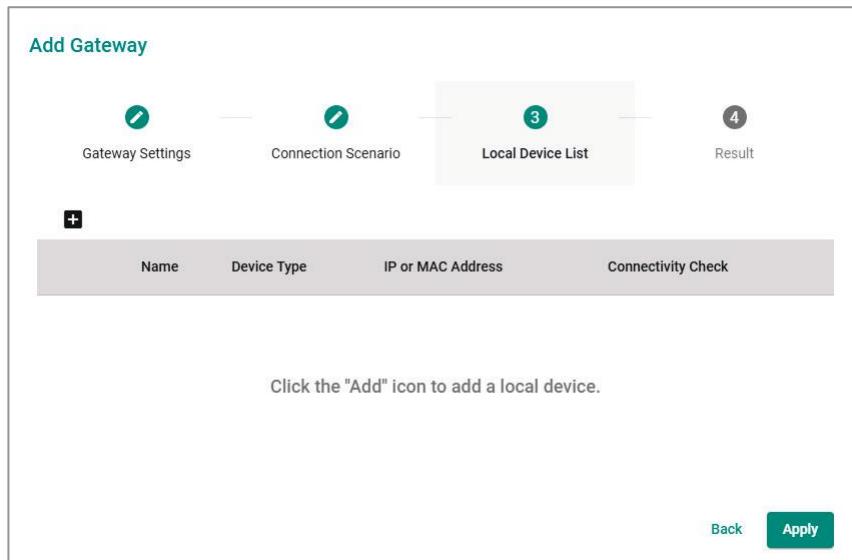
4. Result

Click **Copy** to copy the shown activation key to your clipboard. Paste this activation key into the **Moxa Remote Connect** settings page in the MRC-1002 gateway's interface. Alternatively, click **Download** to download the activation key as a file onto a USB drive. Insert the USB with the key file into the MRC-1002 gateway to activate the device. Refer to MRC-1002.

✎ **Note**

The activation key generated for the MRC-1002 can only be used with MRC-1002 Series devices. Do not apply it to other gateway models.
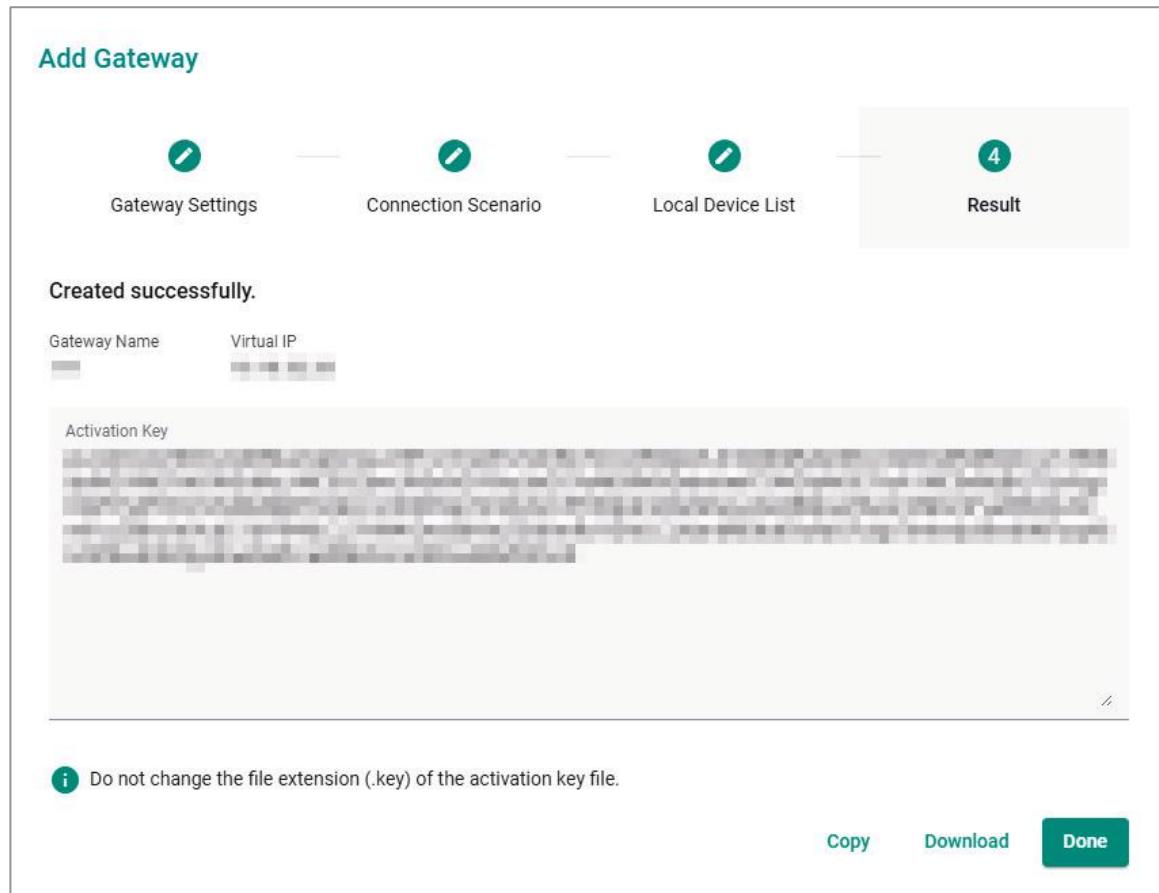
Add Gateway - OnCell 3120

If **OnCell 3120** is selected as the **Model**, configure the following settings:

1. Gateway Settings

UI Setting	Description	Valid Range	Default Value
Gateway Name	Enter a name for the gateway.	1 to 64 characters	N/A
Group	Select a group to assign the gateway to.	N/A	N/A
Remote Service	Enable or disable the remote connection service on the gateway. Enabled: The gateway is allowed to establish a remote connection. Disabled: The gateway is not allowed to establish a remote connection. ✎ **Note** If you do not require remote connections it is recommended to disable this function.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Map Coordinates	Enter the latitude and longitude coordinates for the gateway. ✎ **NOTE** The latitude and longitude information will be used to visualize the gateway on the interactive world map. Refer to the **Show Gateway Location** section for more information.	-90 to 90 / -180 to 180	N/A
Lock to MAC Address	Enter the MAC address of the gateway to bind the gateway to this MAC address. If it does not match the configured MAC, the gateway will not activate successfully. If left blank, the gateway will not be bound.	MAC Address	N/A
Broadcast Forwarding	Enable or disable the Broadcast Forwarding function of the gateway. Some applications may rely on broadcasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward broadcast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward broadcast network traffic to MRC Clients.	Enabled / Disabled	Disabled
Multicast Forwarding	Enable or disable the Multicast Forwarding function of the gateway. Some applications may rely on multicasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward multicast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward multicast network traffic to MRC Clients.	Enabled / Disabled	Disabled
Auto IP Mapping	Enable or disable the Auto IP Mapping service. In distributed systems, it's common for multiple gateways and local devices to have the same IP settings. When there are multiple gateways with overlapping IP/subnet configurations in an application, enabling auto IP mapping is necessary to ensure a valid connection to the designated gateway. Enabled: The gateway will automatically assign an IP to use with the MRC service. Disabled: The gateway will use its original IP for the MRC service.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Gateway-to-gateway	Enable or disable the Gateway-to-gateway function. Enabled: When connecting to MRC Quick Link, the gateway will automatically establish connections with other gateways in the same group that have this function enabled. Disabled: The gateway will only allow remote connections initiated from the MRC Client. ✎ **Note** When Gateway-to-gateway is enabled, the Broadcast Forwarding and Multicast Forwarding services will be disabled to avoid traffic storms. ✎ **Note** When Gateway-to-gateway is enabled, the gateway will default to a Connected status and will consume one node of the associated Concurrent Connect Node license.	Enabled / Disabled	Disabled
Tunnel Control	Select the VPN tunneling method for remote connections. Persistent Connection: The gateway will maintain a constant remote connection until manually disconnected. Controlled by key file from USB drive: A remote connection can be established only when a Moxa ABC-02 Series USB device or a USB drive with an activation key is inserted into the gateway. Once the USB drive is removed, the remote connection permission is disabled.	Persistent Connection / Controlled by key file from USB drive	N/A

Click **Next** to move to the next step.

2. Local Device List

Click the **Add** (➕) icon to add devices connected to the gateway to the local device list for monitoring and for establishing remote connections.

A single gateway supports up to 25 local devices.

Click **Apply** without adding devices to skip this step and add local devices later. Refer to the Add Local Device section for information on how to add local devices.

3. Result

Click **Copy** to copy the shown activation key to your clipboard. Paste this activation key into the **Moxa Remote Connect** settings page in the OnCell 3120 gateway's interface. Alternatively, click **Download** to download the activation key as a file onto a Moxa ABC-02 Series USB device or a USB drive. Insert the ABC-02 USB or USB drive with the key file into the OnCell 3120 gateway to activate the device. Refer to OnCell 3120.

> ✏ **Note**
>
> The activation key generated for the OnCell 3120 can only be used with the OnCell 3120 Series devices. Do not apply it to other gateway models.

Add Gateway - OnCell G4302 & OnCell G4308

If **OnCell G4302** or **OnCell G4308** is selected as the **Model**, configure the following settings:

1. Gateway Settings

UI Setting	Description	Valid Range	Default Value
Gateway Name	Enter a name for the gateway.	1 to 64 characters	N/A
Group	Select the group to assign the gateway to.	N/A	N/A
Service	Enable or disable the remote connection service on the gateway. Enabled: The gateway is allowed to establish a remote connection. Disabled: The gateway is not allowed to establish a remote connection. ✎ **Note** If you do not require remote connections it is recommended to disable this function.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Map Coordinates	Synchronize the gateway's location data with GNSS coordinates. Enabled: The gateway will automatically synchronize GNSS information to MRC Quick Link. To use this option, the GNSS function must be enabled on the gateway. Disabled: The gateway will not synchronize GNSS information to MRC Quick Link. You will be required to manually enter the latitude and longitude coordinates for the gateway. ✎ **Note** The latitude and longitude information will be used to visualize the gateway on the interactive world map. Refer to the **Show Gateway Location** section for more information.	Enabled / Disabled	Enabled
Lock to MAC Address	Enter the MAC address of the gateway to bind the gateway to this MAC address. If it does not match the configured MAC, the gateway will not activate successfully. If left blank, the gateway will not be bound.	MAC Address	N/A
Broadcast Forwarding	Enable or disable the Broadcast Forwarding function of the gateway. Some applications may rely on broadcasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward broadcast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward broadcast network traffic to MRC Clients.	Enabled / Disabled	Disabled
Multicast Forwarding	Enable or disable the Multicast Forwarding function of the gateway. Some applications may rely on multicasting to discover services or facilitate communication, such as PLC management software. Enabled: The gateway is allowed to forward multicast network traffic to MRC Clients. Disabled: The gateway is not allowed to forward multicast network traffic to MRC Clients.	Enabled / Disabled	Disabled

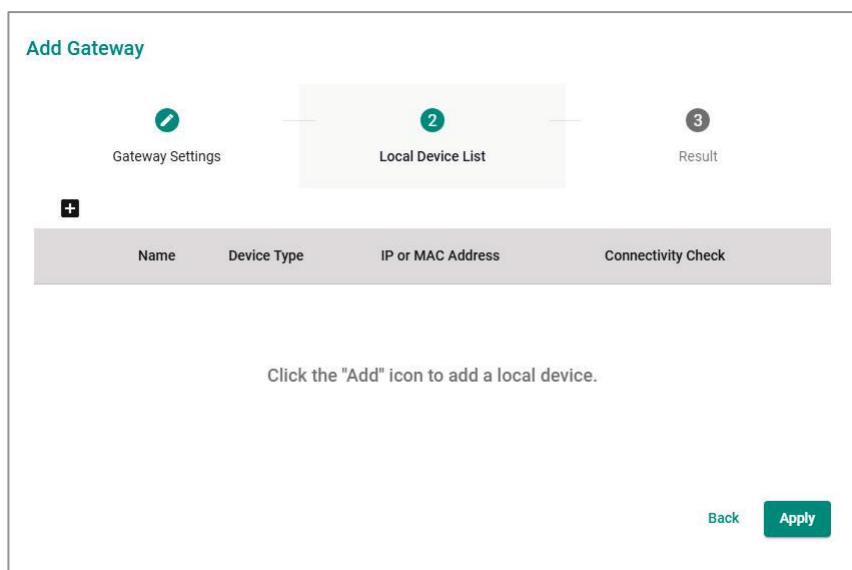| UI Setting	Description	Valid Range	Default Value
Auto IP Mapping	Enable or disable the Auto IP Mapping service. In distributed systems, it's common for multiple gateways and local devices to have the same IP settings. When there are multiple gateways with overlapping IP/subnet configurations in an application, enabling auto IP mapping is necessary to ensure a valid connection to the designated gateway. Enabled: The gateway will automatically assign an IP to use with the MRC service. Disabled: The gateway will use its original IP for the MRC service.	Enabled / Disabled	Enabled
Gateway-to-gateway	Enable or disable the Gateway-to-gateway function. Enabled: When connecting to MRC Quick Link, the gateway will automatically establish connections with other gateways in the same group that have this function enabled. Disabled: The gateway will only allow remote connections initiated from the MRC Client. ✎ **Note** When Gateway-to-gateway is enabled, the Broadcast Forwarding and Multicast Forwarding services will be disabled to avoid traffic storms. ✎ **Note** When Gateway-to-gateway is enabled, the gateway will default to a Connected status and will consume one node of the associated Concurrent Connect Node license.	Enabled / Disabled	Disabled
Tunnel Control	Select the VPN tunneling method for remote connections. Persistent Connection: The gateway will maintain a constant remote connection until manually disconnected. Controlled by key file from USB drive: A remote connection can be established only when a Moxa ABC-02 Series USB device or a USB drive with an activation key is inserted into the gateway. Once the USB drive is removed, the remote connection permission is disabled. Controlled by DI: A remote connection can be established only when a DI signal is received by the gateway. Once the signal is lost, the permission for remote connection is disabled.	Persistent Connection / Controlled by key file from USB drive / Controlled by DI	N/A

Click **Next** to move to the next step.

2. Local Device List

Click the **Add** ( ) icon to add devices connected to the gateway to the local device list for monitoring and for establishing remote connections.

A single gateway supports up to 25 local devices.

Click **Apply** without adding devices to skip this step and add local devices later. Refer to the Add Local Device section for information on how to add local devices.

3. Result

Click **Copy** to copy the shown activation key to your clipboard. Paste this activation key into the **Moxa Remote Connect** settings page in the OnCell G4302 gateway's interface. Alternatively, click **Download** to download the activation key as a file onto a USB drive. Insert the USB with the key file into the OnCell G4302 or OnCell G4308 gateway to activate the device. Refer to OnCell G4302 & OnCell G4308.

> ✎ **Note**
>
> The activation key generated for the OnCell G4302 can only be used with OnCell G4302 Series devices.
>
> The activation key generated for the OnCell G4308 can only be used with OnCell G4308 Series devices.
>
> Do not apply it to other gateway models. The activation keys for the OnCell G4302 and G4308 Series are not interchangeable.

Edit Gateway

Menu Path: Gateway Management

Click the **Edit** (✏️) icon in the row of the gateway you want to edit.

When finished, click **Apply** to save your changes.

Show Gateway Location

Menu Path: Gateway Management

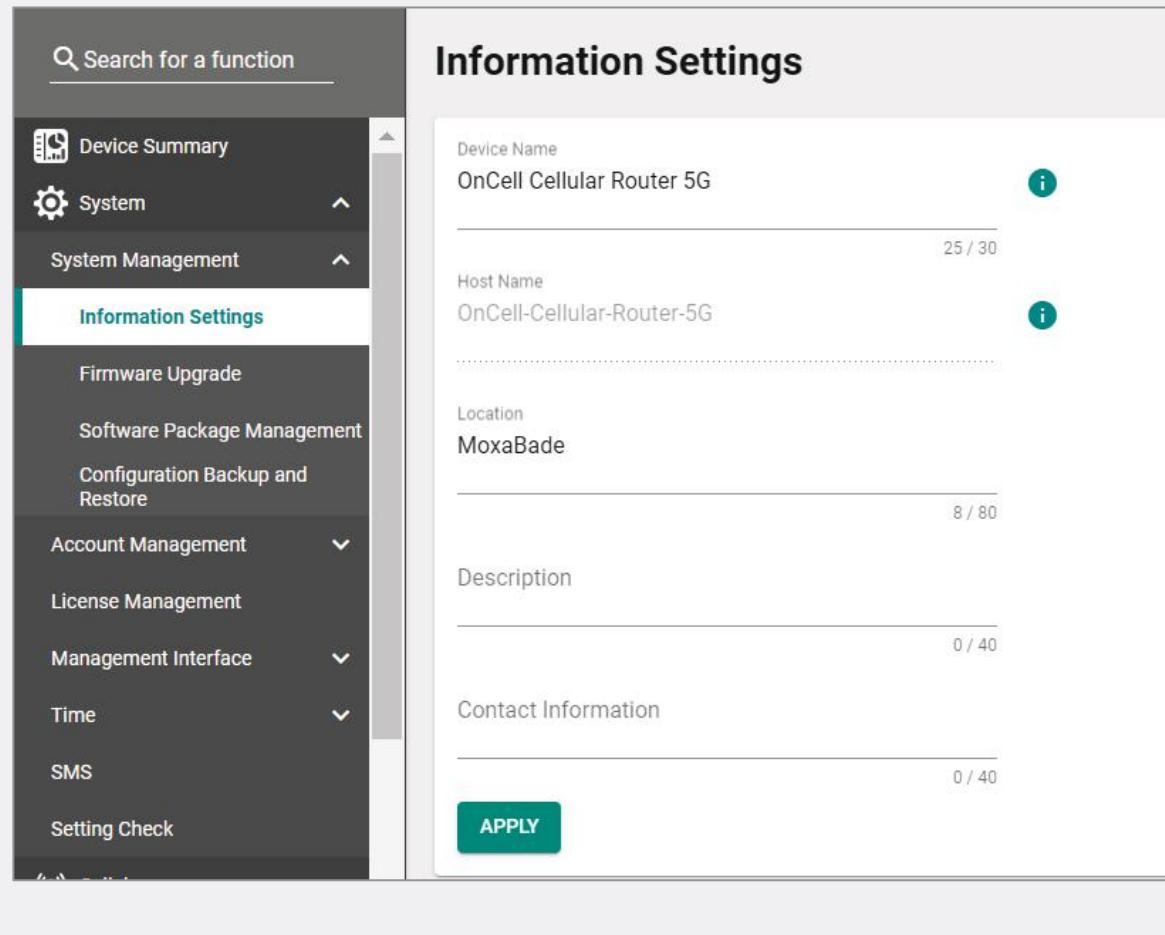Click the **Location** (📍) icon in the row of the gateway you want to view the location of.

The location shown on the map is based on the gateway's synchronized GNSS information or the user-specified latitude and longitude coordinates. To configure the latitude and longitude settings of the gateway, refer to the Add Gateway section.

Download Gateway Activation Key

Menu Path: Gateway Management
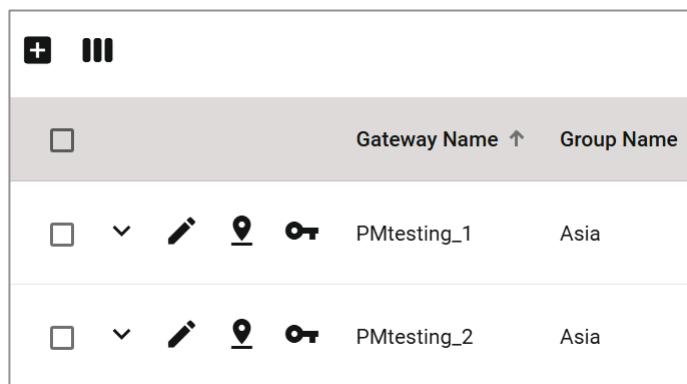
Clicking the **Activation Key** ( ) icon in the row of the gateway you want to download the activation key for. In the Activation Key window, click **Copy** to copy the key to your clipboard, or click **Download** to download the key to your system.
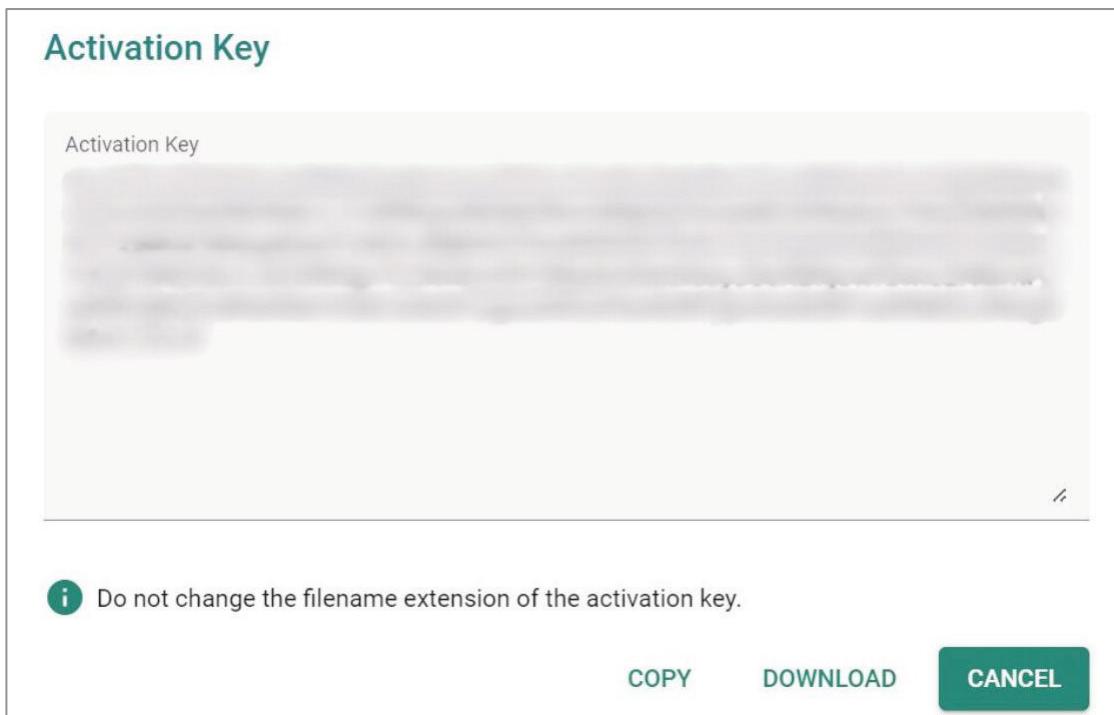
Select Gateways

If you select any gateway, additional function buttons will become available.

Delete Gateway

Check the box of the gateway(s) you want to delete and click the **Delete** (🗑) icon in the top-left corner of the table.

When prompted, click **DELETE** to delete the selected gateway(s).
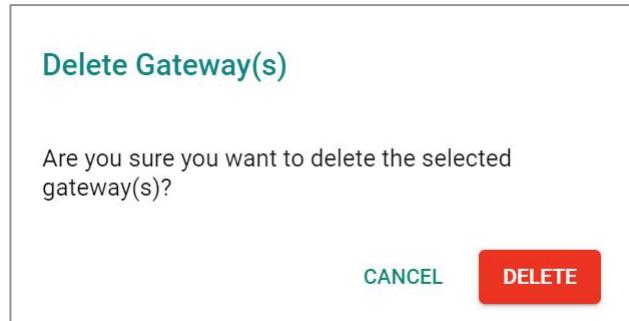
Download All Keys as Zip File

Click the **Download All Keys as Zip File** (🔑) icon in the top-left corner of the table to download the activation keys of the selected gateways as a ZIP file.

Disconnecting Gateways

Menu Path: Gateway Management

You can manually terminate the remote connection of gateways with the Connected status. Check the box of the gateway(s) that you want to disconnect and click the

Disconnect ( ) icon in the top-left corner of the table.

When prompted, click **DISCONNECT** to disconnect the gateway(s).
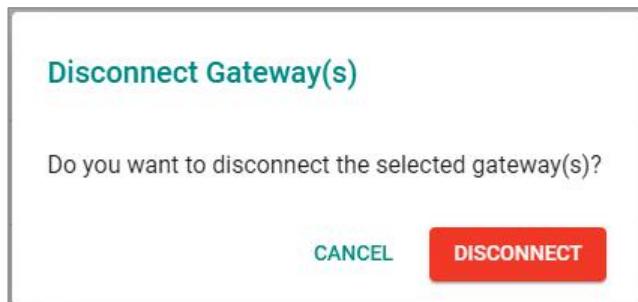
Deactivating Gateways

Menu Path: Gateway Management

You can manually deactivate a gateway to unbind it from the MRC service. Deactivating a gateway will invalidate the activation key and immediately disconnect the gateway. Deactivated gateways will appear as Deactivated in the gateway table.

To re-activate the gateway, you will need to obtain a new activation key. Refer to the **Add Gateway** section.

Check the box of the gateway(s) you want to deactivate and click the **Deactivate** ( ) icon in the top-left corner of the table.

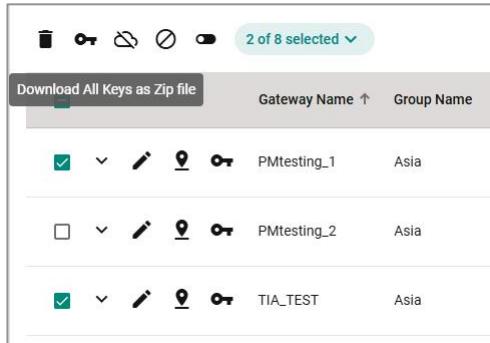When prompted, click **DEACTIVATE** to deactivate the gateway(s).
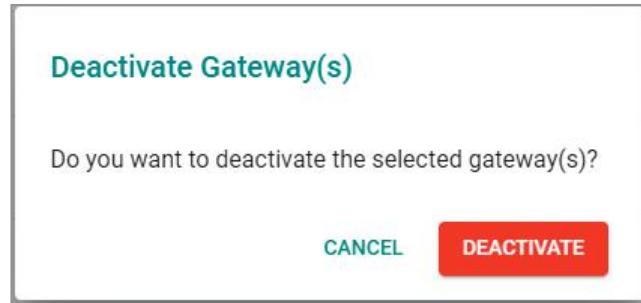
Toggle Remote Service

Menu Path: Gateway Management

Check the box of the gateway(s) that you want to enable or disable remote services for

and click the **Toggle Remote Service** ( ) icon in the top-left corner of the table.

When prompted, select **Enabled** or **Disabled** and click **Apply**.
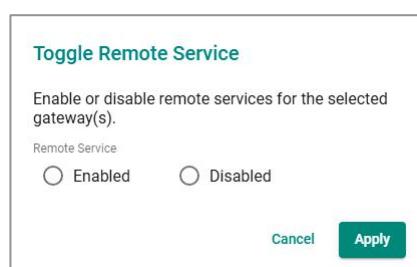
> ✎ **Note**
>
> Disabling remote services will terminate all established remote connections and will change the gateway's status from Connected to Online.

Local Device Table

Menu Path: Gateway Management

Click the **Expand** (⌄) and **Collapse** (⌃) icons in the row of the gateway to expand

or collapse the list of local devices of that gateway.

UI Setting	Description
Name	Shows the name of the local device.
Status	Shows the status of the local device. ● Online: The local device has been successfully detected by the gateway. ● Offline: The local device could not be detected by the gateway. ● ---: The status of the local device is unknown because the gateway was unable to retrieve information on the device.
Device Type	Shows the type of local device. IP Ethernet Device: The IP is configured for the device itself. The connection to the device is confirmed by pinging the device's IP. Layer 2 Ethernet Device: The device has an Ethernet interface but no IP configuration. The connection to the device is confirmed through the physical Ethernet port link. Serial Device: The device has a serial interface. The connection to the device is confirmed through the physical serial port link.
IP or MAC Address	Shows the IP or MAC address of the local device.
Virtual IP	Shows the virtual IP of the local device for remote connections.
Connectivity Check	Shows the type and the checking frequency for verifying the connectivity of the local device.

UI Setting	Description
Rules	Shows the remote access allowlist rules configured for the device. Click the **Rules** (▤) icon.

Add Local Device

Menu Path: Gateway Management

Expand the local device list for the gateway and click the **Add** (➕) icon to add devices connected to the gateway as local devices under the gateway for monitoring remote connections.

A single gateway supports up to 25 local devices.

> ✎ **Note**
>
> Support for local devices depends on the gateway model. Not all gateways support this feature.

Local Device Settings

Available settings and options depend on the selected device type.

UI Setting	Description	Valid Range	Default Value
Local Device Name	Enter a name for the local device.	1 to 64 characters	N/A
Device Type	Select the type of local device. Configurable settings depend on the selected type. IP Ethernet Device: The IP is configured for the device itself. The connection to the device is confirmed by pinging the device's IP. Layer 2 Ethernet Device: The device has an Ethernet interface but no IP configuration. The connection to the device is confirmed through the physical Ethernet port link. Serial Device: The device has a serial interface. The connection to the device is confirmed through the physical serial port link.	IP Ethernet Device Layer 2 Ethernet Device Serial Device	IP Ethernet Device

IP Ethernet Device

If you select **IP Ethernet Device** as the **Device Type**, configure the following settings:

UI Setting	Description	Valid Range	Default Value
IP Address	Enter the IP address of the device.	Valid IP address	N/A
Virtual IP	Select the virtual IP of the device. The system will assign an available IP by default.	N/A	N/A
NAT IP	Enter the NAT IP of the device. It should be in the same subnet as your Ethernet WAN. ✏ **Note** The NAT IP is only shown when using the MRC-1002 in Wired Mode.	Valid IP address	N/A
Connectivity Check Mode	Select the method for checking the connection to the device. Ping Check: The gateway will send out alive check packets to check the connection to the device at the specified Ping Interval. Disable: The gateway will not perform connectivity checks for the device.	Ping Check / Disable	Ping Check
Ping Interval	Enter the interval (in seconds) at which the gateway will send out an alive check packet.	1 to 86400	10

Layer 2 Ethernet Device

If you select **Layer 2 Ethernet Device** as the **Device Type**, configure the following settings:

UI Setting	Description	Valid Range	Default Value
MAC Address	Enter the MAC address of the device.	Valid MAC address	N/A
Connectivity Check Mode	Select the method for checking the connection to the device. Port Link: The gateway will constantly check the status of the specified physical Ethernet port to check the connection to the device. Disable: The gateway will not perform connectivity checks for the device.	Port Link Disable	Port Link
Port	Select the port the device is connected to.	Port number	N/A

Serial Device

If you select **Serial Device** as the **Device Type**, configure the following settings:

Add Local Device

Local Device Settings   Rules

Local Device Name *

0 / 64

Device Type *
Serial Device

Connectivity Check Method *
Serial Link

Cancel   Apply

UI Setting	Description	Valid Range	Default Value
Connectivity Check Mode	Select the method for checking the connection to the device. Serial Link: The gateway will constantly check the status of the serial port to check the connection to the device. Disable: The gateway will not perform connectivity checks for the device.	Serial Link / Disable	Serial Link

Rules

Menu Path: Gateway Management

The **Rules** tab is used to set up the allowlist rules for remote connections to the local device. To access the **Rules** tab, add or edit a local device and navigate to the **Rules** tab.

Available settings and options depend on the selected **Type**.

> ✎ **Note**
>
> Each local device supports a maximum of 16 rules.

UI Setting	Description	Valid Range	Default Value
Type	Select the protocol type allowed for remote connections.	All	All
		TCP (All)	
		UDP (All)	
		ICMP	
		TCP (Custom)	
		UDP (Custom)	
		Ethernet/IP I/O Messaging	
		Ethernet/IP Messaging (TCP)	
		Ethernet/IP Messaging (UDP)	
		HTTP	
		HTTPS	
		Modbus/TCP	
		Modbus/UDP	
		RDP-TCP	
		RDP-UDP	
		SNMP	
		SSH	
		Telnet	
Allowed Clients	Select the clients allowed to establish remote connections.	Client list	All Clients

Click the **Add** ( ) icon to add a rule.

Click the **Copy** ( ) icon to copy the rule to the clipboard.

Click the **Add from clipboard** ( ) icon to add a rule copied from the clipboard.

Click the **Delete** ( ) icon to delete the rule.

When finished, click **Apply** to save your changes.

Edit Local Device

Expand the local device list for the gateway and click the **Edit** ( ) icon in the row of the local device you want to edit. Available settings and options depend on the selected device type.

When finished, click **Apply** to save your changes.

Delete Local Device

Expand the local device list for the gateway and click the **Delete** ( ) icon in the row of the local device you want to delete.

When prompted, click **DELETE** to delete the local device.

Delete Local Device

Are you sure you want to delete the device?

CANCEL   **DELETE**
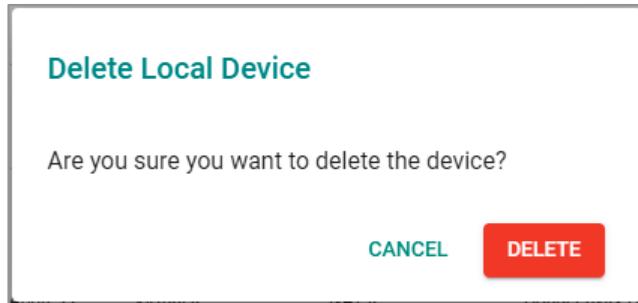
Replace Gateway

Menu Path: Gateway Management

Replacing a gateway lets you migrate the MRC server settings from an existing gateway to a new gateway of the same model. This lets you retain all original configurations without having to add and configure the gateway again on the MRC server.

Click the **Replace Gateway** ( ) icon in the row of the local device you want to replace.

1. Confirm Replacement

Confirm you want to replace the gateway and click **Apply** to move to the next step.

Replace Gateway

① Confirm Replacement   ② Activation Key   ③ Replace Gateway

Are you sure you want to replace the gateway?

Cancel   Apply
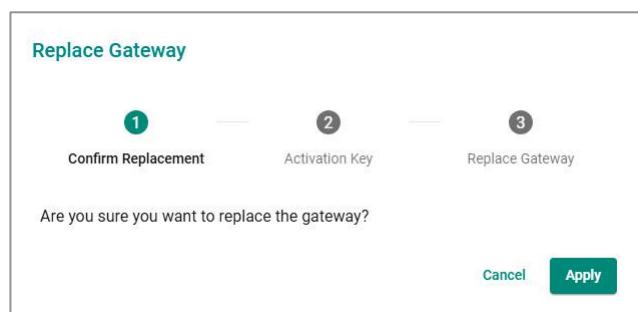
2. Activation Key

Click **Copy** to copy the shown activation key to your clipboard. Alternatively, click **Download** to download the activation key as a file onto a USB drive.
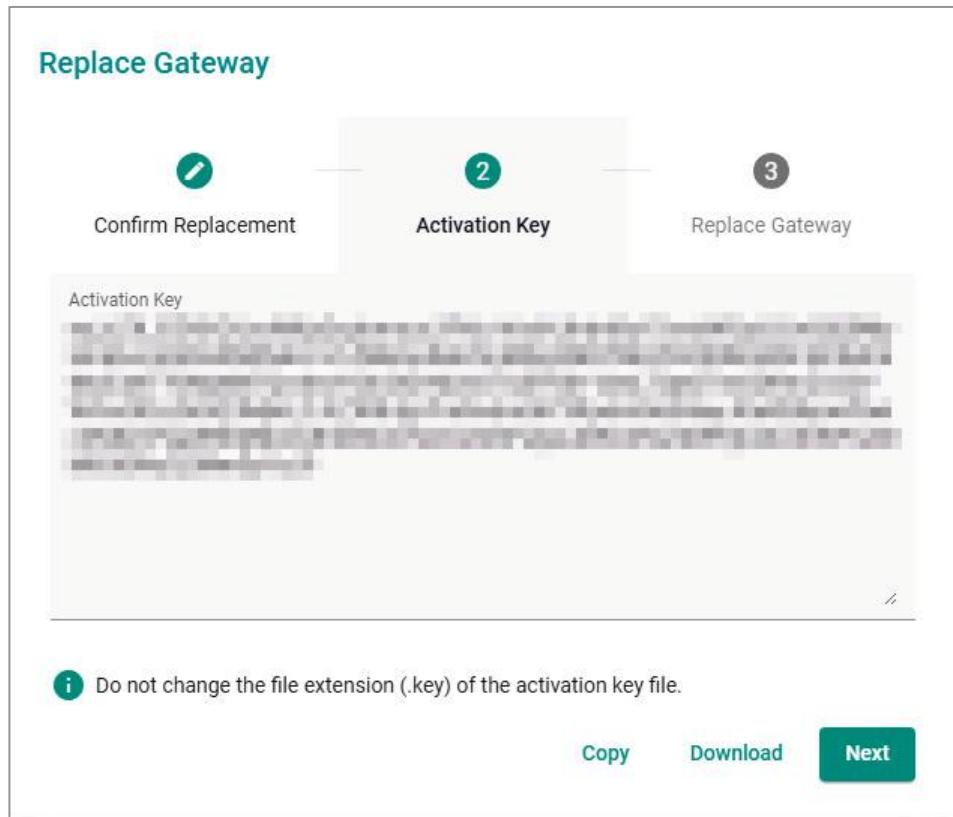
3. Replace Gateway

Click **Close** to close this window. Paste the activation key into the **Moxa Remote Connect** settings page in the replacement gateway's interface, or insert the USB with the key file into the replacement gateway to activate the device.

> ✎ **Note**
> The generated activation key can only be used with gateways of the same model.
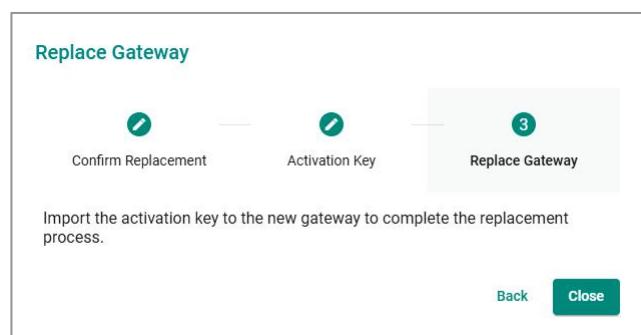
✎ Note

If the activation key has not been applied to the replacement gateway yet, an exclamation mark will show on the Replace icon.
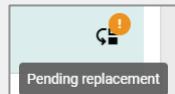
✎ Note

To cancel the replacement process, click the Replace icon again. When prompted to confirm, click Apply.
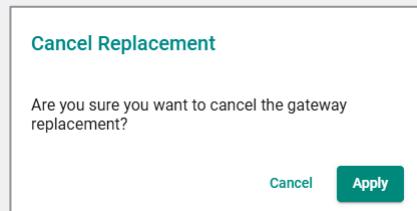
Client Management

From the **Client Management** section, you can check the status of clients and configure client settings.

Dashboard

Menu Path: Client Management

The dashboard shows information about clients, licenses, and data usage.

Auto Refresh

By default, the dashboard will automatically refresh the displayed information every 10 seconds. A timestamp will indicate the time the information was last updated.

You can enable or disable this function by clicking the **Auto Refresh** (↻) icon in the top-left corner of the dashboard.

↻ indicates Auto Refresh is enabled.

⇅ indicates Auto Refresh is disabled.

Dashboard Filter

The **Dashboard Filter** located in the top-right corner of the Dashboard lets you show information for specific groups.

Client Status

This widget shows the status of clients.
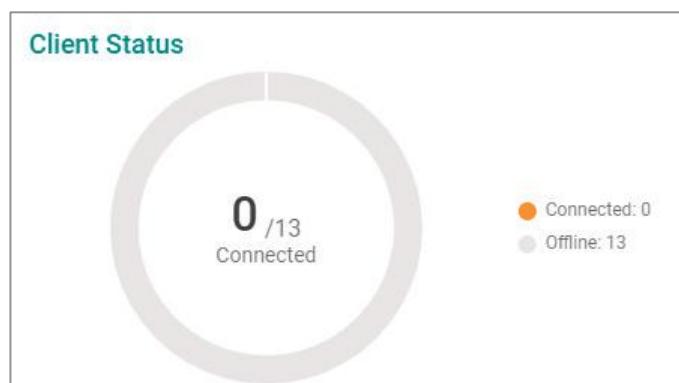
UI Setting	Description
Connected	The first number indicates the number of connected clients. The number after the slash indicates the total number of clients (Connected, Offline).

UI Setting	Description
Connected	Shows the number of clients that have successfully established a remote connection.
Offline	Shows the number of clients that have not yet established a remote connection.

Concurrent Connected Nodes

This widget shows the status of the concurrent connected nodes.
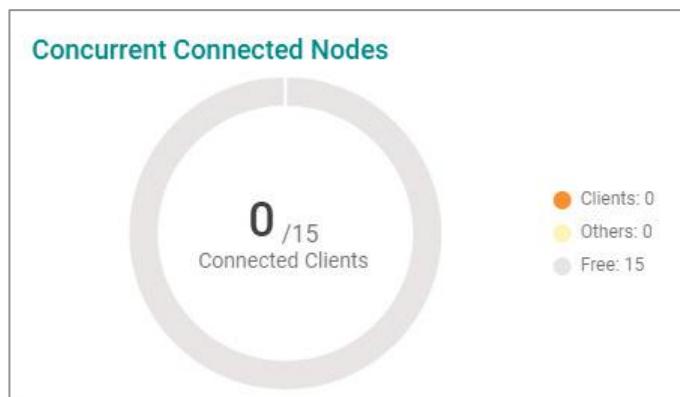
UI Setting	Description
Connected Clients	The first number indicates the number of clients that have successfully established a remote connection. The number after the slash indicates the total number of concurrent connected nodes in the license.
Clients	Shows the number of clients that have successfully established a remote connection within the specified group.
Others	Shows the number of the concurrent connected nodes used besides the connected clients, including connected gateways and concurrent connected nodes used by other groups.
Free	Shows the number of remaining nodes on the license that can still be used to set up remote connections.

MRC Data Usage

This widget shows the overall data usage of the clients using the MRC Quick Link service.
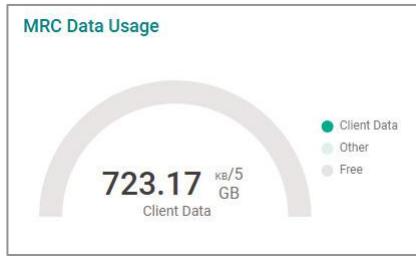
UI Setting	Description
Client Data	The first number indicates the data used by clients in the specified group. The number after the slash indicates the total available data of the license.
Other	Shows the data usage of devices other than the clients, including gateways and data used by other groups.
Free	Shows the amount of available data left on the license.

Client List

Menu Path: Client Management

The Client List screen lets you view and configure client settings.

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

Client Table

UI Setting	Description
Username	Shows the username of the client.
Group Name	Shows the name of the group the client belongs to.
Email	Shows the email address of the client.
Status	Shows the status of the client. 🟢 Connected: The client has successfully established a remote connection. ⚪ Offline: The client has not yet established a remote connection.
Remote Service	Shows the remote service status of the client. Enabled: The client is allowed to establish a remote connection. Disabled: The client is not allowed to establish a remote connection.
MRC Data Usage	Shows the data used by the client.
Virtual IP	Shows the virtual IP of the client for remote connection.
Last Connected	Shows the time the client last established a remote connection. If the client has an active remote connection, this field will show as "---"

Add Client

Menu Path: Client Management

Click the **Add** ( ) icon in the top-left corner of the client list to add a new client.

When finished, click **Apply** to save your changes.

Add Client

Username *

0 / 64

Email *

Group *

Remote Service *
Enabled

Limit Service Period *
Disabled

Two-factor Authentication *
Enabled

Auto Logout *
Enabled

Cancel   Apply

UI Setting	Description	Valid Range	Default Value
Username	Enter a username for the client.	1 to 64 characters	N/A
Email	Enter the email address of the client.	Email address	N/A
Group	Select the groups that this client can access.	Group	N/A
Remote Service	Enable or disable the remote connection service on the client. Enabled: The client is allowed to establish a remote connection. Disabled: The client is not allowed to establish a remote connection.	Enabled / Disabled	Enabled
Limit Service Period	Enable or disable the Limit Service Period feature. Enabled: The client can only establish a remote connection during the specified Service Period. If the Service Period has expired, the **Expired** (⚠) icon will show at the end of the row in the client list. Disabled: The client can establish a remote connection at any time.	Enabled / Disabled	Disabled
Service Period	If **Limit Service Period** is enabled, click the calendar icon to specify the duration of the limited service period.	Date	N/A

UI Setting	Description	Valid Range	Default Value
Two-factor Authentication	Enable or disable Two-factor Authentication. Enabled: After entering the username and password, the client must also enter the Verification Code sent to the specified email address in order to log in. Disabled: The client can log in by just entering the correct username and password.	Enabled / Disabled	Enabled
Auto Logout	Enable or disable the Auto Logout feature. Enabled: After logging in, a pop-up window will appear every 15 minutes asking the client if they wish to continue using the service. If the client does not click **Continue** within 2 minutes, the client will be automatically logged out. Disabled: After logging in, the client will remain logged in disregarding activity.	Enabled / Disabled	Enabled

Edit Client

Menu Path: Client Management

Click the **Edit** ( ) icon in the row of the client you want to edit.

When finished, click **Apply** to save your changes.

UI Setting	Description	Valid Range	Default Value
Username	Shows the client's username which cannot be changed. To modify the username, you must create a new client.	1 to 64 characters	N/A
Email	Enter the email address of this client.	Email address	N/A
Group	Shows the client's group and cannot be changed. To modify the group, you must create a new client.	Group	N/A
Remote Service	Enable or disable the remote connection service on the client. Enabled: The client is allowed to establish a remote connection. Disabled: The client is not allowed to establish a remote connection.	Enabled / Disabled	Enabled

---

UI Setting	Description	Valid Range	Default Value
Limit Service Period	Enable or disable the Limit Service Period feature. Enabled: The client can only establish a remote connection during the specified Service Period. If the Service Period has expired, the **Expired** ( ) icon will show at the end of the row in the client list. Disabled: The client can establish a remote connection at any time.	Enabled / Disabled	Disabled
Service Period	If **Limit Service Period** is enabled, click the calendar icon to specify the duration of the limited service period.	Date	N/A
Two-factor Authentication	Enable or disable Two-factor Authentication. Enabled: After entering the username and password, the client must also enter the Verification Code sent to the specified email address in order to log in. Disabled: The client can log in by just entering the correct username and password.	Enabled / Disabled	Enabled
Auto Logout	Enable or disable the Auto Logout feature. Enabled: After logging in, a pop-up window will appear every 15 minutes asking the client if they wish to continue using the service. If the client does not click **Continue** within 2 minutes, the client will be automatically logged out. Disabled: After logging in, the client will remain logged in disregarding activity.	Enabled / Disabled	Enabled

Toggle Remote Service

Menu Path: Client Management

Check the box of the client(s) that you want to enable or disable remote services for and click the **Toggle Remote Service** ( ) icon in the top-left corner of the table.

When prompted, select **Enabled** or **Disabled** and click **Apply**.
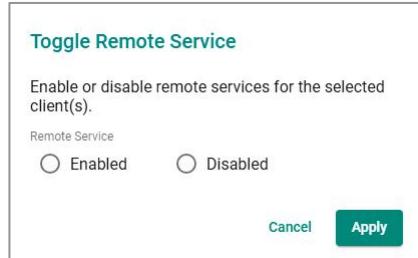
> **✎ Note**
>
> Disabling the remote service will terminate all established remote connections and will change the client's status from Connected to Offline.

Delete Client

Menu Path: Client Management

Check the box of the client(s) that you want to delete and click the **Delete** (🗑) icon in the top-left corner of the table.

When prompted, click **DELETE** to delete the client(s).
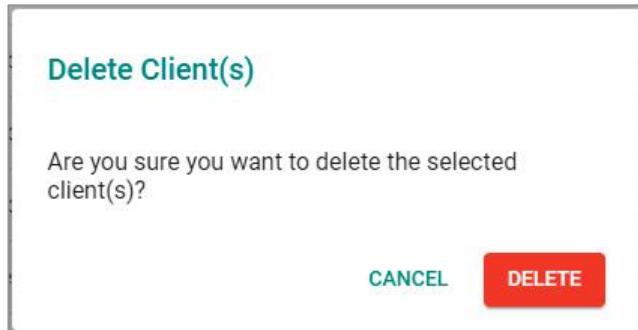
Group Management

From the **Group Management** section, you can check the status of gateways, licenses, data usage, and configure group settings.

This section covers the following topics:
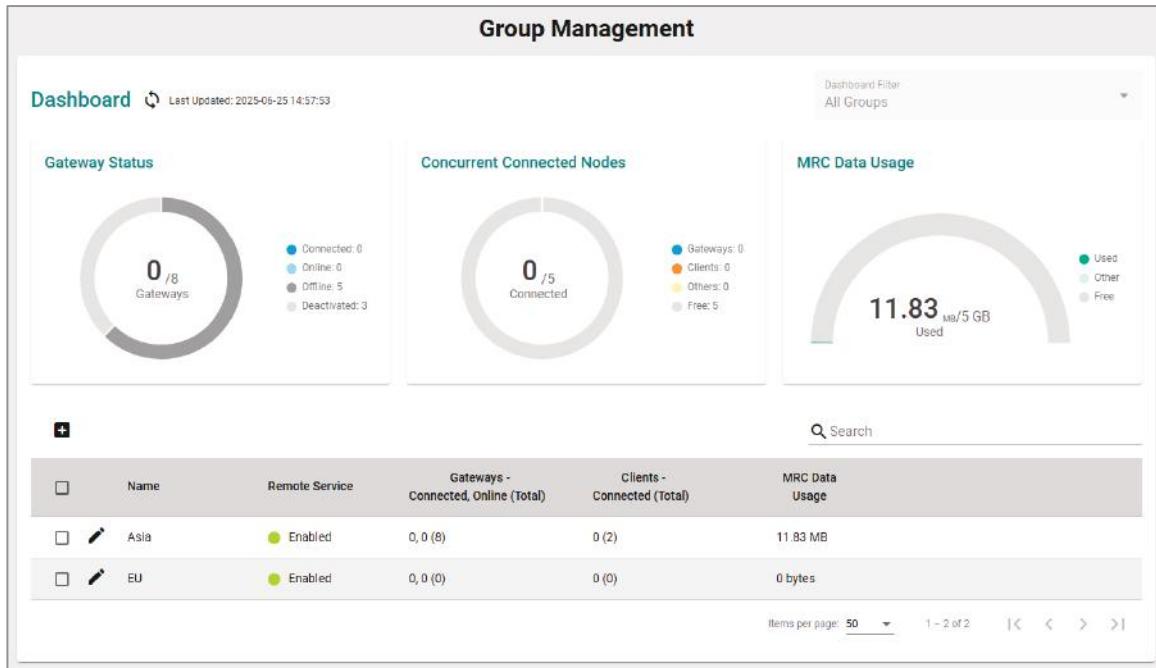
Dashboard

The dashboard shows information about gateways, licenses, and data usage of groups.
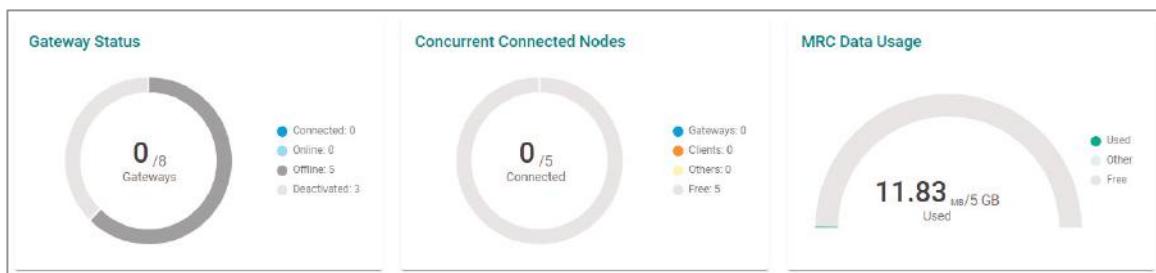
Auto Refresh

By default, the dashboard will automatically refresh the displayed information every 10 seconds. A timestamp will indicate the time the information was last updated.

You can enable or disable this function by clicking the **Auto Refresh** (↻) icon in the top-left corner of the dashboard.

↻ indicates Auto Refresh is enabled.

⇗ indicates Auto Refresh is disabled.

Dashboard Filter

The **Dashboard Filter** located in the top-right corner of the Dashboard lets you show information for specific groups.

Dashboard Filter
All Groups

Gateway Status

This widget shows the status of gateway devices of the shown groups.

Gateway Status

60 /73
Available Gateways

● Connected: 50
● Online: 10
○ Offline: 8
● Deactivated: 5

UI Setting	Description
Available Gateways	The first number indicates the combined number of available gateways (Connected, Online) of all groups. The number after the slash indicates the combined total number of gateways (Connected, Online, Offline, Deactivated gateways) of all groups.
Connected	Shows the number of gateways that have successfully established a remote connection.

UI Setting	Description
Online	Shows the number of gateways that are online but have not yet established a remote connection.
Offline	Shows the number of gateways that are offline or unable to connect to the MRC Quick Link server.
Deactivated	Shows the number of gateways that have been added but have not been successfully activated.

Concurrent Connected Nodes

This widget shows the status of the concurrent connected nodes of the shown groups.
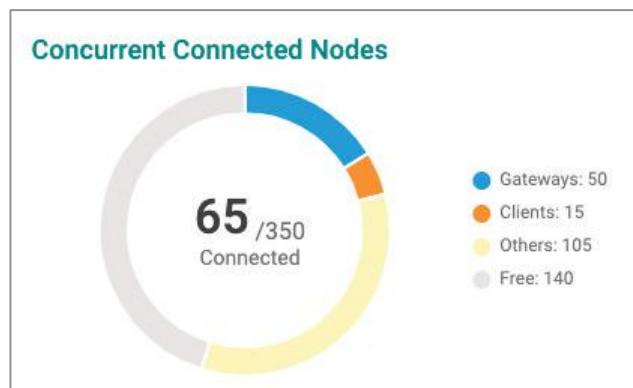
UI Setting	Description
Connected	The first number indicates the combined number of gateways or clients that have successfully established a remote connection of all groups.
	The number after the slash indicates the combined total number of concurrent connected nodes in the licenses of all groups.
Gateways	Shows the number of gateways that have successfully established a remote connection across all groups.
Clients	Shows the number of clients that have successfully established a remote connection across all groups.
Others	Shows the number of nodes used outside of the user's permission group.
Free	Shows the combined number of remaining nodes on the licenses across all groups that can still be used to set up remote connections.

MRC Data Usage

This widget shows the overall data usage of the gateways and clients using the MRC Quick Link service.
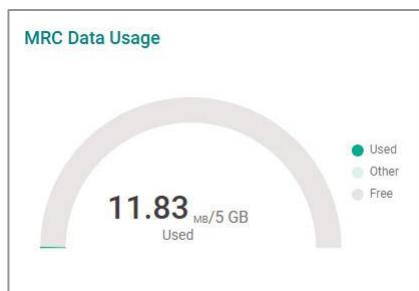
UI Setting	Description
Used	The first number indicates the data used by gateways and clients within the user's permission group. The number after the slash indicates the combined total available data on the licenses across all groups.
Other	Shows the data usage of clients and gateways outside user's permission group.
Free	Shows the combined amount of available data left on the licenses across all groups.

Group List

Menu Path: Group Management

The **Group List** screen lets you view and configure group settings.

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

Group Table

UI Setting	Description
Name	Shows the name of the group.
Remote Service	Shows the remote service status of the group. 🟢 Enabled: Gateways and clients in this group are allowed to establish a remote connection. ⚪ Disabled: Gateways and clients in this group are not allowed to establish a remote connection.
Gateways- Connected, Online (Total)	Shows the status of gateways in the group. The first number indicates the number of connected gateways which have successfully established a remote connection. The second number indicates the number of online gateways which have not yet established a remote connection. The number in parentheses '()' indicates the total number of gateways in the group.
Clients- Connected (Total)	Shows the status of clients in the group. The first number indicates the number of clients which have successfully established a remote connection. The number in parentheses '()' indicates the total number of clients in the group.
MRC Data Usage	Shows the combined data usage of the gateways and clients within this group.

Add Group

Menu Path: Group Management

Click the **Add** ( ) icon in the top-left corner of the group list to add a new group.

UI Setting	Description	Valid Range	Default Value
Group Name	Enter a name for the group.	1 to 64 characters	N/A
Remote Service	Enable or disable the remote connection service for the group. Enabled: Gateways and clients in this group are allowed to establish a remote connection. Disabled: Gateways and clients in this group are not allowed to establish a remote connection.	Enabled/Disabled	Enabled

Edit Group

Menu Path: Group Management

Click the **Edit** (✏) icon in the row of the group you want to edit.

When finished, click **Apply** to save your changes.

UI Setting	Description	Valid Range	Default Value
Group Name	Enter a name for the group.	1 to 64 characters	N/A
Remote Service	Enable or disable the remote connection service for the group. Enabled: Gateways and clients in this group are allowed to establish a remote connection. Disabled: Gateways and clients in this group are not allowed to establish a remote connection.	Enabled/Disabled	Enabled

Delete Group

Menu Path: Group Management

Check the box of the group(s) that you want to delete and click the **Delete** (🗑) icon in the top-left corner of the table.

When prompted, click **DELETE** to delete the group(s).

> ✎ **Note**
>
> Deleting a group will terminate any active remote connections and will delete all gateways and clients under that group.

Delete Group(s)

Deleting a group will also delete all gateways and clients under that group. These devices will need to be manually added to MRC again. Are you sure you want to continue?

Cancel   Delete
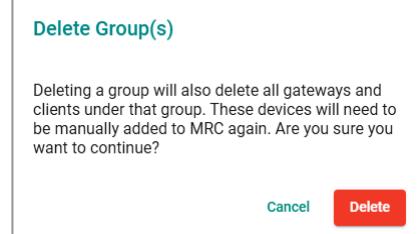
Account Management

From the **Account Management** section, you can view and manage user accounts and configure permissions.

Account List

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

Account Table

UI Setting	Description
Username	Shows the username of the account.
Name	Shows the first and last name of the account.
Email	Shows the email address of the account.
Office Phone Number	Shows the office phone number of the account.
Mobile Phone Number	Shows the mobile phone number of the account.
Group	Shows the groups that the account can access.
Event Notifications	Shows the status of the event notifications setting for the account.
Created on	Shows the time the account was created.
Other Information	Hovering the cursor over the information (ⓘ) icon shows additional information if specified in the account configuration's 'Other Information' field.

Add Account

Menu Path: Account Management

Click the **Add** (➕) icon in the top-left corner of the group list to add a new account.

When finished, click **Apply** to save your changes.

UI Setting	Description	Valid Range	Default Value
Username	Enter a username for the account.	1 to 64 characters	N/A
New Password	Enter a password for the account.	6 to 64 characters	N/A
Confirm Password	Enter the password again to confirm.	6 to 64 characters	N/A
Email	Enter the email address of the account.	Email address	N/A
First Name	Enter the given name of the account user.	0 to 64 characters	N/A
Last Name	Enter the family name of the account user.	0 to 64 characters	N/A
Office Phone Number	Enter the office phone number of the account.	0 to 64 characters	N/A
Mobile Phone Number	Enter the mobile phone number of the account.	0 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Additional Information	Enter any other additional information about this account. This information will appear as a tooltip in the Other Information column.	0 to 254 characters	N/A
Group	Select the groups that this account can access.	Group	N/A
Event Notifications	Enable or disable the event notifications function. Enabled: The account user will receive email notifications if any gateway under their management changes status (online, offline, connected, disconnected). Disabled: The account user will not receive email notifications for gateway status changes.	N/A	Unchecked

Edit Account

Menu Path: Account Management

Click the **Edit** (✏) icon in the row of the account you want to edit.

When finished, click **Apply** to save your changes.

UI Setting	Description	Valid Range	Default Value
Username	The username cannot be modified. To modify the username, you must create a new user account.	1 to 64 characters	N/A
New Password	Only shows after clicking **CHANGE PASSWORD**. Enter a password for this account.	6 to 64 characters	N/A
Confirm Password	Only shows after clicking **CHANGE PASSWORD**. Enter the password again to confirm.	6 to 64 characters	N/A
Email	Enter the email address of the account.	Email address	N/A
First Name	Enter the given name of the account user.	0 to 64 characters	N/A
Last Name	Enter the family name of the account user.	0 to 64 characters	N/A
Office Phone Number	Enter the office phone number of the account.	0 to 64 characters	N/A
Mobile Phone Number	Enter the mobile phone number of the account.	0 to 64 characters	N/A
Additional Information	Enter any other additional information about this account. This information will appear as a tooltip in the Other Information column.	0 to 254 characters	N/A
Group	Select the groups that this account can access.	Group	N/A
Event Notifications	Enable or disable the event notifications function. Enabled: The account user will receive email notifications if any gateway under their management changes status (online, offline, connected, disconnected). Disabled: The account user will not receive email notifications for gateway status changes.	N/A	Unchecked

Delete Account

Menu Path: Account Management

Check the box of the account(s) that you want to delete and click the **Delete** ( ) icon in the top-left corner of the table.

When prompted, click **DELETE** to delete the account(s).
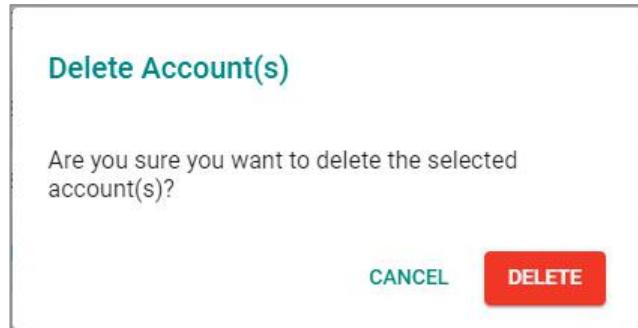
> ✏ **Note**
>
> Superuser accounts are created via the Moxa license portal and cannot be deleted via the MRC Quick Link interface. If you want to transfer a superuser account to a different administrator, contact Moxa for assistance. If you want to delete a superuser account, log in to the Moxa license portal as the superuser and delete the account.

Permissions Table

Refer to the following table for a detailed comparison of superuser and user account permissions.

Function	Superuser	User
Gateway Management	Read (All groups) Write (Add/edit/delete)	Read (Own group only) Write (Add/edit/delete own group only)
Client Management	Read (All groups) Write (Add/edit/delete)	Read (Own group only) Write (Add/edit/delete own group only)
Group Management	Read (All groups) Write (Add/edit/delete)	Read (Own group only) Write (Edit own group only)
Account Management	Read (All accounts) Write (All account/groups)	Read (All accounts) Write (Own account/group only)

Function	Superuser	User
Event Logs	Read	Read
License	Read Write	Read
Wizard	Read Write	Read Write

Event Logs

From the **Event Logs** section, you can view event logs for the MRC Quick Link service.

This section covers the following topics:

Event Logs List

Menu Path: Event Logs

Filter

Click the **Filter** (=) icon to select specific event logs to show.

Refresh

Click the **Refresh** (↻) icon to manually refresh the event log.

Export to CSV Refresh

Click the **Export** ( ) icon to export the event log. If a filter is active, only the filtered logs will be exported.

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

Event Logs Table

Index	Device Type	Message	User	Target	Timestamp
1	Account	[MRC Quick Link] Account Login Success	PM_Test_0604	PM_Test_0604	2025-06-30 11:37:26 +08:00
2	Account	[MRC Quick Link] Account Login Success	PM_Test_0604	PM_Test_0604	2025-06-27 11:50:07 +08:00
3	Gateway	[MRC Quick Link] Gateway Replacement Canceled	PM_Test_0604	testing3	2025-06-26 13:26:59 +08:00
4	Account	[MRC Quick Link] Account Login Success	PM_Test_0604	PM_Test_0604	2025-06-26 11:54:11 +08:00
5	Account	[MRC Quick Link] Account Updated	PM_Test_0604	PM_Test_0604	2025-06-25 18:45:25 +08:00

UI Setting	Description
Index	Shows the index of the event log.
Device Type	Shows the event log type.
Message	Shows information about the event.
User	Shows the account that triggered this event.
Target	Shows the target of this event, which could be an account, gateway, or client.
Timestamp	Shows the timestamp of the event, including the date, time, and UTC time zone adjustment.

Supported Event Logs

The MRC Quick Link service supports the following event logs.

Type	Message	Owner	Target
Account	[MRC Quick Link] Superuser Account Create Success.	---	Account Username
Account	[MRC Quick Link] Account Create Success.	Account Username	Account Username
Account	[MRC Quick Link] Account Delete Success.	Account Username	Account Username
Account	[MRC Quick Link] Account Updated	Account Username	Account Username
Account	[MRC Quick Link] Account Login Success	Account Username	Account Username
Account	[MRC Quick Link] Account Login Failed	Account Username	Account Username
Gateway	[MRC Quick Link] Gateway Created	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Deleted	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Configuration Changed	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Enabled	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Disabled	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Deactivated	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Replaced	Account Username	Gateway Name
Gateway	[MRC Quick Link] Gateway Replacement Canceled	Account Username	Gateway Name
Gateway	[MRC Quick Link] End Device Added	Account Username	Gateway Name

Type	Message	Owner	Target
Gateway	[MRC Quick Link] End Device Updated	Account Username	Gateway Name
Gateway	[MRC Quick Link] End Device Deleted	Account Username	Gateway Name
Gateway	[MRC Quick Link] End Device Service Updated	Account Username	Gateway Name
Gateway	[Gateway] Gateway Activate Success	---	Gateway Name
Gateway	[Gateway] Gateway Activation Failed - Wrong MAC Device.	---	Gateway Name
Gateway	[Gateway] Gateway Activation Failed - Wrong Activation Key.	---	Gateway Name
Gateway	[Gateway] Gateway Activation Failed - Activation Key Already Used.	---	Gateway Name
Gateway	[Gateway] Gateway Configuration Changed	---	Gateway Name
Gateway	[Gateway] Gateway Online	---	Gateway Name
Gateway	[Gateway] Gateway Offline	---	Gateway Name
Gateway	[Gateway] Gateway Connected	---	Gateway Name
Gateway	[Gateway] Gateway Disconnected	---	Gateway Name
Client	[MRC Quick Link] Client Enabled	Account Username	Client Username
Client	[MRC Quick Link] Client Disabled	Account Username	Client Username
Client	[MRC Quick Link] Client Added	Account Username	Client Username
Client	[MRC Quick Link] Client Deleted	Account Username	Client Username
Client	[Client] Client Connected	---	Client Username

Type	Message	Owner	Target
Client	[Client] Client Disconnected	---	Client Username
License	[License] License Code Expired, Service may Experience Interruptions. Please check with the Administrator.	---	License Code
License	[License] Monthly Data Usage Limit Reached. Please Check with Administrator.	---	---

License

From the **License** section, you can view license information for the MRC Quick Link service.

License List

Menu Path: License

Email Notifications

Click the **Mail** (✉) icon in the top-left corner of the table to configure email notification settings. The notifications will be sent to the email addresses configured for the selected recipient(s). User email settings can be configured in the Account Management section.

Refresh

Click the **Refresh** (↻) icon to manually refresh the license table.

Search

Enter the search term in the **Search** field located in the top-right corner. Anything matching the search criteria will be shown in the table.

License Table

Menc Path: License

UI Setting	Description
License Type	Shows the license type. New: Basic license. Add: Add-on license.
Concurrent Connected Nodes	Shows the number of nodes on the assigned Concurrent Connected Nodes license. Each gateway or client connection to the MRC cloud server will consume one node of the license. For example: • When client A establishes a remote connection to gateway A, the connection will use two nodes, one node for the client and gateway connection to the MRC cloud respectively. • When three gateways have the Gateway-to-gateway feature enabled, three nodes will be used, one node for each gateway connection to the MRC cloud.
Data Usage (per month)	Shows the monthly available data on the license. When a gateway or client is connected and establishes a remote connection, it will consume data. Data usage resets on the 1st day of each month. Any unused data at the end of the month is not carried over to the following month.
License Code	Shows the license code. This code can also be found on the **Products and Licenses > View Activated Products** page on the <u>Moxa license portal</u>.
License Service Period (UTC+8)	Shows the validity period of the license. When the license has expired, it will be moved from the **Activated** section to the **Expired** section at the bottom of the table.

✏ **Note**

Licenses are managed at the superuser level and are shared between users and groups under that superuser. If you require additional licenses, you can purchase and activate the necessary add-on licenses from the Products and Licenses > Activate a Product License page on the Moxa license portal.

Wizard

From the **Wizard** section, you can quickly set up a remote connection with MRC Quick Link using a step-by-step process.

If no gateways have been added to MRC, the Wizard will automatically be triggered when logging in. If you have already set up at least one gateway, the **Gateway Management** page will be the default screen when logging in.
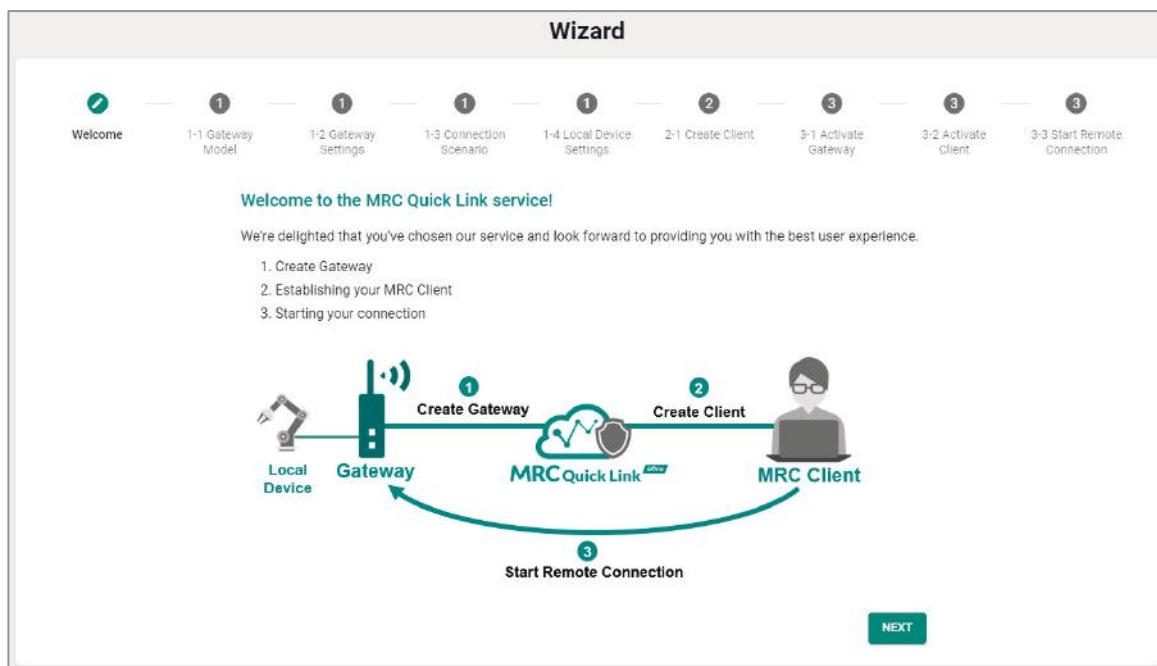
MRC Gateways

OnCell G4302 & OnCell G4308

This section provides information on how to configure MRC functionality on the OnCell G4302-LTE4 Series and OnCell G4308-LTE4 Series gateways and how to establish a connection to the MRC Quick Link cloud platform to monitor and remotely access the gateway.

> ✏ **Note**
>
> The following configurations are performed in the OnCell G4302-LTE4/G4308-LTE4 Series web interface.

Moxa Remote Connect

Menu Path:

System > Management Interface > Moxa Remote Connect

This section lets you establish a connection to the MRC Quick Link cloud platform to monitor and remotely access your device. Visit the Moxa Remote Connect Suite page for more information.

> ✏ **Note**
>
> Availability of this feature may vary depending on your product model and version.

There are two tabs in this section:

- Settings

- Status

OnCell 3120

This section provides information on how to configure MRC functionality on the OnCell 3120 Series gateway and how to establish a connection to the MRC Quick Link cloud platform to monitor and remotely access the gateway.

> ✎ **Note**
> The following configurations are performed in the OnCell 3120-LTE-1 Series web interface.

Moxa Remote Connect (MRC)

Menu Path: Advanced Setup > Moxa Remote Connect (MRC)

This **Moxa Remote Connect (MRC)** page lets you enable or disable the MRC service on the gateway and configure the connection parameters.

MRC Service

UI Setting	Description	Valid Range	Default Value
MRC Service	Enable or disable the MRC service for establishing remote access connections via MRC Quick Link.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Activation Type	Select the Activation Type. **Enter Activation Key:** Manually enter the activation key for authentication. **Import from USB Drive**: Insert a Moxa ABC-02 Series USB device or a USB drive containing the activation key file.	Manual / Import from USB	Enter Activation Key

Click **Submit** to enable MRC Quick Link services on the OnCell device.

Click **Reset Key** to reset the authentication key and terminate the connection to the MRC cloud.

Tunnel Control

UI Setting	Description	Valid Range	Default Value
Tunnel Control	Select the tunnel control type. **Persistent Connection**: Establish a persistent tunnel connection for remote access. The connection will never expire unless manually terminated. **Controlled by key file from USB drive**: The remote connection is only allowed to establish when a Moxa ABC-02 Series USB device or USB drive with an activation key is inserted into the OnCell gateway. ✎ **Note** This feature requires **USB Function** to be enabled in **System Management Interface > Hardware Interface**.	Persistent Connection / Controlled by key file from USB drive	Persistent Connection

Click **Apply** to save your settings.

Status

| UI Setting	Description
Gateway Name	Shows the name of the gateway as configured on the MRC Quick Link cloud platform.
MRC Status	Shows the current status of the connection to the MRC service. **Internet:** The gateway is connected to the Internet. **MRC Cloud:** The gateway has successfully connected to the MRC Quick Link cloud service. **Key Verification:** The gateway has successfully verified the authentication key. **Online:** The gateway is online and ready to establish a remote connection via MRC. **Connected:** A remote connection was established successfully.

Click **Refresh** to update the status.

MRC-1002

This section provides information about the MRC-1002 Series MRC gateways. These devices are specifically designed for use with MRC.

Device Information

LED Indicators
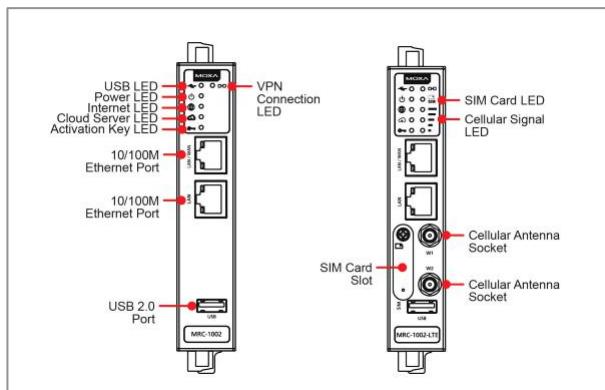
LED Symbol	LED Name	Description
⚡	USB	Steady on: A USB device is connected and working. Off: No USB device is connected.
⏻	Power	Steady on: The gateway is powered on. Off: The gateway is powered off.
🌐	Internet	Off: The WAN interface is not ready (DHCP failure, PPPoE failure, ...). Blinking: Testing the Internet connection. Steady on: The gateway is connected to the Internet.
☁	Cloud Server	Off: The gateway is not connected to the MRC Server. Blinking: The gateway is testing the connection to the MRC server. Steady on: The gateway is connected to the MRC server.
🔑	Activation Key	Off: No activation key detected on the gateway. Blinking: The activation key is invalid. Steady on: A valid activation key is present and the gateway is activated.

LED Symbol	LED Name	Description
⊖⊙	VPN Tunnel	Off: The VPN tunnel is down and remote access is not available. Blinking: The gateway is attempting to establish a VPN tunnel. Steady on: The gateway has successfully established a VPN tunnel.
SIM	SIM Card	Off: No SIM card detected. Blinking: SIM card error. Steady on: The SIM card is ready and active.
(cellular signal icon)	Cellular Signal	The gateway has 3 separate LEDs to indicate the cellular signal strength. 3 LEDs on: Best signal quality. 2 LEDs on: Normal signal quality. 1 LED on: Poor signal quality (may cause the Internet connection to be lost), 0 LED on: Very poor signal quality (no Internet connection).
(ethernet icon)	Ethernet Speed	Steady on (Amber): The Ethernet port is connected at 10 Mbps speed. Steady on (Green): The Ethernet port is connected at 100 Mbps speed.

Reset Button

The reset button can perform three functions depending on how long the button is depressed for. Each function is indicated by different LED behavior.
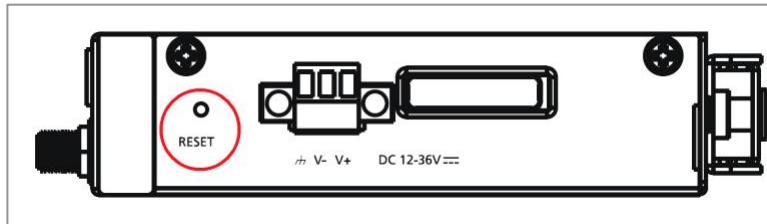
Action	Description	LED Behavior
Press between 1 to 5 seconds and release	Reboots the gateway.	The Internet LED is blinking. (🌐)

Action	Description	LED Behavior
Press between 6 to 10 seconds and release	Temporarily reset the device IP to the factory default. If you have changed the default IP (192.168.127.254), pressing the reset button for 6 to 10 seconds will reset the device IP to the factory default. Restarting the device will restore the user-specified device IP. This function is useful for providing access to the device (e.g. maintenance staff) without exposing the user-defined device IP. For example, if you changed the default IP address to 192.168.127.111, pressing the reset button for 6 to 10 seconds will reset the device IP back to the default IP 192.168.127.254. Restarting the device will restore the user-defined IP 192.168.127.111. ✎ **Note** If the default device IP has not been modified, this function does not do anything.	The Internet and Cloud Service LEDs are blinking. (🌐 ☁)
Press between 11 to 15 seconds and release	Resets all device configurations and removes the activation key. ✎ **Note** If the reset button is depressed for longer than 15 seconds, the MRC gateway will reboot without changing any settings.	The Internet, Cloud Service, and Activation Key LEDs are blinking. (🌐 ☁ 🔑)

Moxa Remote Connect

This section provides information on how to configure MRC functionality on the MRC-1002 Series gateway and how to establish a connection to the MRC Quick Link cloud platform to monitor and remotely access the gateway.

Logging In

The MRC gateway provides a secure web console to perform configurations.

Connect your PC or laptop to the LAN port on the MRC-1002 and open a web browser. Navigate to http://192.168.127.254 to access the MRC-1002's web console.

When prompted, enter your username and password.

After you successfully logged in to the web console, the management portal will show.
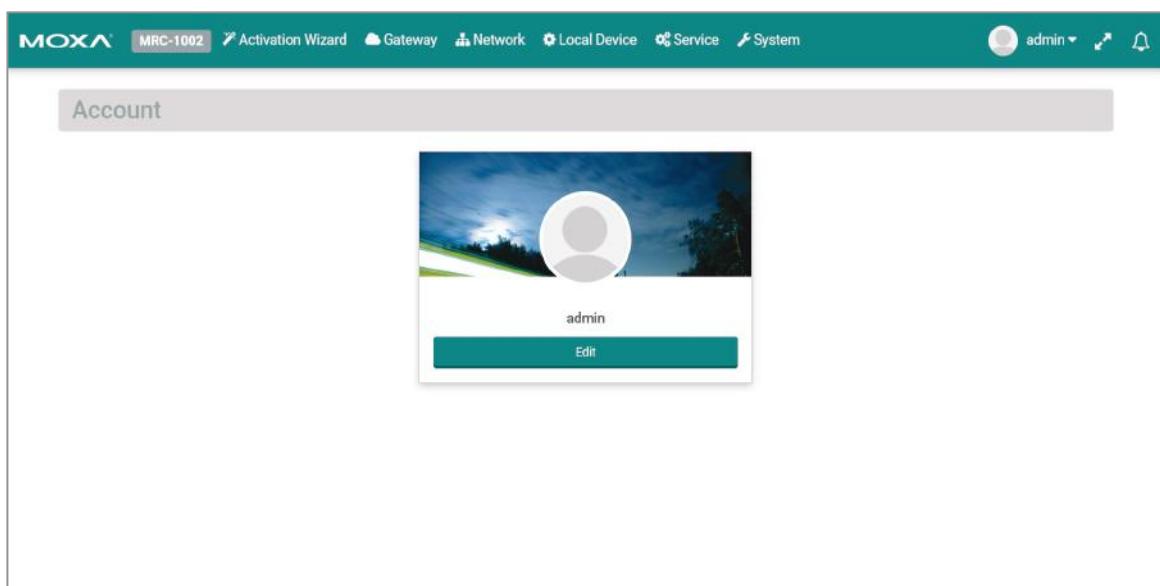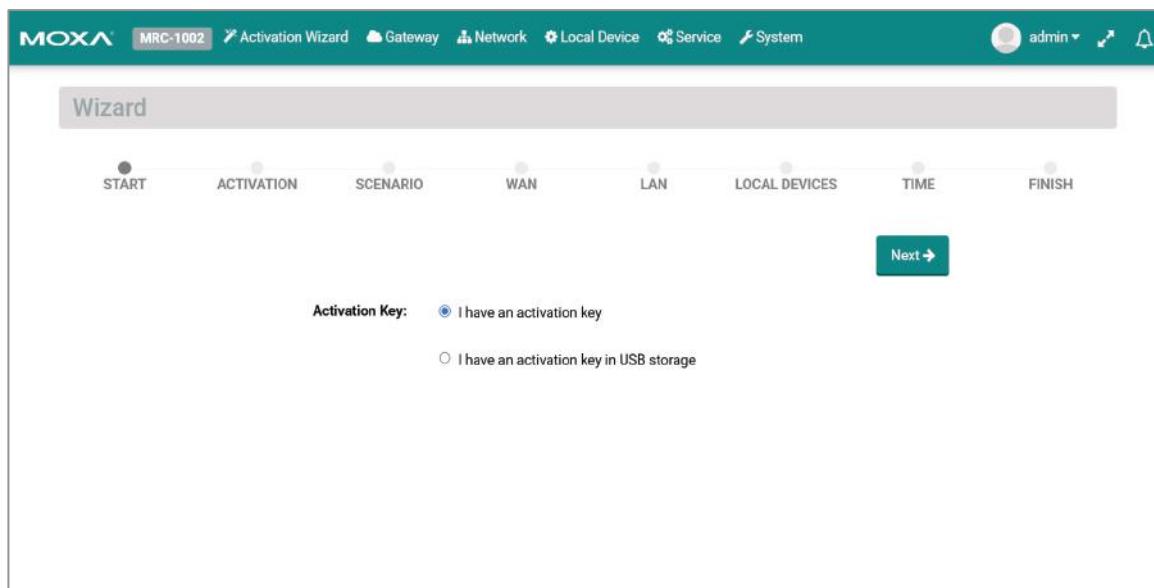
Activation Wizard

Menu Path: Activation Wizard

If the MRC-1002 gateway is not activated yet, run the **Activation Wizard** to perform the step-by-step activation procedure.

Step 1: Start

There are two options to register the MRC-1002 gateway.

| UI Setting	Description
I have an activation key	Enter the activation key string provided by the MRC server administrator to activate the gateway.
I have an activation key in a USB storage	Insert the USB drive containing the activation key file to activate the gateway.

When finished, click **Next**.

Step 2: Activation

If you selected **I have an activation key**, enter the activation key and click **Next**.
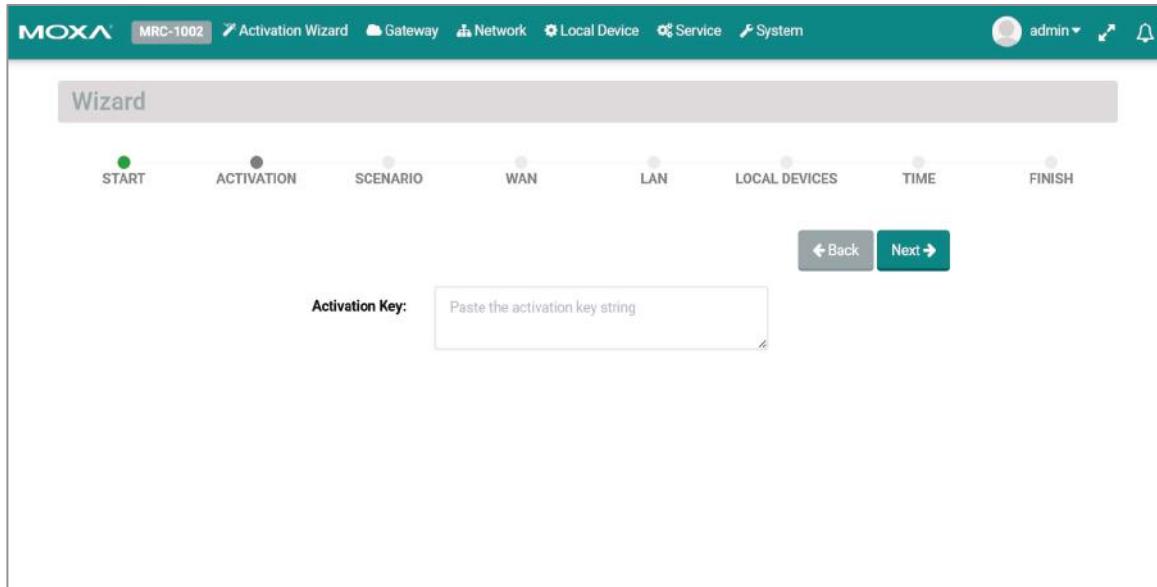
If you selected **I have an activation key in a USB storage**, insert the USB drive with the activation key file and click **Next**.
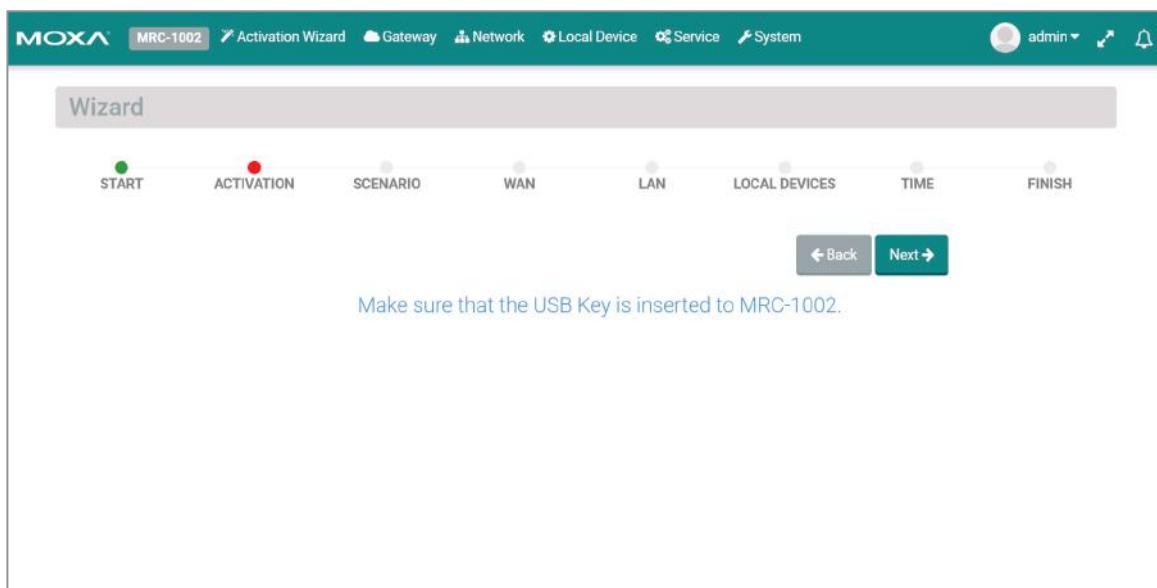
Step 3: Time

Select the time zone where the gateway will be deployed.
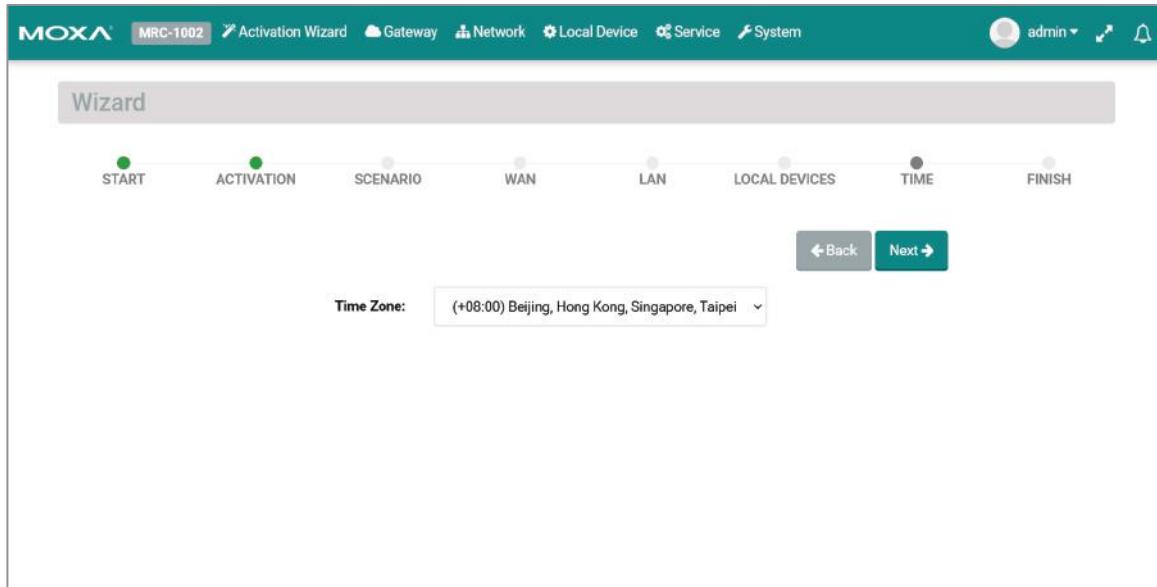
Step 4: Finish

Click **Initialize Now** to activate your gateway. The gateway must be connected to the Internet to complete this step.

Activation Status

Menu Path: Gateway > Activation Status

From the **Activation Status** screen, you can check the current status of the connection to the MRC service.

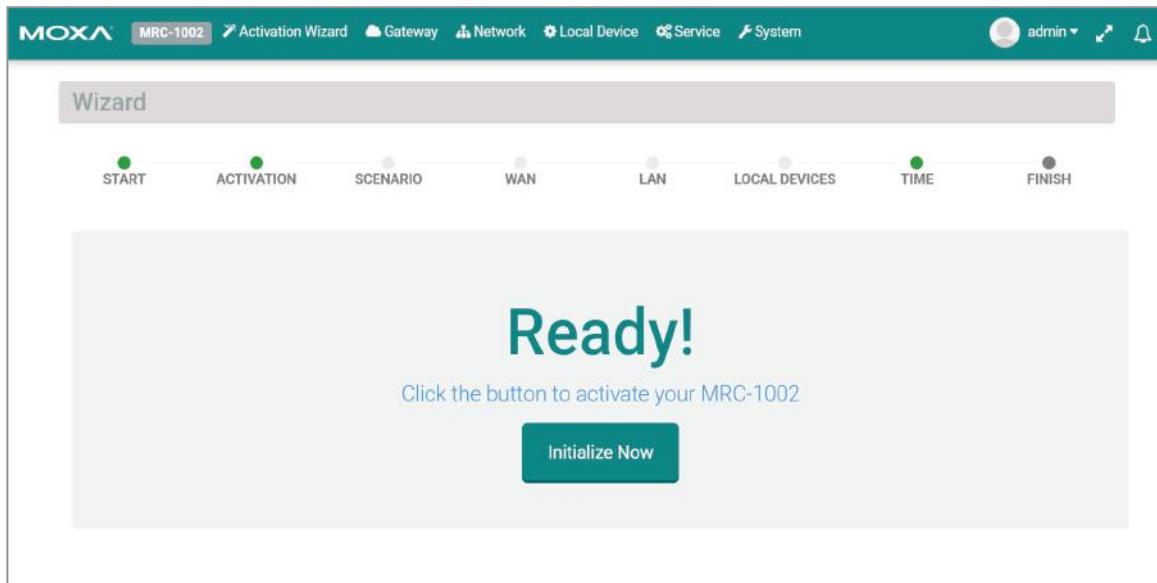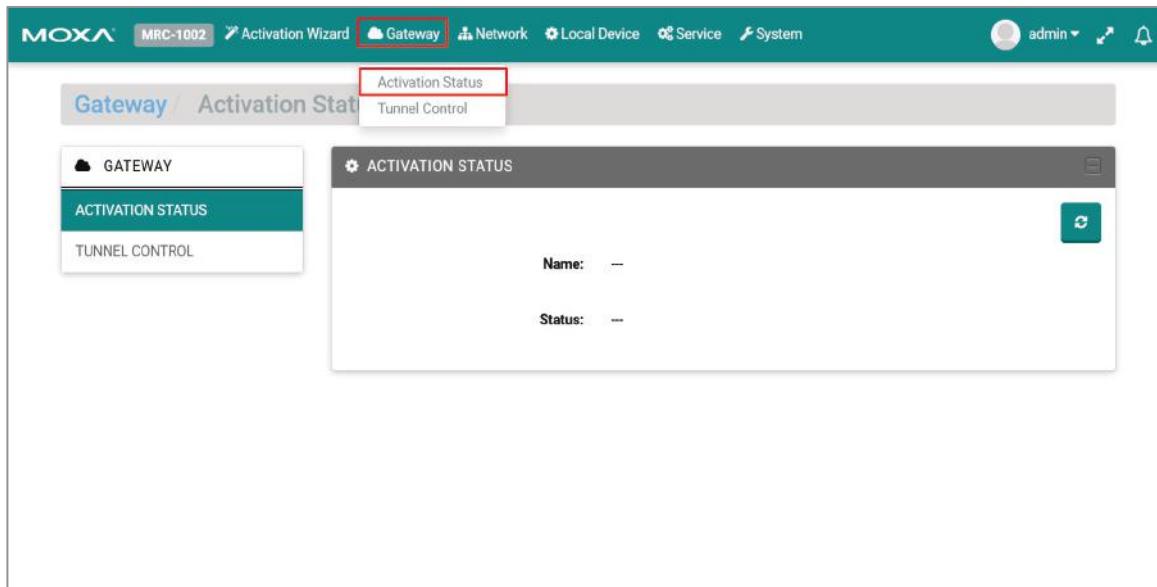| UI Setting	Description
Name	Shows the name of the gateway as configured on the MRC Quick Link cloud platform.
Status	Shows the current status of the connection to the MRC service. **Internet:** The gateway is connected to the Internet. **MRC Cloud:** The gateway has successfully connected to the MRC Quick Link cloud service. **Key Verification:** The gateway has successfully verified the authentication key. **Online:** The gateway is online and is ready to establish a remote connection via MRC. **Connected:** A remote connection was established successfully.

Tunnel Control

Menu Path: Gateway > Tunnel Control

From the **Tunnel Control** screen, you can view the current VPN tunnel status and select the method for establishing tunnels.

UI Setting	Description	Valid Range	Default Value
Tunnel Status	Shows the current VPN tunnel status.	Unknown / Disconnect / Connected	N/A
Tunnel Control	Select the VPN tunneling method for remote connections. Persistent Connection: The gateway will maintain a constant remote connection until it is manually disconnected. Controlled by key file from USB drive: A remote connection can only be established when a Moxa ABC-02 Series USB device or a USB drive with an activation key is inserted into the gateway. Once the USB drive is removed, the gateway can no longer establish remote connections until a USB with the activation key is inserted. Controlled by DI: A remote connection can only be established only when the gateway receives a DI signal. Once the signal is lost, the gateway can no longer establish remote connections until another DI signal is received.	Persistent Connection / Controlled by key file from USB drive / Controlled by DI	Persistent Connection

MRC Client

This section explains how to use the MRC Client software and how to remotely access devices.

# Download the MRC Client Software

Download the MRC Client software from the Moxa MRC webpage and install the software.

> ✎ **Note**
>
> If you encounter any issues during the installation process, please turn off any antivirus software and try again. If the issue persists, contact Moxa Technical Support.

UI Interface Overview

Below is an overview of the MRC Client user interface.
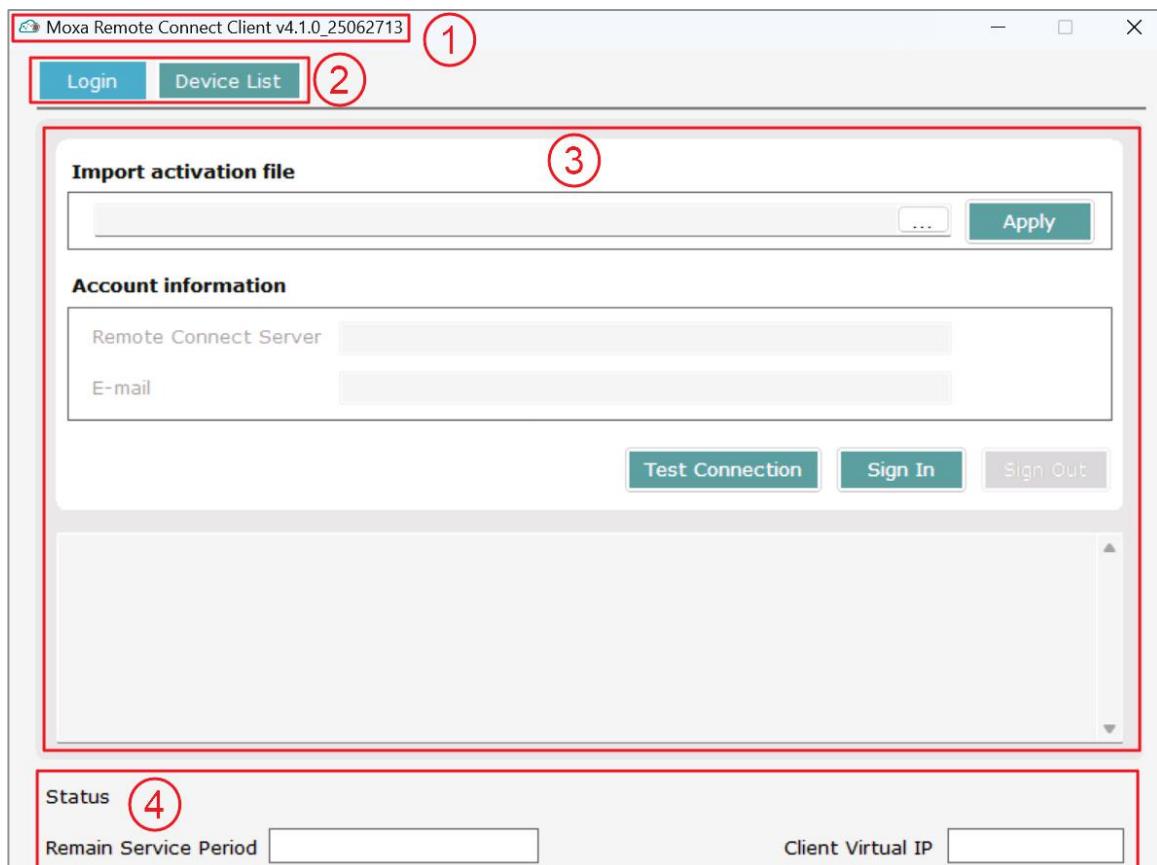
	Section	Description
1	Title header	The title area shows the version information of the MRC Client.
2	Function tab	The function tab allows you to switch between functions by clicking the corresponding tab.
3	Configuration screen	Shows information and configuration options depending on the selected function page.
4	Software Status	Shows the status of the MRC Client software.

Logging In to the MRC Client

From the **Login** section, you can log into the MRC client software, test the connection, and view related event logs.

Login

1. Create an MRC Client account through MRC Quick Link and download the activation file. Refer to the **Getting Started** section.

2. In the **Import Activation File** field, select the activation file and click **Apply**.

3. The activation file information will be shown in the **Account information** section while the status of the activation process will be shown at the bottom of the screen.
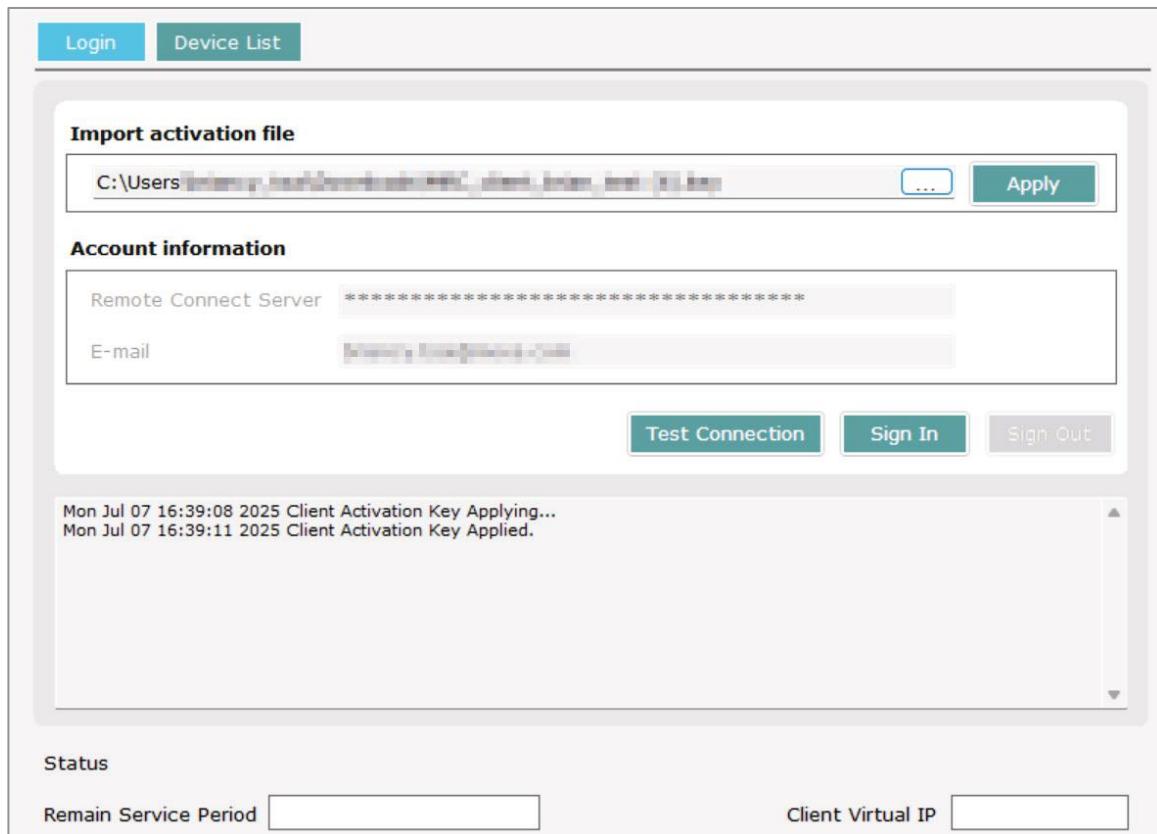
4. Click the **Test Connection** button to test if the connection between the MRC Client and the MRC Quick Link Server is functioning properly.

The results of the test will be displayed in the log area below.
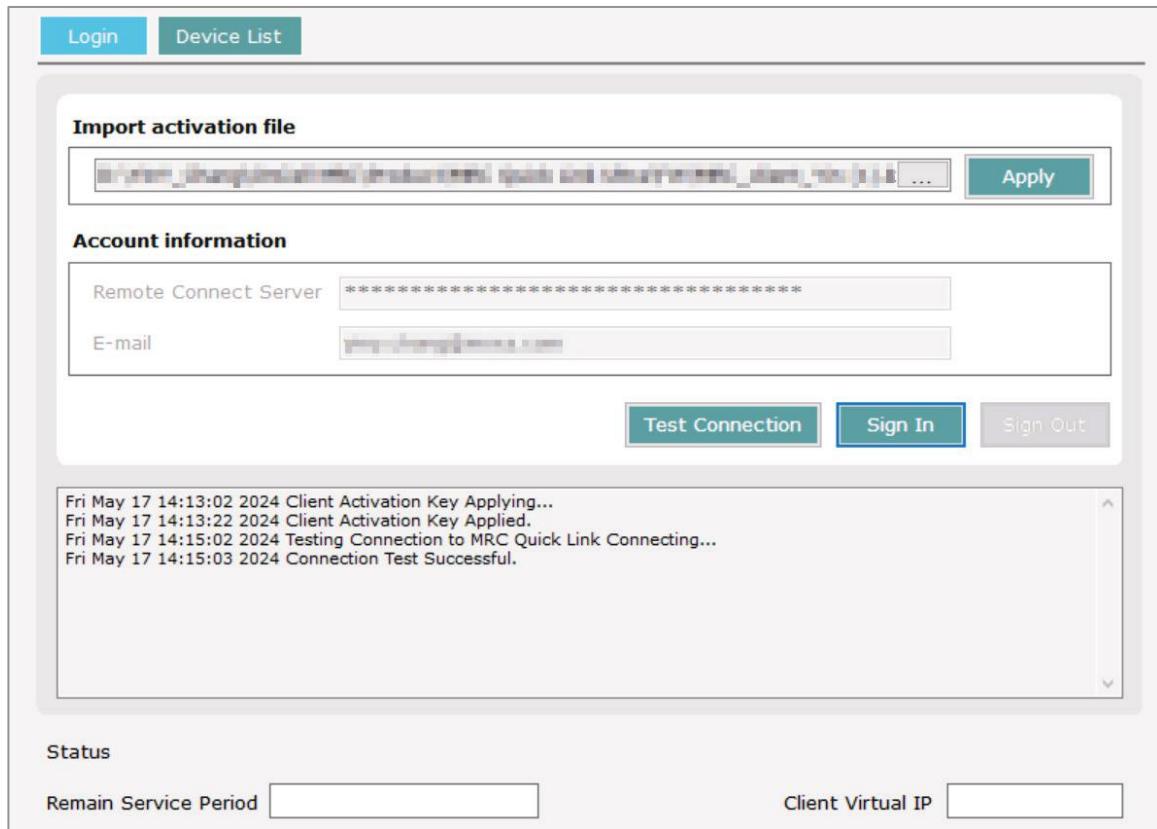
5. Click the **Sign In** button to log in. The connection details will be shown in the log area at the bottom of the screen.

    Once logged in successfully, the screen will automatically switch to the Device List tab.
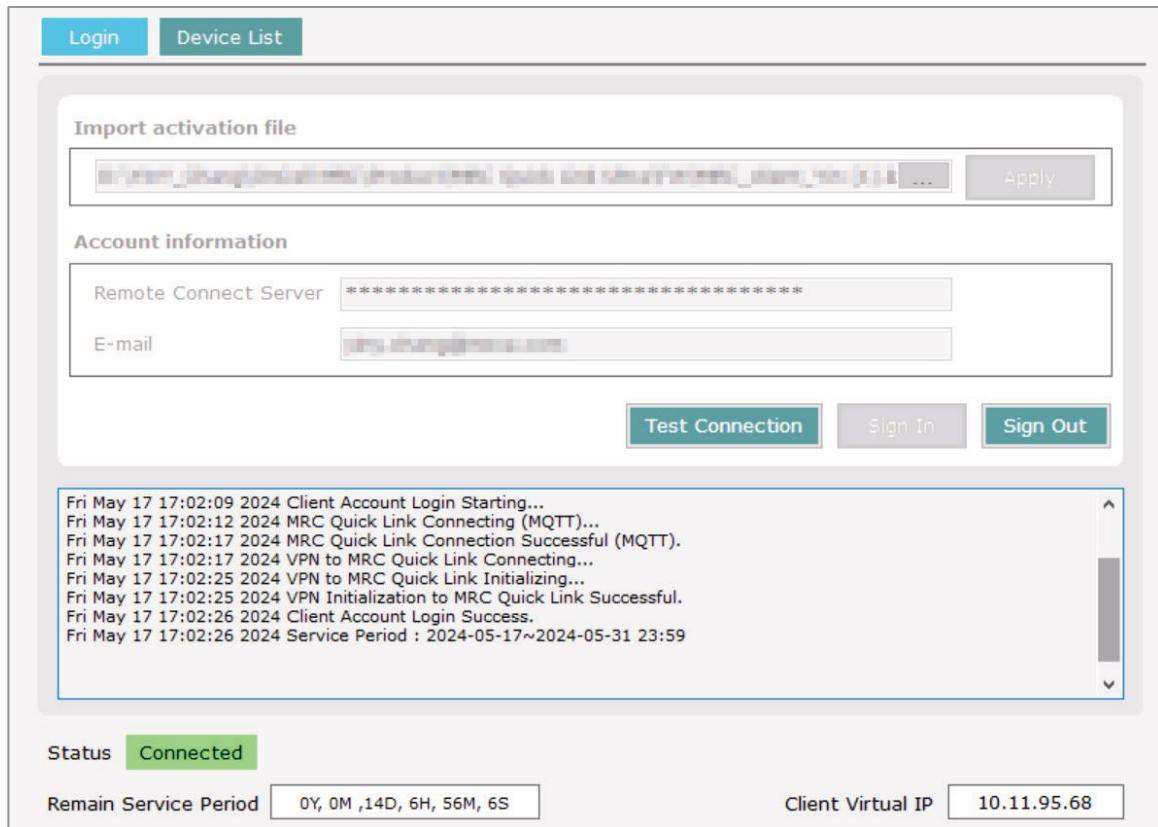
UI Setting	Description
Status	Shows the status of MRC Client. Once logged in successfully, it will show as "Connected".
Remain Service Period	Shows the remaining service time. If the service period is exceeded, the MRC Client will automatically log out, requiring the user to log in again.
Client Virtual IP	Shows the IP used by the MRC Client for MRC Quick Link remote connections.

> ✎ **Note**
>
> Once logged in to the MRC Client, the status of the MRC Client will change to Connected and will occupy one concurrent connected node license node, even if no VPN tunnel to a device has been established yet.

Logout

1. Click **Sign Out** to log out of the MRC Client. The details of the logout will be shown in the log area at the bottom of the screen.
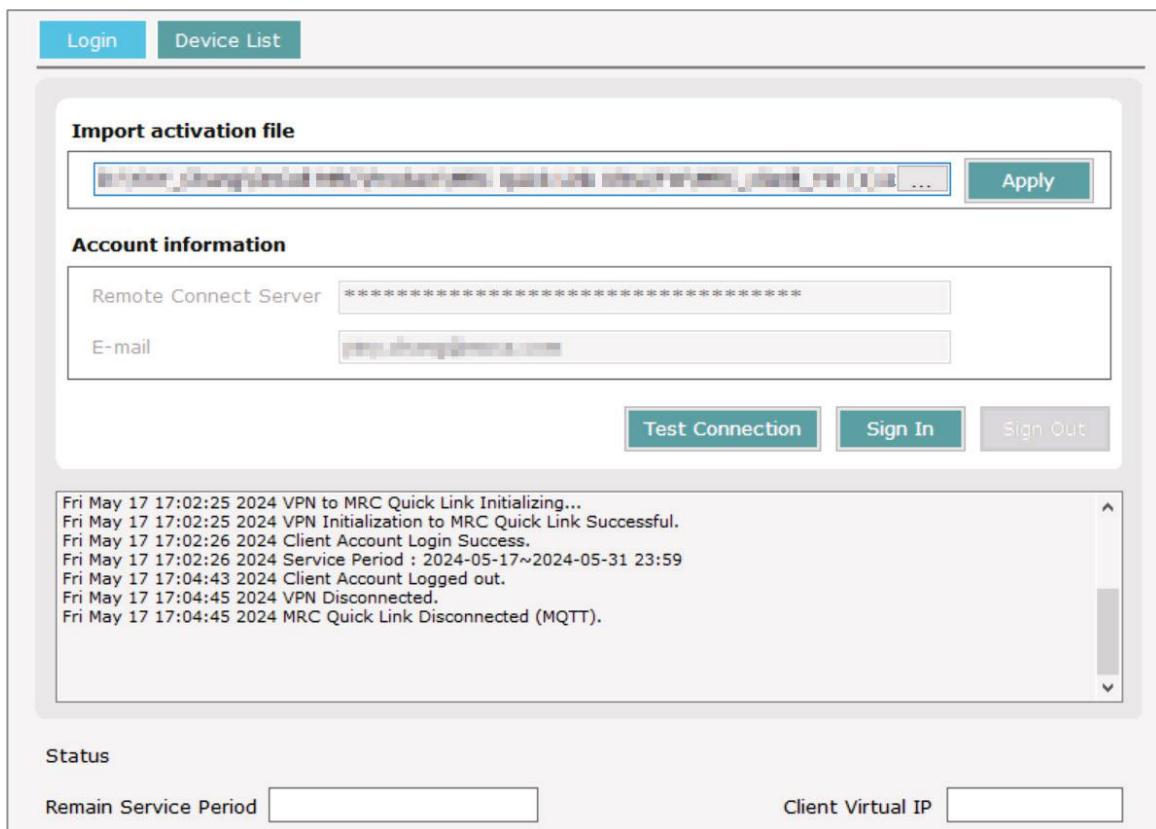
Auto Logout

If the Auto Logout function is enabled on the MRC Client, a prompt will appear every 15 minutes confirming if you want to continue using the software.

If you do not click **Continue Using** within 2 minutes, you will be automatically logged out.

Click **LOG OUT** to manually log out.
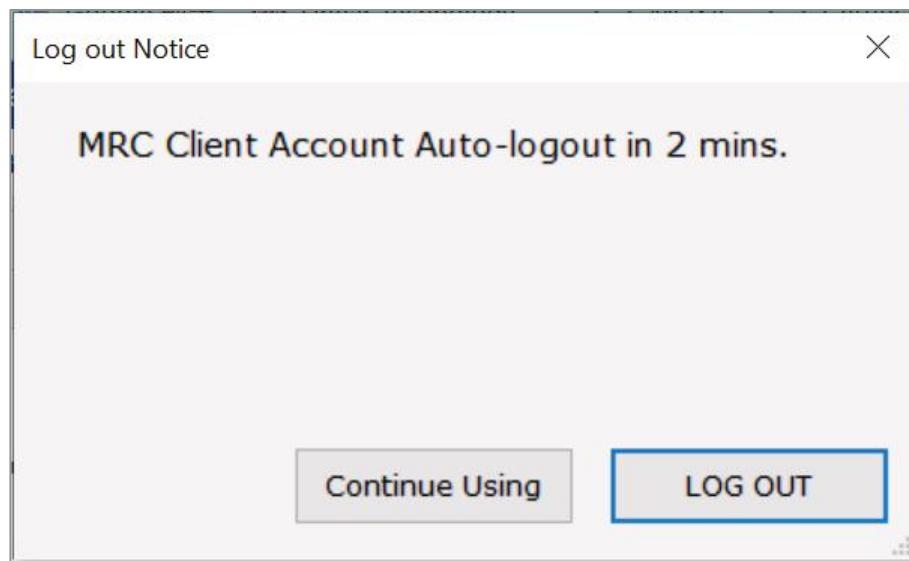
Device List

Menu Path: Device List

UI Setting	Description
Device Name	Shows the name of the device.
Status	Shows the status of the device.

Connected: The device has successfully established a remote connection.

Online: The device is online but has not yet established a remote connection.

Offline: The device is unable to connect to the MRC Quick Link server.

Unknown: The status of the device is unknown because the information could not be retrieved.

UI Setting	Description
Tunnel	Indicates the VPN tunnel is closed. Click this button to open the VPN tunnel and establish a remote connection. Indicates the VPN tunnel is open. Click this button to close the VPN tunnel and terminate the remote connection.
Virtual IP	Shows the virtual IP of the device for remote connection.
Local IP/MAC	Shows the IP or MAC address of the device.

Establish Remote Connection

Establish a remote connection to the gateway

Menu Path: Device List

1. In the device list, find the gateway you want to establish a remote connection to and check the device status is **Online** ( ) or **Connected** ( ).

   > ✎ **Note**
   >
   > If the gateway status shows as Connected, it means the gateway has already established a connection to other devices. This does not affect the remote connection from the MRC Client to the gateway.

2. Click the **Tunnel** ( ) icon to establish a VPN tunnel to the device. The indicator will change to the icon, indicating the tunnel is established.

3. When the tunnel to the gateway is established, the gateway status will change to **Connected** ( ) and the virtual IP will appear in green, indicating the tunnel is active.

   At this point, you can connect to the gateway via the corresponding virtual IP.

> ✎ **Note**
>
> When a gateway changes to Connected, it can establish a remote connection to all local devices under it, depending on the permission rules configured for the local devices. If no permission rules are configured, a tunnel is established to all local devices by default once the gateway's tunnel is active.
>
> If necessary, you can manually close tunnels to local devices. Refer to the Terminate a Remote Connection section.

Establish a remote connection to a local device

Menu Path: Device List

1. In the device list, find the gateway that manages the local device and click the **Expand** (**+**) icon to show all local devices under it.

> ✎ **Note**
>
> Ensure that the local device you want to connect to is showing as Online ( ).

2. Click the **Tunnel** ( ) icon to establish a VPN tunnel to the device. The indicator will change to the icon, indicating the tunnel is established.

> ✎ **Note**
>
> When the local device's tunnel is established, the gateway will also automatically establish a remote connection to the local device.

3. When the tunnel to the local device is established, the device status will remain Online ( ) while the gateway status will change to Connected ( ), and the virtual IP will appear in green, indicating the tunnel is active.
    At this point, you can connect to the local device via the corresponding virtual IP

> ✎ **Note**
>
> Only devices in the Connected ( ) state use up a concurrent connected node license node. Since only the
>
> gateway's status will change to Connected ( ) while local devices remain Online ( ), only one
> concurrent connected node license node is counted no matter how many local devices under a single
> gateway establish remote connections.

Terminate a Remote Connection

Menu Path: Device List

1. In the device list, click the **Tunnel** ( ) icon to terminate the corresponding

   VPN tunnel. The indicator will change to the icon, indicating the tunnel
   was terminated.

> ✏ **Note**
>
> If the device has not established a remote connection to any other devices, its status will change
>
> from Connected (▌) to Online (▌) after terminating the remote connection.

> ✎ **Note**
>
> Even if all VPN tunnels are closed, the status of the MRC Client will remain Connected (█) and will subsequently occupy one concurrent connected node license node.
>
> If you want to free up this node, log out of the MRC Client.

Enable L2/L3 Broadcast/Multicast Forwarding

Menu Path: Device List

Multiple gateways in the device list may have L2/L3 Broadcast/Multicast forwarding enabled at the same time, which could lead to packet storms. To prevent this, the MRC Client only allows one gateway at a time to have L2/L3 Broadcast/Multicast forwarding enabled.

In the **L2/L3 Broadcast Multicast** field, select the gateway to enable Broadcast/Multicast forwarding for.

L2/L3 Broadcast Multicast	None ▾

Refresh

Menu Path: Device List
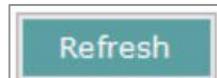
Refresh

Click **Refresh** to update the device list.

Search for a Gateway

Menu Path: Device List

Search Gateway	Search Gateway

Enter the search term in the **Search Gateway** field. Anything matching the search criteria will be shown in the table.

Save the MRC Client Settings as the Default

Save to Default

Click **Save to Default** to save the current tunnel status of the Device List.

When logging in next time, MRC Client will enable and disable the tunnels based on the saved default tunnel status.

You can use this feature to establish a remote connection to specific devices by default each time you log in.

Save the MRC Client Settings

Save as

Click **Save as** to export and save the current tunnel status of the Device List as a configuration file to your system.

Import MRC Client Settings

Load

Click **Load** to import a previously saved MRC Client settings configuration file.

MRC Client Event Log

Menu Path: Login

From the **Event Logs** section, you can view events for MRC Client.

Type	UI Message
Key Apply	Client Activation Key Applying...
	Client Activation Key Applied.
Login / Logout	Client Account Login Starting...
	Client Account Logged out.
	Client Account Login Success.
	Client Account Login Failed.
	Client Activation Key Already Used.
Connection	MRC Quick Link Connecting (MQTT)...
	MRC Quick Link Connection Successful (MQTT).
	MRC Quick Link Connection Failed (MQTT).
Test Connection	Testing Connection to MRC Quick Link Connecting...
	Connection Test Successful.
	Connection Test Failed.
VPN	VPN to MRC Quick Link Connecting...
	VPN Connection Failed. Please Check the Network Status or Check with Administrator.
	VPN Disconnected.
Service Period	Service Period : yyyy-MM-dd ~ yyyy-MM-dd HH:mm:ss
Device List	Device List Updated.
Auto logout	Your MRC Client Software is log out automatically. Please log in again if you want to have remote access

Type	UI Message
Gateway Status Change	Gateway [Gateway Name] Offline.
	Gateway [Gateway Name] Online.
	Gateway [Gateway Name] Connected.
	Gateway [Gateway Name] Disconnected.

Troubleshooting and Common Questions

This section provides guidance on common questions regarding the use of MRC Quick Link.

MRC Licenses

How is data usage calculated?

Answer: On the 1st of every month, the outbound traffic of each connected node (gateway or client) is monitored and billed until the end of that month. The data usage counter resets on the 1st of the following month. Any unused data from the previous cycle cannot be carried over to the following month.

My data usage is about to run out. How can I ensure my service is not affected?

Answer: If required, you can purchase an additional data usage license from the Moxa license portal and activate it following the instructions provided in the Getting Started section. If you have an urgent requirement for remote connections before completing the license purchasing process, please contact your Moxa sales representative to request a temporary license.

What happens if I run out of data?

Answer: If you exceed the available data on the license, all remote connections will be automatically disconnected the following day. Any gateway-to-gateway connections will automatically re-establish after purchasing an additional data license, or once the data counter resets on the 1st of the following month.

I am running out of nodes on my Concurrent Connected Node license. How can I ensure my service is not affected?

Answer: Contact your MRC Quick Link superuser to allocate more node licenses to your instance or use the **Disconnect** function in MRC Quick Link to terminate unnecessary connections and free up nodes on your Concurrent Connected Nodes license.

Alternatively, you can purchase additional Concurrent Connected Node licenses and activate them following the instructions provided in the Getting Started section. If you have an urgent requirement for remote connections before completing the license purchasing process, please contact your Moxa sales representative to request a temporary license.

What happens if I run out of Concurrent Connected Node licenses?

Answer: If all nodes on your Concurrent Connected Node licenses are in use, you will not be able to establish additional remote connections until nodes become available, or until you have purchased and activated additional node licenses.

I have purchased Concurrent Connected Node licenses, but the MRC Client still cannot establish a connection. What should I do?

Answer: Log out of the MRC Client, completely close the program, reopen the program, and log in again. If the problem persists, please contact the designated superuser to open a Moxa Support Account and submit a ticket to the Moxa technical support team.

MRC Quick Link

What should I do if my gateway appears as offline?

Answer: When a gateway shows as offline, it usually indicates a network issue affecting the connection between the gateway and MRC Quick Link. You can use the OnCell gateway's SMS command function to obtain a cellular report for analyzing the connection, or issue an SMS command to restart the device's cellular function or to reboot the gateway.

What can I do when the gateway is online but the local device I want to connect to is offline?

Answer: When the gateway shows as online but the local device shows as offline, it typically indicates a connection issue between the gateway and the local device, which could be due to network problems or a malfunction of the local device. You can connect to the gateway's web console via the MRC Client and restart the interface connecting the local device to try re-establishing the connection to the local device. If the connection still cannot be established, it may indicate a malfunction of the local device that requires on-site intervention.

What can I do if I cannot access the MRC Quick Link Ultra website or establish a remote connection?

Answer: Please check whether your network settings are blocking the "ultravpncloud.org" or "amazonaws.com" domains. Make sure these two domains are not being blocked or filtered to prevent connection issues to the MRC service.

Can devices establish remote connections to devices from different groups?

Answer: No. For security reasons, devices can only establish remote connections to devices within the same group. If your application requires connections across multiple groups, it is recommended to create MRC Client accounts in each target group and save different activation keys. You can switch between these activation keys when logging into the MRC Client to establish connections with different groups.

Can I transfer a gateway or MRC client to a different group?

Answer: No. To use a gateway or client in a different group, you will need to deactivate and reactivate the gateway or MRC Client in the target group using a new activation key.

Can I restrict a local device to only allow connections from specific MRC Clients?

Answer: Yes. You can configure allowlist rules on each local device to set up a list of allowed MRC Clients.

Can I restrict a local device to only allow connections using specific protocols?

Answer: Yes. You can configure allowlist rules on each local device to set up a list of allowed connection protocols.

MRC Gateways

Can I establish remote connections to any device under the gateway through MRC Quick Link?

Answer: If the device has an IP address and is on the same subnet as the gateway, you can establish a remote connection to the device through MRC Quick Link.

To establish a remote connection to serial devices or L2 Ethernet devices without an IP address through MRC Quick Link, the device must be physically connected to the gateway.

Establishing remote connections through MRC Quick Link to devices with interface types other than the ones listed above is not supported.

What should I do if I can ping the local devices but cannot access their web interface?

Answer: Please check whether your browser has HTTPS enabled. Alternatively, you can manually enter the full URL starting with https://.

Will my original data transmission be interrupted when my gateway is using the MRC Quick Link service for remote connections?

Answer: No. The gateway's original data transmissions are not affected by any remote connections established via the MRC Quick Link service.

Can I use the MRC Quick Link service if my gateway is already configured with an IPsec VPN?

Answer: Yes. You can use the MRC Quick Link service to establish remote connections while running IPsec VPN simultaneously.

What should I do if the MRC-1002 shows "MRC-1002 has been activated" when I haven't applied the MRC Gateway key yet?

Answer: Clear your browser cache and try again.

How do I configure the OnCell G4302-LTE4 to use one Ethernet Port as the WAN, one Ethernet Port as LAN, and connect to devices connected by LAN via MRC Quick Link?

Answer: Follow the steps below to configure the OnCell G4302's ports:

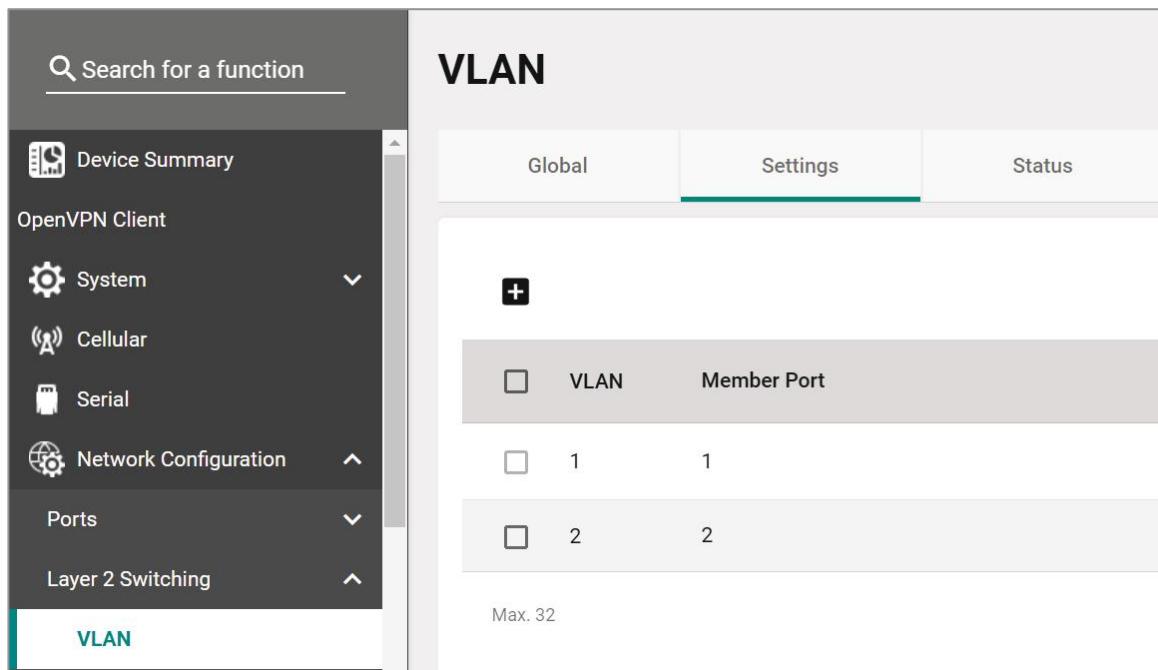1. Navigate to the OnCell G4302's web interface and log in.

2. Navigate to **Network Configuration > Layer 2 Switching > VLAN**.

3. Go to the **Settings** tab.

4. Create VLAN 2 and bind Port 2 to VLAN 2.

> ✎ **Note**
>
> By default, there is only a single VLAN (VLAN 1) with both Port 1 and Port 2 belonging to VLAN 1 acting as LAN ports.

5. Navigate to **Network Configuration > Network Interfaces**.

6. Go to the **WAN** tab.

7. Bind the WAN interface to VLAN 2 and configure the WAN network settings.
   Once configured, Port 1 will act as a LAN port and Port 2 as the WAN interface.

8. Once the WAN settings are applied, a prompt will appear to remind users to configure WAN redundancy settings.

Enable the WAN Redundancy

The WAN configuration has been changed. The device now use cellular as the default route interface for WAN connection. If you want to change the default route interface to Ethernet WAN, please enable the WAN Redundancy function.

CANCEL   NAVIGATE

9. Navigate to **WAN Redundancy**.

10. Set the **WAN Redundancy Mode** to **Backup**.
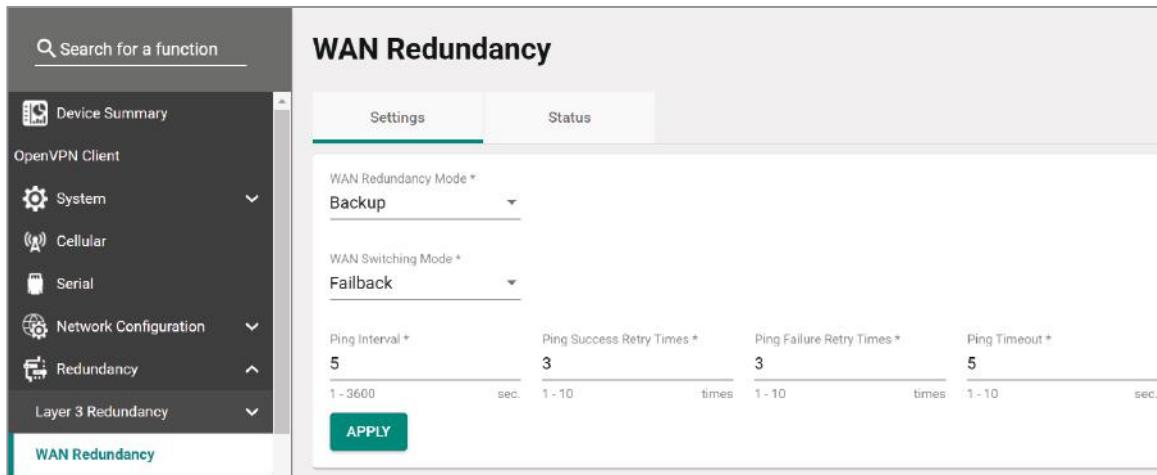
Enable all interfaces in the **WAN Backup Priority** section and configure the interfaces according to the figure below.

11. Navigate to **System > Management Interface > Moxa Remote Connect**.

12. Enable the **MRC Service**, enter the activation key downloaded from MRC Quick Link, and set **Bridge Member** to **1**.

Once configured, you can now establish remote connections to all devices under Port 1 using the MRC service.

✎ **Note**

The IP of the OnCell G4302's web interface will change to the bridge IP address value configured on the Moxa Remote Connect page.
Make sure to keep record of this IP address to access the OnCell G4302's web interface.

MRC Clients

MRC Client displays the following system error message after logging in. What should I do?
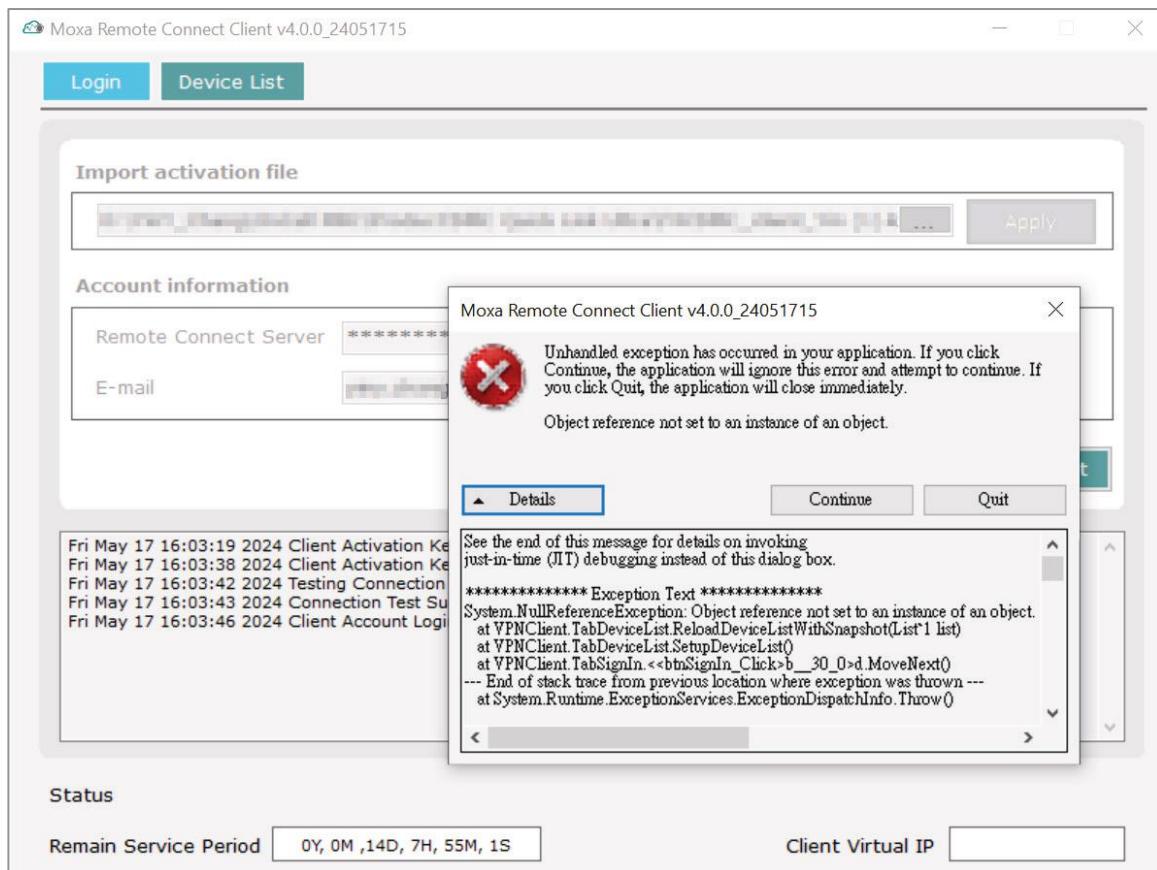
Answer: Uninstall and reinstall the MRC Client software.

The tunnel in the MRC Client software is active, but I cannot establish a remote connection. What should I do?

Answer: Follow the steps below to verify the connection.

1. Ensure the gateway status is **Connected** (▐).

2. Verify that the connection IP matches the virtual IP displayed in the MRC Client.

3. Click **Test Connection** in the MRC Client to check if the connection is normal.

4. Ensure the system time of the gateway is set correctly. If the time is not set correctly, it may cause the connection to fail.

5. If all the above items are valid but the connection still fails, please contact the designated superuser to open a Moxa Support Account and submit a ticket to the Moxa technical support team.

What should I do if I can't establish a VPN connection?

Answer: Make sure that both your MRC Client and MRC Gateway are upgraded to the latest firmware version.

MOXA®

www.moxa.com/products