Getting Started with MRC Quick Link

Moxa Technical Support Team
support@moxa.com

Contents

About Moxa

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Introduction

Moxa Remote Connect (MRC) Quick Link is a cloud-based management platform that allows you to set up a remote connection from any computer to the end devices connected to an MRC gateway from anywhere in the world through the MRC server. This makes it possible to use PC-based software applications to remotely interact with industrial equipment - just as if they are connected directly to the PC.

Setting up a remote connection with MRC Quick Link involves three separate processes carried out by different roles. The administrator is responsible for configuring the gateway and clients for remote access on the MRC server and generating the respective activation keys for the machine operator and support engineer. The machine operator installs the activation key on the physical gateway device on-site. Meanwhile, the support engineer uses the client key in the MRC Client Software to authorize the remote connection to the field device. When the tunnel is successfully established, the support engineer can remotely monitor and manage the equipment.

The following diagram illustrates a common usage scenario utilizing MRC Quick Link to remotely access industrial Ethernet equipment connected to the MRC gateway.

This technical note provides instructions on how to set up and configure a remote connection with MRC Quick Link, as well as two example applications for your reference.

How to Use MRC Quick Link to Connect to Remote Equipment

Step 1: [MRC Admin] Register Your MRC Quick Link Account and Gateway

The first step in setting up remote connections with MRC Quick Link is to create a MRC Quick Link account and register the MRC-1002 gateway serial number. This process is handled by the MRC server administrator.

1. Go to www.moxa.com and click **Sign In** in the upper-right corner.

2. If you already have a Moxa account, enter your login details, click **SIGN IN**, and skip to step **5**. If you do not have a Moxa account, continue with step **3**.

3. Click **Create your Moxa member account** to create a new account.

4. Fill in the required information and click **SIGN UP**.

5. Go to www.moxa.com and sign in using your Moxa account.

6. Once logged in, go to **Software License Management** located under the **Support** tab.

7. Log in to the Software License Management portal using your Moxa account.

8. Click **Activate Your License**.

9. Select **MRC Quick Link** from the Software Package list.

10. Enter your MRC-1002 Gateway's serial number and create a MRC Quick Link ID. After completing the survey, click **Submit**.

Note: The MRC Quick Link ID cannot be changed once created.

11. You will receive a confirmation email with your MRC Quick Link account information.

12. Go to the MRC portal at https://mrcus.moxa.com and log in with your MRC Quick Link ID and the password provided in the confirmation email.

13. When prompted, update the default password and click **OK**.

14. Since this is the first time logging in, the Wizard for adding clients and gateways will automatically open. Do not close the Wizard and continue with **Step 2: [MRC Admin] Configure Remote Access and Generate Activation Keys**.

Step 2: [MRC Admin] Configure Remote Access and Generate Activation Keys

Establishing a remote tunnel connection between the management station and the gateway requires the gateway and clients to be configured on the MRC server first. Once configured, activation keys for the client and gateway can be generated and distributed to the machine operator and support engineer to authorize and enable the remote connection. This process is handled by the MRC server administrator.

This section is further divided into three subsections for creating the client key, gateway key, and generating and distributing the keys. These should be followed in order.

1. Creating MRC Client Keys

In order to establish a remote connection to the gateway, clients need to be created and configured on the MRC server. These clients will be associated with the gateway and be authorized to access the gateway remotely.

1-1. In the Wizard, select **MRC_QuickLink** from the group list and click **Next**.

If you accidentally closed the Wizard, or it unexpectedly closed, you can restart the Wizard by clicking the **Menu** icon (▤) in the top-left corner and select **Wizard**.

Note: Uncheck **Always start with wizard** in the bottom-left to prevent the wizard from automatically showing when logging in next time.

1-2. Click **Create Client**.

1-3. Specify the login ID, email address, and password of the client and click **Next**.

Note: The login ID can be up to 32 characters long. Both the login ID and the email address should be unique. Users can use either the login ID or email address to sign in to the MRC portal.

Note: You can also configure an optional service period time frame to limit when clients can connect to remote devices. For example, you can allow clients to only establish remote connections between 28/10/2020 14:00 and 30/10/2020 14:00.

1-4. Click **Save and Finish** to save the client configuration.

1-5. Repeat steps **1** to **4** to create additional clients.

1-6. When finished, continue to **2. Creating the MRC Gateway Key**.

---

2. Creating the MRC Gateway Key

The gateway and connected end devices have to be configured in the MRC server for remote access. Depending on your network setup, the gateway can be configured using one of three available modes, WAN-LAN, Transparent-LAN, or Cellular-WAN.

Refer to the table below for a description of each mode. Choose a mode and follow the link in the mode description to continue with the gateway configuration.

Note: If you are uncertain of the type of application, or your application does not fit any of these scenarios, pick the mode most appropriate for your current network configuration. You can configure the gateway to meet your requirements afterwards using the local web console. Refer to the MRC Gateway User's Manual for more information.

Mode	Diagram	Description
WAN-LAN Mode		The gateway's WAN port connects to an external Internet router to access the Internet. Target machines are connected either directly to the gateway's LAN port or via a switch. Refer to **<u>Using WAN-LAN Mode</u>** for setup instructions.
Transparent-LAN Mode		The gateway is configured to be in the same subnet as the existing office or factory network to access the Internet. Target machines keep their existing network information and connect directly to the gateway via the LAN port. Refer to **<u>Using Transparent-LAN Mode</u>** for setup instructions.
Cellular-WAN Mode		The gateway connects to the Internet using a cellular network. Target machines are connected either directly to the gateway's LAN port or via a switch. Refer to **<u>Using Cellular-WAN Mode</u>** for setup instructions.

A. Using WAN-LAN Mode

In a WAN-LAN application, the MRC gateway's WAN port is directly connected to a router for Internet access, and the LAN port is either connected to the Ethernet device or to the local network where the machine's network is located via an Ethernet switch. In this mode, Internet access can be configured to use DHCP, static IP, or PPPoE.

A-1. Click the **Menu** icon (▤) in the top-left corner and select **Wizard**.

A-2. Click **Create Gateway**.

A-3. Specify the required information and click **Next**. Refer to the table below for more information about each setting.

Item	Description
Gateway Name	Enter a name for the gateway. This name is how the device will appear in the interface.
Location	Enter a location keyword such as a city name or specific address. The MRC Server will automatically populate the latitude and longitude fields with the Google Maps coordinates of the location closest to the keyword.
Latitude	Enter the latitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Longitude	Enter the longitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Lock to MAC Address	The MRC gateway settings can be locked to the gateway's MAC address. The activation key that has been generated after locking the gateway will only be authorized for use on the MRC gateway that matches the specified MAC address.
Auto IP Mapping	Auto IP Mapping ensures that the MRC gateway and each of the devices connected to the gateway will be assigned an individual virtual IP address within the device group. This virtual IP address represents the device and the MRC clients can use the virtual IP addresses to access each machine without causing an IP address conflict. It is recommended to enable this feature.

Item	Description
Gateway to Gateway	In some applications, machine-to-machine communication is not necessary. Disabling the Gateway to Gateway function will block traffic coming from the machines that are connected to other MRC gateways and only allows the MRC client to access the machines behind the MRC gateway. Enabling the function allows machine-to-machine communications through the MRC gateways.
Broadcast/Multicast Forwarding	The MRC gateway and the MRC portal support different types of industrial communication. For example, an EtherNet/IP application may require you to enable Multicast Forwarding, while enabling Broadcast Forwarding may be necessary for broadcast search applications.

A-4. Select **WAN-LAN Mode** as the scenario and click **Next**. If your application requires transparent or cellular Internet access, go to the respective section listed below:

To configure Transparent-LAN mode, go to Using Transparent-LAN Mode.
To configure Cellular-WAN mode, go to Using Cellular-WAN mode.

A-5. Specify the connection settings. Available options vary depending on which IP Address Mode you select. Refer to the respective connection settings for more information about each option.

If you selected **Static IP** as the IP Address Mode:

Item	Description
IP Address	Enter the local IP address of the gateway.
Subnet Mask	Enter the subnet mask of the gateway.
Gateway	Enter the default gateway address.
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

If you selected **DHCP** as the IP Address Mode:

Item	Description
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

If you selected **PPPoE** as the IP Address Mode:

Item	Description
Username	Enter your PPPoE account username.
Password	Enter your PPPoE account password.
Host Name	Enter the device name. If your ISP has not provided a device name, leave this field blank.
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

A-6. Assign a management LAN IP address and subnet mask for the MRC gateway and click **Next**. The LAN configuration and the subnet mask must match the network settings of the local machines connected to the gateway's LAN port.

A-7. Click the **Add** icon (+) to add devices to the list of remotely accessible devices. Up to 25 devices can be added to the list. If Auto IP Mapping is enabled, each added device will be assigned a virtual IP.

Note: If you have disabled Auto IP Mapping in step **A-3** it is still recommended to manually add devices to this list for security reasons. Skipping adding devices while Auto IP Mapping is disabled will allow all devices in the local subnet based on the gateway's LAN configuration to be remotely accessed. For example, if the gateway is configured to be 192.168.127.254/24, all Ethernet devices or machines in the 192.168.127.x subnet will be available for remote access.

A-8. In the Add Device window, specify the following information and click **Save**.

Item	Description
Local Device Name	Enter a name for the remote device.
Type	Select the type of device. If the device is IP-based, select **IP Ethernet Device**. If the device is an L2 device, select **L2 Ethernet Device**. Depending on which type you choose, different options are available.
Local IP	If you selected **IP Ethernet Device**, specify the device's local IP address.
MAC	If you selected **L2 Ethernet Device**, specify the device's MAC address.
NAT IP	If you selected **IP Ethernet Device**, specify the NAT IP address. This should be in the same subnet as the WAN IP. The NAT IP allows the device to be managed when it is connected to the MRC gateway and allows it to connect to the Internet.
Health Check	If you selected **IP Ethernet Device**, disable or select a method for monitoring the health of the gateway. Select **Ping Check** to set up an interval to ping the gateway. It is recommended to set the interval to be within 60 seconds. Select **Port Link** to configure which port to monitor, for example port #1 (LAN/WAN) or port #2 (LAN). The gateway will update the status to the client accordingly.

A-9. In the device list, click the **Edit** icon (✏️) of the device to edit.

A-10. In the Service window, select which device services will be available for remote access. By default, all services will be available. Multiple service rules can be added to the service whitelist.

In the example below there is a Modbus TCP device that allows client *moxatest* to access its services by adding *moxatest* to the Allowed Client List. Any client not in the list will not be able to access this service.

A-11. When you are done editing the service rules, click (✕) to save the configuration and click **Next** to continue to the next step in the Wizard.

A-12. Select a Tunnel Control method and click **Next**. Refer to the table below for more information about each method.

Note: For remote maintenance purposes, it is recommended to use Controlled by USB or Controlled by DI ON in order to save on data transportation cost and monthly MRC Quick Link data usage. Permanent Connection is recommended to keep the connection to pull data for remote data acquisition purposes.

Item	Description
Permanent Connection	The gateway will maintain a permanent VPN connection to the MRC portal.
Controlled by USB Key	The gateway will only create a VPN connection to the MRC portal when a USB containing the activation key is inserted. If the USB with the key is removed, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable.
Controlled by DI ON	The gateway will only create a VPN connection to the MRC portal when the DI status is ON. When DI is set to OFF, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable. Users can install a button to trigger the DI to open and close the tunnel. An input of +13 to +30 V enables the connection and -30 to +3 V disables the connection. The maximum input current is 8 mA.

A-13. Click **Save and Finish** to complete the Wizard. Click **Continue Wizard** to repeat these steps to add additional gateways.

A-14. Continue to **3. Generate and Distribute the Client and Gateway Keys**.

B. Using Transparent-LAN Mode

In some circumstances, the gateway needs to be integrated in an existing factory network while keeping the original network settings. In Transparent-LAN mode, the MRC gateway is installed in between the target Ethernet device and the original network. The MRC gateway's WAN port is connected to the original network using the factory network's ISP for accessing the Internet. The target Ethernet device is connected directly to the LAN port without needing to change the network configuration of the device.

B-1. Click the **Menu** icon (▤) in the top-left corner and select **Wizard**.

B-2. Click **Create Gateway**.

B-3. Specify the required information and click **Next**. Refer to the table below for more information about each setting.

Item	Description
Gateway Name	Enter a name for the gateway. This name is how the device will appear in the interface.
Location	Enter a location keyword such as a city name or specific address. The MRC Server will automatically populate the latitude and longitude fields with the Google Maps coordinates of the location closest to the keyword.
Latitude	Enter the latitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Longitude	Enter the longitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Lock to MAC Address	The MRC gateway settings can be locked to the gateway's MAC address. The activation key that has been generated after locking the gateway will only be authorized for use on the MRC gateway that matches the specified MAC address.

Item	Description
Auto IP Mapping	Auto IP Mapping ensures that the MRC gateway and each of the devices connected to the gateway will be assigned an individual virtual IP address within the device group. This virtual IP address represents the device and the MRC clients can use the virtual IP addresses to access each machine without causing an IP address conflict. It is recommended to enable this feature.
Gateway to Gateway	In some applications, machine-to-machine communication is not necessary. Disabling the Gateway to Gateway function will block traffic coming from the machines that are connected to other MRC gateways and only allows the MRC client to access the machines behind the MRC gateway. Enabling the function allows machine-to-machine communications through the MRC gateways.
Broadcast/Multicast Forwarding	The MRC gateway and the MRC portal support different types of industrial communication. For example, an EtherNet/IP application may require you to enable Multicast Forwarding, while enabling Broadcast Forwarding may be necessary for broadcast search applications.

B-4. Select **Transparent Mode** as the scenario and click **Next**. If your application requires WAN-LAN or cellular Internet access, go to the respective section listed below:

To configure WAN-LAN mode, go to Using WAN-LAN Mode.
To configure Cellular-WAN mode, go to Using Cellular-WAN Mode.

B-5. Specify the connection settings. Available options vary depending on which IP Address Mode you select. Refer to the respective connection settings for more information about each option.

If you selected **Static IP** as the IP Address Mode:

Item	Description
IP Address	Enter the local IP address of the gateway.
Subnet Mask	Enter the subnet mask of the gateway.
Gateway	Enter the default gateway address.
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

If you selected **DHCP** as the IP Address Mode:

Item	Description
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

B-6. Click the **Add** icon ⊞ to add devices to the list of remotely accessible devices. Up to 25 devices can be added to the list. If Auto IP Mapping is enabled, each added device will be assigned a virtual IP.

Note: If you have disabled Auto IP Mapping in step **B-3** it is still recommended to manually add devices to this list for security reasons. Skipping adding devices while Auto IP Mapping is disabled will allow all devices in the local subnet based on the gateway's LAN configuration to be remotely accessed. For example, if the gateway is configured to be 192.168.127.254/24, all Ethernet devices or machines in the 192.168.127.x subnet will be available for remote access.

B-7. In the Add Device window, specify the following information and click **Save**.

Item	Description
Local Device Name	Enter a name for the remote device.
Type	Select the type of device. If the device is IP-based, select **IP Ethernet Device**. If the device is an L2 device, select **L2 Ethernet Device.** Depending on which type you choose, different options are available.
Local IP	If you selected **IP Ethernet Device**, specify the device's local IP address.
MAC	If you selected **L2 Ethernet Device**, specify the device's MAC address.
NAT IP	If you selected **IP Ethernet Device**, specify the NAT IP address. This should be in the same subnet as the WAN IP. The NAT IP allows the device to be managed when it is connected to the MRC gateway and allows it to connect to the Internet.
Health Check	If you selected **IP Ethernet Device**, disable or select a method for monitoring the health of the gateway. Select **Ping Check** to set up an interval to ping the gateway. It is recommended to set the interval to be within 60 seconds. Select **Port Link** to configure which port to monitor, for example port #1 (LAN/WAN) or port #2 (LAN). The gateway will update the status to the client accordingly.

B-8. In the device list, click the **Edit** icon (⬚) of the device to edit.

B-9. In the Service window, select which device services will be available for remote access. By default, all services will be available. Multiple service rules can be added to the service whitelist.

In the example below there is a Modbus TCP device that allows client *moxatest* to access its services by adding *moxatest* to the Allowed Client List. Any client not in the list will not be able to access this service.

B-10. When you are done editing the service rules, click (✕) to save the configuration and click **Next** to continue to the next step in the Wizard.

B-11. Select a Tunnel Control method and click **Next**. Refer to the table below for more information about each method.

Note: For remote maintenance purposes, it is recommended to use Controlled by USB or Controlled by DI ON in order to save on data transportation cost and monthly MRC Quick Link data usage. Permanent Connection is recommended keep the connection to pull data for remote data acquisition purposes.

Item	Description
Permanent Connection	The gateway will maintain a permanent VPN connection to the MRC portal.
Controlled by USB Key	The gateway will only create a VPN connection to the MRC portal when a USB containing the activation key is inserted. If the USB with the key is removed, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable.
Controlled by DI ON	The gateway will only create a VPN connection to the MRC portal when the DI status is ON. When DI is set to OFF, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable. Users can install a button to trigger the DI to open and close the tunnel. An input of +13 to +30 V enables the connection and -30 to +3 V disables the connection. The maximum input current is 8 mA.

B-12. Click **Save and Finish** to complete the Wizard. Click **Continue Wizard** to repeat these steps to add additional gateways.

B-13. Continue to **3. Generate and Distribute the Client and Gateway Keys**.

C. *Using Cellular-WAN Mode*

Cellular-WAN mode is used for situations where the gateway connects to the Internet using a cellular connection. In this scenario, a SIM card with an active subscription is installed in the gateway and the LAN port connects directly to the target Ethernet device, or to a switch if you need to connect multiple devices to the gateway.

C-1. Click the **Menu** icon ☰ in the top-left corner and select **Wizard**.

C-2. Click **Create Gateway**.

C-3. Specify the required information and click **Next**. Refer to the table below for more information about each setting.

Item	Description
Gateway Name	Enter a name for the gateway. This name is how the device will appear in the interface.
Location	Enter a location keyword such as a city name or specific address. The MRC Server will automatically populate the latitude and longitude fields with the Google Maps coordinates of the location closest to the keyword.
Latitude	Enter the latitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Longitude	Enter the longitude coordinate of the gateway. If using a location keyword, this will be automatically populated by the system.
Lock to MAC Address	The MRC gateway settings can be locked to the gateway's MAC address. The activation key that has been generated after locking the gateway will only be authorized for use on the MRC gateway that matches the specified MAC address.

Item	Description
Auto IP Mapping	Auto IP Mapping ensures that the MRC gateway and each of the devices connected to the gateway will be assigned an individual virtual IP address within the device group. This virtual IP address represents the device and the MRC clients can use the virtual IP addresses to access each machine without causing an IP address conflict. It is recommended to enable this feature.
Gateway to Gateway	In some applications, machine-to-machine communication is not necessary. Disabling the Gateway to Gateway function will block traffic coming from the machines that are connected to other MRC gateways and only allows the MRC client to access the machines behind the MRC gateway. Enabling the function allows machine-to-machine communications through the MRC gateways.
Broadcast/Multicast Forwarding	The MRC gateway and the MRC portal support different types of industrial communication. For example, an EtherNet/IP application may require you to enable Multicast Forwarding, while enabling Broadcast Forwarding may be necessary for broadcast search applications.

C-4. Select **Transparent Mode** as the scenario and click **Next**. If your application requires WAN-LAN or cellular Internet access, go to the respective section listed below:

To configure WAN-LAN mode, go to Using WAN-LAN Mode.
To configure Transparent-LAN mode, go to Using Transparent-LAN Mode.

C-5. Specify the connection settings.

Item	Description
Carrier	Select the carrier of the SIM card installed in the MRC gateway. Select Generic if your SIM card is not provided by Verizon or AT&T.
APN	Enter the SIM card's APN. If you do not have this information, leave this field blank.
PIN	Enter the SIM card's PIN. If you do not have this information, leave this field blank.
Username	Enter the SIM card's user name. Some operators may not provide this. If you do not have this information, leave this field blank.
Password	Enter the SIM card's password. Some operators may not provide this. If you do not have this information, leave this field blank.
Cellular Keep-Alive	Some carriers may stop cellular data services when there is no active traffic for a certain period time. Enable Cellular Keep-Alive to prevent cellular data services from being stopped when idle.
Cellular Watchdog	Cellular Watchdog automatically restarts the cellular module once an unusual connection behavior to the carrier is detected.
DNS 1/2/3	Enter the DNS server address for the gateway. If this is left blank, the gateway will automatically default to the Google DNS (8.8.8.8).

C-6. Click the **Add** icon (+) to add devices to the list of remotely accessible devices. Up to 25 devices can be added to the list. If Auto IP Mapping is enabled, each added device will be assigned a virtual IP.

Note: If you have disabled Auto IP Mapping in step **C-3** it is still recommended to manually add devices to this list for security reasons. Skipping adding devices while Auto IP Mapping is disabled will allow all devices in the local subnet based on the gateway's LAN configuration to be remotely accessed. For example, if the gateway is configured to be 192.168.127.254/24, all Ethernet devices or machines in the 192.168.127.x subnet will be available for remote access.

C-7. In the Add Device window, specify the following information and click **Save**.

Item	Description
Local Device Name	Enter a name for the remote device.
Type	Select the type of device. If the device is IP-based, select **IP Ethernet Device**. If the device is an L2 device, select **L2 Ethernet Device**. Depending on which type you choose, different options are available.
Local IP	If you selected **IP Ethernet Device**, specify the device's local IP address.

Item	Description
MAC	If you selected **L2 Ethernet Device**, specify the device's MAC address.
NAT IP	If you selected **IP Ethernet Device**, specify the NAT IP address. This should be in the same subnet as the WAN IP. The NAT IP allows the device to be managed when it is connected to the MRC gateway and allows it to connect to the Internet.
Health Check	If you selected **IP Ethernet Device**, disable or select a method for monitoring the health of the gateway. Select **Ping Check** to set up an interval to ping the gateway. It is recommended to set the interval to be within 60 seconds. Select **Port Link** to configure which port to monitor, for example port #1 (LAN/WAN) or port #2 (LAN). The gateway will update the status to the client accordingly.

C-8. In the device list, click the **Edit** icon ![edit icon] of the device to edit.

C-9. In the Service window, select which device services will be available for remote access. By default, all services will be available. Multiple service rules can be added to the service whitelist.

In the example below there is a Modbus TCP device that allows client *moxatest* to access its services by adding *moxatest* to the Allowed Client List. Any client not in the list will not be able to access this service.

C-10. When you are done editing the service rules, click (⊠) to save the configuration and click **Next** to continue to the next step in the Wizard.

C-11. Select a Tunnel Control method and click **Next**. Refer to the table below for more information about each method.

Note: For remote maintenance purposes, it is recommended to use Controlled by USB or Controlled by DI ON in order to save on data transportation cost and monthly MRC Quick Link data usage. Permanent Connection is recommended keep the connection to pull data for remote data acquisition purposes.

Item	Description
Permanent Connection	The gateway will maintain a permanent VPN connection to the MRC portal.
Controlled by USB Key	The gateway will only create a VPN connection to the MRC portal when a USB containing the activation key is inserted. If the USB with the key is removed, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable.
Controlled by DI ON	The gateway will only create a VPN connection to the MRC portal when the DI status is ON. When DI is set to OFF, the VPN will be terminated and all connected Ethernet devices and machines will no longer be reachable. Users can install a button to trigger the DI to open and close the tunnel. An input of +13 to +30 V enables the connection and -30 to +3 V disables the connection. The maximum input current is 8 mA.

C-12. Click **Save and Finish** to complete the Wizard. Click **Continue Wizard** to repeat these steps to add additional gateways.

C-13. Continue to **3. Generate and Distribute the Client and Gateway Keys**.

3. Generate and Distribute the Client and Gateway Keys

Once the gateway and clients have been configured on the MRC server, the activation keys can be generated and distributed to the machine operator and support engineer respectively. These activation keys are required to be installed on the MRC Client software and the MRC gateway device in order to establish and authorize the remote connection.

3-1. Click the **Menu** icon (▤) in the top-left corner and select **Gateway Management**.

3-2. Click **Settings** and then click the **Download** button (⬇) to download the activation key file for the MRC gateway.

3-3. Click the **Menu** icon (▤) in the top-left corner and select **Client Management**.

3-4. Click **Settings** and then click the **Download** button (⬇) to download the activation key file for all configured clients.

3-5. Distribute the gateway key to the machine operator and the client key to the support engineer.

3-6. Continue with **Step 3: [Machine Operator] Set up and Pair the Gateway**.

Step 3: [Machine Operator] Set up and Pair the Gateway

Before the gateway can be accessed remotely, the activation key provided by the MRC server admin has to be installed onto the gateway device. This process is handled on-site by the machine operator.

Note: Before continuing this process, please make sure your MRC-1002 gateway is updated to firmware version 2.4 or higher.

---

1. Connect the WAN port of the gateway to the Internet, and the LAN port to the Ethernet device or switch. If the gateway was configured to use a cellular connection, insert the SIM card.
2. Download the gateway key received from the MRC server admin and put it onto a USB drive. Ensure that the activation key is in the root folder of the USB drive.
3. Insert the USB drive with the activation key into the MRC-1002 gateway and power it on.
4. When all LEDs are lit, the MRC gateway is connected to the MRC server and is ready for remote access.
5. Continue with **Step 4: [Support Engineer] Set up and Pair the Clients.**

Connect to Internet

Connect to local network or device

Make sure the activation key is in the root directory

Step 4: [Support Engineer] Set up and Pair the Clients

The MRC Client Software and the client key need to be installed on the PC that is used to remotely connect and interact with the field equipment. This part of the process is handled by the support engineer.

1. Download the MRC Client Software from <u>our website</u> to the target computer. The MRC-Client software can be installed on systems running Windows 7 or Windows 10. Before installing the software, please make sure the system environment is equipped with **Microsoft .NET Framework version 4.0 or higher**.

Note: Before continuing this process, please make sure that the MRC Client Software is version 2.4 or higher.

Note: Windows 7 and Windows 10 already have .NET Framework v4.5 installed. To double-check which version of Microsoft .NET Framework is installed, go to the **Control Panel > Programs > Programs and Features**. The .NET Framework version is shown in the program name.

2. Right-click the MRC Client Software installation package and select **Run as administrator**. Follow the on-screen instructions to complete the installation.

Name	^	Date modified	Type	Size
moxa-moxa-remote-connect-suite-mrc-client-sw-software-package-v2.4.exe		1/21/2020 9:43 AM	Application	20,468 KB

Open
🛡 Run as administrator
Troubleshoot compatibility
Run with graphics processor
Pin to Start
7-Zip
↪ Share

3. Once installed, run the MRC Client Software.

4. Download the MRC client key received from the MRC server admin.

5. Select **Import activation file**, click the browse icon (   ) and locate the MRC client key, and click **Apply**. Next, click **Sign In**.

6. On the Device Pool tab, click the Tunnel icon of the device(s) you want to access remotely. If the icon is green, the tunnel is active. If the icon is red, the tunnel is disabled.

7. The gateway and clients are now configured and the devices can be remotely accessed.

Example Application 1

Case 1: Siemens PLC with TIA portal and no Auto IP mapping

In the following example application, we are using MRC Quick Link to remotely turn on a motor through a Powerflex drive connected to a Siemens PLC with TIA portal. In this example, Auto IP Mapping is disabled.

Network Diagram

Step 1: Set up MRC and Enable Remote Connections

Note: It is highly recommended to create a new Siemens TIA Portal project first and add all the devices to the project before continuing with the MRC configuration.

1. Configure the clients, gateway, and gateway devices on the MRC server. In this example, we named the gateway *MRC_demo* and added the Siemens PLC and Powerflex drive as devices.

2. Download and distribute the gateway and MRC client keys.

3. Install and right-click the MRC Client Software shortcut and click **Run as administrator**. Sign in using the activation key file. The MRC gateway's (*MRC_demo*) status will be green, indicating the MRC gateway is ready for remote access.

4. Expand *MRC demo* in the device list to show all devices under the gateway and switch on the tunnel of each device. This allows the MRC client to establish connections to the Siemens PLC and Powerflex drive.

Step 2: Set up the Powerflex Drive and PLC in TIA Portal

Configure Go Online for the Powerflex Drive

1. Start Siemens TIA portal and open the previously created project. Confirm the PLC and Powerflex drive are shown in the device list on the left-hand side.

2. Perform the following actions to start scanning for the drive:

    2-1. Select the Powerflex drive from the device list.

    2-2. Double-click **Go Online**.

    2-3. Confirm that the IP address of the drive in TIA portal is the same as the IP defined in the MRC Client Software. In this example, the drive IP address should be 192.168.127.55.

    2-4. From the **PG/PC interface** drop-down menu, select **TAP-Windows Adapter V9**.

    2-5. Click **Start search**.

3. Wait for TIA Portal to finish the scan. A pop-up window will appear prompting you to assign an IP address to the PG/PC. Click **Yes**.

4. A confirmation will appear that the IP address was successfully assigned. Click **OK**.

5. The status of the Powerflex drive in the device list should now have a green checkmark, indicating the TIA Portal successfully connected to the drive. Continue to **Configure Go Online for the PLC**.

Configure Go Online for the PLC

1. Open the Siemens TIA portal and make sure the Powerflex drive and PLC are shown in the list on the left-hand side.

2. Perform the following actions to start scanning for the PLC:

   2-1. Select the PLC from the device list.

   2-2. Double-click **Go Online**. The system will automatically search and connect to the PLC based on the previous controller settings.

3. The status of the PLC in the device list should now have a green checkmark, indicating the TIA Portal successfully connected to the PLC. Continue with **Step 3: Control the Powerflex Drive and Turn on the Motor**.

Step 3: Control the Powerflex Drive and Turn on the Motor

1. Select and expand **PLC_1** in the device list.

2. In the expanded tree, click the **Watch and force tables** folder and double-click **Watch table**. The main window will display the watch table. Rows 18 and 19 are the tags for the motor. Row 18 is used for turning the motor on or off, row 19 controls the speed of the motor.

3. Perform the following actions to power on the motor:

3-1. Double-click the **Modify value** field of row 18 and change the value to either **TRUE** or **1**. The Monitor Value column will be highlighted in orange, indicating all tags can be modified.

3-2. Double-click the **Power** icon (⚡1) to execute the command.

4. The Powerflex drive will now power on the motor.

Example Application 2

Case 2: Rockwell PLC with RSLinux portal and Auto IP mapping

In this example, we are using MRC Quick Link to remotely turn on a motor through a Powerflex drive connected to a Rockwell PLC with RSLinx portal. In this example, Auto IP Mapping is enabled.

Network diagram

MRC Server

MRC Gateway
107.10.50.134

Rockwell PLC
107.10.50.136

Powerflex Drive
107.10.50.137

Motor

1. Rockwell RSLinx Classic
2. Rockwell Studio 5000
3. MRC Client Software

Step 1: Set up MRC and Enable Remote Connections

Note: It is highly recommended to create a new Rockwell Studio 5000 project first with Run Mode enabled and add all the devices to the project before continuing with the MRC configuration.

1. Configure the clients, gateway, and gateway devices on the MRC server. In this example, we named the gateway *MRC Rockwell* and added the Rockwell PLC, Powerflex drive, and an optional Stratix5400 switch as devices.

2. Download and distribute the gateway and MRC client keys.

3. Install and right-click the MRC Client Software shortcut and click **Run as administrator**. Sign in using the activation key file. The MRC gateway's (*MRC_Rockwell*) status will be green, indicating the MRC gateway is ready for remote access.

4. Expand *MRC_Rockwell* in the device list to show all devices under the gateway and switch on the tunnel of each device. This allows the MRC client to establish a remote connection to the drive and PLC.

Step 2: Browse Devices with RSLinx Classic

1. Open RSLinx Classic. Right-click **AB_ETHP-1 Ethernet** and click **Configure Driver**.

2. Select **TAP-Windows Adapter V9** and click **Confirm**.

3. Perform the following actions to add the virtual IP addresses of devices to the browse scope. In this example, we are adding the PLC and drive.

    3-1. Double-click **AB_PCL, Ethernet**.

    3-2. Click **Add New** to create a new line. Add one line for the PLC and one line for the drive.

    3-3. Double click the Host Name field of each line and enter the virtual IP address of the PLC (10.0.1.35) and the drive (10.0.1.36). In this example, we also added the optional Stratix switch (10.0.1.34).

    3-4. Click **Apply**.

    3-5. Click **OK**.

4. Check the **Autobrowse** checkbox in the top-left and RSLinx will start to browse for the devices. The devices will appear under **AB, PLC_Ethernet** in the table on the left-hand side. When all devices are discovered, continue to **Step 3: Go Online and configure PLC and Powerflex Drive with Studio 5000**.

Step 3: Go Online and Configure the PLC and Powerflex Drive with Studio 5000

1. Run Studio 5000 and open the previously created user project containing all the devices.

2. If you have not enabled Run Mode when creating the project, click [icon] and select **Run Mode**.

3. Click the **Path** icon (⚙) to open the communication path list and select **AB_PLC\10.0.1.35** from the list, then click **Go Online**.

4. Wait for Studio 5000 to connect to the device. Going online with the controller may take up to 10 minutes. When the event log at the bottom indicates the search is complete, continue to the next step.

5. Double-click the Powerflex drive in the Controller Organizer list and confirm the status is **Running**.

6. Double-click **Controller Tags** from the Controller Organizer list.

7. Expand the **Powerflex_1:O** table and search for **PowerFlex_1:O.start**. Click the Value field and change **0** to **1** to instruct the Powerflex drive to power on the motor.