Stratix 4300 Remote Access Routers

Catalog Numbers 1783-RA2TGB, 1783-RA2TGC4G, 1783-RA2TGW, 1783-RA2TGWC4G, 1783-RA5TGB, 1783-RA5TGC4G, 1783-RA5TGW, 1783-RA5TGWC4G

Allen-Bradley
by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.

Identifies information that is useful and can help to make a process easier to do or easier to understand.

Chapter 1

Remote Access Architecture

Chapter 2

Router Integration

Chapter 3

Router Configuration

Appendix A

Troubleshoot

Appendix B

SIM Card Requirements and Configuration Example

About This Publication

This manual describes how to use the Stratix® 4300 Remote Access™ Routers.

Make sure that you are familiar with use of an EtherNet/IP™ network.

Product compatibility information and release notes are available online within the Product Compatibility and Download Center.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Remote Access Routers	9
Router Configuration	25
Network Address Translation (NAT) Rules	42
Status Indicators	49

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
EtherNet/IP Network Devices User Manual, publication ENET-UM006	Describes how to configure and use EtherNet/IP devices to communicate on the EtherNet/IP network.
Ethernet Reference Manual, publication ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
FactoryTalk® Remote Access™ Help website, rok.auto/help	Describes how to use and troubleshoot FactoryTalk Remote Access.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley® industrial automation controls and assemblies.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.
Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
Stratix 4300 Remote Access Routers Installation Instructions, publication 1783-IN020	Describes how to install a Stratix 4300 Remote Access Router.
Stratix Ethernet Device Specifications Technical Data, publication, 1783-TD002	Describes the technical specifications of Stratix Devices.
System Security Design Guidelines Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.

You can view or download publications at rok.auto/literature.

Notes:

Remote Access Architecture

The Stratix® 4300 Remote Access™ Router provides the ability for manufactures and OEMs to apply the appropriate skills and resources independent of their physical location by enabling our customers to continue to maintain their operations with remote access via VPN. The solution helps reduce costs, add value to customer operations, and encourage collaboration between OEMs and customers.

The router:

- 1 gigabit ports
- Supports configuration via FactoryTalk® Remote Access™ software
- Uses VPN connections that are optimized for industrial communications with reduced latency
- Supports hard-wired, cellular, and wireless connections for communications to FactoryTalk Remote Access software

Factory Talk Remote Access software:

- Manages user and group configurations to segment network access and permissions
- Provides log and audit trails for activities for established connections

Remote Access Solution Overview

Before You Begin

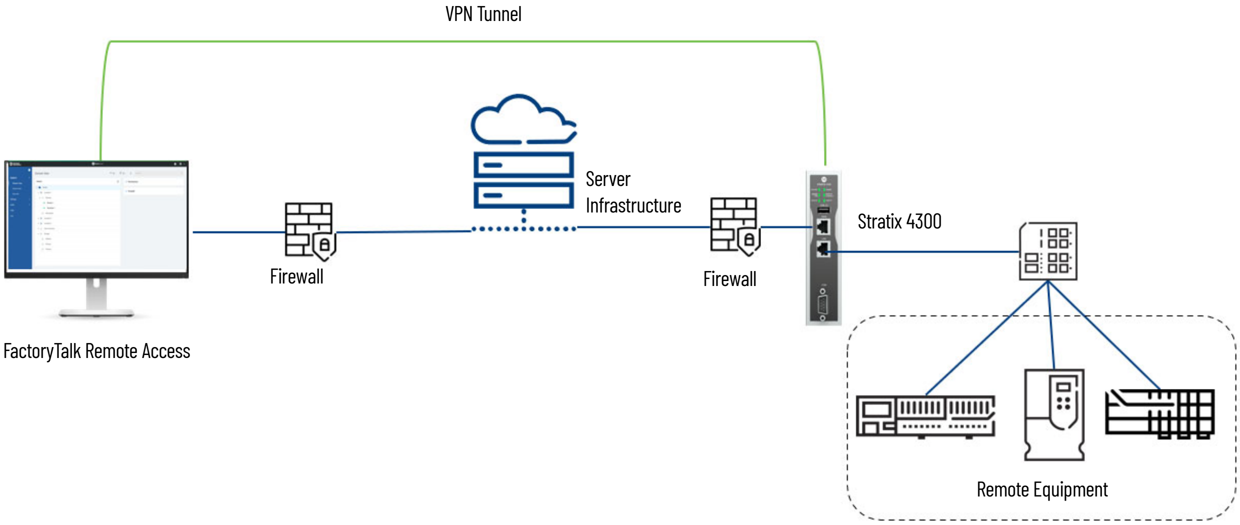
Remote Access for Industrial Equipment enables connectivity to remote machines by leveraging optimized VPN technologies. The remote access solution includes hardware and software.

There are three key components for remote access.

1. The Stratix 4300 Remote Access Router enables access to remote equipment through a VPN connection.
2. Server infrastructure is a distributed cloud-based server infrastructure that facilitates the connections.
3. FactoryTalk Remote access is a web-based client that is used to maintain and initiate remote connections.

Together, these products enable secure access to industrial machines, skids, and assets.

The Stratix 4300 must be registered to FactoryTalk Remote Access before a connection can be initiated.



Best Practices

- FactoryTalk Remote Access Administrator enforces two-factor-authentication.
- The FactoryTalk Remote Access software must be up to date in case security improvements are released.
- Configure strong, complex user passwords.
- These routers must be connected to the Internet through its WAN port. Stratix 4300 routers do not enable any service through that port and only need an outgoing connection through to the configured outgoing port (TCP port 443, 80, or 5935). An additional firewall can provide more protection.
- Undertake a formal threat and risk assessment in relation to remote access.
- Use the provided role-based access control.
- Use the provided physical controls to enable or disable remote access.
- Monitor security incidents and logs pro-actively to provide timely incident response and accurate forensics.
- Conduct regular reviews and assessments of the secure remote access solution and technologies to maintain compliance with policies and procedures.
- Apply defense in depth practices for the secure remote access solution, including practices to secure the remote computer.

Remote Access Routers

Remote Access Router Front Panel View

Figure 1 - Router Front View

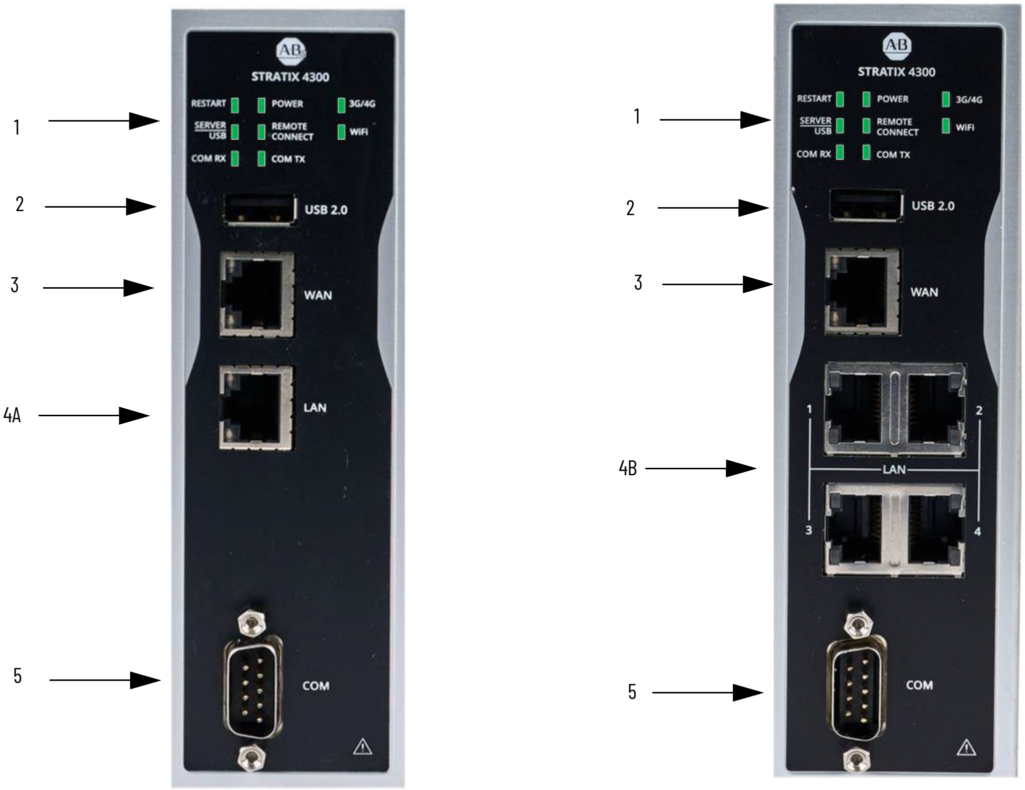


Table 1 - Router Front View

1	Status Indicator[1]s: • Restart Status Indicator • Server/USB Status Indicator • COM RX Status Indicator • Power Status Indicator • Remote Status Indicator • COM TX Status Indicator • 3G/4G Status Indicator • Wi-Fi Status Indicator
2	USB 2.0
3	WAN
4A	LAN
4B	LAN1 LAN2 LAN3 LAN4
5	COM

[1] For more information on status indicators, see Appendix A.

Figure 2 - Router Top View

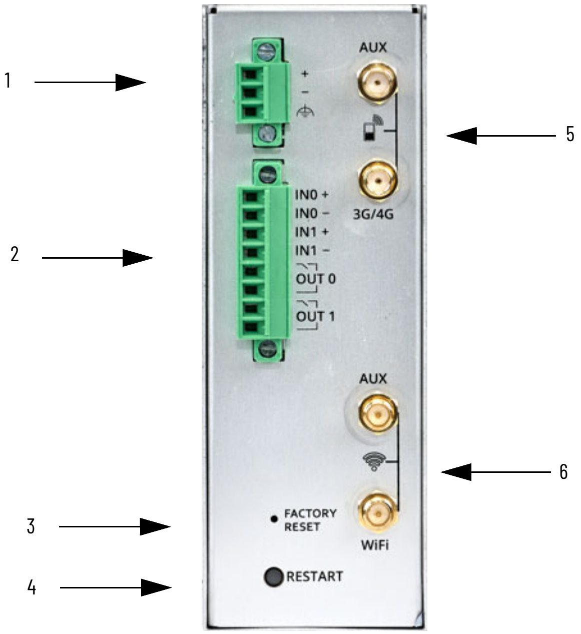


Table 2 - Router Top View

1	Power Connector
2	Digital input/output Connector
3	Factory Reset Button
4	Restart Button
5	Cellular/Auxiliary Cable Port
6	WiFi/Auxiliary Cable Port

WARNING: When you press the Factory Reset button while power is on, an electric arc can occur, which could cause an explosion in hazardous location installations.

Table 3 - Router Top View Definitions

Digital input/output	IN0	This input works as a Connection mode, also referred as selector key input. By default, the status of this input is ignored. When the router is configured to handle the input, it can be controlled from outside the connection to the server. The input can be driven by a mechanical selector, by a key selector, or by a PLC output.
	IN1	This input controls the device restart from outside. The operation corresponds to the restart button. Once the command is received a proper feedback is returned by the status indicator.
	OUT0	The output is active when the router is connected to its associated Domain. The simple connection to the server does not activate the output. The Stratix 4300 is required to be successfully authenticated to the Domain
	OUT1	The output is active when at least one user is remotely connected to the Router.
Factory Reset		A factory reset reverts the router to factory settings. The system software is reset to its original versions including the operating system. To execute the reset, turn off the device. Press and hold down the restart button for at least 10 seconds. To reach the button, use a small tool, such as a paper clip. The status indicator blinks from red to green multiple times when the reset process has started. Wait for the process to be completed and restart the system.
Restart		Forces the device to restart. This command verifies a complete initialization of all internal electronics and software. The restart status indicator turns on.
Wi-Fi		Intel AC9260, IEEE 802.11a/b/g/n/ac, 2.4GHz/5GHz; Security: WEP 64/128 bit, WPA, WPA2, WPS.
Cellular		2G/3G./4G LTE CAT4 Multi-Band, Multi-region support.

Multi-factor Authentication

Multi-factor authentication is a secure way to protect access to your account, available through FactoryTalk Remote Access.

Multi-factor authentication is enabled when you first sign in to FactoryTalk Remote Access. You receive a message that multi-factor authentication must be configured and activated before use.

1. To display a QR Code for configuration, click the activation link.

   This link can be scanned with any application that supports the Google Authenticator standard.
2. To download and authenticator app, use one of the following links from your device:

- Authy
- Google Authenticator
- Duo
- Microsoft® Authenticator

If your device cannot scan the QR Code, click the link “Cant Read?” to view the security code to be used with your authentication application as an alternative to scanning the QR Code.

After the first sign in, each following sign in asks for your authenticator code. This code is updated every 3 minutes.

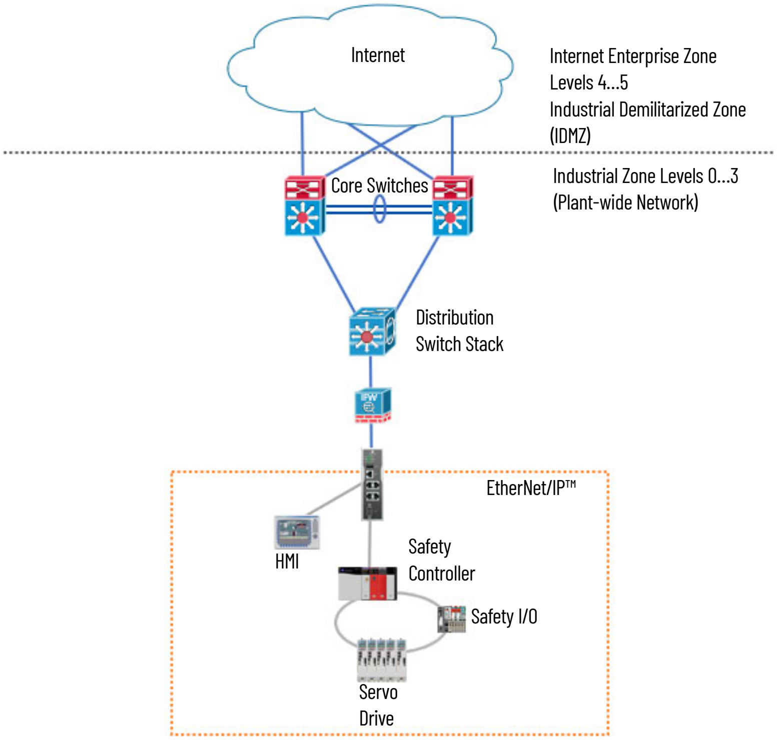
3. Open the authenticator application on your device and type in the current code that is assigned to your account.

Typical Remote Access Architectures

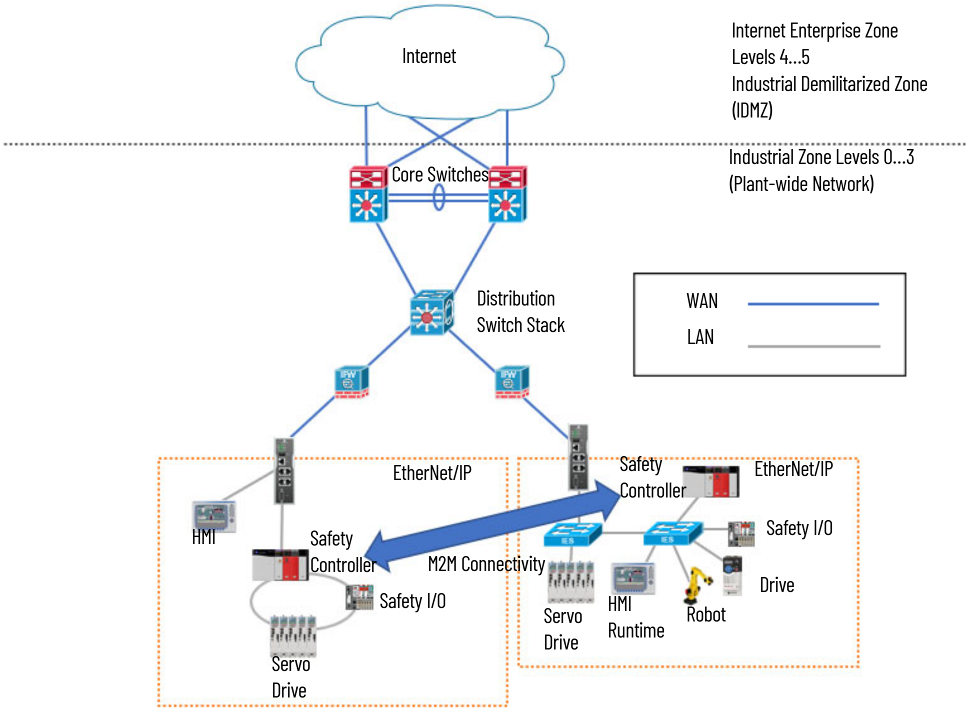
The following examples are common remote access architecture diagrams.

Secure Remote Connectivity - Use Case: Cell/Area Zone SRA

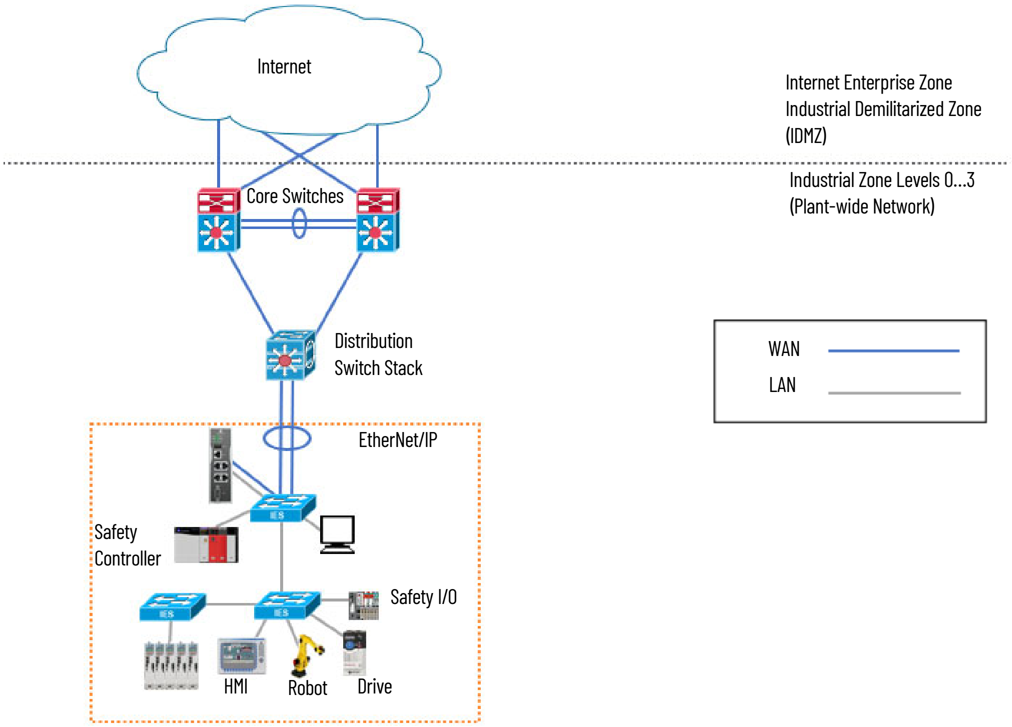
This architecture is highlighting the usage of the Stratix 4300 for remote access purposes and, if needed, for NAT/Routing purposes for the cell/area zone. Without NAT or Routing, there are no North or South data flows through the Stratix 4300. East or West data flow (for example from the HMI to the Safety Controller) within the cell/area zone occurs in the embedded switch of the Stratix 4300.



The following architecture is highlighting the use of the Stratix 4300 for remote access purposes and NAT/Routing purposes. The Stratix 4300 provides remote access to each individual cell/area zone. If there is a need for peer-to-peer or machine-to-machine communication, the Stratix 4300 NAT or Routing features can be configured to allow successful communication.

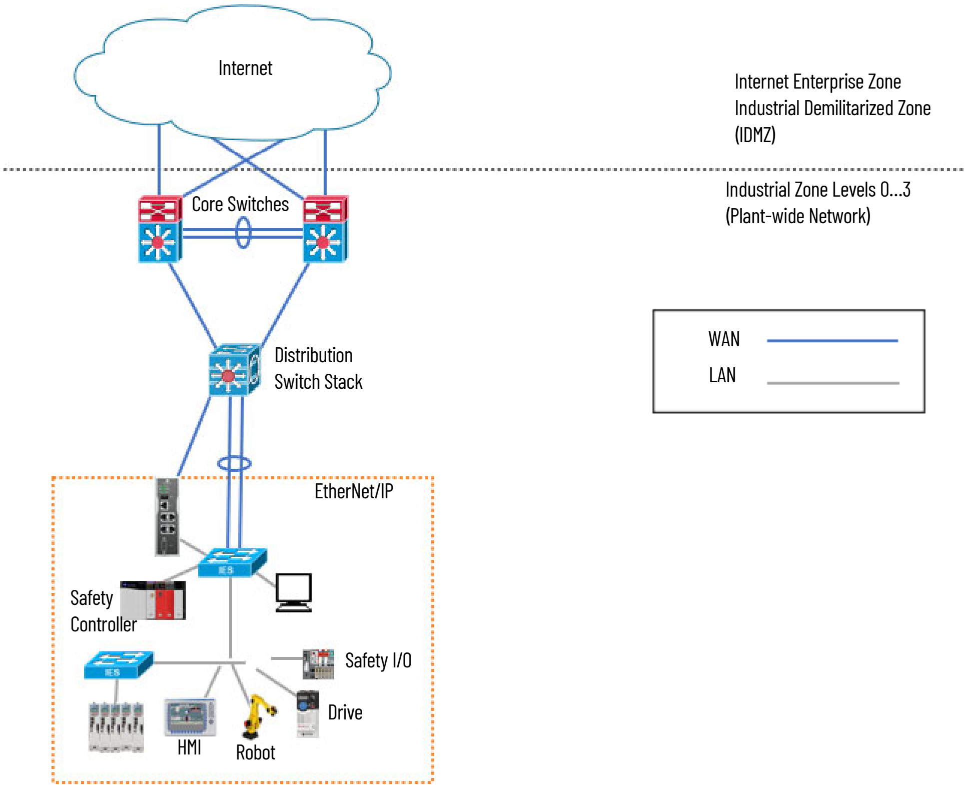


The following architecture is highlighting the use of the Stratix 4300 for remote access purposes. An IES is positioned in the cell for any other North/South and East/West traffic. The IES switching infrastructure also provides routing and switching services to all devices including the Stratix 4300. The VLAN required for Internet access or WAN must be extended into the cell/area zone IES to provide this is to verify that the Stratix 4300 has Internet access for remote access.



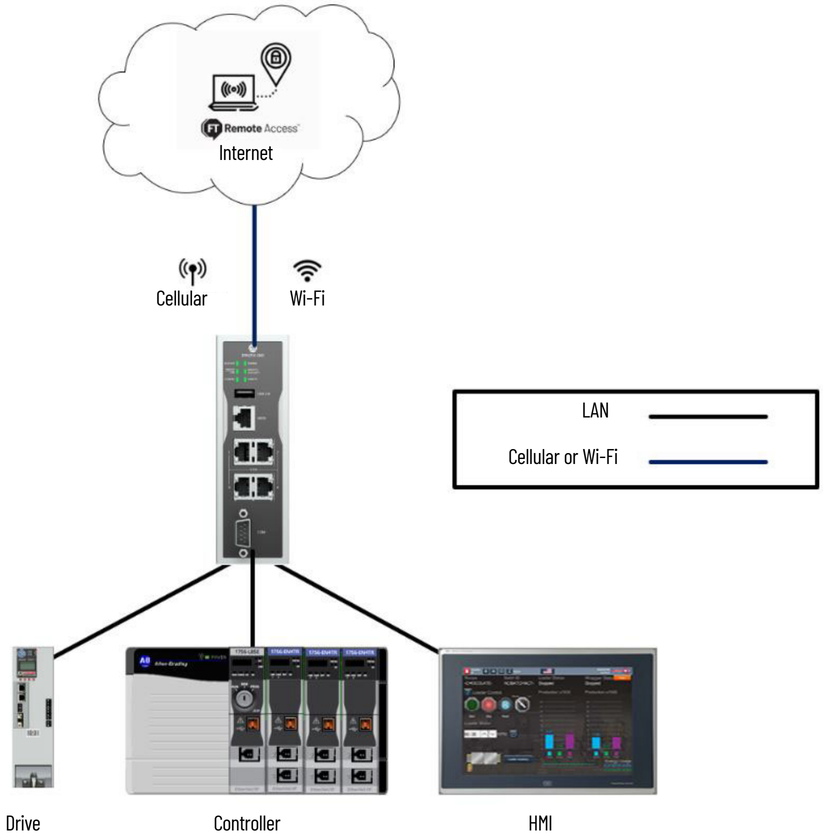
The following architecture is highlighting the usage of the Stratix 4300 for remote access purposes. An IES is positioned in the cell for any other North/South and East/West traffic. The IES switching infrastructure also provides routing and switching services to all devices. In this case, the IES is not providing routing to the Stratix 4300 WAN connection.

The WAN is connected directly to distribution to ease routing requirements. Any cloud or remote access-related traffic from the Stratix 4300 goes directly to the distribution switch. Generally, the distribution switch is the central router for the industrial architecture before the Core routes traffic. No VLAN or routing extends to the Cell/Area Zone in this architecture unless the industrial application requires it.



Secure Remote Connectivity - Use Case: Modem Direct/Isolated Machine

The following architecture highlights a remote isolated cell. For the Internet connection in this architecture, an Internet modem like those provided by most Internet service providers is used. For the Internet connection in this architecture, a cellular or wireless connection to the Internet can be used.



Router Integration

The Stratix® 4300 Remote Access™ Router can be configured using an Ethernet connection to the device. You need access to the hardware, FactoryTalk® Hub™, FactoryTalk® Remote Access™, and an Internet connection for this configuration. It is recommended that you correct directly to the router via Ethernet for configuration with system manager. See Router Configuration.

FactoryTalk Hub

To use FactoryTalk Hub, either create an organization or join an existing organization. The organization that you belong to control the services available to you in FactoryTalk Hub.

Authentication

FactoryTalk Hub uses your MyRockwell user profile to authenticate your access and determine your organization. You can be a member of multiple organizations.

After your account has been authenticated, your browser displays the FactoryTalk Hub Home screen. Panels are displayed that identify the services entitled for your use.

The organizational administrator can use the Portal Menu to add an entitlement, manage the FactoryTalk Hub subscription, define resources, create user profiles, and invite additional users to the organization.

If the link isn't visible, you are not logged in as an organizational administrator.

Open a Service

To open a service:

1. Click the panel for the service, such as FactoryTalk® Designs Tools™ or FactoryTalk Remote Access.
2. To return to the Home screen, click Home.

Each service has a "Getting Started" section and "help" to assist you in learning how to perform different tasks.

Verify account

Before you can sign in, your account must be verified. Make sure that the information provided is accurate to receive your verification code. Account verification is automated and occurs within 5 minutes of completion of the service sign-up.

Verification emails come from the sender myrockwell.com. If you have not received the verification email, check your junk or spam folders for the email.

Create a Domain

To start using FactoryTalk Remote Access, you must create a domain to access and use the services. Your domain must have a unique name.

IMPORTANT	To create and use the domain, you must have a working Internet connection on the PC and your organization must have the FactoryTalk Remote Access entitlement.

To create a domain, use the following steps.

1. Sign in to FactoryTalk Hub.
2. Select the FactoryTalk Remote Access service tile.
3. When you are prompted, authenticate yourself with your authenticator code.
4. In Create domain, provide a name for the domain. The domain name is required and must be unique.

IMPORTANT	Domain names cannot be changed after they are created.

5. Click Create Domain.

   Once the domain is successfully created, a confirmation message appears. Each newly created domain is immediately usable.

The first time the domain is accessed, sign in with an administrator user account.

Domain Membership

Features that can be part of a FactoryTalk Remote Access domain are listed in Table 4.

Table 4 - Domain Features

Entity	Description
User Accounts	User accounts are the individual users that sign in to FactoryTalk Hub and use the FactoryTalk Remote Access domain and access remote machines. Each use is authenticated before entering the domain of the organization. Users must have been invited to join the FactoryTalk Remote Access domain to access the service. See Add user accounts.
Groups	A group is used to assign permissions to multiple user accounts. You create the groups according to the types of user accounts in your organization. Common categories for groups are roles and regions. FactoryTalk Remote Access provides the Admin, Contributor, and Owner groups by default in each domain. You can belong to multiple groups.
Remote Device	A remote device is the Stratix 4300 Remote Access router.
Folders	A folder is a container of objects, such as devices, firewall policies, and groups. Like folders and documents on your computer, you can organize objects in different folders. Folders can be added as needed. Once an object is placed in a folder it can be moved to another folder, but it cannot be in multiple folders simultaneously.
Permissions	Permissions are rules that are applied to user accounts that allow or deny them access to folders and devices.
Firewall Policies	Firewall policies are rules that are applied to VPN packets that control if certain protocols, ports, IP addresses are allowed or denied access to devices. Firewall policies have to be imported or defined first then applied either to folders to apply the policy to all devices in the folder or directly to one device. The firewall policies that are applied are defined according to the user account, so different user accounts can be assigned different policies.

Domain Connectivity

The basic requirement for FactoryTalk Remote Access functioning is a working Internet connection. FactoryTalk Remote Access uses outgoing connections, which most firewall systems allow. FactoryTalk Remote Access acts as a "client" of the FactoryTalk Remote Access Cloud Infrastructure, which accepts incoming connections.

FactoryTalk Remote Access must have at least one of the following TCP ports open to connect to the FactoryTalk Remote Access Cloud Infrastructure:

- 80
- 443
- 5935

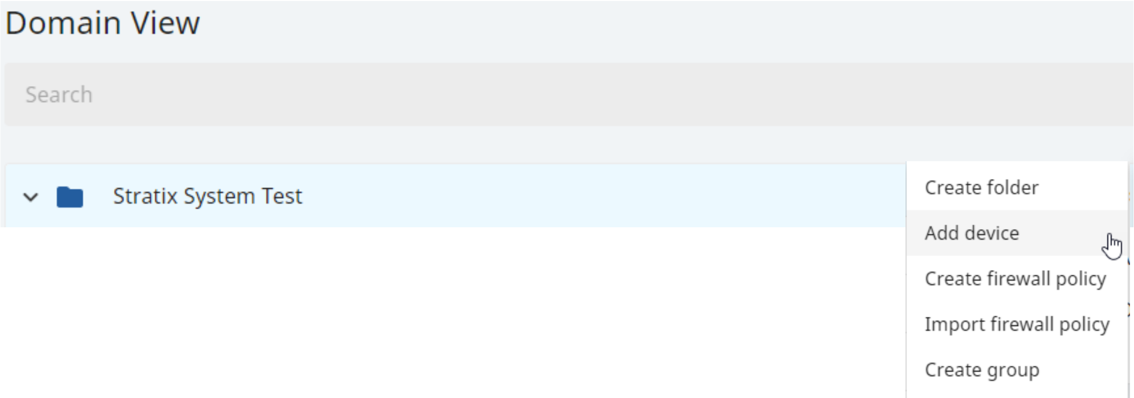
The first open port is used to connect clients to the FactoryTalk Remote Access Servers, after a scan of the available ports; after that, an end-to-end connection the remote device and FactoryTalk Remote Access is established.

IMPORTANT	All FactoryTalk Remote Access connections, regardless of the port that is used, are made using the secure SSL/TLS protocol to help confirm a safer information exchange over the Internet. The use of the SSL/TLS protocol allows FactoryTalk Remote Access to verify the identity of the FactoryTalk Remote Access Server and later the confidentiality of the information that is exchanged with the server and the remote device.

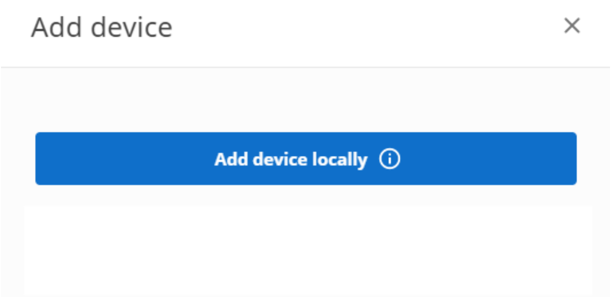
Associate the Router with a Domain

1. In the FactoryTalk Remote Access environment, choose your domain and click the plus (+) option.

   A tab with the five options that are shown below appears.
2. Click Add Device.

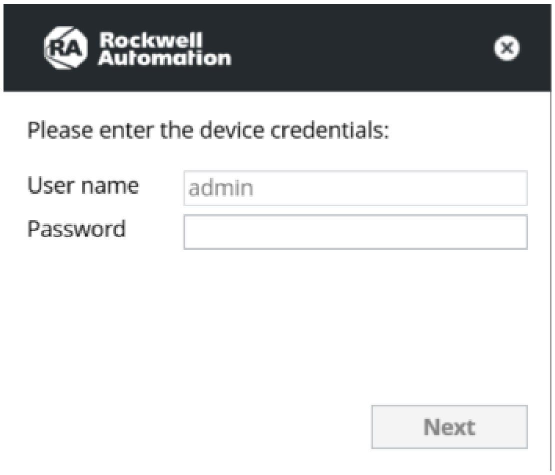


3. To add the router to your FactoryTalk Remote Access remote environment, add a local device,



4. To add the device, reenter the router credentials.

IMPORTANT	Your PC must be in the same subnet as the Stratix 4300 you are adding to the domain.



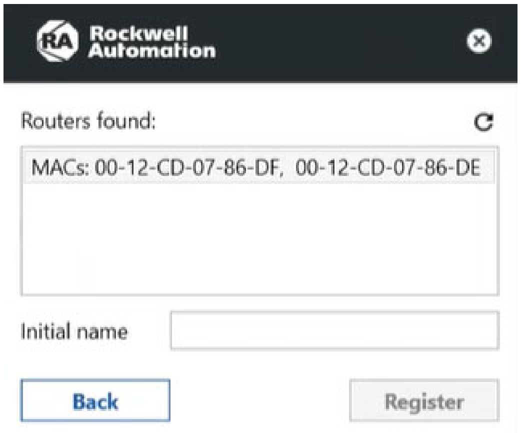
Please enter the device credentials:

User name: admin

Password:

5. Find your router in the list that appears.
6. Name the router in the "Initial name" box, and click Register.

   To determine the correct MAC address for the Stratix 4300, you can either check the side of the physical device, or the Device Manager pages.



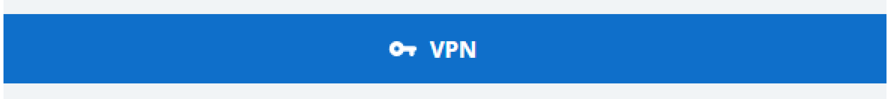
Routers found:

MACs: 00-12-CD-07-86-DF, 00-12-CD-07-86-DE

Initial name:

After naming the router, refresh your online view and you see the name of your router in your Domain view.

7. To connect the device over VPN, click the VPN bar on the right of the screen, which is shown in the image below.

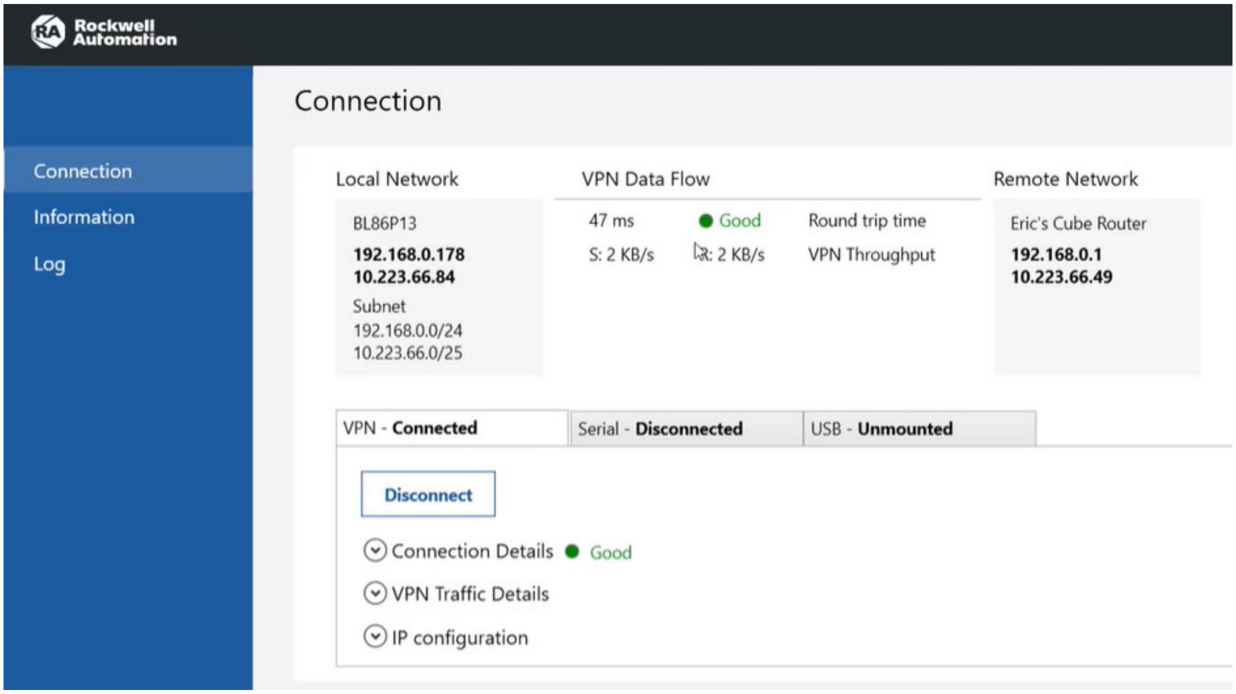


After you click the VPN bar, an image for the VPN blinks in your PC's toolbar at the bottom of your screen.

8. Click the VPN icon in the toolbar.

The connection screen to your device appears.

You can also connect or disconnect from the router with the toggle option you see under the "VPN-Connected" tab.



Connection

Local Network
BL86P13
192.168.0.178
10.223.66.84
Subnet
192.168.0.0/24
10.223.66.0/25

VPN Data Flow
47 ms ● Good Round trip time
S: 2 KB/s R: 2 KB/s VPN Throughput

Remote Network
Eric's Cube Router
192.168.0.1
10.223.66.49

VPN - **Connected** | Serial - **Disconnected** | USB - **Unmounted**

Connection Details ● Good
VPN Traffic Details
IP configuration

For more information on the Serial and USB options, refer to the help file in FactoryTalk Remote Access.

Protect Against Unwanted Domain Change

The Stratix 4300 Remote Access router features additional security for protection against unwanted or unauthorized Domain change attempts.

Once you register a domain, the server stores the details of the binding and blocks any possibility to change the domain without the execution of the dedicated procedure.

This security block is useful if a router is restored to factory settings with the intent to bypass the correct procedure.

A sequence of two flashing red lights on status indicators on the front panel reports this condition, and the router becomes unusable.

For more information on domain change, see FactoryTalk Remote Access Help.

Remove and Move Devices

A device associated to a domain can be deleted at any time and moved, if necessary, to another domain.

To delete a device from a domain, click once on the device icon and execute the delete command from the menu.

After the device has been removed, the router can be registered to a new domain.

Set Up Your FactoryTalk Remote Access Connection

To register and configure the Stratix 4300 Remote Access router and make a VPN connection, download and install FactoryTalk Remote Access™ Tools.

Download the Tools

Use the following steps to download FactoryTalk Remote Access Tools.

1. Sign in to the FactoryTalk Hub with an administrator user account.
2. Start FactoryTalk Remote Access and access the domain.
3. On the main FactoryTalk Remote Access toolbar, click the Help icon and select Software Downloads.

   Your web browser opens to the Product Compatibility and Download Center.

If the download does not start automatically, use the following steps.

1. Type FactoryTalk Remote Access in the Search bar.
2. Select FactoryTalk Remote Access XX.xx.
3. In the Available Downloads window, select Tools for FactoryTalk Remote Access.
4. To add the item to your Download Cart, select downloads.
5. In the Download Cart window, select Download Now to start the download.

After the software download starts, perform the following steps.

1. Review the Rockwell Automation End User License Agreement, and then click Accept and Download to continue.
2. If prompted, click Save File.
3. If the download does not start automatically, click the download link to open Direct Downloads.
4. In the Direct Downloads window, click the download link for FactoryTalkRemoteAccessToolsSetup*XX.xx*.exe to download the software.

Install the Tools

Use the following steps to install the FactoryTalk Remote Access Tools.

1. Run FactoryTalkRemoteAccessToolsSetup*XX.xx*.exe.
2. To allow the software to change your device, click yes.

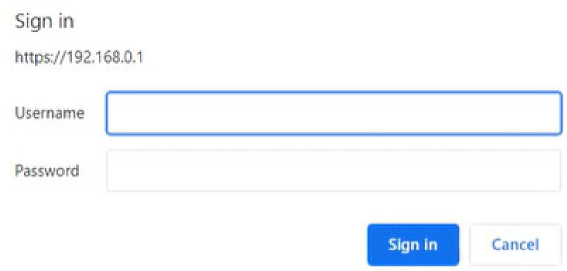
   The FactoryTalk Remote Access Tools installation wizard starts.
3. To install the software, follow the steps in the wizard.

Connect Via Ethernet

1. Sign in with the default IP address to the device in the Stratix 4300 Device Manager.

   The default IP address and LAN ports are set to 192.168.0.1. WAN ports are set to request an address via DHCP

   The default user name and password are both "admin".



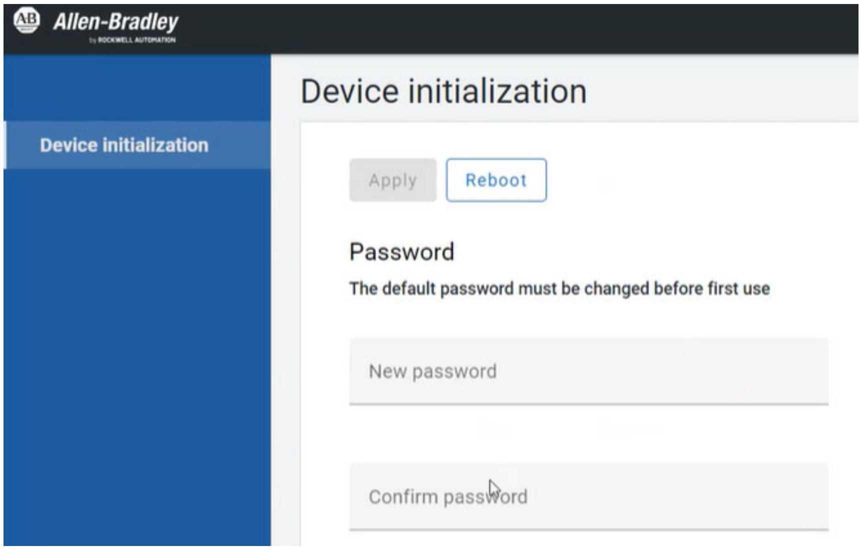
Sign in

https://192.168.0.1

Username

Password

2. When you are prompted, change the password to your device.



Device initialization

Password

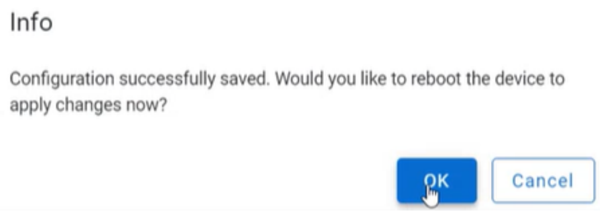
The default password must be changed before first use

New password

Confirm password

The password change prompts the device to restart.

3. To apply the changes, restart your device.



Info

Configuration successfully saved. Would you like to reboot the device to apply changes now?

After your device reboots, the device manager opens on the general tab. From this point, you can explore more options the Device Manager has in the Router Configuration section in Chapter 3.

Notes:

Router Configuration

The Stratix® 4300 industrial router system software has been designed to simplify initial configuration by modifying a few mandatory settings.

This section provides an overview of how to configure the router with the system software Device Manager.

General

Upon logging into the Device Manager of the router the general tab is displayed.

The general tab in Device Manager allows you to change the host name of the router, choose from which interfaces Device Manager is accessible from, configure the date and time, enable and disable external storage device and view the system information of the router.

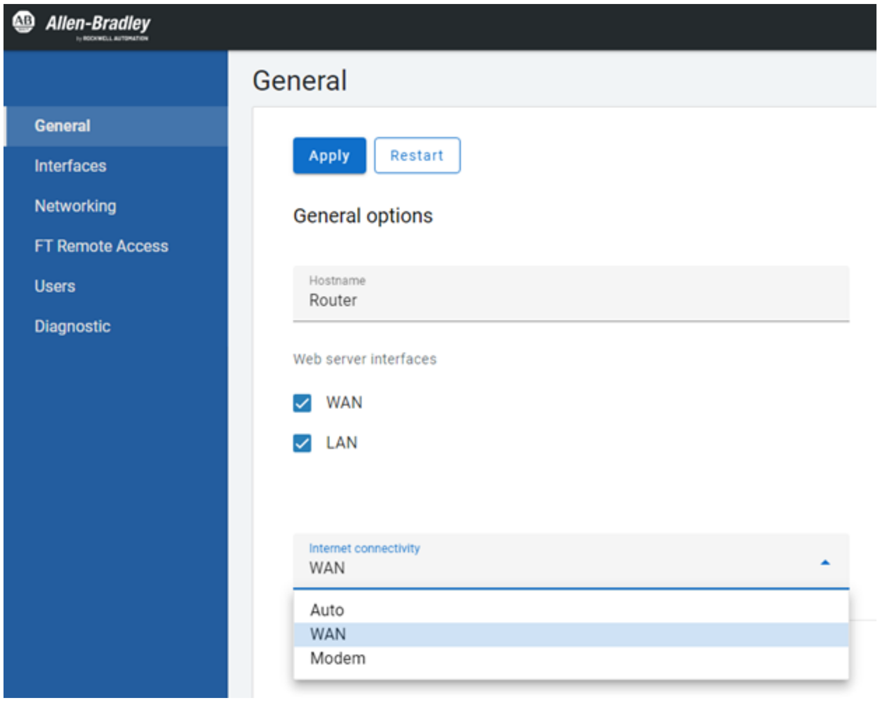
General Options

The general options section of the general tab allows you to be able to set the device name (Hostname) of the router.

By default, both the WAN and LAN checkboxes are checked under the web server interfaces. This means that Device Manager is accessible by an Internet browser for configuration using either the WAN or LAN IP addresses that are configured on the router. Web server interfaces can be disabled by unchecking the checkboxes for the desired interface thus resulting in loss of access to the Device Manager for that interface.

Internet connectivity has three options:

1. Auto - the router attempts to connect via WAN. If this is not possible, the router attempts to connect via modem.
2. WAN or WAN/Wi-Fi (if the device is equipped with a Wi-Fi card) - the router attempts to connect via WAN only.
3. Modem - the router always attempts to connect via modem.



General

General options

Hostname
Router

Web server interfaces

☑ WAN

☑ LAN

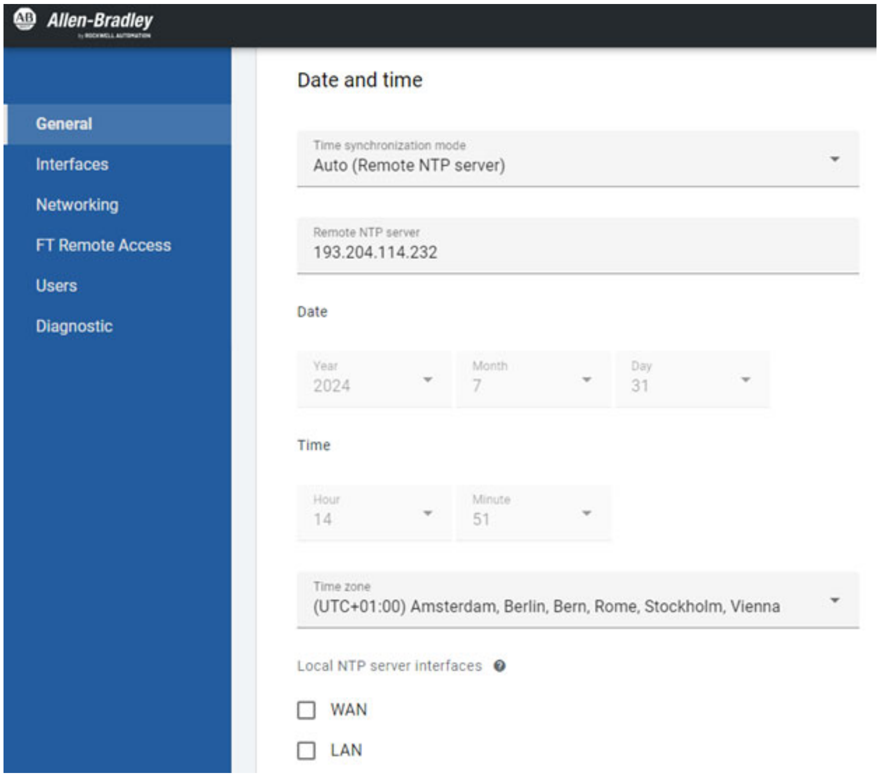
Internet connectivity
WAN

Date and Time

The date and time section of the General tab allows you to configure the date and time automatically via an NTP (Network Time Protocol) server by specifying its IP address or name or manually setting the date and time.

The "Set local NTP server interfaces" checkbox enables the local NTP server on the selected interfaces.

Selecting at least one interface enables a local NTP server that listens for connections on the standard UDP port 123. Selecting no interface disables the local NTP server.



Date and time

Time synchronization mode: Auto (Remote NTP server)

Remote NTP server: 193.204.114.232

Date

Year: 2024 Month: 7 Day: 31

Time

Hour: 14 Minute: 51

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

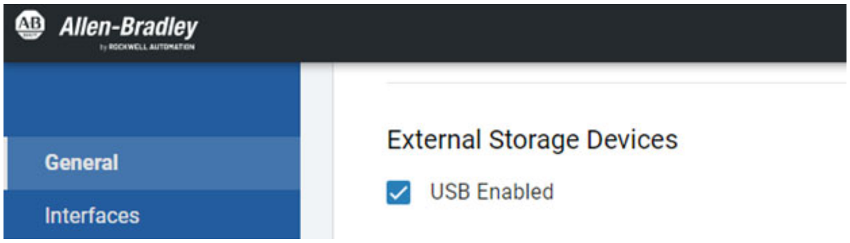
Local NTP server interfaces

□ WAN

□ LAN

External Storage Devices

Device Manager now gives you the ability to enable and disable USB storage devices. By default this feature is enabled.

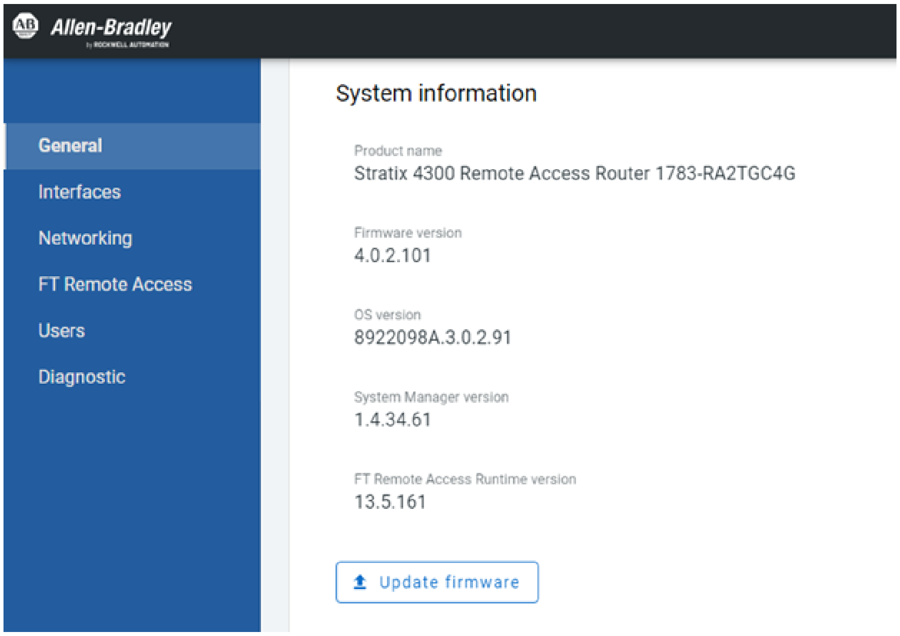


External Storage Devices

☑ USB Enabled

System Information

System information about your router can also be found under the General tab.



System information

Product name
Stratix 4300 Remote Access Router 1783-RA2TGC4G

Firmware version
4.0.2.101

OS version
8922098A.3.0.2.91

System Manager version
1.4.34.61

FT Remote Access Runtime version
13.5.161

⚠ **ATTENTION:** Update Firmware is a new feature that can update future firmware with Device Manager. This is an alternative upgrade procedure from using the USB stick for upgrades. For upgrades from version 3.0.3.91 to version 4.0.2.101 the USB stick upgrade procedure is the only upgrade option.

Interfaces

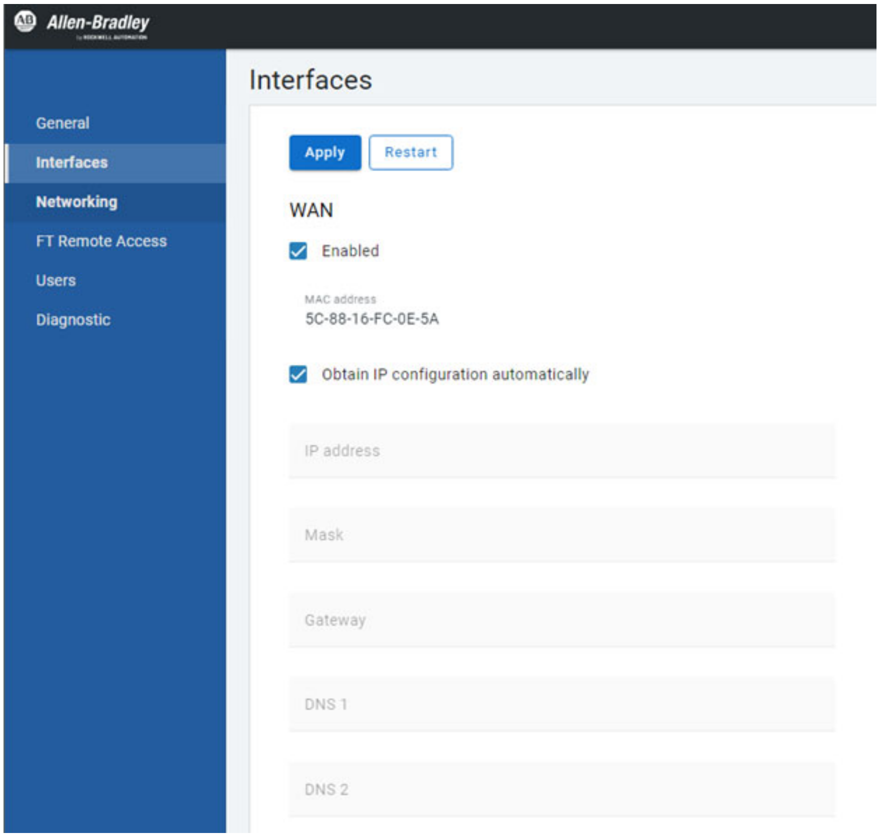
WAN

In this section, you can configure the WAN interface that is used by the router to get Internet access.

The information that is shown at the first screen visualization correspond to the actual device parameters values.

The “Obtain IP configuration from DHCP” checkbox has to be marked if you must use the DHCP server for the IP address configuration.

If you must specify a fixed IP, remove your selection in the checkbox and complete the form below.



Interfaces

WAN

☑ Enabled

MAC address
5C-88-16-FC-0E-5A

☑ Obtain IP configuration automatically

IP address

Mask

Gateway

DNS 1

DNS 2

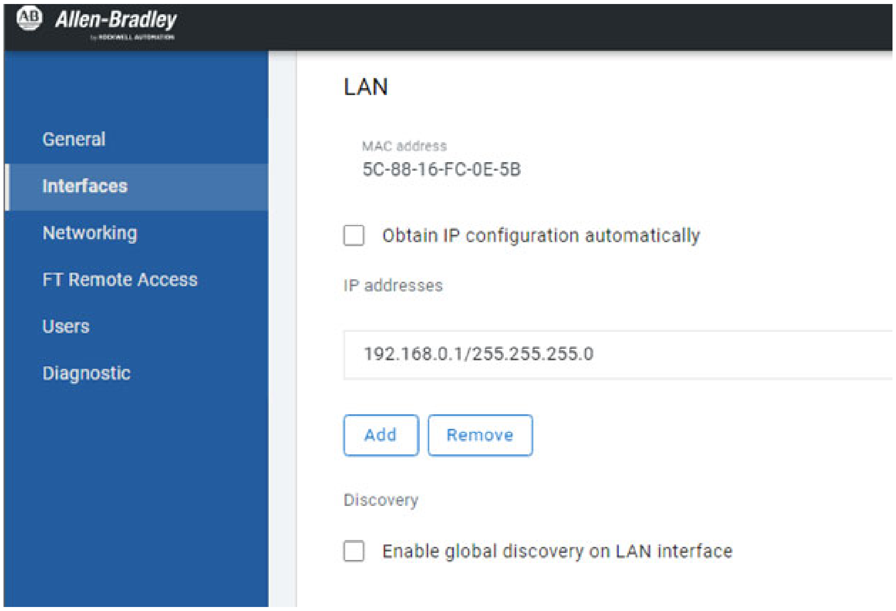
LAN

In the interfaces section, you can configure the LAN interface parameters. This interface is connected to the machine network, which is reachable from the VPN.

The information that is shown on the first screen corresponds to the device parameter values.

The “Obtain IP configuration from DHCP” checkbox has to be marked if you want to use the DHCP server for the IP address configuration.

The “Obtain IP configuration from DHCP” checkbox has to be marked if you want to use the DHCP server for the interface IP configuration. More common for the LAN interface is to use a fixed IP and, in this case, remove your selection in the checkbox and specify the IP with the mask. After this, click then the “Add” button. The IP is added to the list.



LAN

MAC address
5C-88-16-FC-0E-5B

□ Obtain IP configuration automatically

IP addresses

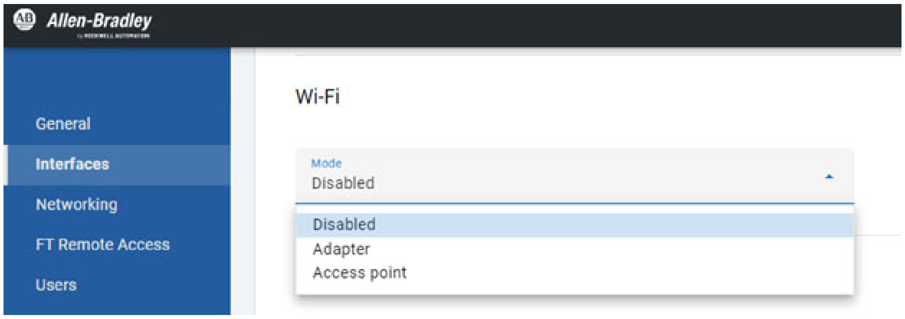
192.168.0.1/255.255.255.0

Discovery

□ Enable global discovery on LAN interface

Wi-Fi

The Wi-Fi card supports three modes: Disabled (default), Adapter and Access Point. The two operating modes require a specific configuration and they are described below.



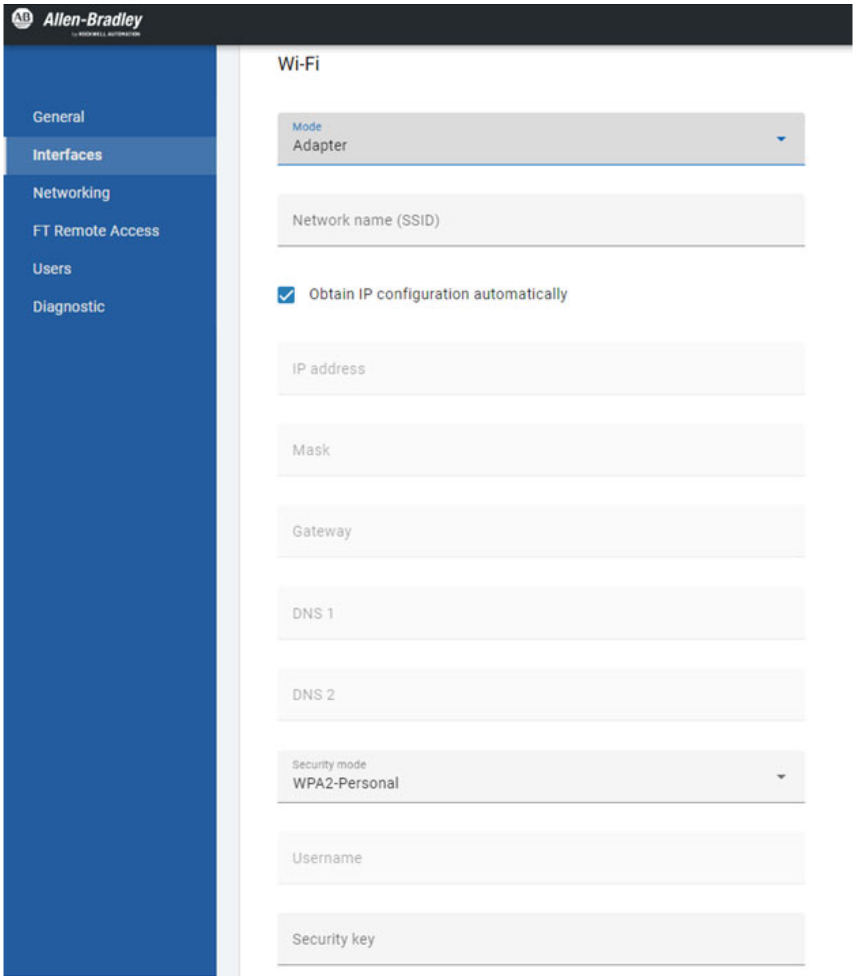
Wi-Fi

Mode
Disabled

Wi-Fi Adapter

The router connects to an existing Wi-Fi network. The parameters to configure are as follows:

- Network Name (SSID). Write the name of the Wi-Fi network to connect to.
- Obtain IP configuration from the DHCP server. If the option is selected (default), then the card receives the network configuration parameters from a DHCP server, otherwise they are manually specified.
- IP address, Mask, Gateway, DNS 1, and DNS 2. The configuration parameters of the Wi-Fi network to be specified if a DHCP server is not used to set them automatically.
- Security Mode - The type of the WPA2 security protocol used. It can take the values WPA2-Personal (default) or WPA2-Enterprise.
- Username - The user name to use to connect to a Wi-Fi network if WPA2-Enterprise mode is selected.
- Security Key - The security key to use to connect to the Wi-Fi network. (if WPA2-Personal is used) or the user password (if WPA2-Enterprise is used).



Mode: Adapter

☑ Obtain IP configuration automatically

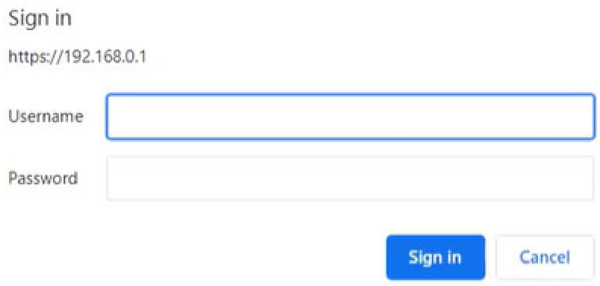
Security mode: WPA2-Personal

Connect Via Ethernet

1. Sign in with the default IP address to the device in the Stratix 4300 Device Manager.

   The default IP address and LAN ports are set to 192.168.0.1. WAN ports are set to request an address via DHCP

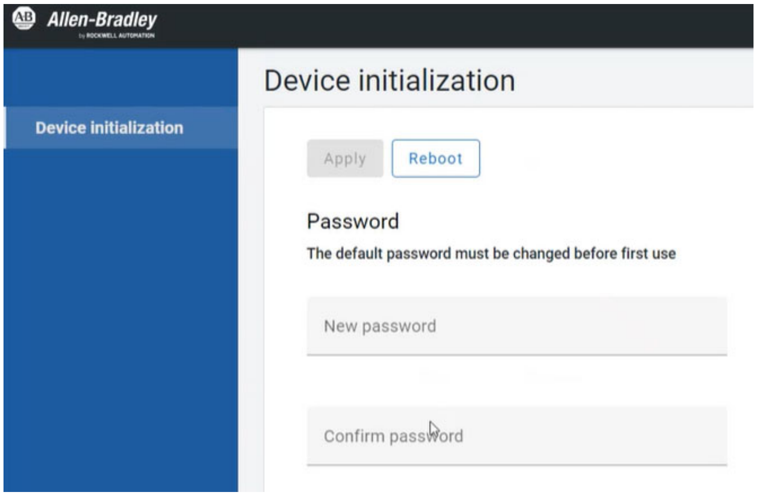
   The default user name and password are both “admin”.



Sign in

https://192.168.0.1

2. When you are prompted, change the password to your device.



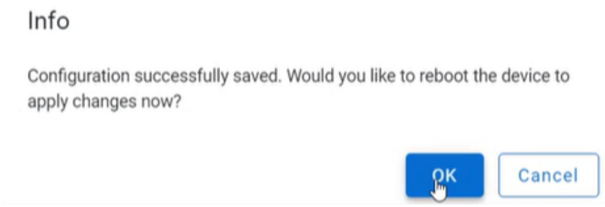
Device initialization

Password

The default password must be changed before first use

The password change prompts the device to restart.

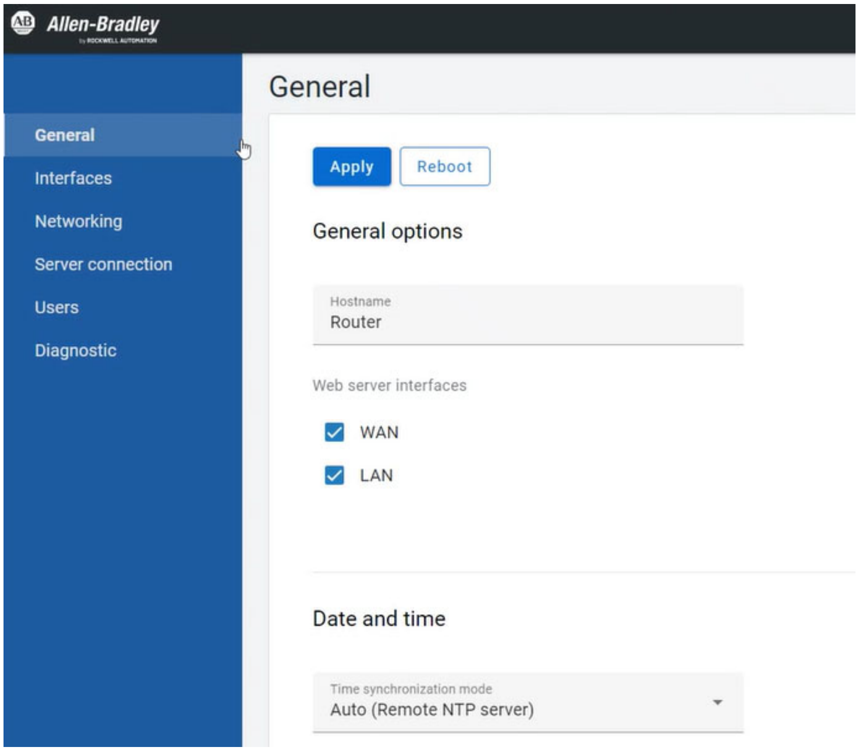
3. To apply the changes, restart your device.



Info

Configuration successfully saved. Would you like to reboot the device to apply changes now?

After your device reboots, the device manager opens on the general tab. From this point, you can explore options the Device Manager has.



General

General options

Hostname: Router

Web server interfaces

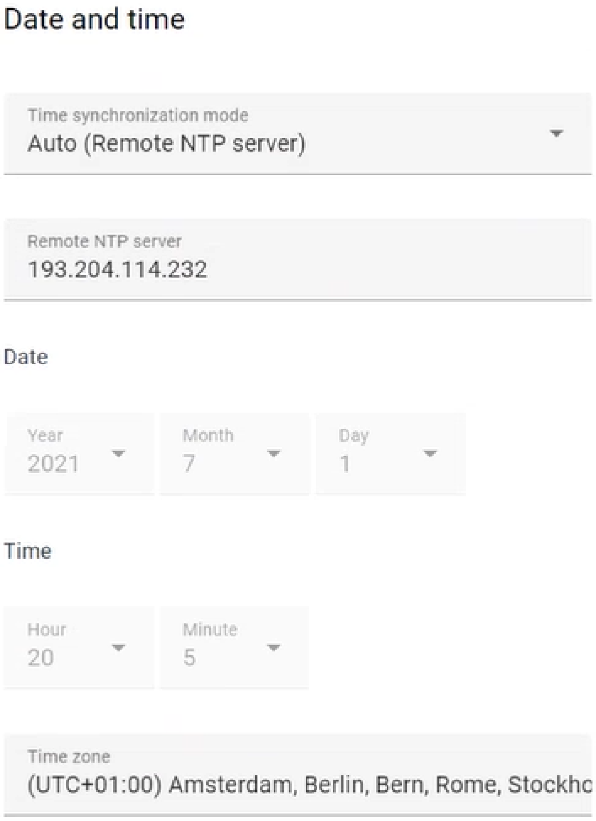
☑ WAN

☑ LAN

Date and time

Time synchronization mode: Auto (Remote NTP server)

The date and time settings, and Local NTP Server interfaces can both be found under the General tab.



Date and time

Time synchronization mode: Auto (Remote NTP server)

Remote NTP server: 193.204.114.232

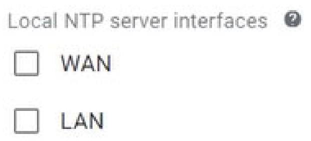
Date

Year: 2021 Month: 7 Day: 1

Time

Hour: 20 Minute: 5

Time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockho

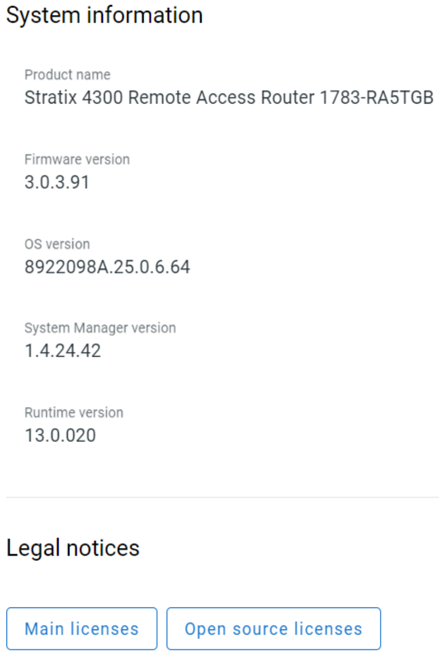


Local NTP server interfaces

☐ WAN

☐ LAN

System information about your router can also be found under the General tab.



System information

Product name
Stratix 4300 Remote Access Router 1783-RA5TGB

Firmware version
3.0.3.91

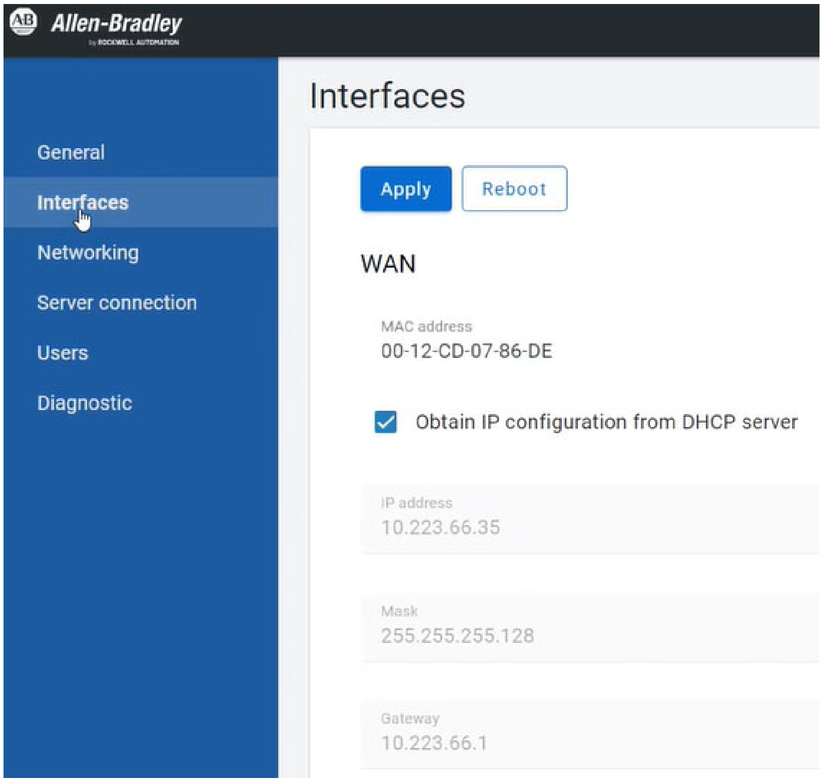
OS version
8922098A.25.0.6.64

System Manager version
1.4.24.42

Runtime version
13.0.020

Legal notices

The interface tab shows what the ports on the device are doing, and the location of the MAC address for the WAN port.



Interfaces

WAN

MAC address
00-12-CD-07-86-DE

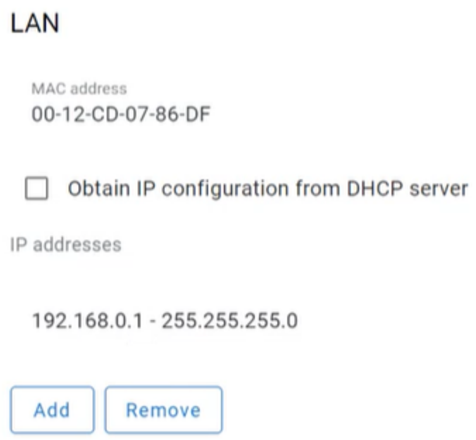
☑ Obtain IP configuration from DHCP server

IP address
10.223.66.35

Mask
255.255.255.128

Gateway
10.223.66.1

All LAN port information is also listed under the Interface tab, including the MAC address.



LAN

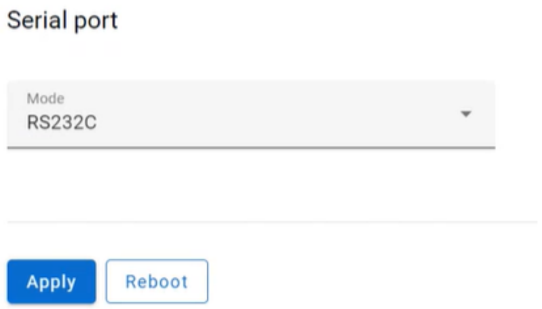
MAC address
00-12-CD-07-86-DF

☐ Obtain IP configuration from DHCP server

IP addresses

192.168.0.1 - 255.255.255.0

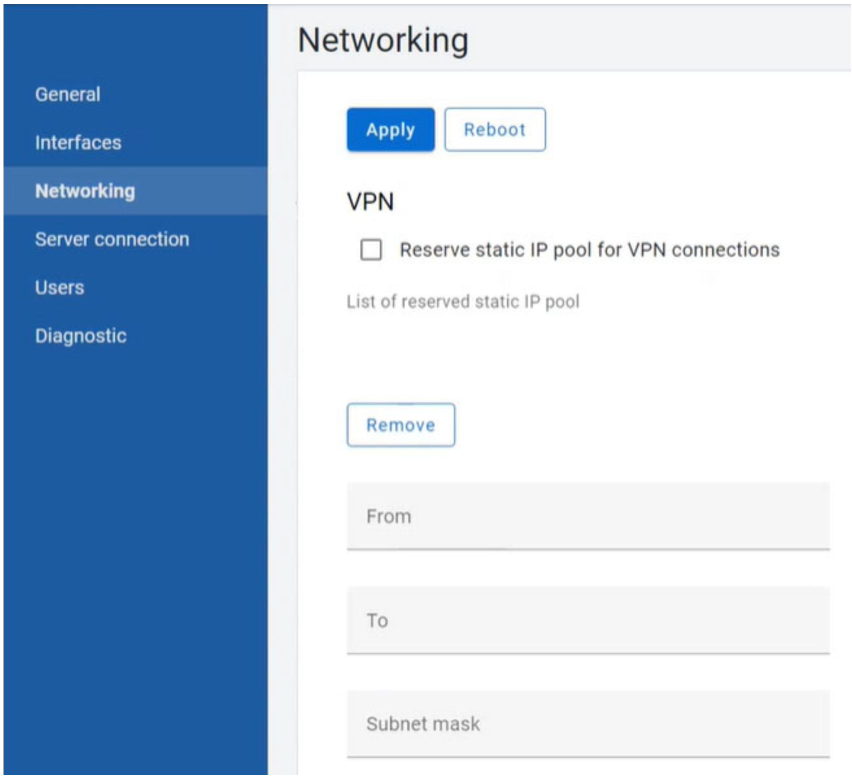
From the Interface tab, you can choose your Serial port mode.



Serial port

Mode
RS232C

Under the Networking tab, you can find options for your VPN connection.



Networking

VPN

☐ Reserve static IP pool for VPN connections

List of reserved static IP pool

From

To

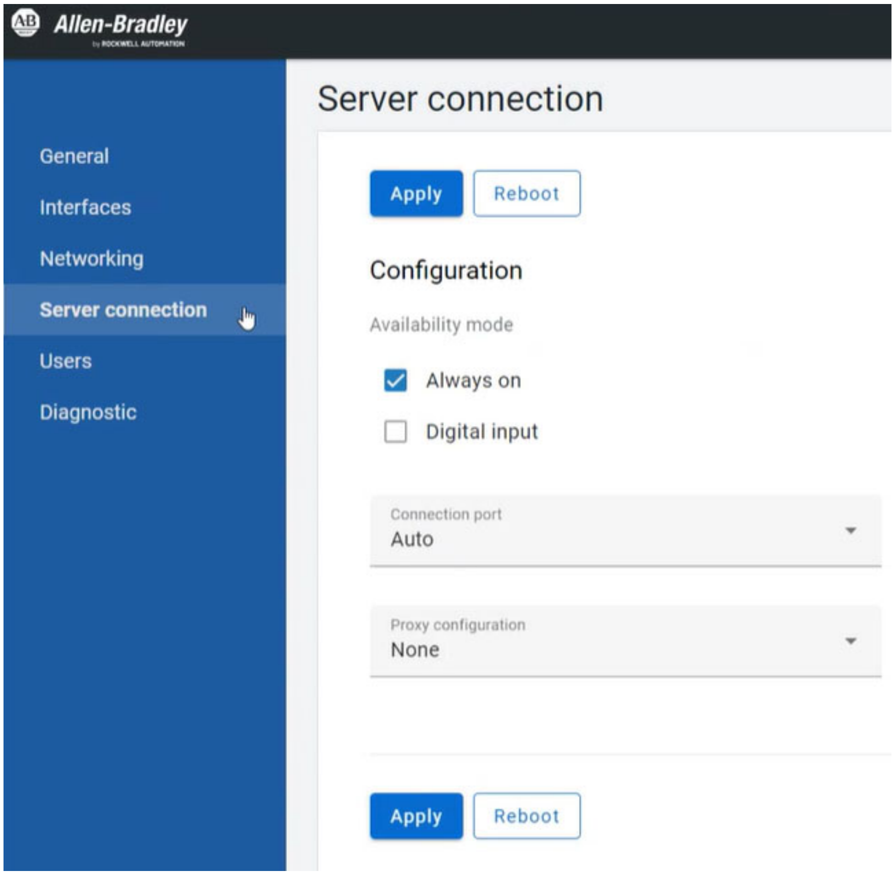
Subnet mask

The server connection tab has configuration options for remote connectivity.

There are two options for availability mode.

If you select the mode, “Always on”, the router connects to the Domain immediately after power-up. When a working Internet connection is available, it also restores the connection if dropped for any reason.

If you select “Digital input”, the router connects to the configured Domain only and exclusively when the proper electric input (IN0) is activated.



Server connection

Configuration

Availability mode

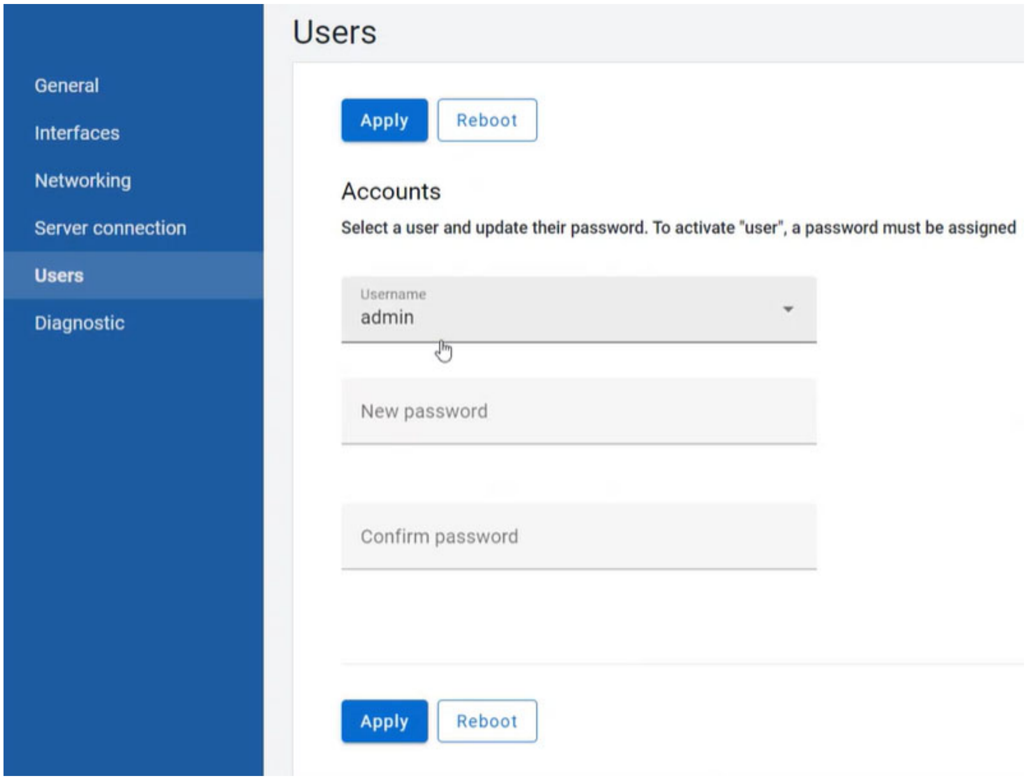
☑ Always on

□ Digital input

Connection port: Auto

Proxy configuration: None

All user accounts local to the Stratix 4300 are located under the Users tab. This tab is where you find your administrator account or change your current password.



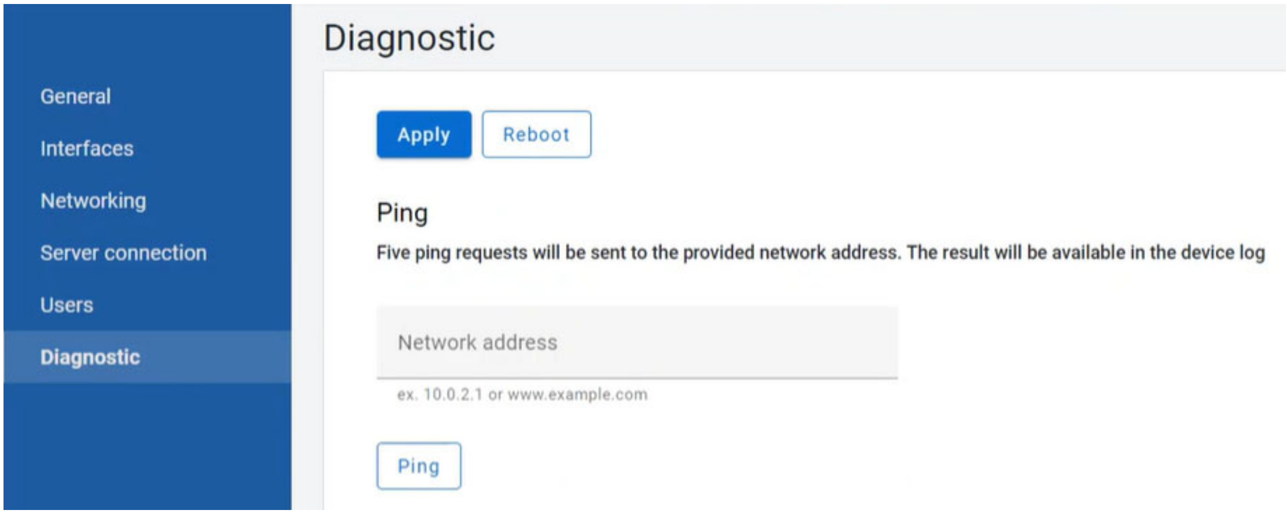
Users

Accounts

Select a user and update their password. To activate "user", a password must be assigned

Username: admin

Under the diagnostic page, you can ping a network address. A log of the sent pings are tracked in a list below the Ping option.



Diagnostic

Ping

Five ping requests will be sent to the provided network address. The result will be available in the device log

ex. 10.0.2.1 or www.example.com

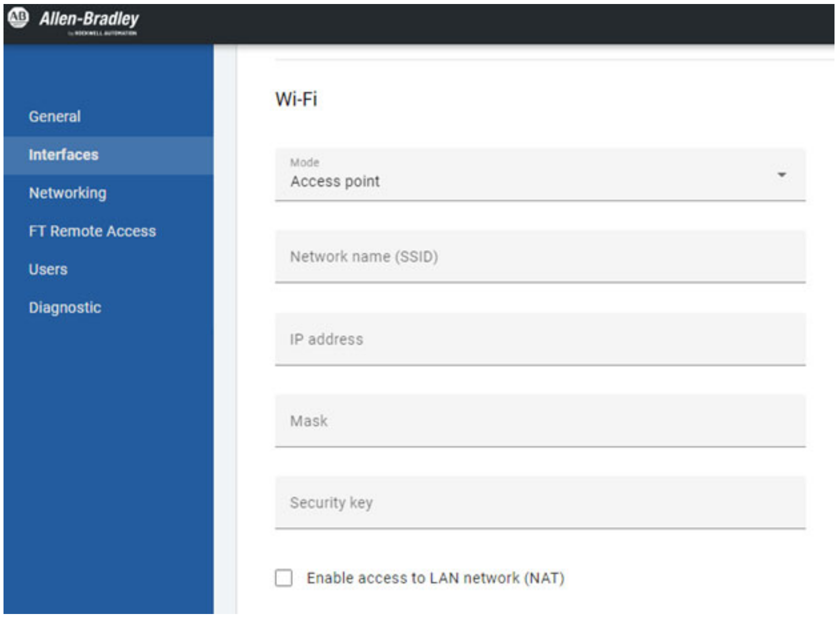
Wi-Fi Access point

The router becomes a Wi-Fi access point to which external devices can connect. The parameters to configure are as follows:

- Network Name (SSID). Write the name of the Wi-Fi network that you want to create.
- IP address e Mask. The IP address and the mask of the router.

The IP address must belong to a private network different from the ones that are used to configure the WAN and LAN ports. For example, if the WAN port has an address of class 172.16.0.0/12 and the LAN port has an address of class 192.168.0.0/16, then you can assign the Wi-Fi network to an address of class 10.0.0.0/8.

- Security key. The security key is used to connect to the access point. The security protocol that is used is WPA2.
- Enable access to LAN Network (NAT). Enables access to the LAN network to devices connected in Wi-Fi to the router.



Wi-Fi

Mode: Access point

Network name (SSID)

IP address

Mask

Security key

☐ Enable access to LAN network (NAT)

In this mode, the router, through its DHCP server, assigns an IP address compatible with the one entered in the IP address field to the connecting devices. For example, if you specify an IP address of 10.0.10.1, the first device that connects is assigned 10.0.10.2 as its IP, the second are assigned 10.0.10.3 and so on. If Internet Sharing is active on the Wi-Fi network interface, the router only activates the DNS service on this interface, so the connecting devices can access the Internet network without having to manually specify DNS servers.

Modem

This section is used to configure the integrated modem parameters.

Status can assume the following values:

- Connected - the modem is connected
- Disconnected - the modem is disconnected
- Error: <ErrorCode> - one of the following errors was detected:
    - No SIM
    - PIN required
    - PIN2 required
    - PUK required
    - PUK required
    - Wrong PIN
    - Only one PIN insertion retry left
    - No PIN insertion retry left
    - Modem not present or initialized
    - A valid APN was not found for the current operator
- Initialization - the Modem is initializing

Carrier mode shows the technology type that is used by the radio infrastructure to communicate with the Modem.

Signal strength is the power of the signal that is detected by the Modem.

The PIN code field is used to enter the SIM card PIN code, when required.

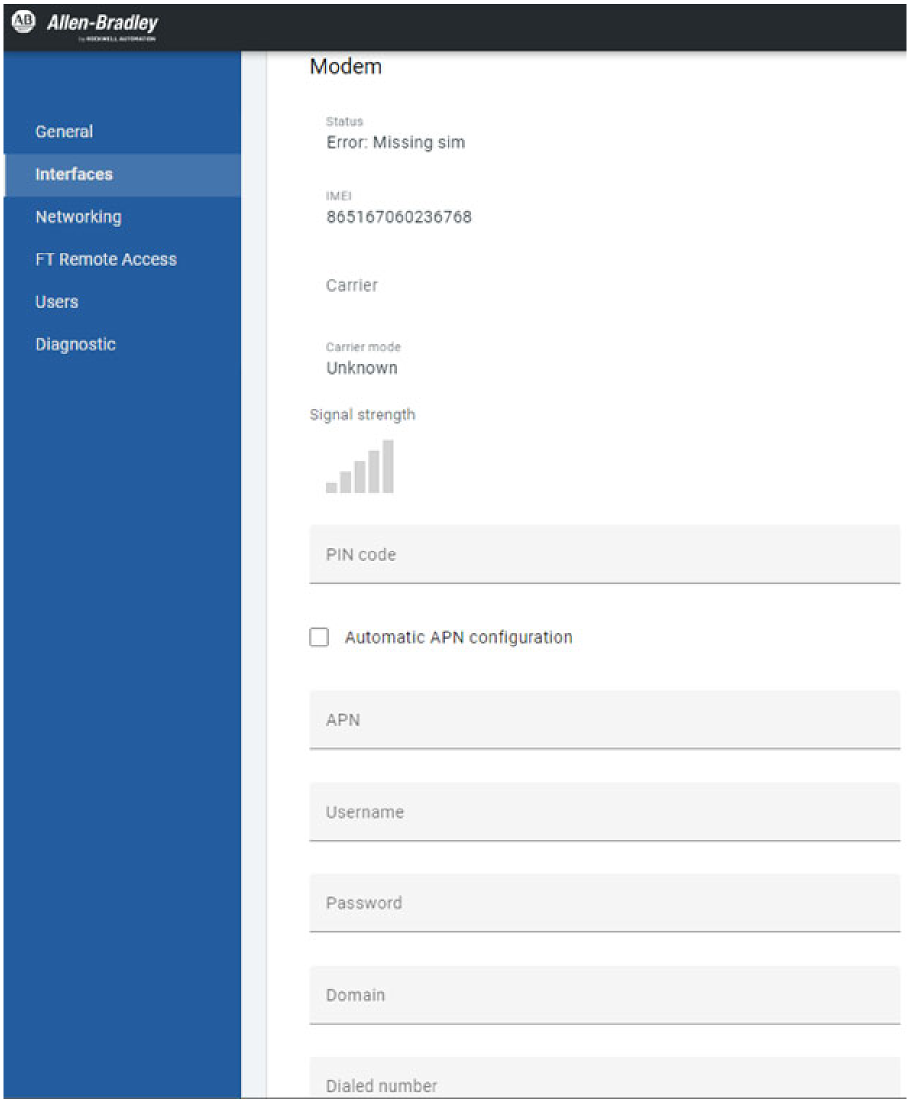
For more information on the SIM card, see Appendix B.

The Automatic APN configuration checkbox enables automatic searching of connection settings such as APN, Username, and Password. If the search is successful, the values that are found are automatically completed their respective fields, otherwise, an Error message is shown in the status field. The automatic search process is performed again when the SIM card is changed.

The APN field is used to enter the Access Point Name, required to connect the Modem to the Internet.

The Username, Password, and Domain fields are used to enter credentials that are given by the provider to connect the Modem to the Internet.

The Dialed number field is used to enter the telephone number for the Modem to call to connect.



Modem

Status
Error: Missing sim

IMEI
865167060236768

Carrier

Carrier mode
Unknown

Signal strength

PIN code

□ Automatic APN configuration

APN

Username

Password

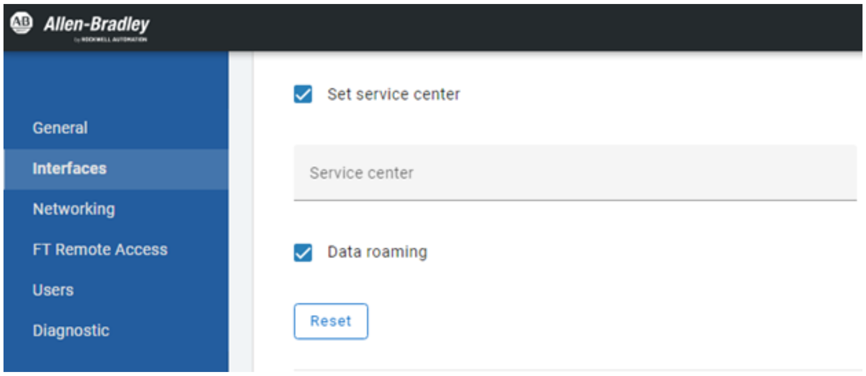
Domain

Dialed number

The Set service center checkbox allows you to set the Message Service Center number on your SIM card.

The checkbox Data roaming allows you to use the data traffic in roaming.

ATTENTION: The SIM cannot be removed or replaced while the router is operating.



☑ Set service center

Service center

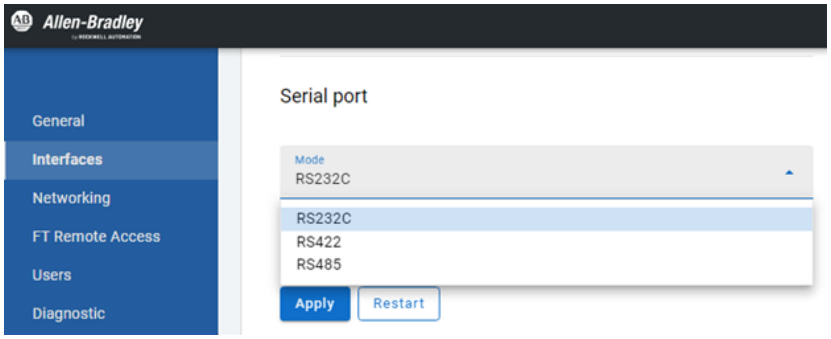
☑ Data roaming

Serial Port

This section allows you to configure the serial port for the serial pass-through.

Click the combo box to access to the available options. The options are the following:

- RS-232C
- RS-422
- RS-485



Serial port

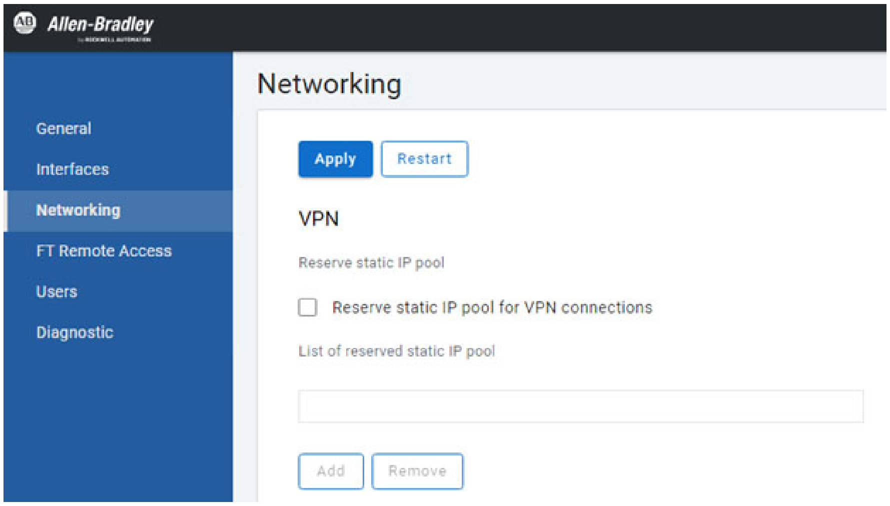
Mode
RS232C

Networking

VPN

The reserve static IP pool for VPN connections gives you the ability to adjust the way the IP addresses are assigned to the VPN virtual adapter during a VPN session.

ATTENTION: The IP addresses that are included in the pool are not subject to any check; it is under the user's responsibility to verify that there is no conflict on the subnet.



Networking

VPN

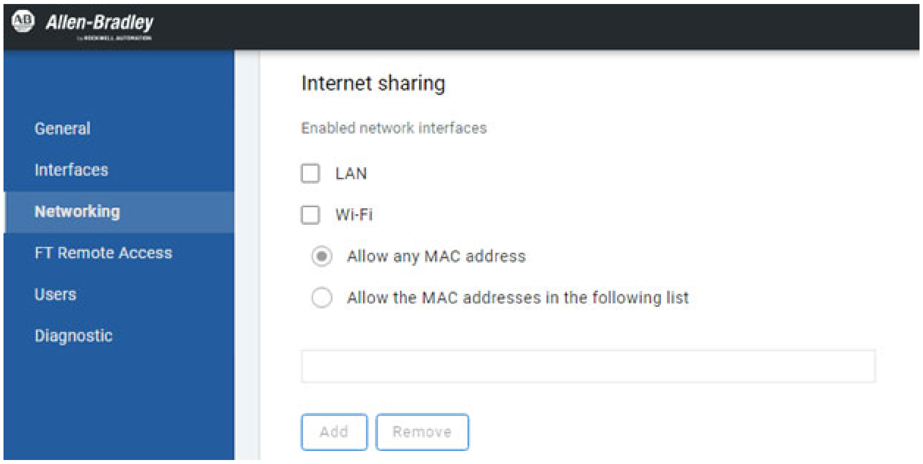
Reserve static IP pool

☐ Reserve static IP pool for VPN connections

List of reserved static IP pool

Internet Sharing

Internet sharing allows users to share the Internet connection to a device on an automation subnetwork.



Internet sharing

Enabled network interfaces

☐ LAN

☐ Wi-Fi

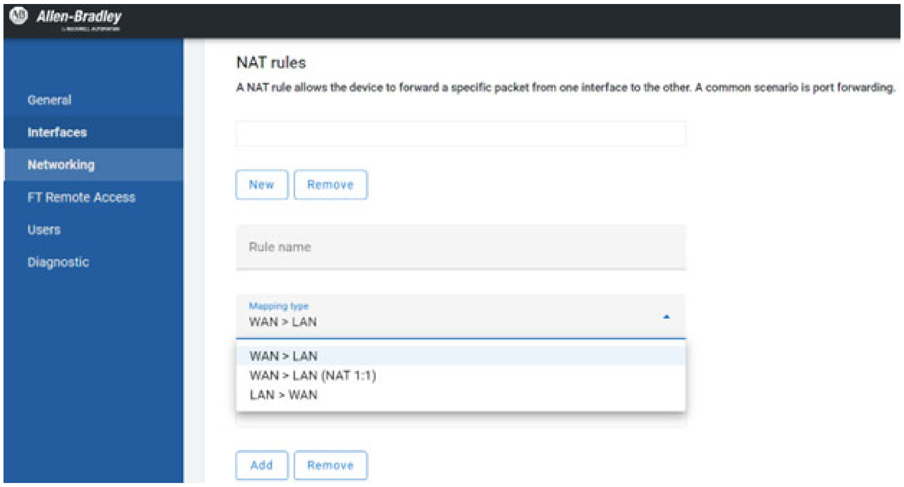
● Allow any MAC address

○ Allow the MAC addresses in the following list

Network Address Translation (NAT) Rules

There are three mapping types of NAT Rules. The mapping types are the following:

- WAN > LAN
- WAN > LAN (NAT 1:1)
- LAN > WAN



NAT rules

A NAT rule allows the device to forward a specific packet from one interface to the other. A common scenario is port forwarding.

Mapping type
WAN > LAN

The NAT consists of changing the IP addresses of packets in transit between the two interfaces of the router and between the communication of two hosts.

The router implements the D-NAT. This means changing the destination address of the packet that begins the new connection.

For example, the D-NAT allows the implementation of the “port forwarding”, which is the operation that allows the transfer of data (forwarding) from one computer to another over a specific communications port. This technique can be used to allow an external user to reach a host with a private IP address (inside a LAN) through a port of the public IP address of the router.

The parameters in the NAT rules are listed in Table 5.

Table 5 - NAT Rule Parameters

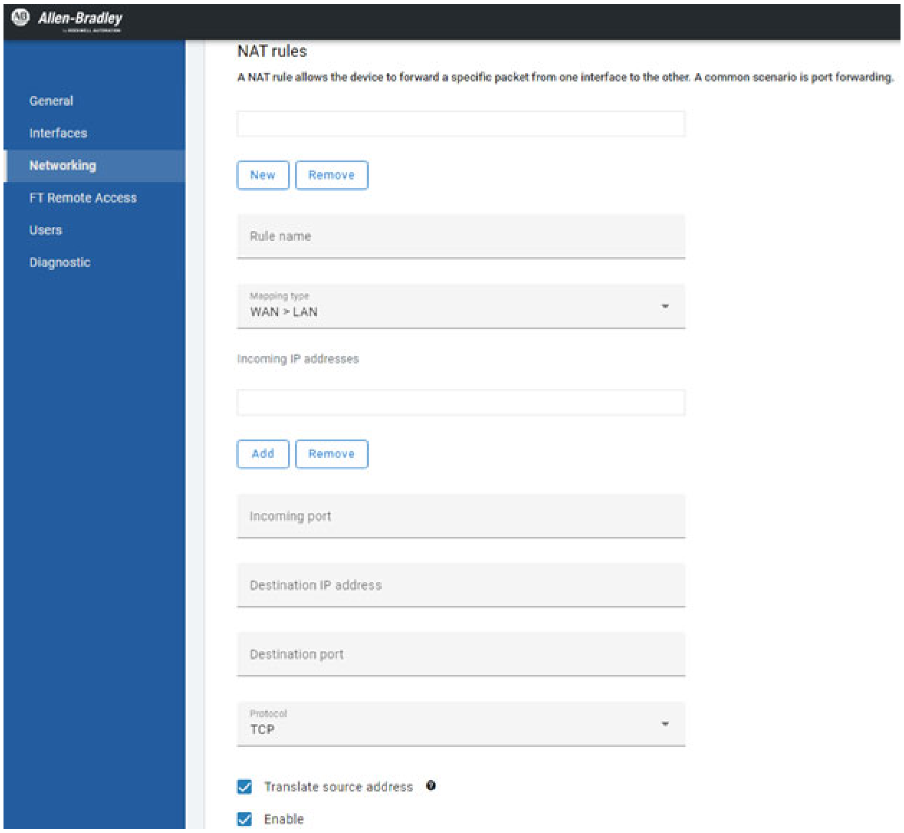
Parameter	Description
Rule name	Name that is assigned to the rule. This name must be unique.
Direction	Packet direction between the interfaces.
Incoming IP addresses	List of IP addresses from where packets arrive. You can enter single IP addresses or ranges of IP addresses.
Incoming port	Port number on which the router is listening for incoming connections.
Destination IP address	The destination of the IP address.
Destination port	The destination of the port number.
Protocol	Ethernet protocol on which the rule applies. The possible options are the following: • TCP • UDP • FTP • HTTP
Translate source address	Enabled by default. The NAT rule applies the translation of the source IP address as well.
Enable	This enables or disables the single rule. When a rule is disabled, its name is followed by the “Disabled” label.

To create a rule, input the parameters and click “Save”.

An existing rule can be modified by selecting it from the list, applying the changes, and then saving them with the “Save” button.

The “New” button clears the form.

The “Remove” buttons allow you to delete the selected rule.



NAT rules

A NAT rule allows the device to forward a specific packet from one interface to the other. A common scenario is port forwarding.

Rule name

Mapping type
WAN > LAN

Incoming IP addresses

Incoming port

Destination IP address

Destination port

Protocol
TCP

☑ Translate source address

☑ Enable

IMPORTANT	NAT rules are limited to a maximum of 10 rules.

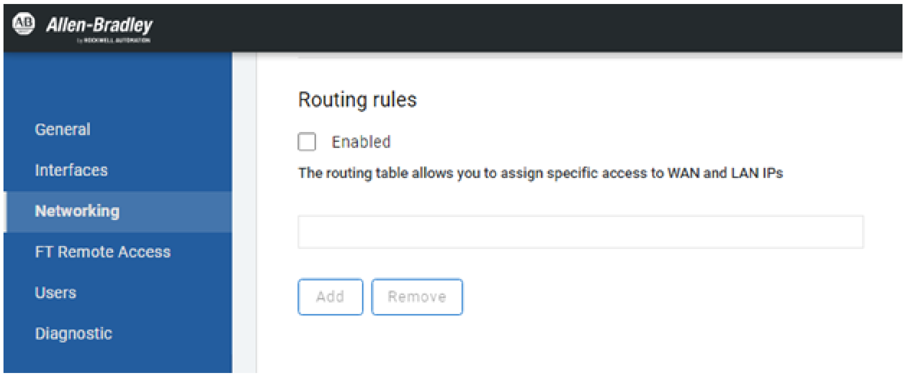
Routing Rules

Routing rules are configured for static routes between the two router interfaces (LAN and WAN). Rules for routing single IP addresses or ranges of addresses can be applied.

The rules must be applied to the LAN interface and to the WAN interface indicating the addresses concerned by the routing on both interfaces.

ATTENTION: LAN-WAN routing is NOT supported in the following scenarios:

- Internet connection via modem
- Gateway address NOT specified for the WAN interface
- Internet sharing is enabled.



Routing rules

□ Enabled

The routing table allows you to assign specific access to WAN and LAN IPs

FactoryTalk Remote Access

The FactoryTalk® Remote Access™ tab has the configuration options for remote connectivity.

The available choices can be one of the following:

Availability "mode" has three options:

1. Always-on
2. Digital input
3. SMS

When selecting the option "Always-on", the router connects to the Domain immediately after power-up and when a working Internet connection is available; it also restores the connection if dropped for any reason.

When selecting "Digital input", the router connects to the configured Domain only and exclusively when the proper electric input (IN0) is activated.

If "SMS" is selected, the router connects to the configured domain only when an SMS is received from the user.

Audit Logs

The FactoryTalk® Remote Access clients automatically record the operations that are performed on their domain resources by users and send the information to the FactoryTalk Remote Access domain. The audit log can be queried at any time by administrators using FactoryTalk Remote Access and cannot be disabled or deleted, not even administrators.

Each log holds:

- The user that performed the operation
- The operation code (such as rename of a device)
- The resource that was the object of the operation
- The time stamp
- A description

The audit trail contains:

- Login/logout of users.
- All CRUD (create, rename, update, delete) operations that are performed on all domain resources:
    - Users
    - Groups
    - Permissions
    - Device
    - Configurations
- All remote access operations, with starting time and ending time.

Connection Port

The “Port” dropdown menu is used to select the port that the Control Center uses to connect to the infrastructure. The available options are the following:

- Auto: use the first available port (TCP or UDP) 443, 80, 5935.
- 443: use port 443 to connect.
- 80: use port 80 to connect.
- 5935: use port 5935 to connect.

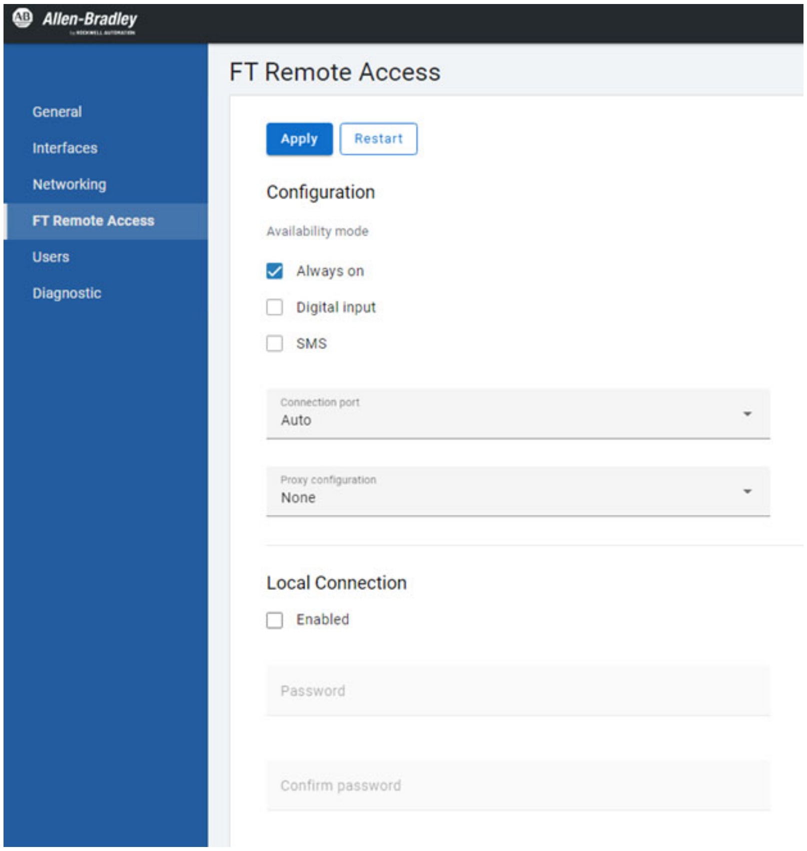
Proxy Configuration

Type can be one of the following:

- None: no Proxy is used for the connection.
- HTTP: HTTP Proxy type supports authentication with user name and password.
- SOCKS5: SOCKS5 Proxy type supports authentication with user name and password.

Local Connection

Local connection allows you to access the interactive access features connecting to a runtime on the same LAN with the need for accessing the Internet.



FT Remote Access

Configuration

Availability mode

☑ Always on

☐ Digital input

☐ SMS

Connection port: Auto

Proxy configuration: None

Local Connection

☐ Enabled

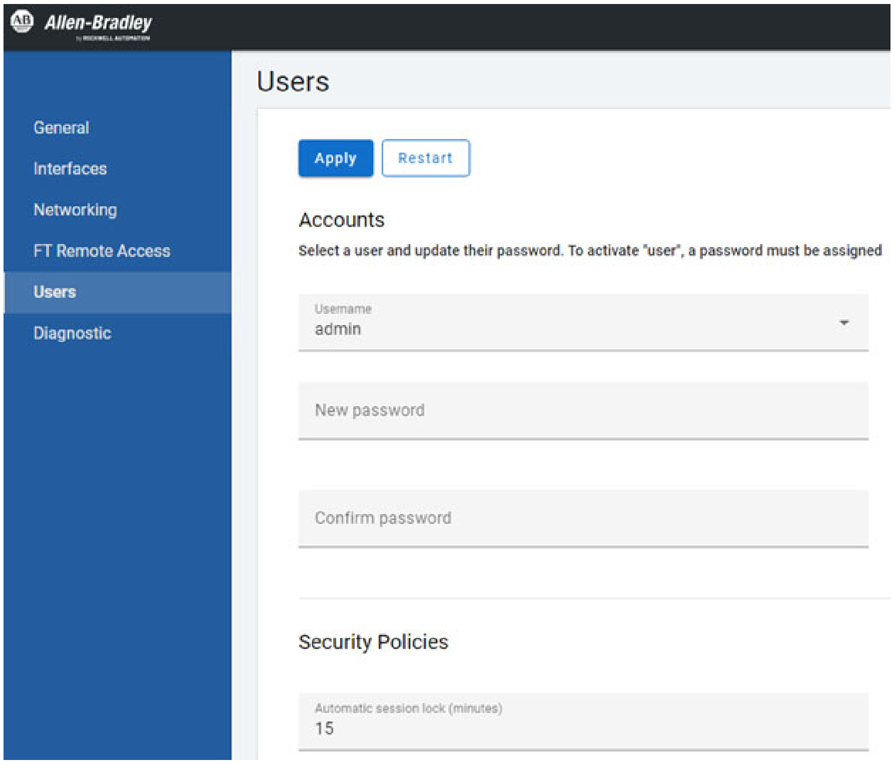
Password

Confirm password

Users

Device Manager access can be updated under the Users tab. From here users can update the admin password and create user accounts to be able to access Device Manager.

The session timeout can be changed under the user tab security policies. By default, the automatic timeout session lock is set to 15 minutes.



Users

Accounts

Select a user and update their password. To activate "user", a password must be assigned

Username: admin

New password

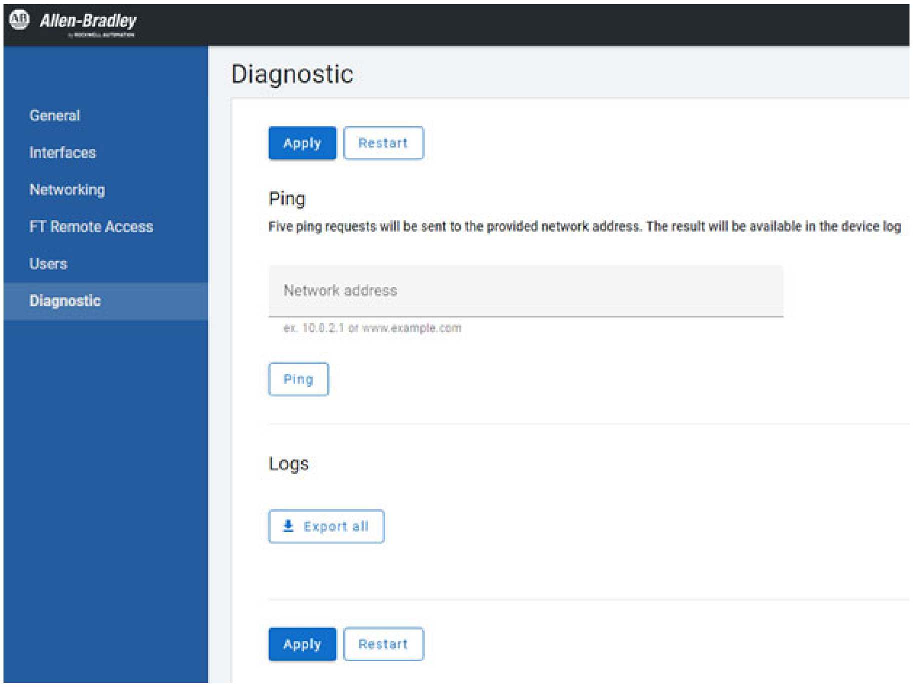
Confirm password

Security Policies

Automatic session lock (minutes): 15

Diagnostic

The diagnostic tab has a ping utility that allows users to troubleshoot and verify connectivity to network devices available to the router. Five ping requests are sent to the provided network address and the results are available in the SystemManager_log.



Diagnostic

Ping

Five ping requests will be sent to the provided network address. The result will be available in the device log

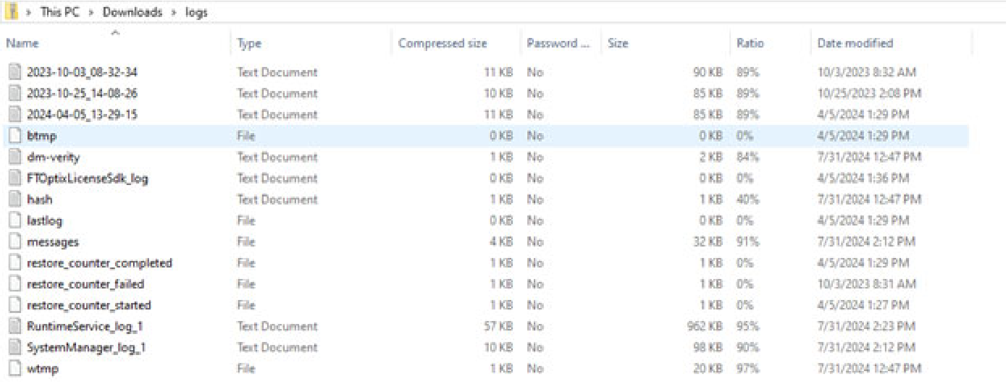
Network address

ex. 10.0.2.1 or www.example.com

Logs

Logs

Users can now use the export all button to download the Device Manager logs.



This PC › Downloads › logs

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
2023-10-03_08-32-34	Text Document	11 KB	No	90 KB	89%	10/3/2023 8:32 AM
2023-10-25_14-08-26	Text Document	10 KB	No	85 KB	89%	10/25/2023 2:08 PM
2024-04-05_13-29-15	Text Document	11 KB	No	85 KB	89%	4/5/2024 1:29 PM
btmp	File	0 KB	No	0 KB	0%	4/5/2024 1:29 PM
dm-verity	Text Document	1 KB	No	2 KB	84%	7/31/2024 12:47 PM
FTOptixLicenseSdk_log	Text Document	0 KB	No	0 KB	0%	4/5/2024 1:36 PM
hash	Text Document	1 KB	No	1 KB	40%	7/31/2024 12:47 PM
lastlog	File	0 KB	No	0 KB	0%	4/5/2024 1:29 PM
messages	File	4 KB	No	32 KB	91%	7/31/2024 2:12 PM
restore_counter_completed	File	1 KB	No	1 KB	0%	4/5/2024 1:29 PM
restore_counter_failed	File	1 KB	No	1 KB	0%	10/3/2023 8:31 AM
restore_counter_started	File	1 KB	No	1 KB	0%	4/5/2024 1:27 PM
RuntimeService_log_1	Text Document	57 KB	No	962 KB	95%	7/31/2024 2:23 PM
SystemManager_log_1	Text Document	10 KB	No	98 KB	90%	7/31/2024 2:12 PM
wtmp	File	1 KB	No	20 KB	97%	7/31/2024 12:47 PM

The exported files are able to be viewed in File explorer as seen above. This allows users to save and view diagnostic logs to aid in troubleshooting issues.

There are two main logs:

- RuntimeService_log

  Includes all information about the status of the Stratix service. You can find more details about the configuration of the network interfaces, and the VPN connection phase such as the chosen relay server or the use of the virtual USB port.

- SystemManager_log

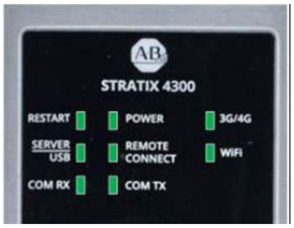
  Includes everything about the status of the device. It includes the type of device, licenses activated via tags, and IP addresses assigned to Ethernet ports.

Appendix A

Troubleshoot

Status Indicators

The following graphics show the status indicators for these routers.



Status Indicators Descriptions

Table 6 - Status Indicators

Status Indicator	Status	Description
Restart	Red	Active when pressing the restart button or indicates a nonrecoverable hardware fault.
Power	Green	The router is active.
Server/USB	Green	The router started and connected to the server.
	Red	The router started and did not connect to the server.
	Flashing Green	The router started and is connecting to the server.
	Flashing Red	The router started but is not connecting to the server because it is not associated to a domain.
	2 Red Flashes	An attempt to connect to a different domain than the first initial registration occurred.
	2 Green Flashes	Configuration from the USB stick was successfully completed.
	2 Red Flashes	User credentials for domain access are not valid.
	3 Green Flashes	Represents the start and finish of a router update from the USB stick. **IMPORTANT:** During the entire update phase, the status indicator is flashing from red to green.
	3 Red Flashes	The router update from the USB stick failed.
	4 Red Flashes	Factory restore has started.
	5 Red Flashes	An error occurred in the router runtime execution.This follows with a system restart.
	6 Red Flashes	The USB stick data format is not correct or has an unknown error.
Remote Connection	Green	Only active when at least one control center client is connected to the router.
COM RX/COM TX	Green/Yellow	The indicators are directly connected to the serial port RX/TX signals and show traffic through the lines.
3G/4G	Off	The modem has not detected the SIM card.
	Amber or Green Low Frequency Blink	The modem has detected network signal.
	Amber or Green High Frequency Blinking	The modem is exchanging data.
	Steady Red	The modem has not detected network signal.
	Blinking Red	The modem has not detected network signal.
Wi-Fi	Off	The Wi-Fi board is disabled.
	Green Low Frequency Blinking	The Wi-Fi board is connected to the network (Adapter mode) or is in Access Point mode. In both scenarios there is no data exchange.
	Green High Frequency Blinking	The Wi-Fi board is connected and is exchanging data.
	Red	Malfunction or incorrect configuration in Adapter mode.

Notes:

Appendix **B**

SIM Card Requirements and Configuration Example

The following is an example of how to configure your SIM Card with the use of the AT&T Network. The use of the Stratix® 4300 Remote Access™ Router.

AT&T SIM Card Requirements

AT&T SIM Card Requirements for configuration include the following:

- The Stratix 4300 Remote Access Router industrial router was tested certified for use on the AT&T Network.
- The Stratix 4300 Remote Access Router supports a 2FF or standard size SIM card, and the card must be purchased from AT&T.
- SIM Cards must use an IoT (Internet of Things) Data Plan from AT&T. A non-IoT SIM card is not supported.
- You must access the AT&T Control Center and obtain a custom APN (Access Point Name) to connect and manage AT&T SIM Cards.

AT&T SIM Card Procurement Process

To use our IoT program at AT&T, you can go to the following site to order an IoT Data plan starter kit.

https://att.m2m.com/

The starter kit includes the following items:

- AT&T IoT SIM card with unlimited domestic connectivity.
- Unlimited data for up to 3 months.

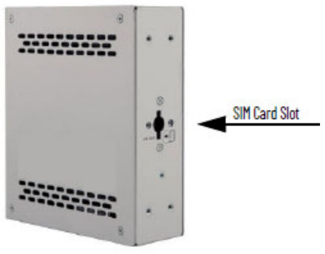
Once you complete the form for the starter kit, you are assigned to an AT&T IoT account manager who on-boards you into the IoT program from a formal contract and billing perspective.

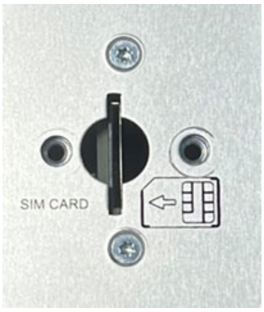
SIM Card Installation

The SIM Card can be installed in the router using the following steps:

1. Remove power from the device.
2. Remove the router from the DIN rail mount.
3. Insert the 2FF IoT SIM card.

   The card only fits into the device one way as seen in the image below.
4. Reinstall the DIN rail mount.
5. Power on the device.





IMPORTANT	Make sure to be careful inserting the SIM card. If you miss the slot, the SIM card can fall into the device, and the case must be removed to retrieve the SIM card.

SIM Card Configuration Example

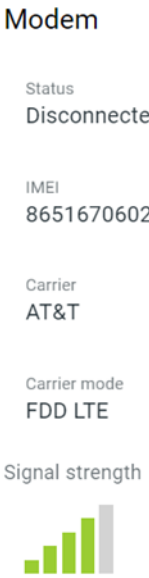
The following steps explain how to configure the SIM Card:

1. Power off the device, and install the AT&T IoT SIM Card.
2. Power on the device, and sign in to the System Manager interface.
3. Once you are logged into System Manager, go to Interfaces and then Modem.

   The modem shows that it is initializing while going through the SIM Card connection process.

Once the initialization process is complete, the status shows that it is disconnected, but you can see the Carrier as AT&T, Carrier Mode, and Signal Strength.

If not, there is an issue with the SIM Card, and you must test the connectivity of the SIM card in the AT&T Control Center.



Modem

Status
Disconnected

IMEI
865167060236867

Carrier
AT&T

Carrier mode
FDD LTE

Signal strength

4. Remove the check for Automatic APN configuration and enter in the APN provided from AT&T. Your APN can be found in the AT&T Control Center.
5. Make sure Set Service Set and Data Roaming are unchecked.
6. Apply the configuration and the device reloads.
7. Once the device reloads, the SIM Card status still says disconnected.
8. Add the device to FTRA, once the device has established a connection with FTRA. The status shows it is connected.

Index

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800