



Stratix 4300 Remote Access Routers

Catalog Number 1783-RA2TGB, 1783-RA5TGB



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.

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).

	Preface	5
	About This Publication	5
	Summary of Changes	5
	Additional Resources	5
	Chapter 1	
Remote Access Architecture	Remote Access Solution Overview	8
	Before You Begin	8
	Best Practices	9
	Remote Access Routers	10
	1783-RA2TGB	10
	1783-RA5TGB	11
	Multi-factor Authentication	13
	Typical Remote Access Architectures	14
	Secure Remote Connectivity -	
	Use Case: Cell/Area Zone SRA	14
	Secure Remote Connectivity -	
	Use Case: Modem Direct/Isolated Machine	19
	Chapter 2	
Router Integration	FactoryTalk Hub	21
	Authentication	21
	Open a Service	21
	Verify account	22
	Create a Domain	22
	Domain Membership	23
	Domain Connectivity	23
	Associate the Router with a Domain	24
	Protect Against Unwanted Domain Change	27
	Remove and Move Devices	27
	Set Up Your FactoryTalk Remote Access Connection	27
	Download the Tools	27
	Install the Tools	28
	Connect Via Ethernet	28
	Add an IP Address	35
	Firewall Policies	35
	Create a Firewall Policy	36
	Update the System	38
	Factory Reset	38
	Router Restart	39

Troubleshoot

Appendix A

Status Indicators..... 41

 Status Indicators Descriptions..... 41

Export Logs 42

Audit Logs..... 42

Index43

About This Publication

This manual describes how to use 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
FactoryTalk Hub	21
Domain Membership	23
Domain Connectivity	23
Set Up Your FactoryTalk Remote Access Connection	27
Firewall Policies	35

Additional Resources

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

Resource	Description
Cloud Connectivity to a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD017	Converged Plantwide Ethernet (CPwE) is a collection of architected, tested, and validated designs. The testing and validation follow the Cisco® Validated Design (CVD) and Cisco Reference Design (CRD) methodologies.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	The Implementation Guide represents a collaborative development effort from Cisco Systems and Rockwell Automation®. It is built on, and adds to, design guidelines from the Cisco Ethernet-to-the-Factory (EttF) solution and the Rockwell Automation Integrated Architecture®.
Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD002	The Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG) outlines several use cases for designing, deploying and managing industrial firewalls throughout a plant-wide Industrial Automation and Control System (IACS) network infrastructure.
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 Stratix 4300 router:

- Full gigabit router
- Supports configuration via FactoryTalk® Remote Access software
- Uses VPN connections that are optimized for industrial communications with reduced latency

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

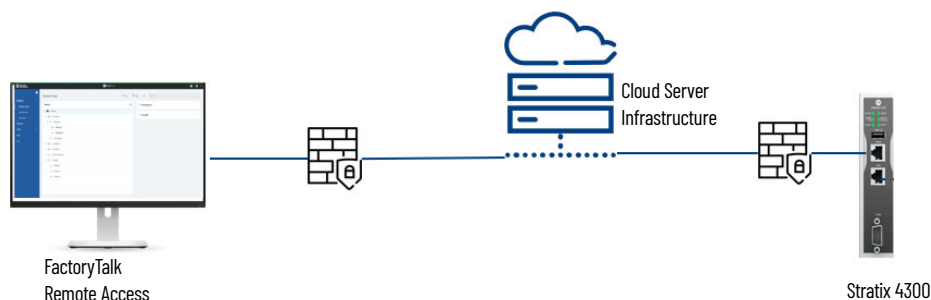
Before You Begin

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

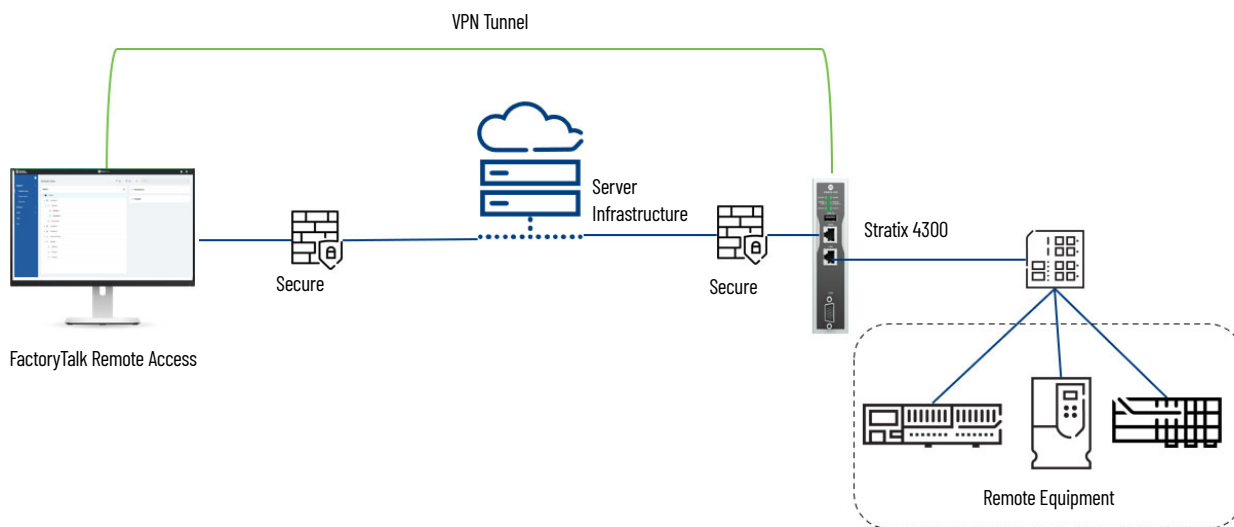
There are three key components for remote access.

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.
- Stratix 4300 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

1783-RA2TGB

Figure 1 - 1783-RA2TGB

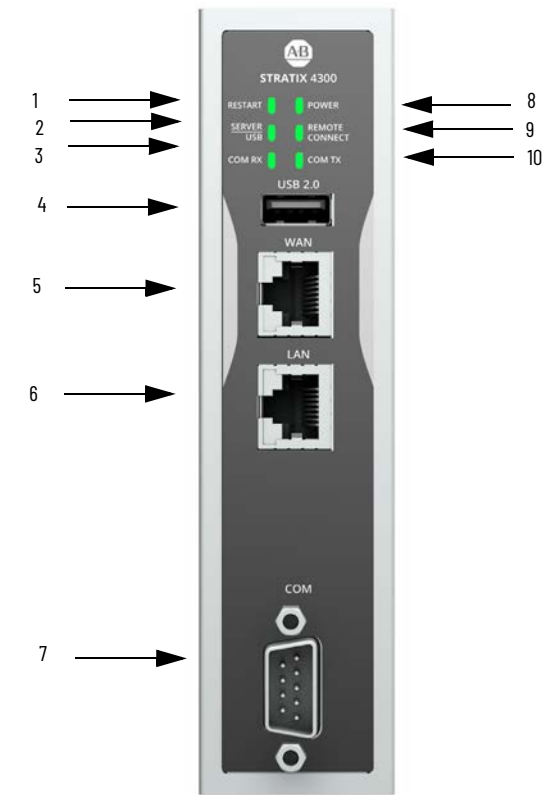


Table 1 - 1783-RA2TGB Router Front View

1	Restart Status Indicator
2	Server/USB Status Indicator
3	COM RX Status Indicator
4	USB 2.0
5	WAN
6	LAN
7	COM
8	Power Status Indicator
9	Remote Connect Status Indicator
10	COM TX Status Indicator

1783-RA5TGB

Figure 2 - 1783-RA5TGB

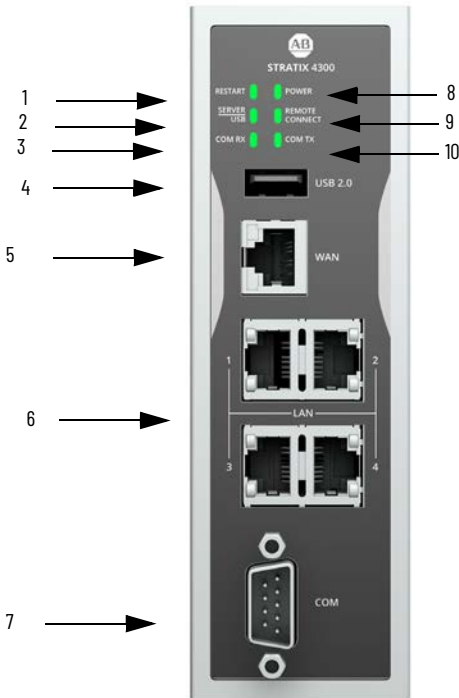


Table 2 - 1783-RA5TGB Router Front View

1	Restart Status Indicator
2	Server/USB Status Indicator
3	COM RX Status Indicator
4	USB 2.0
5	WAN
6	LAN1 LAN2 LAN3 LAN4
7	COM
8	Power Status Indicator
9	Remote Connect Status Indicator
10	COM TX Status Indicator

Figure 3 - Router Top View

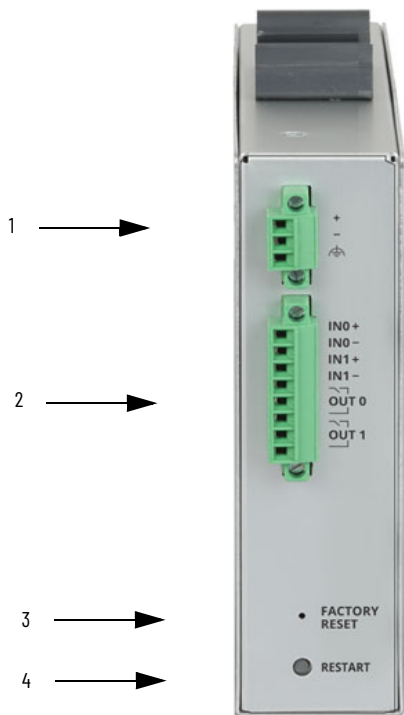


Table 3 - Router Top View

1	Power Connector
2	Digital Input/Output Connector
3	Factory Reset Button
4	Restart Button



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 4 - 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 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.

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. Use one of the following links from your device to download an authenticator app:
 - [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 login, each following login asks for your authenticator code. This code is updated every 3 minutes.

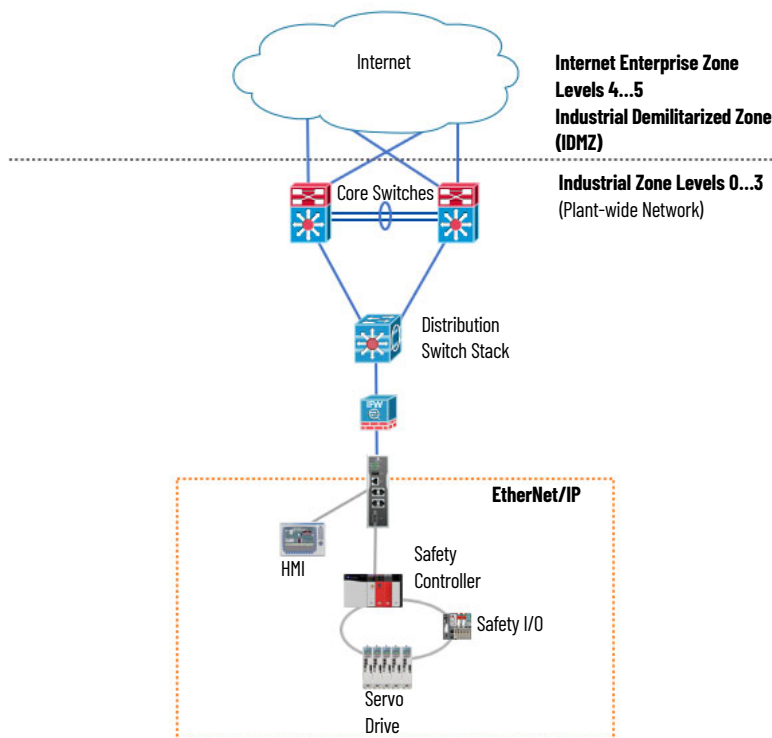
3. Open the authenticator application on your device and type in the current code that is assigned to your account.

Typical Remote Access Architectures

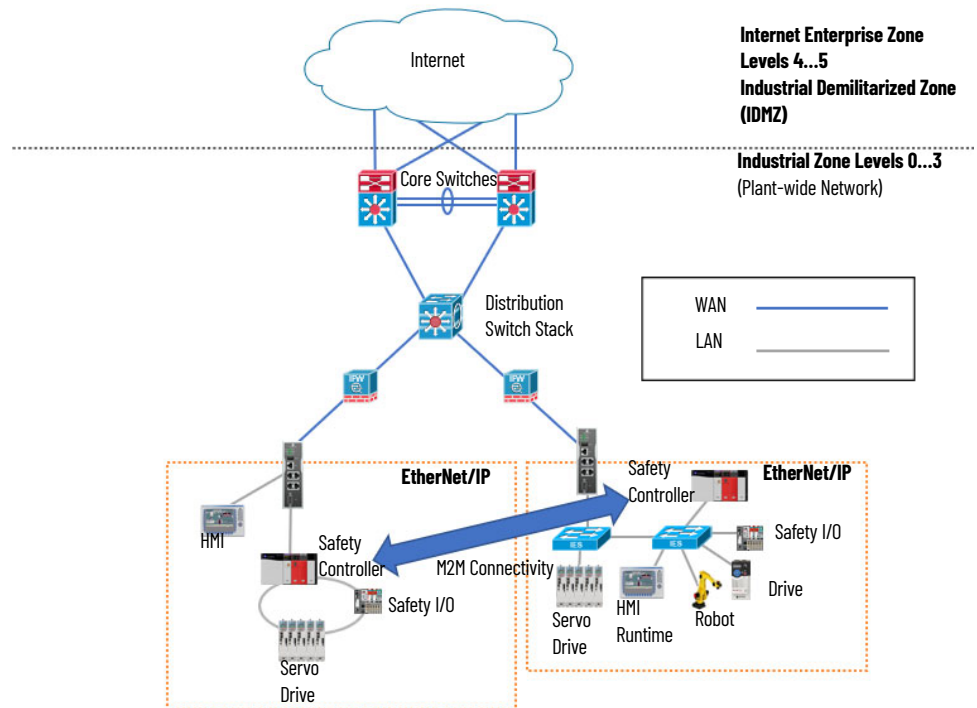
The following examples are common remote access architecture diagrams.

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

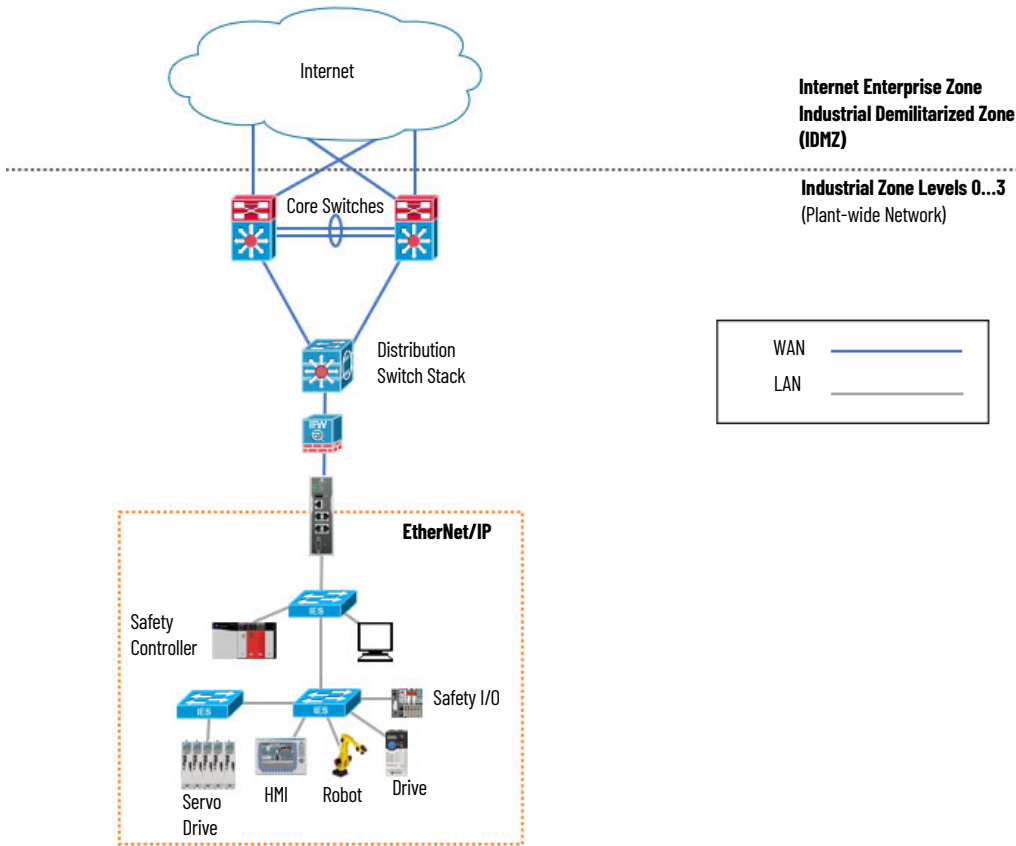
This architecture is highlighting the usage of the Stratix 4300 for remote access purposes and, if needed, for NAT/Routing purposes for the cell/area zone. Without NAT or Routing there are no North or South data flows through the Stratix 4300. East or West data flow (for example from the HMI to the Safety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



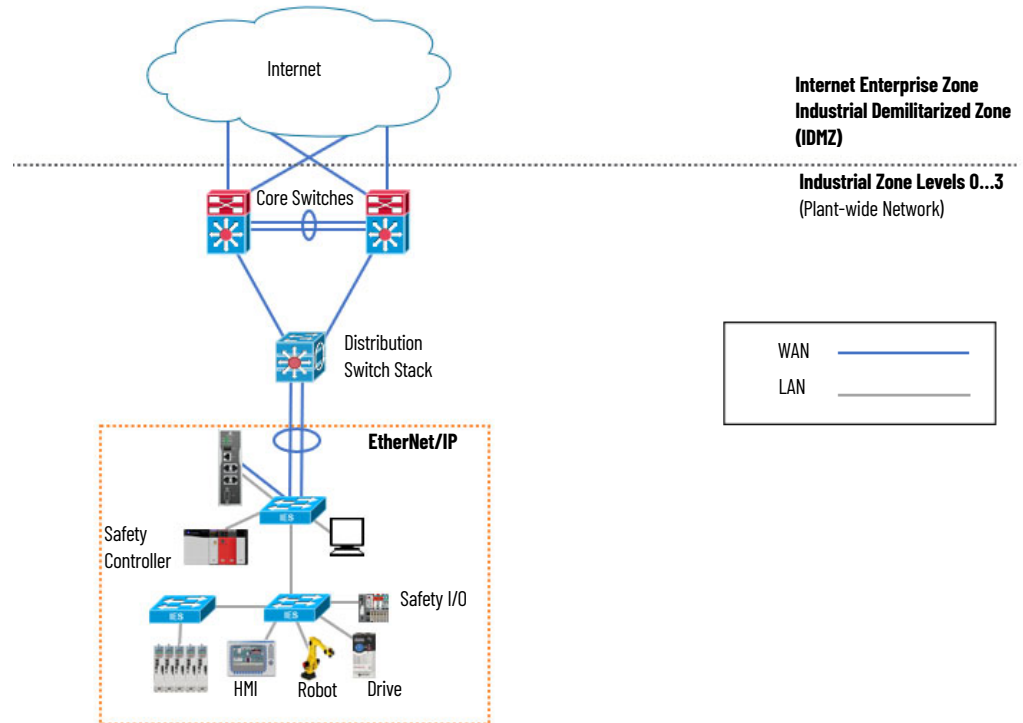
The following architecture is highlighting the use of the Stratix 4300 for remote access purposes and NAT/Routing purposes. The Stratix 4300 provides remote access to each individual cell/area zone. If there is a need for peer-to-peer or machine-to-machine communication, the Stratix 4300 NAT or Routing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



The following architecture is highlighting the use of the Stratix 4300 for remote access purposes. The switch optionally provides some NAT/Routing services for the Cell/Area Zone for LAN to WAN communication. Without NAT or Routing there are no North/South data flows. Most other data flows in the cell occur at the industrial Ethernet switch.

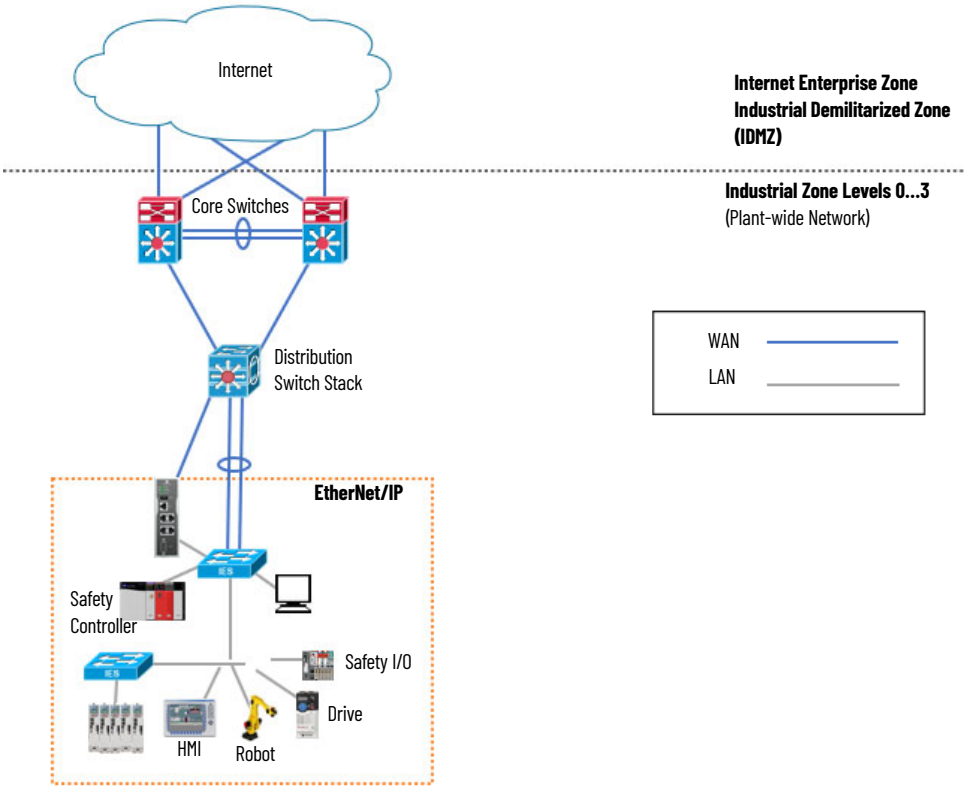


The following architecture is highlighting the use of the Stratix 4300 for remote access purposes. An IES is positioned in the cell for any other North/South and East/West traffic. The IES switching infrastructure also provides routing and switching services to all devices including the Stratix 4300. 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.



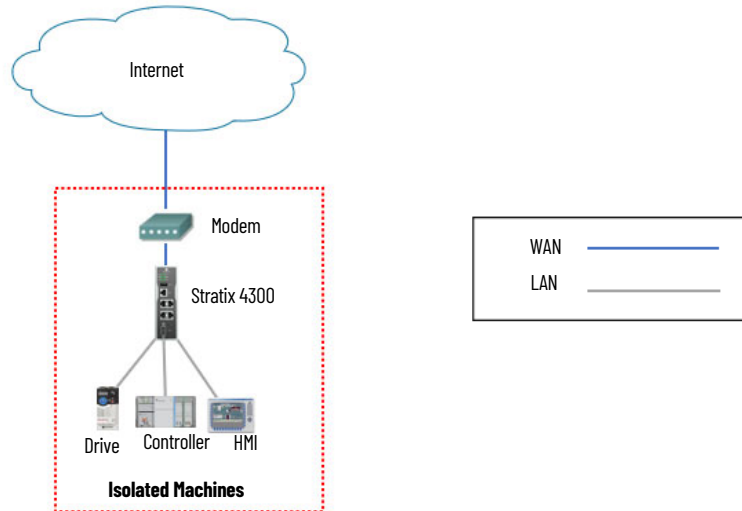
The following architecture is highlighting the usage of the Stratix 4300 for remote access purposes. An IES is positioned in the cell for any other North/South and East/West traffic. The IES switching infrastructure also provides routing and switching services to all devices. In this case, the IES is 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 would extend to the Cell/Area Zone in this architecture unless it is required by the industrial application.



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.



Notes:

Router Integration

The Stratix 4300® 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.

FactoryTalk Hub

To use FactoryTalk Hub, either create an organization or join an existing organization. The organization that you belong to controls 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 organization.

After your account has been authenticated, your browser will display 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 Design Tools or FactoryTalk Remote Access.
2. Click Home to return to the Home screen.

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 using 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 using an administrator user account.

Domain Membership

Features that can be part of a FactoryTalk Remote Access domain are listed in the following table.

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 efficiently 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 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 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 are allowed by most firewall systems. FactoryTalk Remote Access act 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:

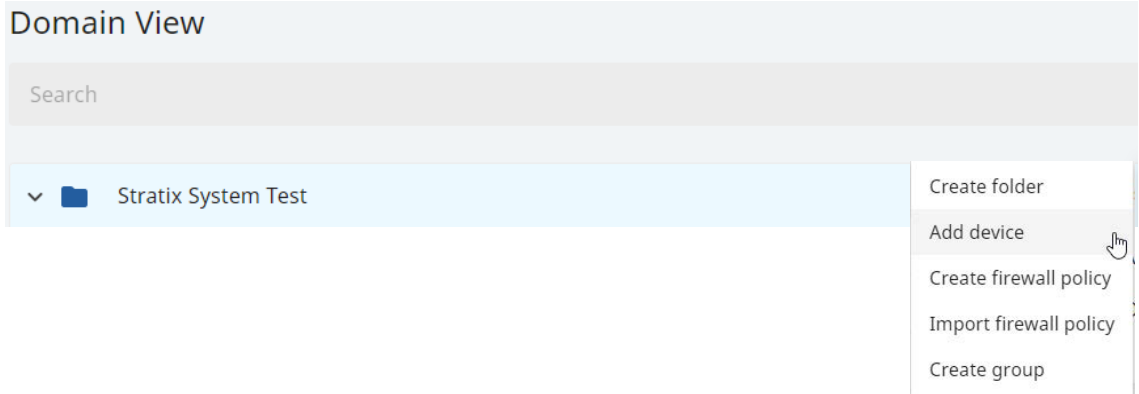
- 80
- 443
- 5935

The first open port will be 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 will be established.

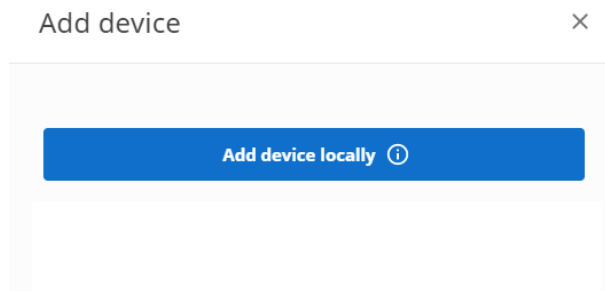
IMPORTANT All FactoryTalk Remote Access connections, regardless of the port used, are made using the secure SSL/TLS protocol to help ensure a safer information exchange over the internet. The use of the SSL/TLS protocol allows FactoryTalk Remote Access to verify the identity of the FactoryTalk Remote 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,



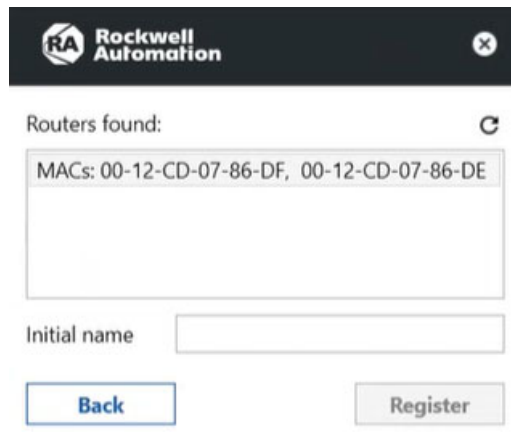
4. To add the device, reenter the router credentials.

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

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.



A screenshot of a Rockwell Automation dialog box titled "Routers found:". The dialog box has a dark header with the Rockwell Automation logo and a close button. Below the header, it says "Routers found:" followed by a refresh icon. A text box displays "MACs: 00-12-CD-07-86-DF, 00-12-CD-07-86-DE". Below this is an empty text box for the "Initial name". At the bottom are two buttons: "Back" and "Register".

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.



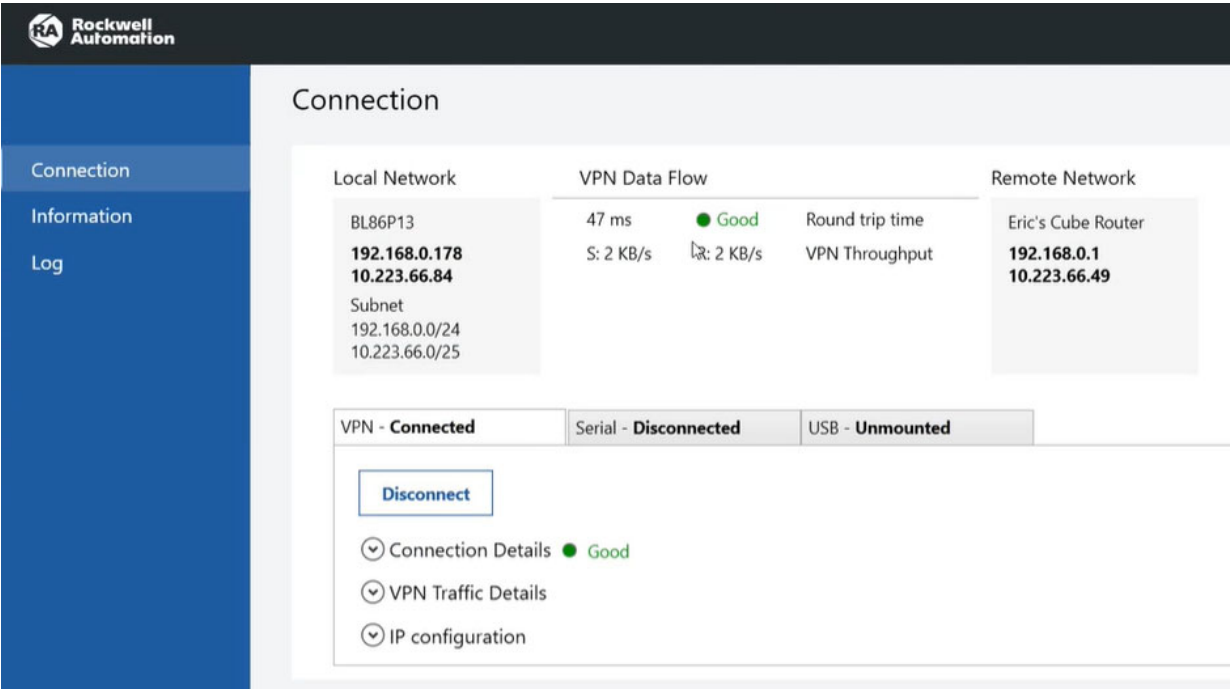
After you click the VPN bar, an image for the VPN will blink in your PC's toolbar at the bottom of your screen.

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.



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 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 in the event that a router is restored to factory settings with the intent to bypass the correct procedure.

A sequence of two blinking 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 required, 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 make changes to 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. Login 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

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

Allen-Bradley
by ROCKWELL AUTOMATION

Device initialization

Apply Reboot

Password
The default password must be changed before first use

New password

Confirm password

The password change prompts the device to restart.

- To apply the changes, restart your device.

Info

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

OK Cancel

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

Allen-Bradley
by ROCKWELL AUTOMATION

General

General

Interfaces

Networking

Server connection

Users

Diagnostic

Apply Reboot

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

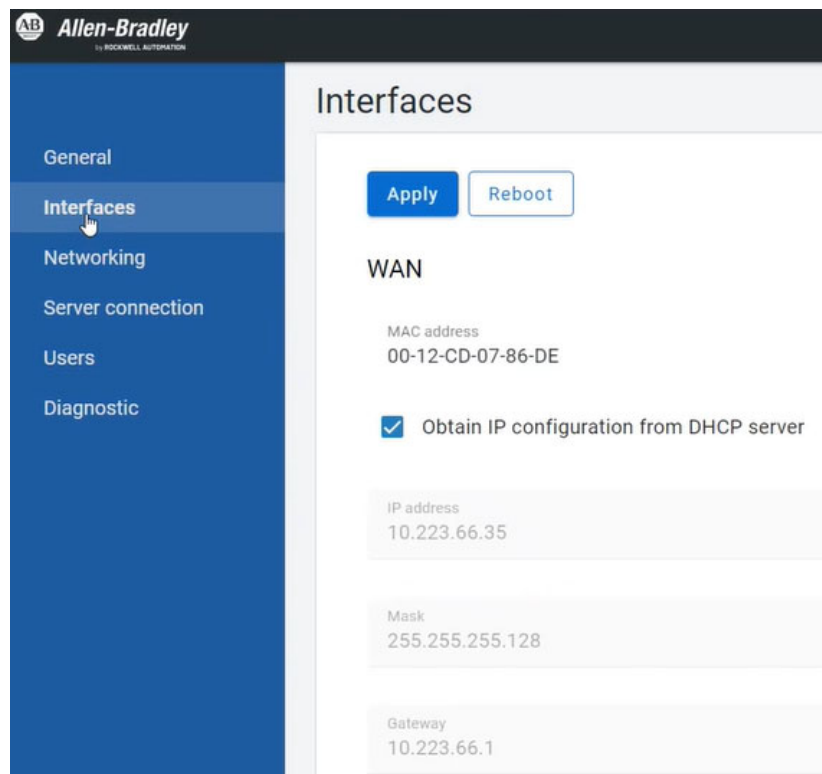
System Manager version
1.4.24.42

Runtime version
13.0.020

Legal notices

[Main licenses](#)
[Open source licenses](#)

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



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

Add

Remove

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

Serial port

Mode
RS232C

Apply

Reboot

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

General

Interfaces

Networking

Server connection

Users

Diagnostics

Networking

Apply

Reboot

VPN

☐ Reserve static IP pool for VPN connections

List of reserved static IP pool

Remove

From

To

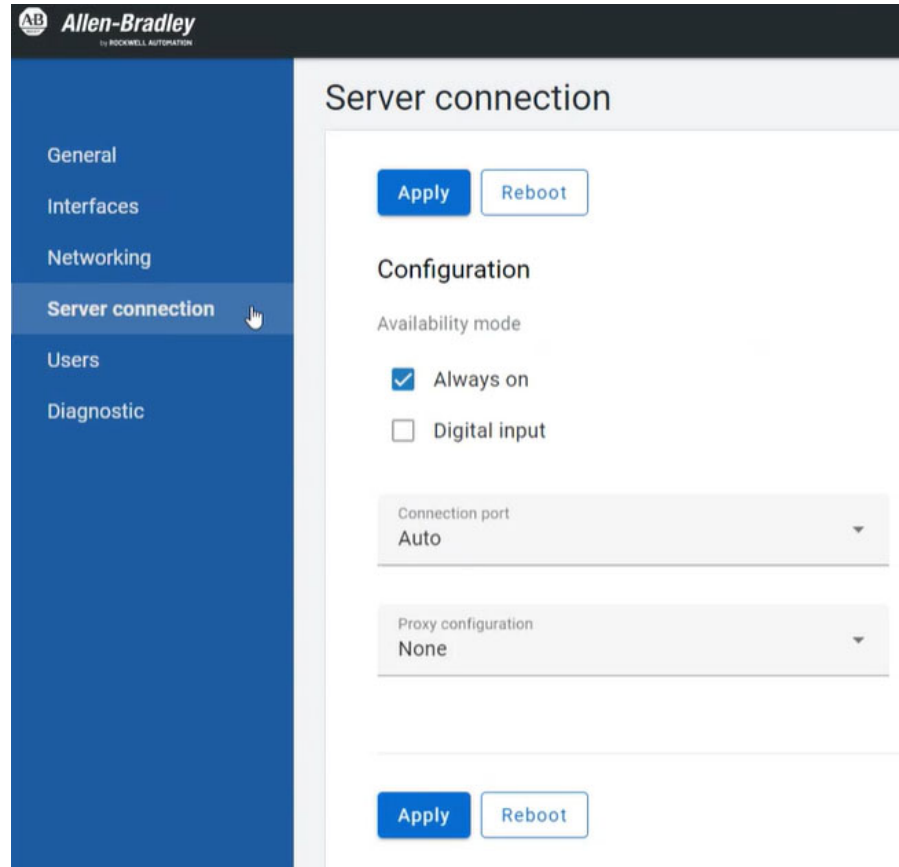
Subnet mask

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 will also restore 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 (INo) is activated.



The screenshot shows the Allen-Bradley configuration interface. On the left is a blue sidebar with a menu containing: General, Interfaces, Networking, **Server connection** (highlighted with a mouse cursor), Users, and Diagnostic. The main content area is titled "Server connection" and contains two "Apply" and "Reboot" buttons at the top. Below these is a "Configuration" section. Under "Availability mode", there are two radio button options: "Always on" (which is selected with a blue checkmark) and "Digital input". Below the radio buttons are two dropdown menus: "Connection port" set to "Auto" and "Proxy configuration" set to "None". At the bottom of the configuration section, there are another pair of "Apply" and "Reboot" buttons.

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.

General

Interfaces

Networking

Server connection

Users

Diagnostic

Users

Apply

Reboot

Accounts

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

Username

admin

New password

Confirm password

Apply

Reboot

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

General

Interfaces

Networking

Server connection

Users

Diagnostic

Diagnostic

Apply

Reboot

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

Ping

Add an IP Address

To add an IP address, under the interfaces tab, find the list of existing IP addresses, and click add. The following screen appears.

Add IP address

IP address
Mask

Add Cancel

After adding the IP address, you will be prompted to restart.

Info

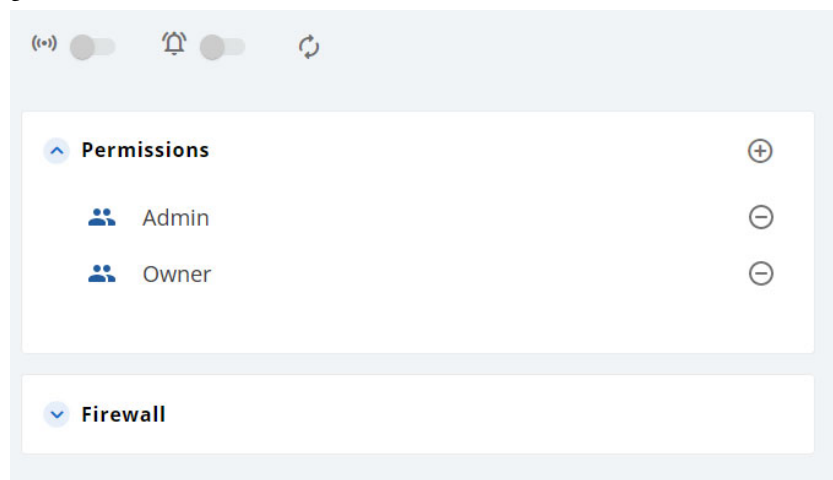
Configuration successfully saved. Would you like to reboot the device to apply changes now?

OK Cancel

Firewall Policies

The firewall included with FactoryTalk Remote Access defines and applies policies to VPN traffic to improve security and reduce traffic between remote devices and FactoryTalk Remote Access.

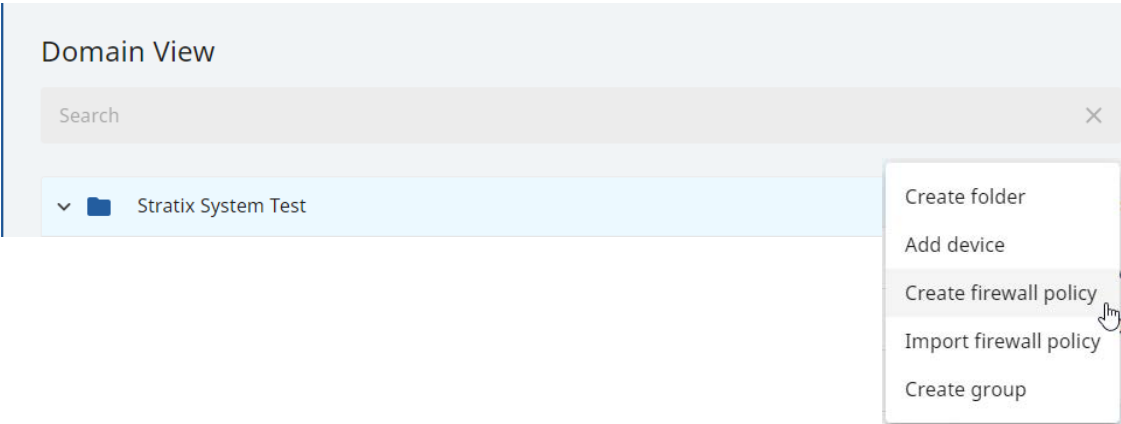
To add a firewall policy, you must be in the FactoryTalk Remote Access environment. The firewall option is listed on the right of the Domain View page.



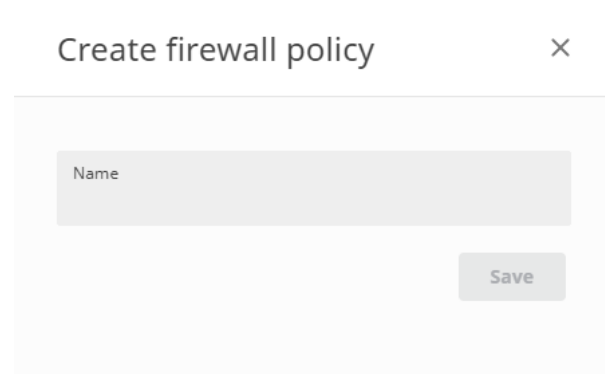
Create a Firewall Policy

From the domain view, you can create or import a firewall policy.

1. To create a firewall policy, click the folder where you want to define the policy and then click Create firewall policy.



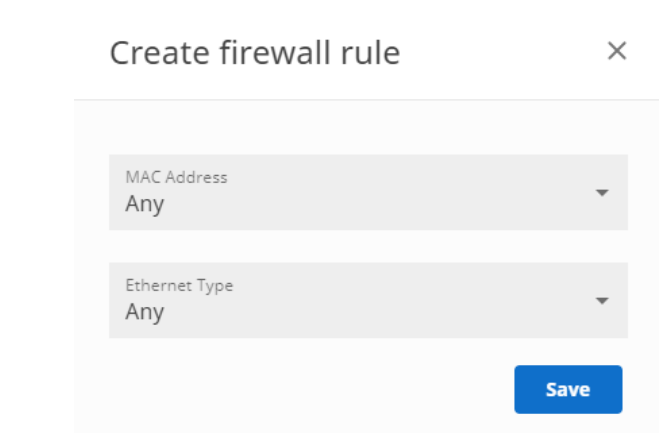
2. Type the name of the policy in the space provided. Confirm that the name is correct, then click “Save” to create the policy.



3. To display the policy configuration panel where you can define the rules of the firewall policy, click the policy name.

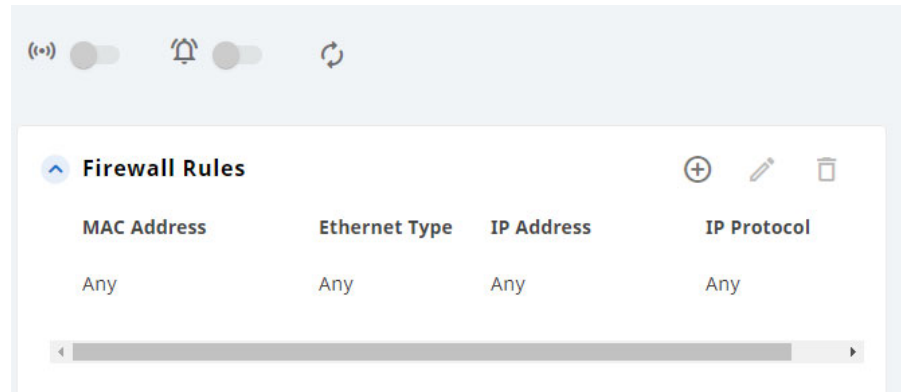


4. Click Add to configure a rule in the policy definition.
5. Add a MAC address and an Ethernet Type.



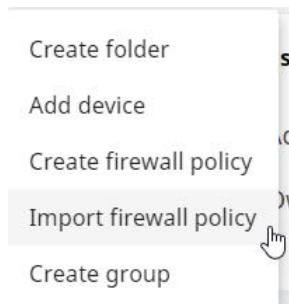
FactoryTalk Remote Access VPN supports the virtualization of the datalink layer and the integrated firewall supports the definition of networking connection rules.

The Ethernet type lists the Ethernet communication protocols. After selecting the Ethernet type, the appropriate configurable properties are displayed. For example, after selecting IP the configurable properties displayed are IP address, IP protocol, and IP ports.



Import a Firewall Policy

1. To import a firewall policy, start with the same process as creating one and select import.



2. Select the firewall policy that you want to import from the list then click OK. The policy is imported into the domain

Associate policy association ×

Update the System

The software components upgrades are distributed in the format of one file that works as “container” for the components to be replaced.

To execute an update, copy the file on the root folder of the USB Stick. Insert the USB stick into the routers USB port and cycle the power. During the power-up phase, the router recognizes the USB stick with the update and it starts the system software update procedure.

No further action is needed. The update is completed after the router automatically restarts.



You can also update by clicking the update link in the cloud portal page.

Factory Reset

The factory settings for the Ethernet interfaces are shown in the following table.

Interface	IP Address	Mask
LAN	192.168.0.1	255.255.255.0
WAN	DHCP	

The access to the Router configuration is protected with a combination user/password.

The default username and password are both “admin.”



This protection is independent from the security handling that is related to the Domain users. The user/password account is a local device protection.

The factory settings information is printed on the Router side with the MAC addresses of the two network interfaces. The MAC addresses assigned to the two network interfaces are also printed.

To complete a factory reset, use the following steps.

1. Turn off the device.
2. Press and hold the factory reset button and turn on the device.
3. When the Server/USB status indicator is alternating blinking red and green for at least 15 seconds, release the button.

Following these steps, the router performs the deletion of the system and a complete reset. Do not to turn off or remove the power supply to the router in this phase.

During the factory reset, the Server/USB indicator blinks green. This blink signals that the process is working. Wait until the process is automatically completed. If the router shuts down during this process, the factory reset is not completed.

At the end of the reset process, the Server/USB indicator turns on and starts to blink. When the indicator is blinking red, the reset is complete.

Router Restart

The restart function forces a complete initialization of all internal electronics and software.

The Restart status indicator returns the feedback.

To restart the router, use the following steps.

1. Turn on the device.
2. Press and release the restart button.

The restart status indicator turns red. The indicator blinks green four times to indicate that the restart has been completed.

The router can also be restarted from Device Manager over VPN.

Notes:

Troubleshoot

Status Indicators

The following graphics show the status indicators for these routers.



Status Indicators Descriptions

Table 5 - 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.

Export Logs

The following table defines export logs found on the Stratix® 4300 Device Manager webpage.

Table 6 - Export Logs

Tag	Description
RuntimeService_log	Includes all the 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.
NetworkDriver_log	Includes all the information about the status of the driver needed to manage the VPN channel and other network options in charge of the Stratix service.

Audit Logs

The FactoryTalk® Remote Access clients automatically record the operations 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.

A

audit logs 42

B

best practices 9

C

connect via ethernet 28
add an IP address 35

E

export logs 42

F

factory reset 38
firewall policies 35
create a firewall policy 36
import a firewall policy 37

I

integrate a secure remote access solution 19

M

move devices 27
multifactor authentication 13

R

remote access architecture
1783-RA2TGB 10
1783-RA5TGB 11
remove devices 27
router features 12
firewall 14
multifactor authentication 13
router integration 21
router restart 39

S

secure remote access solution 19
secure remote connectivity - use case
cell/area zone SRA 15
modem direct/isolated machine 19
status indicators 41

T

troubleshoot 41
typical remote access architectures 14

U

unwanted domain change 27
update the system 38

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
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 information on its website at rok.auto/pec.

Allen-Bradley, expanding human possibility, FactoryTalk, Rockwell Automation, Stratix, and VersaView are trademarks of Rockwell Automation, Inc.

EtherNet/IP is a trademark of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, Çerenköy, 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, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846