



# Embedded Edge Compute Module

Catalog Number 1756-CMEE1Y1



***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.

|   |  |    |
|---|--|----|
|   | <b>Preface</b>                                     |    |
|   | About This Publication .....                       | 5  |
|   | Summary of Changes .....                           | 5  |
|   | Download Firmware, AOP, EDS, and Other Files ..... | 5  |
|   | Additional Resources .....                         | 5  |
|   | <b>Chapter 1</b>                                   |    |
| <b>ControlLogix Embedded Edge<br/>Compute Module</b>            | Catalog Number Explanation .....                   | 7  |
|   | Minimum Requirements .....                         | 7  |
|   | Module Components .....                            | 8  |
|   | Module Location .....                              | 10 |
|   | Status Indicators .....                            | 12 |
|   | Connection Options .....                           | 12 |
|   | USB 3.0 Port .....                                 | 12 |
|   | Ethernet Ports .....                               | 13 |
|   | Rotary Switches .....                              | 14 |
|   | Reset Button .....                                 | 14 |
|   | Factory Restore Button .....                       | 15 |
|   | Replace the microSD Card .....                     | 15 |
|   | FactoryTalk Optix Applications .....               | 16 |
|   | <b>Chapter 2</b>                                   |    |
| <b>Configure the Module with<br/>Studio 5000 Logix Designer</b> | Overview .....                                     | 17 |
|   | Device Definition .....                            | 18 |
|   | Device Information .....                           | 19 |
|   | FactoryTalk Optix Studio .....                     | 20 |
|   | Restart .....                                      | 20 |
|   | Internet Protocol .....                            | 21 |
|   | IP Mismatch .....                                  | 22 |
|   | Port Configuration .....                           | 23 |
|   | Port Diagnostics .....                             | 24 |
|   | <b>Chapter 3</b>                                   |    |
| <b>System Manager</b>   | Factory Settings .....                             | 25 |
|   | Access System Manager from a Browser .....         | 25 |
|   | System Manager Menu .....                          | 26 |
|   | General .....                                      | 26 |
|   | Protection Mode .....                              | 26 |
|   | General options .....                              | 27 |
|   | Date and Time .....                                | 28 |
|   | External Storage Devices .....                     | 29 |
|   | System Information .....                           | 30 |
|   | Legal Notices .....                                | 30 |

|                            |    |
|----------------------------|----|
| FactoryTalk Optix .....    | 31 |
| Configuration.....         | 31 |
| Application.....           | 31 |
| Entitlement .....          | 32 |
| Interfaces .....           | 34 |
| CMEE Display .....         | 34 |
| Eth1: WAN .....            | 34 |
| Eth2: LAN .....            | 35 |
| FT Remote Access .....     | 36 |
| Connection.....            | 36 |
| Configuration.....         | 37 |
| Local connection.....      | 38 |
| VPN .....                  | 39 |
| Docker .....               | 40 |
| Services .....             | 40 |
| Containers .....           | 41 |
| Remote Management .....    | 42 |
| Container Storage.....     | 43 |
| Private Registries .....   | 43 |
| Proxy.....                 | 44 |
| Users .....                | 44 |
| Accounts .....             | 44 |
| Security Policies .....    | 46 |
| Diagnostic .....           | 47 |
| Ping.....                  | 47 |
| Export Logs .....          | 47 |
| Maintenance .....          | 48 |
| Configuration Import ..... | 48 |
| Configuration Export ..... | 49 |

## Chapter 4

### Remote Access

|   |    |
|---|----|
| FactoryTalk Hub .....   | 51 |
| Authentication.....   | 51 |
| Open a Service.....   | 51 |
| Verify account.....   | 51 |
| Add the Module to FactoryTalk Remote Access .....                           | 52 |
| Deploy a FactoryTalk Optix Application With FactoryTalk Remote Access ..... | 52 |

## Appendix A

### Update the Device Firmware

|   |    |
|---|----|
| Update Through System Manager.....                            | 53 |
| Update Through USB Memory Stick .....                         | 53 |
| Remote Update Through FactoryTalk Remote Access Manager ..... | 54 |

## About This Publication

This manual explains how to configure and use ControlLogix® Embedded Edge Compute modules.

## 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 |
|---|------|
| Updates to existing sections in the System Manager chapter.   | 25   |
| The VPN section that was previously under the Networking section has been moved to the FactoryTalk® Remote Access™ section, and the Networking section was removed. | 36   |
| Added Docker® section to the System Manager chapter.  | 40   |
| Added Maintenance section to the System Manager chapter.  | 48   |
| Added Appendix A: Update the Device Firmware  | 53   |

## Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at [rok.auto/pcdc](http://rok.auto/pcdc).

## Additional Resources

These documents contain additional information concerning related products from Rockwell Automation. You can view or download publications at [rok.auto/literature](http://rok.auto/literature).

| Resource  | Description  |
|---|--|
| ControlLogix Embedded Edge Compute Module Installation Instructions, publication <a href="#">1756-IN091</a> . | Describes how to install the ControlLogix Embedded Edge Compute Module.                            |
| ControlLogix I/O Modules Specifications Technical Data, publication <a href="#">1756-TD002</a> .              | Provides specifications for the ControlLogix Embedded Edge Compute module.                         |
| FactoryTalk® Optix Studio™ Help   | Provides help on how to use FactoryTalk Optix Studio.  |
| FactoryTalk Remote Access Help  | Provides help on how to use FactoryTalk Remote Access.   |
| EtherNet/IP Network Devices User Manual, <a href="#">ENET-UM006</a>   | Describes how to configure and use EtherNet/IP™ devices to communicate on the EtherNet/IP network. |
| Ethernet Reference Manual, publication <a href="#">ENET-RM002</a>   | Describes basic Ethernet concepts, infrastructure components, and infrastructure features.         |
| Industrial Automation Wiring and Grounding Guidelines, publication <a href="#">1770-4.1</a>                   | Provides general guidelines for installing a Rockwell Automation industrial system.                |
| Product Certifications website, <a href="http://rok.auto/certifications">rok.auto/certifications</a> .        | Provides declarations of conformity, certificates, and other certification details.                |

**Notes:**

# ControlLogix Embedded Edge Compute Module

The ControlLogix® Embedded Edge Compute module is a chassis-based module that can communicate directly with Logix controllers, and has read and write access to all controller tags through the backplane and front Ethernet port.

The Embedded Edge Compute module:

- Enables FactoryTalk® Optix Studio™, a development platform for creating human machine interface (HMI) and Internet of Things (IoT) applications.
- Contains a FactoryTalk® Optix™ XS runtime license with five tokens, and a FactoryTalk® Remote Access™ Runtime Pro license.
- Supports Docker® software, a container platform for creating and deploying applications (with module firmware revision 6.0.0.192 and later).

## Catalog Number Explanation

The ControlLogix Compute Embedded Edge module catalog number indicates specific information about the module. The module uses the format **1756-CMEExyz**, where the following apply:

- 1756 is the Bulletin number.
- CMEE = Embedded Edge Compute Module
- x represents the microSD™ card capacity
- y represents the embedded OS that is installed on the module
- z represents the application that is shipped on the module

### ControlLogix Embedded Edge Compute Module Catalog Number (1756-CMEE1Y1)

| Variable | Attribute                                 | Possible Value                     |
|----------|---|------------------------------------|
| x        | microSD card capacity                     | 1 = 32 GB                          |
| y        | Operating system                          | Y = Embedded Yocto Linux OS 64-bit |
| z        | Application that is shipped on the module | 1 = No application                 |

## Minimum Requirements

The module has these minimum requirements:

- ControlLogix Chassis, Series C (Series B chassis function within a derated temperature range)
- ControlLogix Chassis Power Supply
- FactoryTalk Optix Studio version 1.20 or later
- If you want to use the Studio 5000 Logix Designer® application to configure the module, you need:
  - A ControlLogix 5570 or 5580 controller with firmware revision 28.011 or later.
  - Studio 5000 Logix Designer version 28.00.00 or later.
  - Add-on Profile for 1756 Embedded Edge Compute version 40.00.45 or later

# Module Components

This table describes the components available on the Embedded Edge Compute module.

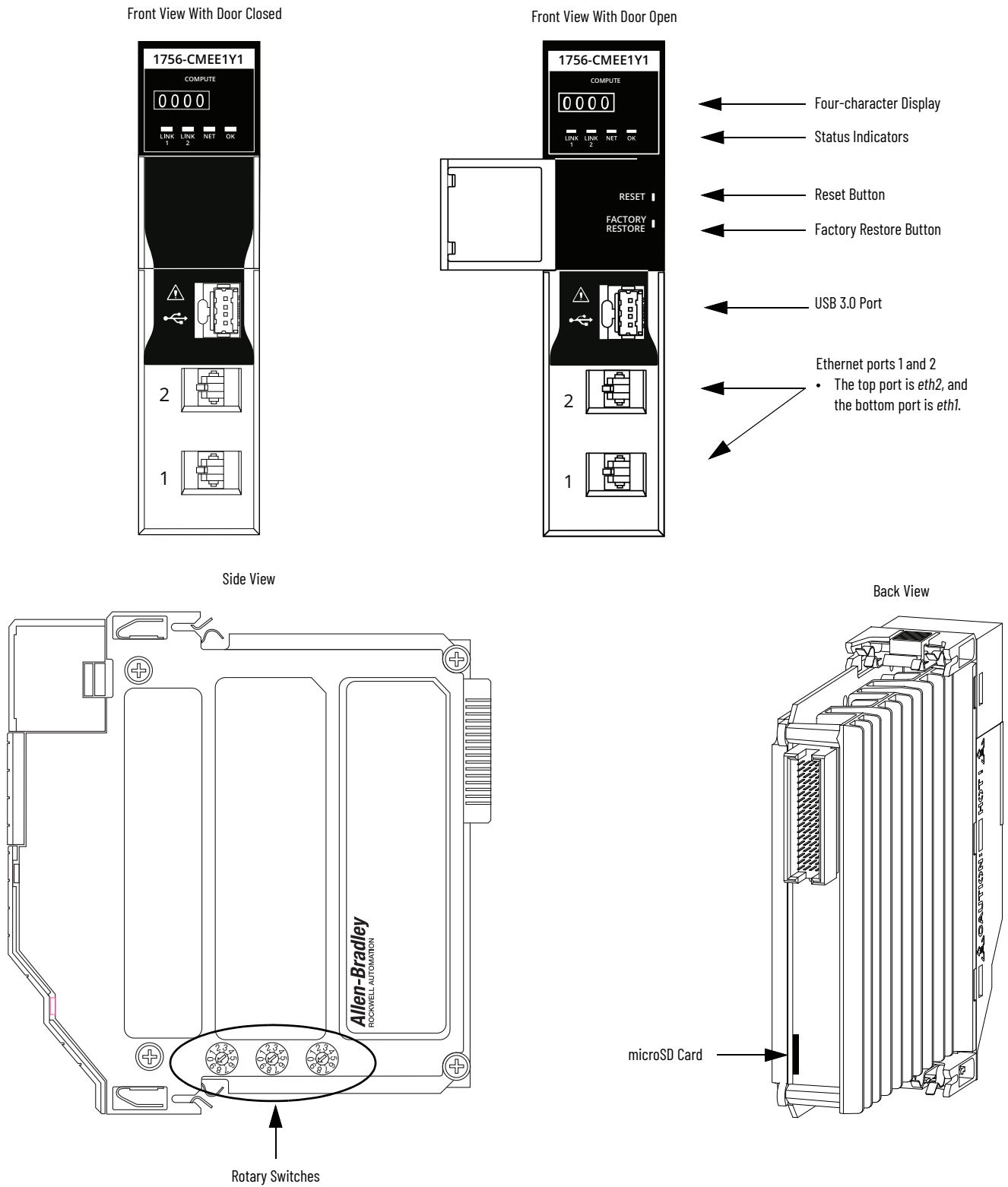
**Embedded Edge Compute Module Components**

| Component                      | Description   |
|--------------------------------|---|
| Linux Yocto 64-bit embedded OS | Embedded operating system.  |
| Onboard memory                 | 4 GB - RAM  |
| eMMC memory                    | 20 GB - Mass storage  |
| Four-character display         | Scrolls information about the module.   |
| Status indicators              | Shows information about the module status and health.   |
| Reset button                   | Used with the embedded OS to restart the module.  |
| Factory Restore button         | The factory restore button: <ul style="list-style-type: none"><li>• Resets all settings.</li><li>• Restores the operating system and module firmware</li><li>• Removes the FactoryTalk Remote Access identity.</li></ul>  |
| USB 3.0 port                   | Connect USB peripherals.  |
| Two 1 Gb Ethernet ports        | Used with the Ethernet protocol.  |
| Rotary switches                | Not functional currently.   |
| microSD Card (1784-MSDHC32)    | <ul style="list-style-type: none"><li>• 32 GB</li><li>• One microSD card is included in the product and is considered a part of the product.</li><li>• Declared data retention and Factory Reset times are valid only when using the microSD card included in the product.</li><li>• Rockwell Automation recommends you only replace the microSD card if it fails.</li><li>• Replacing the microSD card for any other reason is not recommended, and is taken at your own risk.</li></ul> |



This figure shows the components that are visible on the module.

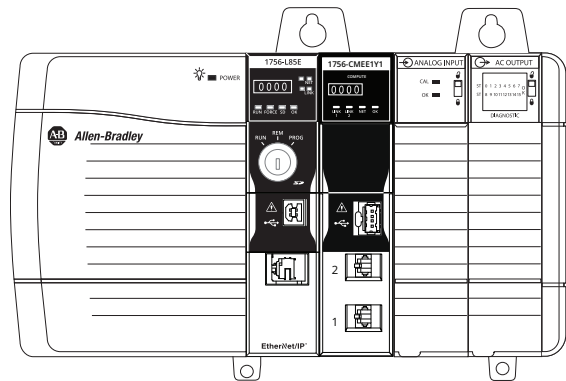
### ControlLogix Embedded Edge Compute Module Components



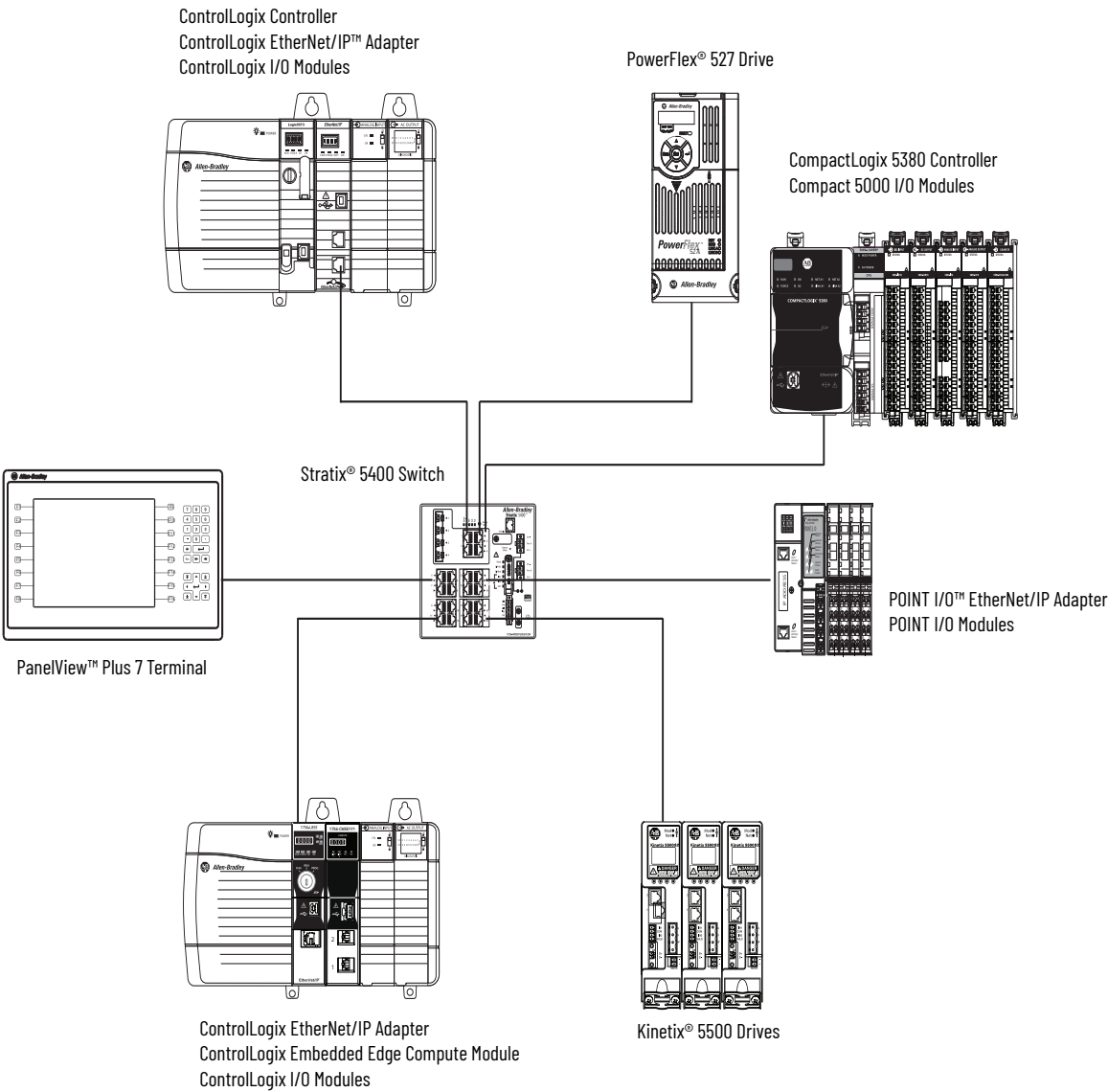
# Module Location

The module can reside locally in the same chassis as the controller or in a chassis that is remote from the controller with which it communicates.

## Local Chassis - ControlLogix 5580 System with Embedded Edge Compute Module



## Control Application with Embedded Edge Compute Module in Remote Chassis

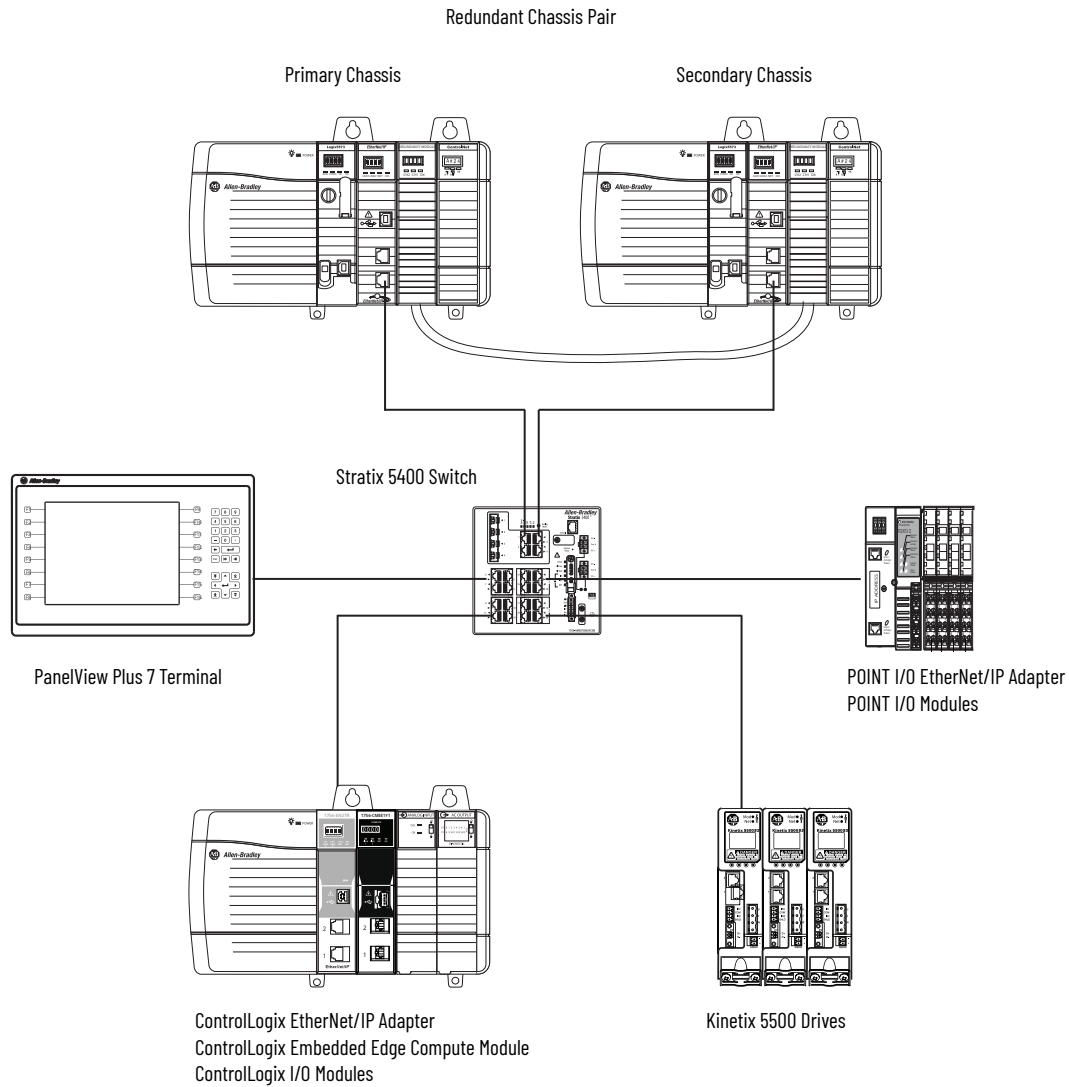


## Embedded Edge Compute Module in a Redundancy System

You can use the module in a ControlLogix redundancy system, but the module must reside in a remote chassis. The module communicates with the ControlLogix controller over an EtherNet/IP™ network.

**IMPORTANT** The module cannot reside in the primary or secondary chassis.

### ControlLogix Redundancy System with Embedded Edge Compute Module in Remote Chassis



# Status Indicators

The module uses a 4-character display and status indicators to show the module state at any point in time.


| Indicator        | State              | Description  |
|------------------|--------------------|--|
| LINK 1<br>LINK 2 | Off                | No activity. One of these conditions exists: <ul style="list-style-type: none"><li>• The device is not connected to a network.</li><li>• The port is administratively disabled.</li></ul>  |
|                  | Steady green       | The device is connected to a network but is not actively communicating.  |
|                  | Flashing green     | The device is actively communicating on a network.   |
| NET              | Off                | One of these conditions exists: <ul style="list-style-type: none"><li>• The module is not powered.<ul style="list-style-type: none"><li>– Verify that there is chassis power.</li><li>– Verify that the module is completely inserted into the chassis and backplane.</li><li>– Make sure that the module has been configured.</li></ul></li><li>• The module is powered but does not have an IP address. Assign an IP address to the module.</li><li>• The port is administratively disabled.</li></ul> |
|                  | Flashing green     | The module has an IP address, but no active connections are established.   |
|                  | Steady green       | The module has an IP address and at least one established active connection.   |
|                  | Steady red         | Duplicate IP address or invalid configuration.   |
|                  | Flashing Green/Red | The module is performing its power-up testing.   |
| OK               | Off                | No power is applied to the module.   |
|                  | Flashing red       | One of the following is true: <ul style="list-style-type: none"><li>• The device has a recoverable fault.</li><li>• The device firmware is being updated.</li><li>• Factory reset is in progress.</li></ul>  |
|                  | Steady red         | One of the following is true: <ul style="list-style-type: none"><li>• The module is powered, but is inoperable.</li><li>• The module has a major nonrecoverable fault.</li></ul>   |
|                  | Flashing green     | The module is booting.   |
|                  | Steady green       | The module is operating normally and the boot phase is completed.  |

# Connection Options


The module has USB and Ethernet ports.

## USB 3.0 Port

You use the USB port to connect peripherals to the module. The USB port supports the use of a USB hub. FAT32 and exFAT file systems are supported.



**WARNING:** If you connect or disconnect the USB cable with power applied to this module or any device on the USB network, an electric arc can occur. This can cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.



We recommend that you connect any peripherals to the USB port before you power up the module.

**IMPORTANT**

When fully inserted, the USB connectors lock into the USB port. Before you remove a USB connector, press the silver release tab on the left side of the USB port.

## Ethernet Ports

There are two Ethernet ports on the module.

### Embedded Edge Compute Module Default Ethernet Port Configuration<sup>(1)</sup>

| Port Position on Module | Module Properties Port Default Name | System Manager Port Default Name | Default IP Address |
|-------------------------|-------------------------------------|----------------------------------|--------------------|
| Top Port                | Port 2 (LAN) <sup>(2)</sup>         | Eth2                             | 192.168.0.1        |
| Bottom Port             | Port 1 (WAN)                        | Eth1                             | Assigned by DHCP   |

(1) Device Level Ring topologies are not supported.

(2) FactoryTalk Optix RA EtherNet/IP driver only supports Port 2.



**WARNING:** If you connect or disconnect an Ethernet cable with power applied to this module or any device on the network, an electric arc can occur. This can cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

### Port 2

The FactoryTalk® Optix™ RA EtherNet/IP driver only supports Port 2. Only Port 2 can be used for EtherNet/IP communication. This Ethernet port can communicate on an EtherNet/IP network at a maximum network communication speed of 1 Gbps.

You can configure this port either with the Module Properties dialog in the Studio 5000 Logix Designer application, or with System Manager.

- To configure with the Module Properties Dialog, see [Internet Protocol on page 21](#).
- To configure with System Manager, see [Interfaces on page 34](#).

### Port 1

Port 1 can support enterprise-wide Ethernet communication. This Ethernet port can communicate on an Ethernet network at a maximum network communication speed of 1 Gbps.

You can only configure this port with System Manager. See [Interfaces on page 34](#).

### Considerations

- You can use any IP address and mask values in your application.
- You can configure the IP address and mask to be static or dynamic.
  - If an IP address and mask are static, they remain assigned to the port after power is cycled to the module.
  - If an IP address and mask are dynamic, they are cleared from the port each time power is cycled to the module. A DHCP server must reassign values. Remember, the IP address and mask values that are assigned after a power cycle can differ from the ones that were used before a power cycle.

We recommend that you set the IP addresses to be static.

### Other Communication Drivers

All other communication drivers in FactoryTalk Optix can run on both Port 1 and Port 2:

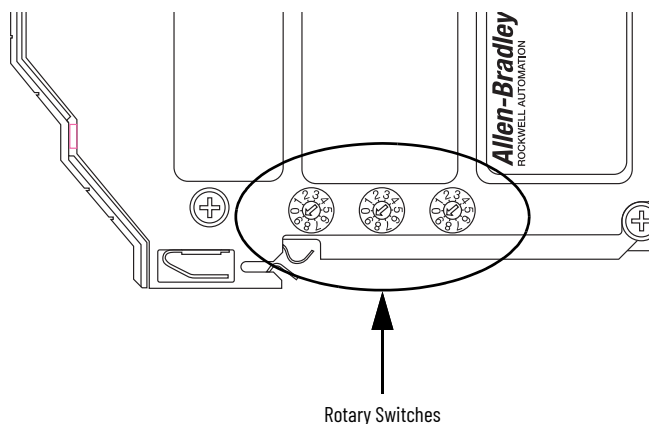
- Modbus
- MELSEC FX3U
- MELSEC Q
- S7TCP
- S7 TIA PROFINET
- OMRON EtherNet/IP
- OMRON FINS
- CODESYS
- TwinCAT
- SerialPort

For more information, see Communication Drivers Overview in the FactoryTalk Optix Studio Help.

## Rotary Switches

There are rotary switches on the side of the module. Out-of-the-box, the switches are set to 000 and are planned for future use.

### Embedded Edge Compute Module Rotary Switches



## Reset Button

Embedded Edge Compute modules have a reset button behind the door that powers off and reboots the device.



**WARNING:** When you press the reset button while power is on, an electric arc can occur. This can cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

An example of when you would use the reset button include:

- To restart the embedded OS after a module crash.

Use a tool with a small head, for example, a small screwdriver, to press the reset button when the module is powered.

## Factory Restore Button

Embedded Edge Compute modules have a factory restore button behind the door. The factory restore button:

- Resets all settings.
- Restores the operating system and module firmware
- Removes the FactoryTalk Remote Access identity.



**WARNING:** When you press the factory restore button while power is on, an electric arc can occur. This can cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Use a tool with a small head, for example, a small screwdriver, to press the factory restore button when the module is powered on.

### IMPORTANT

Before proceeding, make sure to back up any important data stored on the device. This procedure erases all user settings, configurations, and data like the FactoryTalk Optix application and the related FactoryTalk Optix runtime.

### IMPORTANT

The Factory Restore procedure takes about 20 minutes due to low-level format of the user memory, including both the eMMC and the microSD card. This procedure makes sure that the device is restored to factory default settings, and all sensitive data is permanently and securely erased from the device.

To restore your device to its factory defaults, follow these steps:

1. Power Off the device.
2. Power On the device while pressing and holding the Factory Restore button.  
The OK status indicator flashes red and the countdown: "4 3 2 1 FACTORY RESET IN PROGRESS" scrolls across the 4-character display.
3. Release the Factory Restore button.

Depending on the result of the Factory Reset:

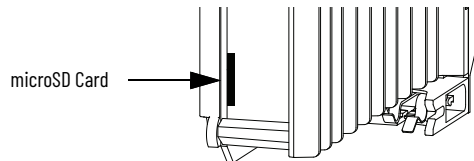
- Factory Reset failure: the OK status indicator is steady red and the error message "FACTORY RESET FAILED" scrolls across the 4-character display.
- Factory Reset OK: the OK status indicator is steady green, "FACTORY RESET OK" scrolls across the 4-character display, and then the module reboots.

## Replace the microSD Card

If the microSD card fails, you can order a replacement 1784-MSDHC32 microSD card.

To replace the microSD card:

1. Remove power from the module.
2. Remove the module from the chassis.
3. On the rear of the module, remove the failed microSD card.



4. Insert the new microSD card.
5. Inset the module in the chassis.
6. Apply power to the module.

## FactoryTalk Optix Applications

FactoryTalk Optix Studio is available as a web and a desktop development environment that you use to build FactoryTalk Optix Applications and deploy them to client systems. You can access the FactoryTalk Optix Studio web version through FactoryTalk® Hub™.

FactoryTalk Optix Studio provides a communication path to REST API, OPC UA, and MQTT to meet the needs of various applications.

Example FactoryTalk Optix applications for the Embedded Edge Compute module include:

- HTML5 web-based HMI/dashboarding applications that run on the Embedded Edge Compute module and are visualized on web panels or web clients.
- OPC UA client/server applications.
- MQTT publisher/subscriber applications with any broker, supporting TLS and any JSON encoding. This enables you to develop cloud gateway applications.
- Data collection and visualization applications.
- All features that are provided by FactoryTalk Optix can be extended and customized through the FactoryTalk Optix C# API to address scenarios like recipe managers, alarm handling, etc.

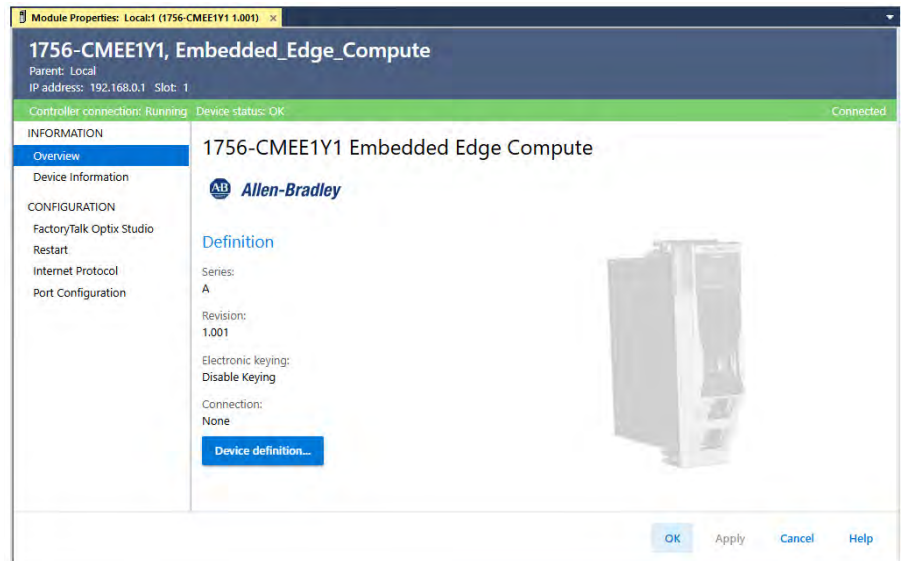
For information on how to use FactoryTalk Optix Studio to develop and deploy applications, see the FactoryTalk Optix Studio Help. The help has a number of application examples and tutorials.



## Overview

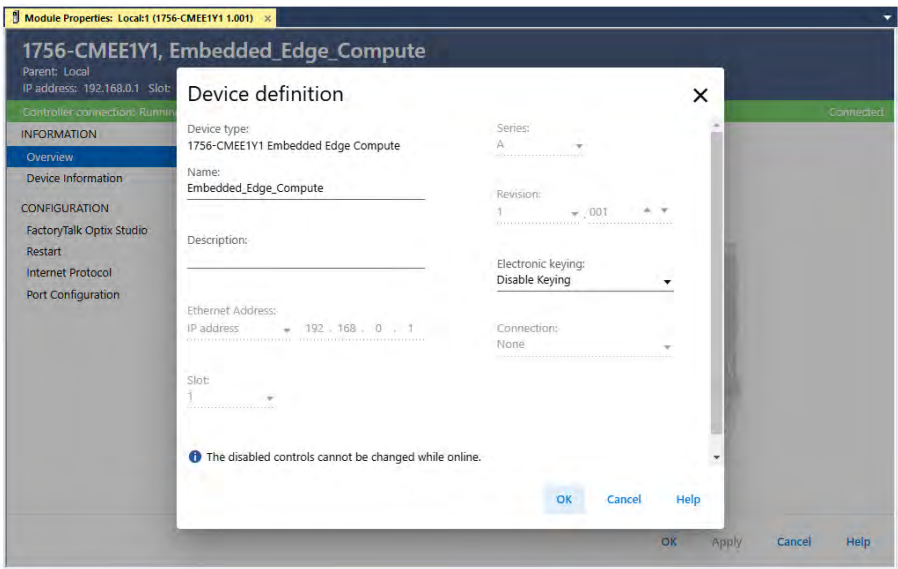
# Configure the Module with Studio 5000 Logix Designer

This chapter describes how to configure the Embedded Edge Compute module with Studio 5000 Logix Designer®. You can also use [System Manager](#) to configure the module and update the module firmware.



## Device Definition

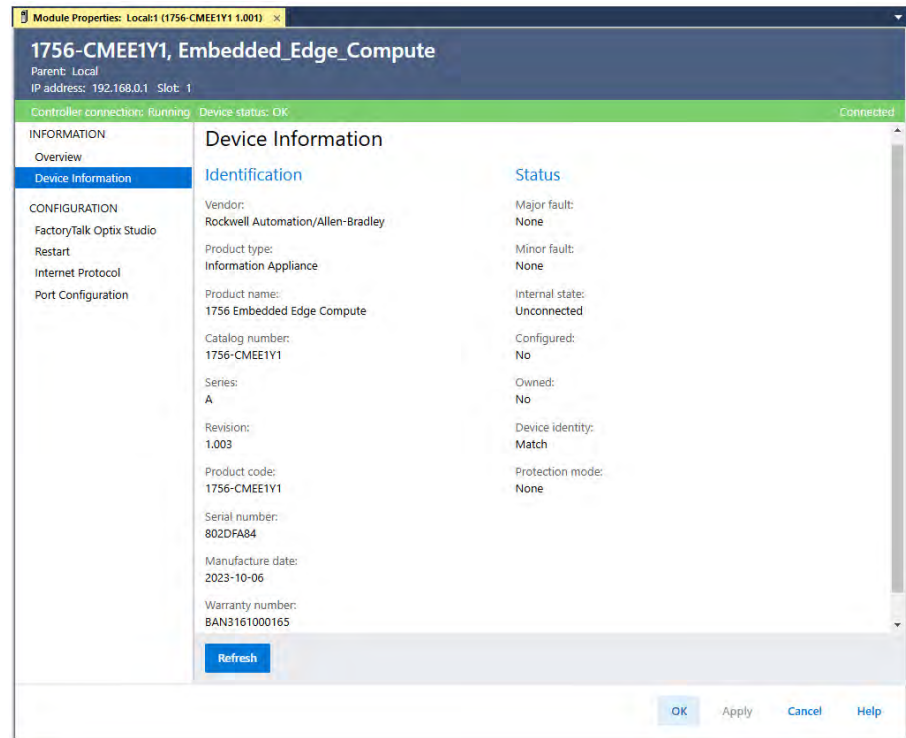
When you first create the module, the software automatically launches the Device Definition window since the Name and IP Address of the module is the minimal configuration that is needed to create the module. To change the Device Definition later, you will need to launch Device Definition from the Overview page.



| Parameter         | Description   |
|-------------------|---|
| Device type       | Displays the device catalog number and type.  |
| Name              | Displays a user-defined name for the module.  |
| Description       | Displays the user-defined device description.   |
| Ethernet address  | Displays the IP address that is assigned to the module.   |
| Slot              | Displays the slot in the chassis that the module resides in.  |
| Series            | Displays the module series.   |
| Revision          | Displays the module major and minor revisions.  |
| Electronic keying | Displays the electronic keying that is used for the module. Electronic keying compares the module that is defined in the project to the installed module. If keying fails, a fault occurs.<br>Valid values include: <ul style="list-style-type: none"><li>Exact Match</li><li>Compatible Module</li><li>Disable Keying</li></ul> For detailed information on Electronic keying, see Electronic Keying in Logix 5000® Control Systems Application Technique, publication <a href="#">LOGIX-AT001</a> . |
| Connection        | None  |

## Device Information

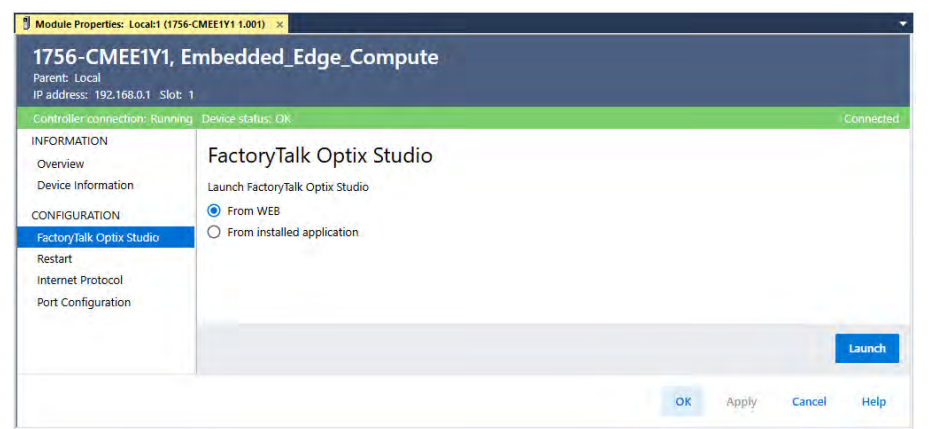
Use the Device Information view to view device and status information when the device is online.



| Parameter                  | Description   |
|----------------------------|---|
| Identification             | Displays information that identifies the module.  |
| Status - Major/Minor fault | Displays whether there is a major and minor fault.  |
| Status - Internal State    | Displays the module's current operational state. <ul style="list-style-type: none"> <li>Self-test</li> <li>Flash update</li> <li>Communication fault</li> <li>Unconnected</li> <li>Flash configuration bad</li> <li>Major fault</li> <li>Run mode</li> <li>Program mode</li> <li>(16#xxxx) unknown</li> </ul>   |
| Status - Configured        | Displays Yes or No indicating whether the module was configured by the owner controller connected to it. Once a module is configured, it stays configured until the module is reset or power is cycled, even if the owner drops connection to the device.   |
| Status - Owned             | Displays Yes or No indicating whether an owner controller is connected to the device.   |
| Status - Device identity   | Displays whether the physical device matches or mismatches with the configuration in the Overview view. <ul style="list-style-type: none"> <li>Match - The physical device agrees with what is specified in the Overview view, and all of these must agree: <ul style="list-style-type: none"> <li>Vendor</li> <li>Device type (the combination of Product type and Product code for a particular Vendor)</li> <li>Major revision</li> </ul> </li> <li>Mismatch - If the physical device does not agree with what is specified in the Overview view.</li> </ul> |
| Status - Protection mode   | Displays the device protection when online. The protection mode depends on the device and may include: <ul style="list-style-type: none"> <li>Explicit</li> <li>Implicit</li> <li>None</li> </ul> Tip: When the device is offline or if a communication failure to the device occurs, the field is blank.   |
| Refresh                    | Retrieves and displays the latest values from the device.   |

# FactoryTalk Optix Studio

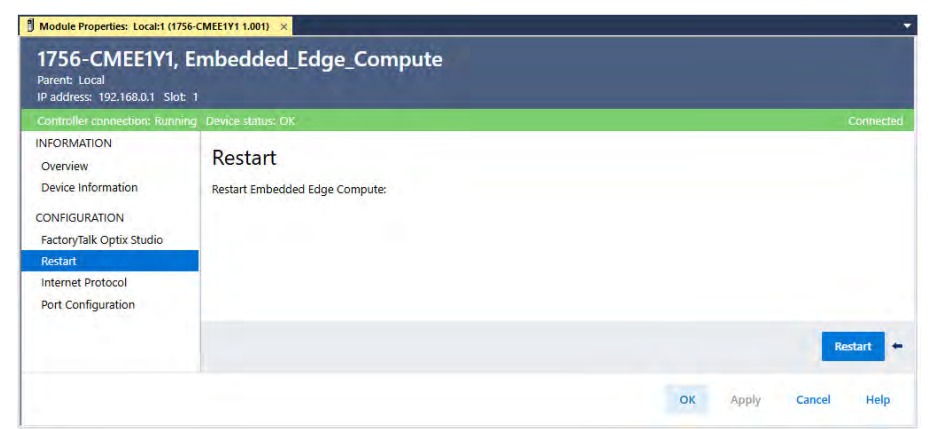
You can use the FactoryTalk® Optix Studio™ software to configure and program the application for the Edge Compute module. FactoryTalk Optix Studio can be installed as a desktop application or run in the cloud within a web browser.



| Parameter                  | Description   |
|----------------------------|---|
| From WEB                   | Opens FactoryTalk Optix Studio software from the cloud in a web browser.  |
| From installed application | Opens FactoryTalk Optix Studio software from the application that is installed on your computer. You can only launch the desktop application when the software is installed on the local machine. |

## Restart

Select Restart to restart the device. A prompt appears asking if you want to restart the device. If the project is offline, no online data is shown.



| Button  | Description  |
|---------|--|
| Restart | Restarts the operating system on the module. This powers off and reboots the module. |

## Internet Protocol

Use Internet Protocol to configure the IP settings of Port 2. The configured values display only when the module is online. Use Internet Protocol to:

- Specify whether to manually configure IP settings or obtain the IP settings automatically using DHCP.
- Configure the Physical device IP address, Subnet mask, Gateway address, Primary DNS server address, Secondary DNS server address, Domain name, and Host name.

Module Properties: Local1 (1756-CMEE1Y1 1.001) x

**1756-CMEE1Y1, Embedded\_Edge\_Compute**  
 Parent: Local  
 IP address: 192.168.0.1 Slot: 1

Controller connection: Running Device status: OK Connected

**Internet Protocol**

**Internet Protocol (IP) Settings**  
 IP settings can be manually configured or can be automatically configured if the network supports this capability

☒ Manually configure IP settings  
☐ Obtain IP settings automatically using DHCP

**IP Settings Configuration**

Physical device IP address:  
 192 . 168 . 0 . 1

Subnet mask:  
 255 . 255 . 255 . 0

Gateway address:  
 0 . 0 . 0 . 0

Domain name:

Primary DNS server address:  
 0 . 0 . 0 . 0

Secondary DNS server address:  
 0 . 0 . 0 . 0

Host name:  
 1756-CMEE1

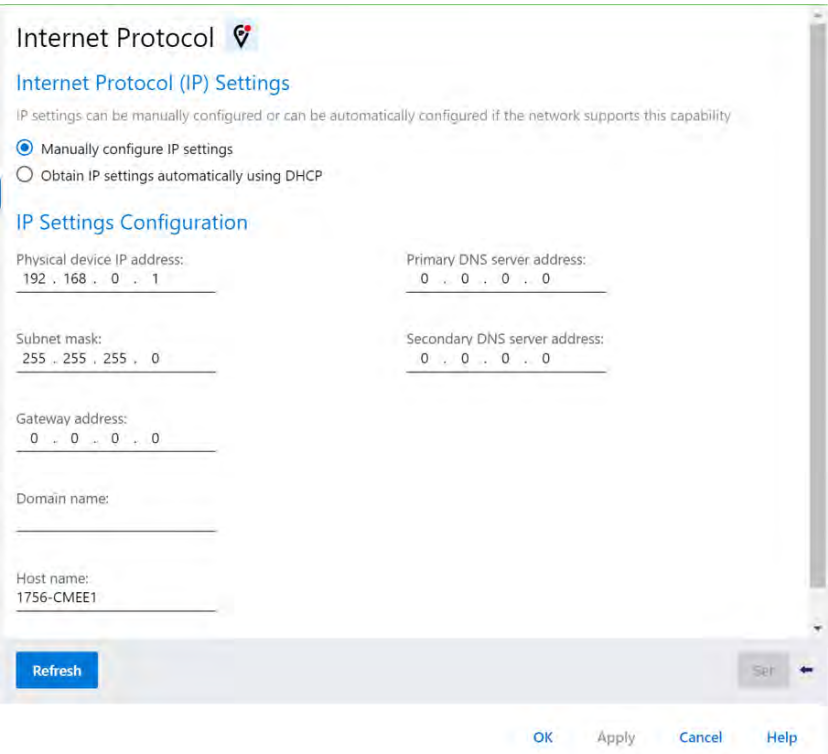
Refresh

OK Apply Cancel Help

| Parameter                    | Description   |
|------------------------------|---|
| Internet Protocol Settings   | The device's IP settings configuration mode.  |
| Physical device IP Address   | Address used by the IP protocol to route information to and from the device.                                  |
| Subnet mask                  | An extension of the IP address scheme that lets a site use one net ID for multiple physical networks.         |
| Gateway address              | Address used to connect individual physical networks into a system of networks                                |
| Primary DNS server address   | IP address for the primary DNS server that holds the master copy of the data.                                 |
| Secondary DNS server address | IP address for the secondary DNS server that holds a copy of the data in case the primary DNS is unavailable. |
| Domain name                  | A name that is associated with a physical IP address on the Internet.   |
| Host name                    | Unique identification string for the device.  |
| Refresh                      | Retrieves and displays the latest device information.   |
| Set                          | Writes pending edits to the device.   |

## IP Mismatch

The Internet Protocol view displays this icon  next to the Internet Protocol title if there is an IP address mismatch.



Select the icon to open the IP Mismatch Dialog:



## Port Configuration

Use the Port Configuration view to configure the port settings for non-controller devices.

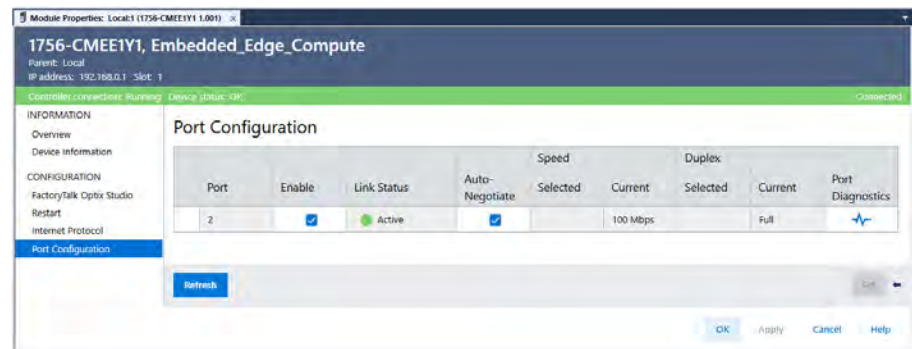
- You must be online and communicating with the device.
- Ensure that a connection interruption at this time is acceptable.

### IMPORTANT

Configuring the port settings requires data to be written to the device, which interrupts the connection to the device and to any other device that is connected through it. Connections from other controllers can be interrupted as well. You must not interrupt the connection on a device that is currently being used for control.

To configure the port settings:


1. In the Port Configuration view, configure the settings as needed.
2. Select Set to write the changes to the device.



| Parameter         | Description  |
|-------------------|--|
| Enable            | Enable or Disable Port 2.  |
| Link Status       | Displays the status of the port communication on the network.  |
| Auto-Negotiate    | Indicates that the device automatically selects the best method for communication. If cleared, the port speed and duplex must be set manually.   |
| Speed - Selected  | Specifies the configured port speed for sending and receiving data. Available options are device-dependent.<br>Tip: Selected Speed is unavailable if Auto-Negotiate is selected.   |
| Speed - Current   | Displays the actual speed at which the port is sending and receiving data.   |
| Duplex - Selected | Specifies the configured port duplex setting: <ul style="list-style-type: none"> <li>• Half - Indicates sending and receiving data in one direction at a time.</li> <li>• Full - Indicates sending and receiving data in both directions simultaneously.</li> </ul> Tip: Selected Duplex is unavailable if Auto-Negotiate is selected. |
| Duplex - Current  | Displays the actual duplex method that the port is using to send and receive data.   |
| Port Diagnostics  | Opens Port Diagnostics to view the interface and media counters for the port.  |
| Set               | Writes pending edits to the device.  |
| Reset             | Initiates a reset operation on the device, which returns the device to its power-up state by emulating the cycling of power and causes the changes that are made to become the port's current settings.  |

## Port Diagnostics

Use Port Diagnostics to view diagnostic information for a port.

1. To view diagnostics information for a port
2. On the tab for the device, select Port Configuration.
3. In the Port Diagnostics column for the port, select .

In Port Diagnostics, view the diagnostics information as needed.



| Parameter          | Description  |
|--------------------|--|
| Interface Counters | <p>Values only appear when the device is online.</p> <ul style="list-style-type: none"> <li>• Octets Inbound: Number of octets received on the interface.</li> <li>• Octets Outbound: Number of octets transmitted on the interface.</li> <li>• Unicast Packets Inbound: Number of unicast packets received on the interface.</li> <li>• Unicast Packets Outbound: Number of unicast packets transmitted on the interface.</li> <li>• Non-unicast Packets Inbound: Number of non-unicast packets received on the interface.</li> <li>• Non-unicast Packets Outbound: Number of non-unicast packets transmitted on the interface.</li> <li>• Packets Discarded Inbound: Number of inbound packets that are received on the interface but discarded.</li> <li>• Packets Discarded Outbound: Number of outbound packets that are transmitted on the interface but discarded.</li> <li>• Packets With Errors Inbound: Number of inbound packets that contain errors (excludes discarded inbound packets).</li> <li>• Packets With Errors Outbound: Number of outbound packets that contain errors (excludes discarded outbound packets).</li> <li>• Unknown Protocol Packets Inbound: Number of inbound packets with unknown protocol.</li> </ul>  |
| Media Counters     | <p>Values only appear when the device is online.</p> <ul style="list-style-type: none"> <li>• Alignment Errors: Number of frames received that are not an integral number of octets in length.</li> <li>• FCS Errors: Number of frames received that do not pass the FCS check.</li> <li>• Single Collisions: Number of successfully transmitted frames that experienced exactly one collision.</li> <li>• Multiple Collisions: Number of successfully transmitted frames that experienced multiple collisions.</li> <li>• SQE Test Errors: Number of times an SQE test error message was generated.</li> <li>• Deferred Transmissions: Number of frames for which the first transmission attempt is delayed because the medium is busy.</li> <li>• Late Collisions: Number of times a collision is detected later than 512 bit-times into the transmission of a packet.</li> <li>• Excessive Collisions: Number of frames for which transmission fails due to excessive collisions.</li> <li>• MAC Transmit Errors: Number of frames for which transmission fails due to an internal MAC sub layer transmit error.</li> <li>• MAC Receive Errors: Number of frames for which reception on an interface fails due to an internal MAC sub layer receive error.</li> <li>• Carrier Sense: Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.</li> <li>• Frame Too Long: Number of frames received that exceed the maximum permitted frame size.</li> </ul> |
| Reset Counters     | <p>Sets the interface and media counter values on the device to zero and updates the values that are displayed in the dialog box with the current counter values. Reset Counters is only enabled when the device is online.</p>  |



# System Manager

You can use System Manager to configure the module and update the module firmware.

## Factory Settings

There are two Ethernet ports on the module.

Embedded Edge Compute Module Default Ethernet Port Configuration

| Port Position on Module | Module Properties Port Default Name | System Manager Port Default Name | Default IP Address |
|-------------------------|-------------------------------------|----------------------------------|--------------------|
| Top Port                | Port 2 (LAN) <sup>(1)</sup>         | Eth2                             | 192.168.0.1        |
| Bottom Port             | Port 1 (WAN)                        | Eth1                             | Assigned by DHCP   |

(1) The FactoryTalk® Optix™ RA EtherNet/IP™ driver only supports Port 2.

Access to device configuration is protected by a username and password:

- The default **username** is **admin**.
- The default **password** is **admin**.

## Access System Manager from a Browser

You can remotely access System Manager through the Ethernet connection, by typing the device IP address into a web browsing bar.

1. Enter the device IP address into a web browsing bar. Each device comes pre-configured with a default IP address, which can vary depending on the specific Ethernet interface to which the device is connected.

**Note:** You are warned that the connection is not private and the security certificate is not trusted. In this case, select Advanced and proceed.

2. If you access System Manager for the first time, enter the default credentials:
  - username: admin
  - password: admin
3. Once you sign in, you are prompted to change your password.

From the second sign in on, you can access System Manager by using admin as a username and the newly configured password, or through the user's account if activated by an Admin user.

**Note:** Create a strong password to reduce cybersecurity risk.

Your password must be:

- Be at least eight characters long
- Include at least three of the following requirements:
  - at least one uppercase character
  - at least one lowercase character
  - at least one numeric character
  - at least one symbolic character

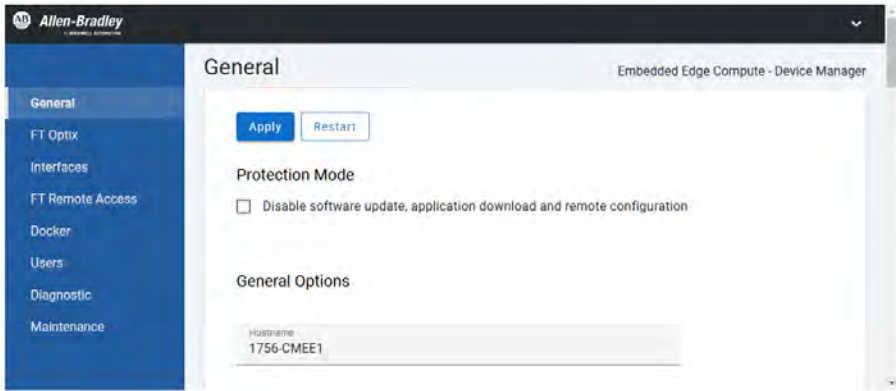
Use passphrases longer than eight characters to enhance password strength. Strong passwords increase the time needed to guess them.

|                  |  |
|------------------|--|
| <b>IMPORTANT</b> | Make sure to save your password. You must sign in as an Admin to transfer a FactoryTalk® Optix™ application through FactoryTalk® Optix Studio™. If you lose your password, you must restore the device to factory default settings. This operation causes the deletion of any FactoryTalk Optix Applications and system updates. |
|------------------|--|

# System Manager Menu

The System Manager menu is divided into the following sections:

- General
- FactoryTalk Optix
- Interfaces
- FactoryTalk® Remote Access™
- Docker
- Users
- Diagnostic
- Maintenance



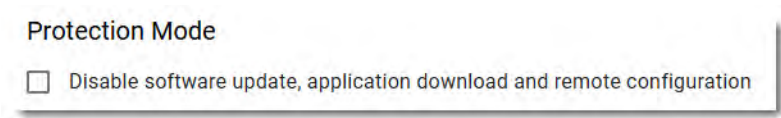
The Apply and Restart buttons appear at the top and bottom of each section.

| Button  | Description  |
|---------|--|
| Apply   | When you apply any changes within each section, click Apply. A message appears, confirming that any change has been saved. |
| Restart | Depending on the changes applied, you might have to restart your device.   |

## General

### Protection Mode

Protection Mode is disabled by default for all out-of-the-box products and after a factory reset. Enable this setting in a production environment to help prevent any unauthorized access and potential cybersecurity risks.



#### Disable software update, application download and remote configuration

Enable this mode to enhance your device security. Once enabled, your device rejects the following operation:

- Interface updates: TCP/IP configuration (configuration method, network address, hostname), Ethernet Link configuration (link enablement, speed, and duplex) and remote configuration requests via CIP™.
- Firmware updates via USB or remotely through FactoryTalk Remote Access Manager.
- FactoryTalk Optix application updates.

The device accepts settings and restart requests through the System Manager web interface, FactoryTalk Optix System Tags, and FactoryTalk Remote Access Manager tools, which require user authentication. This allows any changes to only be implemented by authorized Admin users.

## General options

Configure the Hostame and Web server interfaces for the module.

### General Options

Hostname  
1756-CMEE1

#### Web server interfaces

- ☒ WAN
- ☒ LAN

### Hostname

The Hostname is a unique identifier that is assigned to the device. It is used to identify and communicate with the device over the network and can be used to configure or troubleshoot the device. This name is the device name that is visualized on the FactoryTalk Remote Access organization.

### Web server interfaces

- WAN: Enable this option to allow access to the System Manager through the device's WAN port (Port 1). This makes it easy for you to remotely manage and configure the device via the web interface.
- LAN: Enable this option to use the System Manager through the device's LAN port (Port 2). This allows you to access the web interface for device management and configuration via the local network.



It is recommended to configure these options to let the web server be only accessible from the strictly needed interfaces, to reduce surface exposure to cyberattacks. Ideally, it should be only enabled when the configuration must be changed.

## Date and Time

Configure the date and time settings.

Date and Time

Time synchronization mode

Auto (PLC)

PLC route

Backplane\0

Date

Year

Month

Day

21

9

12

Time

Hour

Minute

21

9

Time zone

(UTC-05:00) Eastern Time (US & Canada)

Local NTP server interfaces

☐ WAN

☐ LAN

### Time synchronization mode

|                          |  |
|--------------------------|--|
| Auto (PLC)               | Synchronizes the date and time automatically with a controller.<br>The PLC route is visible only when the Time synchronization mode is Auto (PLC), allowing to set the slot number of the ControlLogix® Controller with this syntax: Backplane\slot number.  |
| Auto (Remote NTP server) | Synchronizes the date and time automatically with a remote Network Time Protocol (NTP) server.<br>The remote NTP server is visible only when the Time synchronization mode is Auto (Remote NTP server), allowing to set the IP address of the NTP server.<br>The device can be configured to automatically adjust the date and time from a remote NTP server and provide the same service to connected devices (local NTP server). |

### Date and Time

Displays the synchronized date and time.

### Time zone

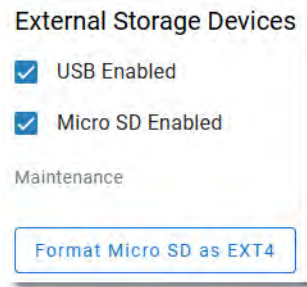
Sets the time zone.

### Local NTP server interfaces

The Local NTP server interfaces checkboxes activate the local NTP server on the specified interface (WAN and/or LAN), maintaining accurate timekeeping across your network. Selecting at least one interface enables the local NTP server to listen for connections on the standard UDP port 123. Selecting no interface disables the local NTP Server.

## External Storage Devices

The device allows the use of USB Memory or microSD™ cards as storage devices.



### USB Enabled

Activate or deactivate any storage devices that are mounted on the device USB ports. This selection does not impact the recognition or usage of any USB devices, such as keyboards, mice, or other HID devices.

### Micro SD Enabled

Activate any micro SD card storage devices.

### Format Micro SD as EXT4

This is the preferred file system if the micro SD card in use is used to extend the content of an eMMC memory, for example as storage for a FactoryTalk Optix application embedded database file.

While USB Memory is used as temporary storage (file transfers, logs, system updates), microSD cards can be used as permanent storage. For these reasons, different file systems are supported:

| Storage type | File system supported        | Usage                                  |
|--------------|------------------------------|--|
| USB Memory   | FAT32                        | Suggested if used as temporary storage |
| microSD Card | FAT32                        |  |
|              | EXT4 (supported on Linux OS) | Suggested if used as permanent storage |

The EXT4 file system is inherently compatible with the Linux operating system. Therefore, if you want to access data from a microSD Card that uses the EXT4 file system on a Microsoft Windows® operating system, you would need to use a third-party application, such as Ext2Explore.

### Access External Storage Devices

To access external storage devices through a FactoryTalk Optix Application, use the system path that is shown in this table:

| Storage type | Folder  |
|--------------|---|
| USB Memory   | /storage/usb1   |
|              | /storage/usb2   |
|              | /storage/usb3   |
|              | Access storages by entering the related progressive numbers after /storage/usb... |
| microSD Card | /storage/sd1  |

## System Information

This section shows essential details about your device, such as the Product Name, the firmware revision, the OS version, the System Manager version, and the FactoryTalk Remote Access Runtime version. Both the OS version and System manager version are dependent on the Firmware version.

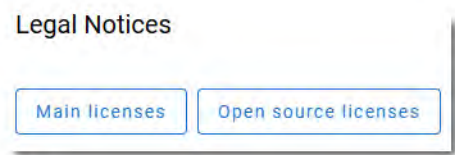


### Update firmware

Select Update Firmware to upload a firmware image (.img file) onto the device directly from the browser. See [Update Through System Manager on page 53](#).

## Legal Notices

Each button in this section shows a specific set of licenses that are used in System Manager.



| Button               | Description                    |
|----------------------|--------------------------------|
| Main licenses        | Commercial software licenses.  |
| Open source licenses | Open-source software licenses. |

## FactoryTalk Optix

FactoryTalk Optix provides a development environment for creating HMI projects that can then be deployed to a device. This section allows you to configure any settings that are related to the FactoryTalk Optix Runtime, and any entitlements that are associated with it.

### Configuration

#### Configuration

- ☒ Run FT Optix Application Update Service at system startup
- ☐ Load only password protected applications

#### Run FactoryTalk Optix Update Service at system startup

When this setting is enabled, the FactoryTalk Optix update server activates at device startup, allowing the download and update of FactoryTalk Optix applications using FactoryTalk Optix Studio. If not enabled, downloading, and updating FactoryTalk Optix applications on the device is not possible.

#### Load only password protected applications

In FactoryTalk Optix Studio, you can configure a password policy for users of the application at runtime. When Load only password protected applications is enabled, FactoryTalk Optix only loads applications that are password protected.

### Application

You can load and delete applications.

#### Application

Application name  
DefaultOptixApplication

FT Optix Runtime version  
1.2.0.257

Load application

Load

Delete current application

Delete

#### Application name


This section displays the name of the project that has been loaded onto the device.

#### FactoryTalk Optix Runtime version

This section displays the version of the FactoryTalk Optix Studio Runtime that was used to develop the loaded project. The FactoryTalk Optix Studio Runtime provides a development environment for creating and testing HMI projects before deploying them to the device. The version number is important to ensure compatibility between the project and the runtime environment and can be useful for troubleshooting issues that are related to project development and deployment.

## Load application

Select Load to transfer a FactoryTalk Optix application from a USB memory stick to a device.

1. In FactoryTalk Optix Studio, select  (Save), Export > FactoryTalk Optix Application, then select your target device.
2. Define a password for the application package.
3. Transfer the application package to a USB memory stick.  
See [External Storage Devices on page 29](#) for further information on the supported file system formats.
4. Plug the USB memory stick into the USB port of the target device.
5. In System Manager, access FTOptix > Application, then click Load.
6. In the dialog window, enter the previously defined password.

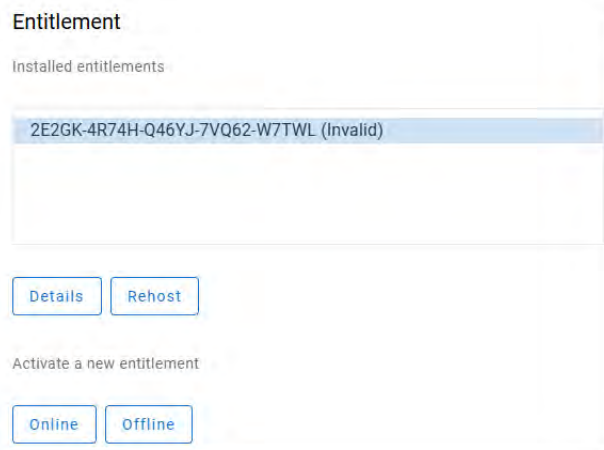
## Delete current application

Select Delete to delete the FactoryTalk Optix application that is installed on the module. Once you click Delete, you can select Delete all application files. This is useful if you are updating a FactoryTalk Optix application and you want to clear all historical data of the project, such as data sourced in datalogger databases, persistent databases, and so on.

## Entitlement

You can purchase upgraded Runtime entitlement packages on the Rockwell Automation [Commerce Portal](#). To do so, refer to the Runtime entitlements upgrade procedure that is related to your device, under the FactoryTalk Optix Runtime entitlements and upgrade section in the FactoryTalk Optix Installation Guide.

Once purchased, your license becomes available on the FactoryTalk® Hub™ and you can allocate it to your Organization. Then, the license entitlement appears on the FactoryTalk Optix landing page, under Organization Entitlements. See the FactoryTalk Optix Installation Guide for further information on this subject.



### Installed entitlements

Shows any Runtime entitlement keys currently in use. Your device comes with a pre-activated Runtime entitlement worth a specific size in tokens.

- Select an entitlement key row and click Details to view the Runtime entitlement details in a dialog window.
- Select Rehost to make the entitlement available to the FactoryTalk Optix dashboard (under Organization Entitlements) on FactoryTalk Hub, so that it can be allocated to another device.



Any factory-set entitlement cannot be rehosted.



## Activate a New entitlement

You can activate a Runtime entitlement either through an online procedure for devices that are connected to the Internet, or an offline procedure for devices without Internet access.

### Activate Online

1. If your device is online, select Online. A dialog window appears, and prompts you to enter the entitlement key.
2. Select Activate. Your device validates the key and activates the entitlement on the device through the FactoryTalk Optix servers. A dialog box confirms whether the activation process was successful.

### Activate Offline

1. If your device is offline, select Offline.
2. A dialog window appears. Select Export an entitlement Activation Request for this device to a file.
3. A dialog window appears, prompting you to enter the entitlement key. Enter the entitlement key and select Create: a .req file is generated.
4. On a device with internet access, open Entitlement Manager and select Online.  
Entitlement Manager belongs to the FactoryTalk Optix Runtime Tools. You must install Runtime Tools on the device to access the Entitlement Manager. See the Runtime Tools-related sections in the FactoryTalk Optix Installation Guide.
5. Select Activate an entitlement for a different device and Next.
6. Browse for and select the Activation Request (.req) file that you retrieved from the device.
7. Select Activate.
8. Select OK.
9. An Explorer window opens to save the newly activated entitlement file.
10. Accept the file name and select Save.
11. Select OK.
12. On the offline device, open System Manager, access FT Optix > Entitlement and select Offline.
13. Select Install an already activated entitlement file into this device and Next.
14. Browse for the activated entitlement file that you copied and select Open.
15. Select OK. System Manager now displays the installed entitlement. A dialog box confirms whether the activation process was successful.

# Interfaces

You can configure device interfaces and their related settings.

**IMPORTANT**

The FactoryTalk Optix RA EtherNet/IP™ driver only runs on Port 2 (Eth2). Only Port 2 can be used for EtherNet/IP communication. This Ethernet port can communicate on an EtherNet/IP network at a maximum network communication speed of 1 Gbps.

## CMEE Display

Select Hide IP addresses on front display to hide any IP addresses on the device display.

CMEE Display

☐ Hide IP addresses on front display

## Eth1: WAN

Eth1: WAN

☒ Enabled

MAC address

5C-88-16-FC-19-1E

☐ Obtain IP configuration automatically

IP address

192.168.0.17

Mask

255.255.255.0

Gateway

DNS 1

DNS 2

| Item                                  | Description   |
|---------------------------------------|---|
| Enabled                               | Enabled is selected by default and enables the WAN interface.   |
| MAC address                           | Displays the unique identifier for Port 1 of the module. This address is essential for network communication and device identification purposes.  |
| Obtain IP configuration automatically | This allows the automatic acquisition of any IP address, subnet mask, and default gateway from a DHCP server on the local network.<br>If the WAN port is set to automatically obtain its IP configuration, and the DHCP server supplies an updated configuration, you might have to toggle to another System Manager tab first to view the newly set configuration. |
| IP address <sup>(1)</sup>             | Enter the IP address of the device connected through the WAN interface.   |
| Mask <sup>(1)</sup>                   | Enter the mask of the device connected through the WAN interface.   |
| Gateway <sup>(1)</sup>                | Enter the gateway of the device connected through the WAN interface.  |
| DNS 1 <sup>(1)</sup>                  | Enter the primary DNS of the device connected through the WAN interface.  |
| DNS 2 <sup>(1)</sup>                  | Enter the secondary DNS of the device connected through the WAN interface.  |

(1) This setting is only available if the Obtain IP configuration automatically is not selected.

## Eth2: LAN

### Eth2: LAN

MAC address  
5C-88-16-FC-19-1F

☐ Obtain IP configuration automatically

IP addresses

192.168.0.1/255.255.255.0

Add

Remove

Gateway

DNS 1

DNS 2

FactoryTalk Remote Access Device Discovery

☐ Enable enhanced discovery on Eth2:LAN interface 

| Item                                       | Description  |
|--|--|
| MAC address                                | Displays the unique identifier for Port 2 of the module. This address is essential for network communication and device identification purposes.   |
| Obtain IP configuration automatically      | This allows the automatic acquisition of any IP address, subnet mask, and default gateway from a DHCP server on the local network.<br>If the LAN port is set to automatically obtain its IP configuration, and the DHCP server supplies an updated configuration, you might have to toggle to another System Manager tab first to view the newly set configuration.  |
| IP addresses <sup>(1)</sup>                | Enter one or more IP addresses of the devices that are connected through the LAN interface, and the related subnet mask. Select Add or Remove to add or remove any IP address configuration.   |
| Gateway <sup>(1)</sup>                     | Enter the gateway of the device connected through the LAN interface.   |
| DNS 1 <sup>(1)</sup>                       | Enter the primary DNS of the device connected through the LAN interface.   |
| DNS 2 <sup>(1)</sup>                       | Enter the secondary DNS of the device connected through the LAN interface.   |
| FactoryTalk Remote Access Device Discovery | Select Enable enhanced discovery on Eth2:LAN interface to allow your device to be discovered on the LAN by the Device Setup or Device Discovery Tool in FactoryTalk Remote Access Manager.<br><b>Note:</b> The device can not be discovered in certain network topologies that can consist of different subnets, and where a default gateway is missing. Indeed, the device where the Device Discovery or Device Setup Tool is running and the remote device are on different subnets. |
| Gateway Priority                           | In Mode, select the default gateway priority between Eth2: LAN and Eth1: WAN, if both the interfaces have a default gateway configured. <ul style="list-style-type: none"> <li>• Auto: Sets the gateways priority according to metrics automatically assigned by the OS.</li> <li>• WAN: Sets the gateway of the WAN port to use.</li> <li>• LAN: Sets the gateway of the LAN port to use.</li> </ul>  |

(1) This setting is only available if the Obtain IP configuration automatically is not selected.

## FT Remote Access

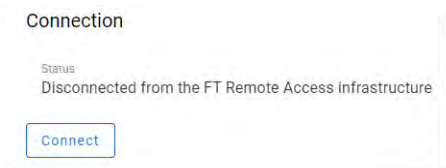
You can manage settings for connecting your device to a FactoryTalk Remote Access organization.

To learn how to register a device to a domain, refer to the *Device registration to domain* chapter in the FactoryTalk Remote Access Manager online manual.

You can unregister a device from its FactoryTalk Remote Access organization by removing the device from the FactoryTalk Remote Access Manager.

### Connection

The Connect/Disconnect button lets you manage the connection/disconnection of the device to/from the FactoryTalk Remote Access Network. By pressing Connect, if the device has never been registered to a FactoryTalk Remote Access domain, the ID and Password will appear to be used for the registration.



### Status

Displays the connection status to FactoryTalk Remote Access Manager. The available connection statuses are:

- Disconnected from the FactoryTalk Remote Access infrastructure
- Connecting
- Connected to the FactoryTalk Remote Access infrastructure
- Disconnecting
- Protocol error
- A newer version of firmware is required
- This firmware version is not supported by the server
- Device registration error

## Configuration

This section outlines the configuration parameters that are related to the device connection to FactoryTalk Remote Access Manager.

**Configuration**

Availability mode

☐ Always on

☒ Reconnect to server on restart if left connected

Connection port

Auto

Server

Public

Proxy configuration

None

### Always on

Help prevent the device from being disconnected from the FactoryTalk Remote Access network infrastructure or connected and disconnected to/from the FactoryTalk Remote Access network infrastructure through FactoryTalk Optix.

### Reconnect to server on restart if left connected

Automatically re-establish a connection to the server after restarting the device.

### Connection port

Select a port for connecting your device to the FactoryTalk Remote Access network infrastructure. The available options include Auto (automatic selection), 80, 443, or 5935.

### Server

Determine the FactoryTalk Remote Access network infrastructure to which you want to connect your device:

- **Public:** The device connects to the public network infrastructure hosted by Rockwell Automation (default value).
- **Private:** The device connects to an on-premise/private network infrastructure (currently inactive).
- **Private address:** Enter the private server address to which you want your device to connect.
- **Import CA:** Upload a Certificate Authority (CA) file. This file is necessary to authenticate the private server that you have previously defined in the Private address field.

### Proxy configuration

Configure the connection parameters for the FactoryTalk Remote Access organization if a proxy is required. The available options for proxy types are: None (no proxy), SOCKS5, and HTTP. Choose the option that best aligns with your network requirements and security policies.

## Local connection

The Local Connection allows you to establish a connection with the device, transfer files, manage processes, and establish a VPN connection through the FactoryTalk Remote Access Manager Local Connection Tool, without the need of any Internet connection.

See the FactoryTalk Remote Access Manager Tools and Local Connection sections in the FactoryTalk Remote Access Manager manual for further information on this topic.

A screenshot of a software window titled "Local Connection". It contains a checkbox labeled "Enabled" which is currently unchecked. Below the checkbox are two text input fields. The first field is labeled "Password" and the second field is labeled "Confirm password". Both input fields have a small circular icon with a key symbol on the right side, indicating password strength or visibility toggles.

### Enabled

Activate the Local Connection feature, allowing a connection to the device through FactoryTalk Remote Access Manager.

### Password

Define a local password to establish a device Local Connection.

## VPN

Select the Network interface for which you want to establish a VPN connection through FactoryTalk Remote Access Manager.

## WAN

Allows you to reach all WAN subnet devices through the VPN connection, unless prevented by any Firewall policies set through FactoryTalk Remote Access Manager.

## LAN

Allows you to reach all LAN subnet devices through the VPN connection, unless prevented by any Firewall policies set through FactoryTalk Remote Access Manager.

### Point-to-point virtual Ethernet adapter

Allows you to reach the device by establishing a VPN connection through the IP address of the virtual Ethernet adapter (10.173.249.x).

### Reserve static IP pool for VPN connections

Select Reserve static IP pool for VPN connections to enable the assignment of static IP addresses to the remote device where the FactoryTalk Remote Access Manager Tools are installed.

Add or Remove one or more IP pools that you want to use to dynamically assign an IP address to the remote device where the FactoryTalk Remote Access Manager Tools are installed.

### IMPORTANT

The IP addresses specified in the Static IP pool do not undergo any verification process. It is your responsibility to ensure that these addresses do not conflict with either WAN or LAN subnets.

## Docker

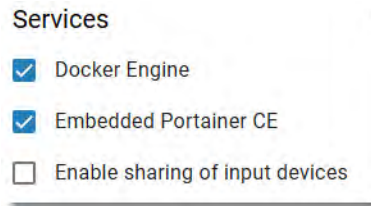
The Docker® section allows you to manage the Docker daemon configuration, shows your containers status and allows you to enable or disable the remote Docker management.

The Embedded Edge Compute module supports the Docker engine and Docker API, so you can use deployment tools that interact with the Docker API. For example, Docker CLI, Portainer, and Ansible.

As an optional feature, the device offers an integrated instance of Portainer CE (Community Edition). This allows for the management of Docker containers directly through the web interface that is provided by Portainer CE, and eliminates the need for any additional external tools.

For more information on Docker, go to <https://www.docker.com/>.

### Services



#### Docker Engine

Activates the Docker daemon rootless service.

#### Embedded Portainer CE

Installs the latest Portainer image. This image gets downloaded in the background, when you click Apply. Once the download is complete, you can access it via the HTTP port 9000 or the HTTPS port 9443.



You can only download Portainer CE on a device that is still configured with factory default settings.

Before proceeding with downloading Portainer CE, make sure that your device is connected to the Internet.

#### IMPORTANT

Do not expose port 9000 to the Internet. This port uses the HTTP protocol, which is susceptible to Man-in-the-Middle (MITM) attacks. Exposing this port can compromise the security of your system and data.

#### Enable sharing of input devices

Allow Docker containers to access input devices that are connected to your device.

For example, if you connect a barcode scanner to your device through a USB connection and you upload a Docker container with an app that is compatible with the barcode scanner you can operate this latter through the Docker container.



## Containers

### IMPORTANT

- The responsibility to deploy only secure images and harden the deployed images lies with the user.
- Expose containers to the Internet only if strictly necessary.
- Enabling container access to the backplane by mounting a specific library using Dockerfile allows any user within the container to access the backplane. Ensure that only trusted and secure containers are granted this access to help prevent unauthorized use.
- Do not enable any remote command-line interfaces, such as SSH, in containers. This is especially critical if users have poor password hygiene and the container is exposed to the Internet. Enabling remote command-line interfaces significantly increases the cyberattack surface, making it easier for threat actors to compromise the container. Moreover, if the container has access to the backplane, an threat actor could gain access to critical system components.

The Containers table shows information about the containers in the device.

Containers

| CONTAINER_ID             | NAME | STATE | IMAGE | CREATED_AT | RUNNING_FOR | PORTS | CPU% | MEM_USAGE/LIMIT | MEM% | NET_I/O | BLOCK_I/O |
|--------------------------|------|-------|-------|------------|-------------|-------|------|-----------------|------|---------|-----------|
| There are no containers. |      |       |       |            |             |       |      |                 |      |         |           |

Import docker image via USB

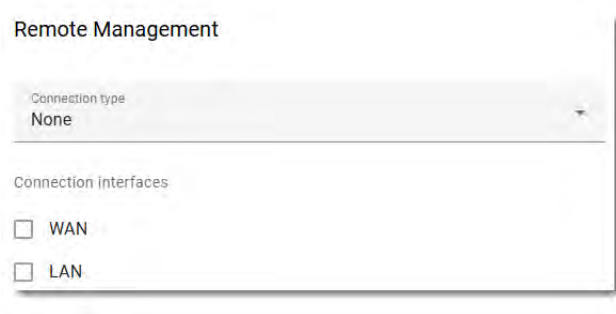
Select Import docker image via USB to import a Docker image from a USB memory stick, and run the container as defined in the .yaml file that is associated to the image.

### IMPORTANT

- The USB memory stick must include only a .yaml (Docker composer) and a .tar file (uncompressed Docker image).
- Do not compress the .tar file
- Only a System Manager Admin user can import these files.

## Remote Management

Select the connection type of the Remote Management Tools in use, such as Docker CLI, Portainer, Ansible.



### None

The Docker daemon does not accept any incoming connections.

### Unencrypted on port 2375

The Docker daemon accepts incoming unencrypted connections on port 2375 for remote management.

---

|                  |  |
|------------------|--|
| <b>IMPORTANT</b> | Do not use in a production environment. Access to the daemon on port 2375 is both unencrypted and unauthenticated. This vulnerability allows any user on the network, or even on the Internet, if exposed, to connect and run commands on the Docker engine. Such exposure can lead to severe security breaches and unauthorized control over your Docker containers.<br>System Manager also warns users not to use Unencrypted on port 2375 in production environments. |
|------------------|--|

---

### Encrypted on port 2376

The Docker daemon accepts incoming encrypted connections on port 2376 for remote management and requires a certificate installation. You can import any certificates with their related private keys by selecting Import. You can verify both certificates and private keys by selecting Verify.

### Connection interfaces

Select the interface (WAN or LAN) that is made accessible to the client connection type that you previously selected for Connection type

## Container Storage

### Container Storage

Data Root  
Internal

### Internal

The internal MMC to store any Docker data such as images, containers, volumes, and configuration files.

### Micro SD

The Micro SD to store any Docker data.

## Private Registries

Manage a list of secure or unsecure registries where any container image can be pulled from or pushed to. Secure private registries require a security certificate.

---

**IMPORTANT** Use insecure registries only in test environments or in strictly controlled or air-gapped environments.

---

Communication with these registries occurs via HTTP, which is unencrypted, exposing users to Man-in-the-Middle (MITM) attacks. This risk is high if the registry is on a different network.

The responsibility to select trusted public registries and protect their personal registries lies with the user.

To add a private registry:

1. Select Add.

### Private Registries

There are no private registries.

Add

2. Enter a URL for the private registry, and click Select certificate to upload a certificate.

### Add a private registry

URL

☒ Secure

Select certificate

No file chosen

Add

Cancel

3. Select Add.

## Proxy

Enter the address and port of the HTTP proxy server that the Docker daemon and related containers can use to access the Internet.

Proxy

HTTP proxy address

HTTP proxy port

## Users

This section allows you to set up and manage your device users' credentials, as well as any passwords and session security policies.

### Accounts

While an Admin account can manage all the device settings, a User account is least-privileged and can be activated only if an Admin user sets a password for them.

Accounts

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

Username

admin

New password

Confirm password

### Username

Select Admin or User and set up a password.

The password must meet the following requirements:

- Be at least 8 characters long.
- Include at least three of the following:
  - One uppercase character
  - One lowercase character
  - One numeric character
  - One symbolic character



An Admin user can reset a User's password as needed.

A User account can manage the following features:

| Section          | Subsection         | Feature  |
|------------------|--------------------|--|
| General          | Date and time      | Time synchronization mode<br>Auto (Remote NTP Server)<br>Auto (PLC)<br>Date<br>Time<br>Time zone                   |
|                  | System Information | Product name<br>Firmware version<br>OS version<br>System Manager version<br>FT Remote Access Runtime version       |
|                  | Legal Notices      | Main licenses<br>Open source licenses  |
| FT Optix         | Application        | Load application   |
|                  | Entitlement        | Listbox of installed entitlements<br>Details<br>Rehost<br>Activate a new entitlement<br>Online/Offline             |
| Interfaces       | WAN (Link1)        | Enabled<br>MAC address<br>Obtain IP configuration automatically<br>IP address<br>Mask<br>Gateway<br>DNS 1<br>DNS 2 |
|                  | Gateway priority   | Mode   |
| FT Remote Access | Configuration      | Connection port<br>Proxy configuration<br>SOCK5/HTTP   |
|                  | Local Connection   | Enabled<br>Password  |
| Users            | Accounts           | New password   |
| Diagnostic       | Ping               | Ping   |
|                  | Export Logs        | Export all<br>Apply<br>Restart   |

## Security Policies

You can set the time for the Automatic Session time out. This signs you out of System Manager.

### Security Policies

|                                  |    |
|----------------------------------|----|
| Automatic session lock (minutes) | 15 |
| Maximum password age (days)      | 0  |
| Enforce password history         | 1  |
| Minimum password age (days)      | 0  |

#### Automatic session lock (minutes)

Specify the period of inactivity (in minutes) during which System Manager stays operational.

When the inactivity period elapses, a dialog window warns the user by showing a 30-second countdown timer. At the end of this inactivity period, the user is logged out and directed to the login page.

#### Maximum password age (days)

Specify the maximum duration time (in days) during which a password remains valid before a change is required.

Set a value between 0 (that means disabled) and 365 that is greater than the value set for the Minimum password age (days).



If you set a Maximum password age (days) value that is lower than the Minimum password age (days), a conflict may arise.

#### Enforce password history

Determine the number of instances in which users are restricted from reusing any of their previously used passwords.

You can set a value between 1 and 20.

#### Minimum password age (days)

Specify the minimum duration time (in days) during which a password cannot be changed.

Set a value between 0 (that means disabled) and 365 that is lower than the value set for the Maximum password age (days).



If you set a Maximum password age (days) value that is lower than the Minimum password age (days), a conflict may arise.

## Diagnostic

The Diagnostic section provides tools for troubleshooting and identifying issues with the device. This section includes two options: Ping and Export Diagnostic Logs.



The Diagnostics section is only visible if you access System Manager from a browser.

### Ping

This feature tests a host reachability over a network, by sending ping requests.

Enter an IP address in the Network address field, then select Ping.

System Manager generates a log file named SystemManager\_log\_\*.txt and stores it into the Logs section. In addition, System Manager automatically launches a browser window that displays the results extracted from the Ping log file.

The screenshot shows a web interface for the 'Ping' tool. At the top, the title 'Ping' is displayed. Below it, a message states: 'Five ping requests will be sent to the provided network address.' There is a text input field labeled 'Network address'. Below the field, a hint text reads: 'ex, 10.0.2.1 or www.example.com'. At the bottom of the form is a button labeled 'Ping'.

### Export Logs

The logs provided in this section include valuable information for diagnosing any device activity issues and identifying their root cause.

Select Export all to download any activity log files.

The screenshot shows a web interface for the 'Logs' section. The title 'Logs' is at the top. Below it is a button with a download icon and the text 'Export all'.

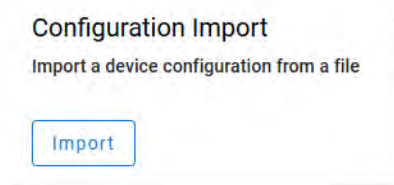
## Maintenance

This section allows you to configure a new device or a replacement device, by importing an existing device configuration or exporting any device settings for later use on another device.

### Configuration Import

You can share a device configuration among devices of the same type. You can import a device configuration both locally and remotely.

- You can import a device configuration into non-initialized devices only by using a USB memory stick.
- You can use an exported configuration file on another device; however, the exported configuration file is not editable. For instance, modifications to LAN settings, such as IP addresses, are not permitted.



#### Local configuration via USB memory stick

1. In System Manager, export a configuration file from the source device. See [Configuration Export on page 49](#).
2. Load the previously exported configuration file into a USB memory stick.
3. Plug the USB memory stick into the USB port of the target device.
4. Depending on whether the device is initialized or not:
  - Initialized device: Under Maintenance > Configuration Import, select Import and browse to the configuration .json file.
  - Non-initialized device: Restart the device while the USB memory stick is still plugged in. The importer searches for a .json file that is named after the device serial number, such as a {hostname}\_{serial\_number}.json file. If the importer does not find any serial number, it searches for a generic file named DeviceConfiguration.json. Once the device restarts, you are prompted you enter a password to initialize the device.

**Note:** Any error occurring during the process is logged into the System Manager Diagnostics > Logs section.

---

**IMPORTANT** The device might automatically restart during the process.

---

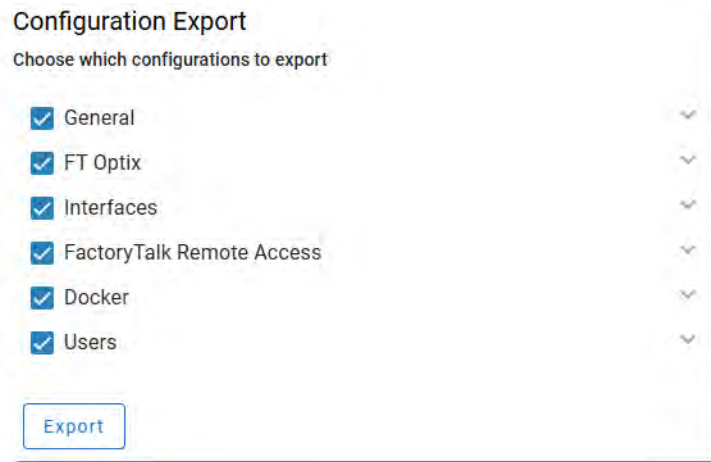
#### Remote configuration through System Manager

1. Remotely access System Manager. See [Access System Manager from a Browser on page 25](#).
2. Export a configuration file from the source device. See [Configuration Export on page 49](#).
3. Under Maintenance > Configuration Import, select Import.
4. A dialog window opens to let you browse to a previously exported configuration file in the .json format.



## Configuration Export

The process might differ, depending on whether you are accessing System Manager from a browser or directly from the device.



### Local configuration via USB memory stick

1. In System Manager, access Maintenance > Configuration Export.
2. Select the device configurations that you want to export, then click Export.
3. A {hostname}\_{serial\_number}.json configuration file is generated, downloaded, and stored on the USB memory stick if you inserted any into the device USB port.

### Remote configuration through System Manager

1. Remotely access System Manager. See [Access System Manager from a Browser on page 25](#).
2. Access Maintenance > Configuration Export.
3. Select the device configurations that you want to export, then click Export.
4. A dialog window opens to let you download a {hostname}\_{serial\_number}.json configuration file.

**Notes:**

## Remote Access

You can configure the ControlLogix® Embedded Edge Compute module to use FactoryTalk® Remote Access™ to transfer a FactoryTalk® Optix™ application to the module, update the module image, and connect to a Logix Controller remotely.

You access FactoryTalk Remote Access through FactoryTalk® Hub™.

## 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 organizations.

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 Optix 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.

## Add the Module to FactoryTalk Remote Access

To register the module in a FactoryTalk Remote Access organization:

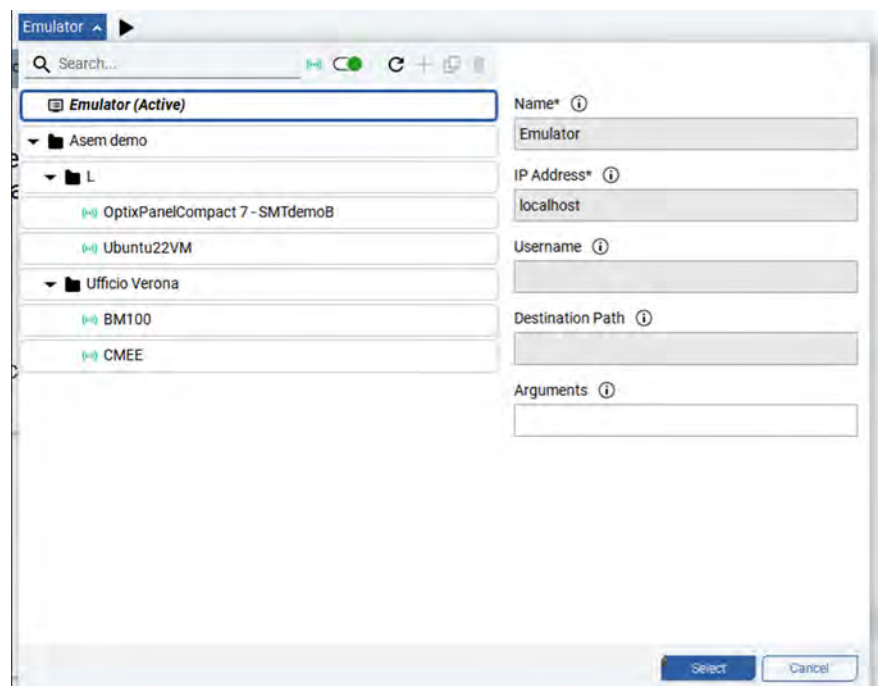


See the FactoryTalk Remote Access Help for additional information on how to get access to FactoryTalk Remote Access Manager and how to register a device in an organization.

1. Sign on to System Manager.
2. On the Networking page:
  - a. Unselect WAN, LAN, and Reserve static IP pool for VPN connections.
  - a. Select Point-to-Point Virtual Ethernet adapter.
3. Press Apply. The module reboots.
4. Sign on to System Manager.
5. On the FactoryTalk Remote Access page:
  - a. In Connection, press Connect.
  - b. Note the Device ID and Password.
6. Navigate to FactoryTalk Hub, and make sure you have joined the correct organization.
7. Select the FactoryTalk Remote Access Tile.
8. Create a folder under the Organization.
9. Right-click and select Add a device.
10. Select Add the device remotely.
11. Use the DeviceID and Password from the Embedded Edge Compute module.
12. Once connected, you can give it a name.
13. Navigate through the properties.

## Deploy a FactoryTalk Optix Application With FactoryTalk Remote Access

When you use FactoryTalk® Optix Studio™ while you are signed on to a FactoryTalk Hub organization with the FactoryTalk Remote Access domain, you can connect to remote devices directly from FactoryTalk Optix Studio to deploy a FactoryTalk Optix application.



## Update the Device Firmware

You can update your device firmware through System Manager, FactoryTalk® Remote Access™ Manager or with a USB memory stick.

The firmware image is a single file that works as a “container” for the components to be updated. The container files are identified by the .img file extension and for convenience, firmware images are available on the Product Compatibility and Download Center (PCDC) portal.

### Update Through System Manager

#### IMPORTANT

The process takes approximately two minutes to complete. During this time, do not to turn off the device, nor disconnect it from the power supply.

1. In System Manager, access General > System Information, then select Update Firmware to browse for and upload a firmware image onto the device.



The upload process of the firmware image can stop and resume.

2. Once the firmware image upload process is complete, select Restart.
3. Restart the module. While restarting, the device detects the firmware image file, checks for its validity and starts the updating process. The MOD status indicator blinks green during the restart phase, then turns steady green, and eventually blinks red during the updating process.
4. The device restarts automatically and the MOD status indicator blinks green, then turns steady green. The firmware update is complete.

### Update Through USB Memory Stick

The firmware image contains the module firmware, Yocto Linux OS, FactoryTalk® Optix™ runtime application, and the FactoryTalk Remote Access runtime application. Firmware images are available on the Product Compatibility and Download Center ([PCDC](#)), and identified by the extension .img.



Firmware update by USB is supported only via USB Memory device with FAT32 and exFAT file systems. microSD™ Cards are not supported for firmware updates.

#### IMPORTANT

The process takes approximately 2 minutes to complete. During this time, it is important NOT to turn off the device or remove power.

To update the module:

1. Copy the file to the root folder of an empty USB Memory device.
2. Insert the USB Memory device into the USB port on the module.
3. Restart the module.

While restarting, the module detects the USB Memory device with the firmware image file, checks if it is valid, and starts the update process. The status indicator blinks green during the restart phase, then turns steady green, and eventually blinks red during the update process while the UPDATE IN PROGRESS message scrolls across the 4-character display.

4. After the update, the device restarts.
5. After restart, the OK status indicator flashes green.
6. Once the OK status indicator is steady green, the update is complete.

# Remote Update Through FactoryTalk Remote Access Manager

You can update the device firmware remotely by moving the firmware image through FactoryTalk Remote Access Manager.

**IMPORTANT**

Before you start this process, you must register your device to a FactoryTalk Remote Access Manager organization. See the FactoryTalk Remote Access Manager user manual to learn how to access FactoryTalk Remote Access Manager and register a device to an organization.

The process takes approximately two minutes to complete. During this time, do not to turn off the device, nor disconnect it from the power supply.

1. In FactoryTalk Remote Access Manager, access the Explorer > Domain view section and select the device.
2. Click the Interactive Access (Tools) button.
3. In the Interactive Access Tool, access the Explorer section on the left menu and copy the firmware image from the local system into the folder that is shown in the table.

| Local system folder     | Remote device folder                        |
|-------------------------|---|
| ...\<FirmwareImage>.img | persistent\data\Updates\<FirmwareImage>.img |

4. Restart the module. While restarting, the device detects the firmware image file, checks for its validity and starts the updating process. The OK status indicator blinks green during the restart phase, then turns steady green, and eventually blinks red during the updating process.
5. The device restarts automatically and the OK status indicator blinks green, then turns steady green. The firmware update is complete.



# 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. | <a href="http://rok.auto/support">rok.auto/support</a>           |
| Local Technical Support Phone Numbers            | Locate the telephone number for your country.   | <a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a> |
| Technical Documentation Center                   | Quickly access and download technical specifications, installation instructions, and user manuals.      | <a href="http://rok.auto/techdocs">rok.auto/techdocs</a>         |
| Literature Library                               | Find installation instructions, manuals, brochures, and technical data publications.                    | <a href="http://rok.auto/literature">rok.auto/literature</a>     |
| Product Compatibility and Download Center (PCDC) | Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.      | <a href="http://rok.auto/pcdc">rok.auto/pcdc</a>                 |

## 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](http://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](http://rok.auto/pec).

Allen-Bradley, ControlLogix, expanding human possibility, FactoryTalk Hub, FactoryTalk Optix, FactoryTalk Optix Studio, FactoryTalk Remote Access, Kinetix, Logix 5000, Stratix, Studio 5000 Logix Designer, PanelView, Point I/O and Rockwell Automation are trademarks of Rockwell Automation, Inc.

CIP and EtherNet/IP is a trademark of ODVA, Inc.

microSD is a trademark of SD-3C.

Microsoft Windows is a trademark of Microsoft Corporation

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, 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