

CIP Security with Rockwell Automation Products

Allen-Bradley
by ROCKWELL AUTOMATION

Application Technique

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.

Table of Contents

Chapter 3

CIP Security Implementation Process

Chapter 4

CIP Security Implementation Example Architecture

Chapter 5

Add or Replace A Device In a CIP Security System

Appendix A

CIP Security Compatibility

Appendix B

History of Changes

Index

About This Publication

This manual explains how to implement the Common Industrial Protocol (CIP™) Security standard in your industrial automation control system (IACS). The term CIP Security™ is used throughout the rest of this manual.

Make sure that you are familiar with the following before you use this manual:

- Basic understanding of EtherNet/IP™ networking fundamentals
- Basic understanding of network security terminology and concepts
- Use of Rockwell Automation® software, for example:
  - FactoryTalk® Policy Manager
  - FactoryTalk System Services
  - FactoryTalk Linx
  - Studio 5000 Logix Designer®

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.

Summary of Changes

This table contains the changes that are made to this revision of the publication. Change bars indicate changes throughout the publication.

Topic	Page
Added information about downloading firmware, AOP, EDS, and other files	7
Added content to the Security Assessment section	11
Added the PowerFlex 6000T drives to table CIP Security Hardware	18
Added content to the Disable CIP Security section	37
Added the Subject Alternative Name description	44
Updated the descriptions in table CIP Security Device State Icons	46
Moved content to Remove Security Policy From a Device Via FactoryTalk Policy Manager - Option 2 section	70
Updated the Set Mask Parameters to Maintain Security with information about the PowerFlex 6000T drives	71
Added categories to the Syslog Even Facility Codes table	76
Added categories to the Event Security Risk Severity Levels table	77
Add a CompactLogix 5380 controllers example architecture	88
Add the PowerFlex 6000T drives to table CIP Security-capable Devices That Do Not Support APD	108
Added Studio 5000 Logix Designer application, version 36, to table CIP Security With Logix Controllers in Logix Designer Applications	111
Added Studio 5000 Logix Designer application, version 36, to table ControlLogix 5580 and 5570 Controller Redundancy With a CIP Security System	112
Added the PowerFlex 6000T drives to the Other Devices Used With a CIP Security System table	113
Updated the History of Changes section	115

Additional Resources

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

Resource	Description
FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.	Describes how to install and use FactoryTalk System Services and FactoryTalk Policy Manager.
FactoryTalk Security Application Technique, publication SECURE-AT002	Describes how to use FactoryTalk Security to implement authentication and authorization in your industrial automation system, how to enforce product-specific security for Studio 5000 Logix Designer, FactoryTalk View, and FactoryTalk AssetCentre
FactoryTalk Security System Configuration Guide Quick Start, publication FTSEC-QS001	Describes how to use FactoryTalk Services Platform with FactoryTalk Security.
Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD022	Describes security architecture use cases for designing and deploying CIP Security technology across plant-wide or site-wide Industrial Automation and Control System (IACS) applications.
System Security Design Guidelines Reference Manual, publication SECURE-RM001	Describes guidelines for how to use Rockwell Automation products to improve the security of your industrial automation system.
Armor PowerFlex User Manual, publication 35-UM001	Provides basic information on how to install, configure, and program, the Armor PowerFlex drives.
CompactLogix 5380 and Compact GuardLogix 5380 Controllers User Manual, publication 5069-UM001	Describes how to design, implement, and maintain an industrial control system that uses CompactLogix or Compact GuardLogix-based controllers.
ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Describes how to design, implement, and maintain an industrial control system that uses ControlLogix® or GuardLogix® controllers.
ControlLogix EtherNet/IP Network Devices User Manual, publication 1756-UM004	Describes how to use ControlLogix EtherNet/IP communication modules with a Logix 5000™ controller and communicate with devices on the Ethernet/IP network.
Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Describes how to use Kinetix® 5700 drive system with associated power supplies, single-axis inverters, dual-axis inverters, and accessory modules in a Logix 5000 control system.
PowerFlex Drives with TotalFORCE Control Programming Manual, publication 750-PM101	Provides detailed information on startup, control algorithms, and status indicators.
Kinetix 5300 Servo Drives User Manual, publication 2198-UM005	Describes how to use a Kinetix 5300 drive system with associated power supplies and accessory modules in a Logix 5000 control system.
CIP Security Proxy User Manual, publication 1783-UM013	Describes how to use a CIP Security Proxy to provide secure communication for non-CIP Security-capable devices.
Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley industrial automation controls and assemblies.
Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

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

Industrial Security Overview

This section provides an overview of CIP Security™.

Industrial Automation Control Systems Environment

Historically, industrial automation control systems (IACS) have been air-gapped environments, isolated systems that are running proprietary control protocols. But IACS networks are evolving toward smart manufacturing.

Smart manufacturing represents a gateway to digital transformation that connects plant-level and enterprise networks, and securely connects people, processes, and technologies.

Collectively, this opens new windows to connected smart devices for visibility into processes, data, and analytics. The visibility enables better and faster decision-making and seamless connectivity for remote locations.

As EtherNet/IP™ becomes a growing standard, evolving these isolated IACS networks towards smart manufacturing, network convergence, and industrial security become a necessity.

Security Threats

As IACS networks transition to open standards of Ethernet-media and Internet Protocol (IP) to meet the needs of end-to-end connectivity of entities, the threat landscape broadens.

With an increase of smart devices and end-to-end connectivity come more assets to protect and a greater risk of security threats.

Security risks can take many forms, for example:

- Threat actors that try to gain unauthorized, and undetected, access to an IACS network with the intention to commit malicious acts.
- Well-intentioned personnel with no malicious intention but who make mistakes that can result in unintended consequences.

IMPORTANT This publication focuses on threat actors with malicious intentions, also called attackers. The word attacker is used throughout the rest of the publication.

In this publication, attacker refers to a range from one individual or to an Advanced Persistent Threat (APT), that is, or a group of attackers working collectively.

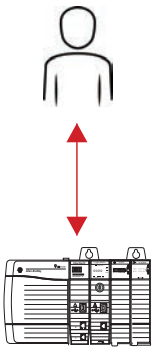
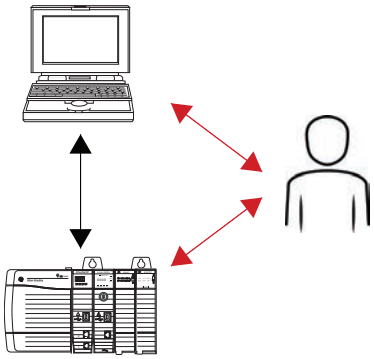
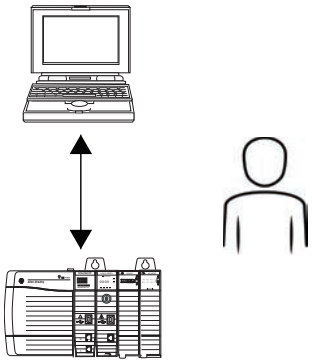
Vulnerability and Exploits

By default, IACS communication protocols are proprietary and insecure. They lack the security properties such as authentication, integrity, and confidentiality. As a result, data and endpoints are at risk. These security properties are necessary for IACS devices to defend themselves against a network-based attack.

Insecure communication protocols can be exploited to make data accessible for anyone to collect, and vulnerable endpoints can become open targets for denial-of-service (DoS) and other types of attacks.

When attackers access a system, they use many ways to exploit the IACS communication protocol vulnerabilities.

Table 1 - Attack Types

Attack Type	Description	
DoS (Denial-of-service))	An attacker executes a DoS attack that renders the CIP™ device inoperable.	
Man-in-the-Middle	The attacker eavesdrops on data in transit to alter the communication between CIP™ devices.	
Monitor Data	The attacker monitors or views sensitive or classified data that is exchanged between CIP devices.	

Security Assessment

Getting a security assessment is the starting point for any security implementation. An assessment provides a picture of your current security posture and what mitigation techniques that can be used to achieve an acceptable risk state.

An assessment is a collaborative process, between Operational Technology (OT) and Information Technology (IT) personnel to maximize the protection of confidentiality, integrity, and availability while still providing functionality and usability.

There are three steps to perform a security assessment.

1. Conduct a threat assessment.

   A threat assessment considers a range of threats from natural, criminal, terrorist, to accidental for a given facility/location. Based on business requirements, a company should evaluate the likelihood for each threat.

2. Perform a vulnerability assessment.

   A vulnerability assessment is designed to identify methods by which threats can exploit vulnerabilities and to provide recommendations on how to address these vulnerabilities.

   Each vulnerability should be rated for the probability or ease of exploitation and the resulting impact in terms of cost or injury should the exploit be successful. This establishes a risk score for each vulnerability.

3. Perform a risk assessment.

   A risk assessment evaluates the risk scores and assigns responses to each risk. One of the following actions should be taken for each risk:

   - **Mitigated** - A mitigated risk requires an explanation of what was done to help prevent the vulnerability from being exploited.
   - **Terminated** - A terminated risk requires an explanation of what was removed or disabled to help prevent the vulnerability from being exploited.
   - **Transferred** - A transferred risk requires an explanation of what is being done outside this system to help prevent or respond to the vulnerability being exploited.
   - **Accepted** - An accepted risk requires notation of the authority accepting the risk.

   Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to your IACS assets.

Defense in Depth Architecture

Industrial security is best implemented as a complete system across your operations. The defense-in-depth (DiD) approach is common to security standards. Common to security standards is the concept of DiD.

The DiD security approach establishes multiple layers of protection that are based on diverse technologies through physical, electronic, and procedural safeguards.

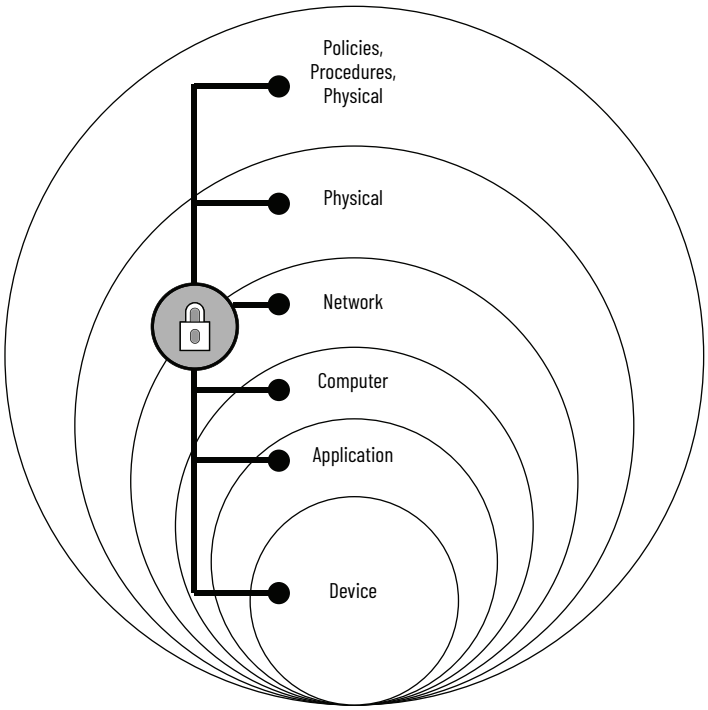
For example, you restrict physical access to managed switches with port locks. Then you position edge industrial firewalls to restrict access and block unapproved traffic flows. Finally, you employ an industrial demilitarized zone (IDMZ) as a perimeter buffer zone between the Industrial and Enterprise zones. The IDMZ lets secure data sharing and services take place without direct connection.

The following are key tenets of the DiD security approach:

- Multiple layers of security are more resilient to attack
- Each layer adds to the one above it
- It does not replace the need for firewalls or other security infrastructure in a system.

The expectation of the DiD approach is that in case an attacker breaches one layer of defense, there's always an additional layer that thwarts their effort.

Figure 1 - Defense in Depth Architecture



CIP Security is an ODVA Standard

As attackers become more sophisticated and network convergence opens more potential gateways to industrial zones, CIP-connected devices must be able to defend themselves.

Recognizing the need for CIP-connected device protection, ODVA developed CIP Security. It's an open-standard secure communication mechanism for EtherNet/IP™ networks.

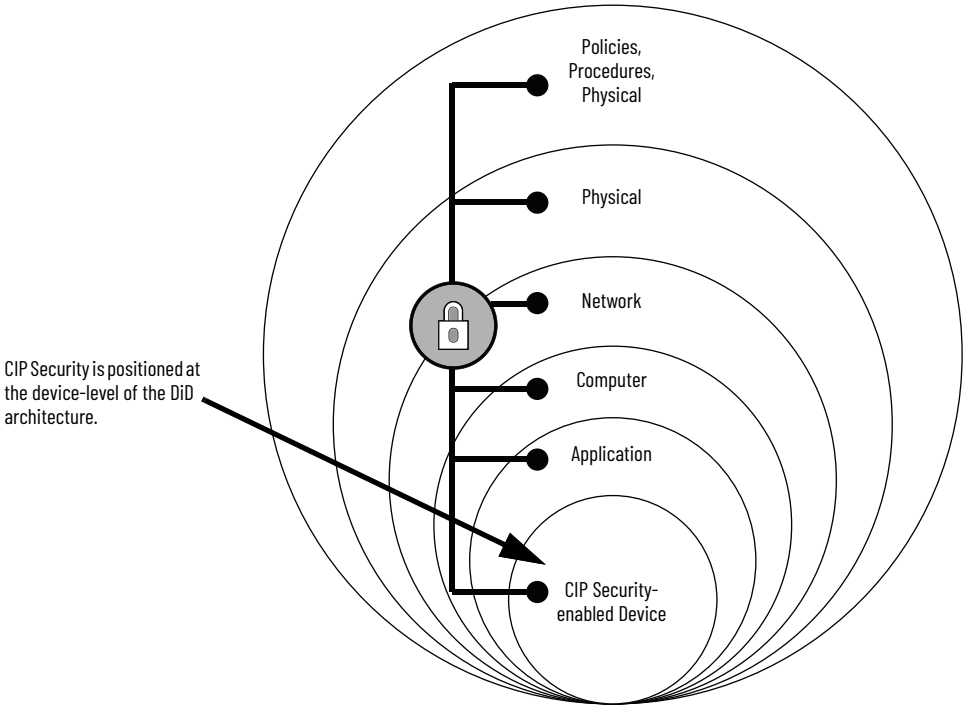
The following CIP Security properties are countermeasures that address the security risks:

- Device identity and authentication
- Data integrity and authentication
- Data confidentiality (encryption)

Positioned at the device-level in the DiD architecture, CIP Security enables CIP-connected devices to authenticate each other before transmitting and receiving data. Device connectivity is limited to only trusted devices.

Optionally, to increase the overall device security posture, it can be combined with data integrity to guard against packet tampering and message encryption to avert unwanted data reading and disclosure.

Figure 2 - CIP Security As Part of Defense in Depth Architecture



Device Identity/Authentication

Before devices start communicating, each device must be able to verify that the identity of the device with which it wants to communicate is authentic. This protects legitimate devices from a rogue device gaining access to the system by pretending to be a system component.

To build this endpoint trust, a certificate or pre-shared (secret) key can be used to provide identity to the device:

- **Certificate** is used to provide identity based on the X.509v3 standard.

  Certificates are an agreement between communicating parties and a common entity that is called a Certificate Authority (CA). A trusted CA signs and issues certificates to requesters to prove their identities. Mutual trust can be established when communicating parties exchange certificates signed by a common CA.

  FactoryTalk® System Services is the certificate authority. It is the service that signs and issues certificates to give assurance for a communicating party's authenticity.

  An advantage to using certificates is that they provide a greater level security than pre-shared keys.
- **Pre-shared keys** are used to prove identity that is based on keys that are shared in advance among the communicating parties.

  Pre-shared keys are agreement between two entities to the parameters that determine identity and authentication. The entities are the devices that communicate with each other.

  An advantage to using pre-shared keys is that they provide less performance impact on when establishing connections.

IMPORTANT Devices can only use one pre-shared key, as a result, any conduits that are required between any Zones that are configured with pre-shared key must be created using Trusted IP.

Secure Data Transport

CIP Security is based on Transport Layer Security (TLS) (RFC 5246) and Datagram Transport Layer Security (DTLS) (RFC 6347) protocols to protect EtherNet/IP data while in transit.

TLS and DTLS are network protocols that facilitate data transfer privately and securely between an originator and a target device.

TLS provides the following security properties:

- **Authentication** - Allows each device to confirm their identity through certificate exchange or pre-shared keys
- **Integrity** - Makes sure that the data has not been tampered with, or falsified, while in transit, with TLS Hash-based Message Authentication Code (HMAC)
- **Confidentiality** - Data is encrypted while being transmitted between the originator and target device. Encrypting the data helps prevent unauthorized parties from reading it.

DTLS is based on TLS but is used for User Datagram Protocol (UDP) connections instead of Transmission Control Protocol (TCP) connections.

For complete descriptions of the security properties, see the ODVA home page available at: https://www.odva.org/.

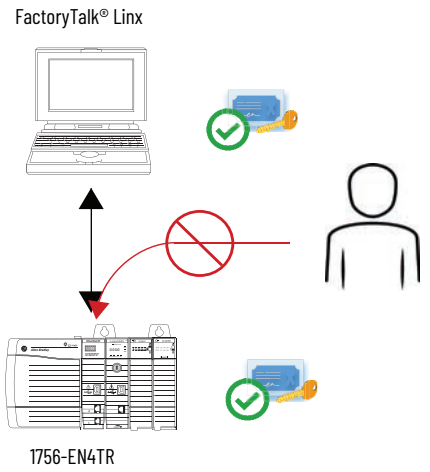
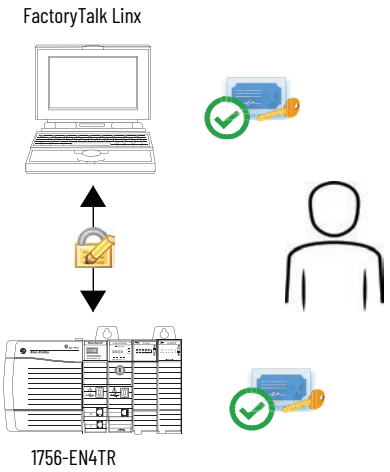
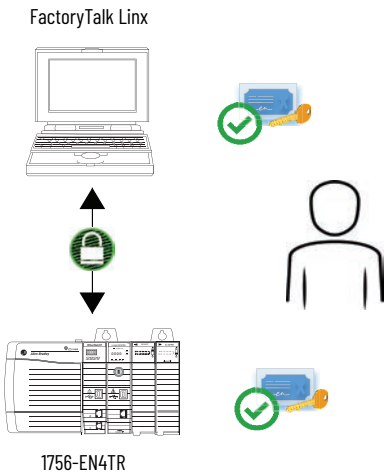
Table 2 defines the icons that are used in Table 3 on page 15.

Table 2 - CIP Security Icons

Name	Symbol	Definition
Certificate		An electronic representation of an identity. A certificate binds the identity's public key to its identifiable information, such as, name, organization, email, user name, and/or a device serial number. This certificate is used to authenticate a connection to a zone or device. Selected by default when CIP Security is enabled.
Pre-shared key		A secret that is shared among trusted entities to represent identities. FactoryTalk Policy Manager can create a key that can be shared.
Integrity		Checks whether data was altered and whether a trusted entity sent the data. Altered and/or untrusted data is rejected.
Check mark		Symbol used to indicate that the endpoints for communication between devices have been authenticated and can be trusted.
Encryption		Encodes messages or information to help prevent reading or viewing of EtherNet/IP data by unauthorized parties.

Table 3 describes how secure data transport enables a CIP-connected device to help protect itself from malicious communication.

Table 3 - CIP Security Properties

Security Properties	Description	
Device Identity and Authentication	Method of providing secure identity for a device. The following methods can be used: • **Certificates** (recommended) • Pre-shared keys Together, these properties help the device take the following actions: • **Reject messages** that untrusted devices send. • **Help prevent unauthorized** devices from establishing connections.	 Threat actor can't connect to the CIP-connected device.
Data Integrity and Authentication	Method of providing data integrity and message authentication to EtherNet/IP network communication. Lets the device take the following actions: • **Reject data** that has been altered. • **Help prevent tampering** or modification of communication.	 Attacker can see the data but can't change the data.
Data Confidentiality	Means of using encryption to encode messages or information that is exchanged across an EtherNet/IP network. Lets the device take the following actions: • **Help prevent viewing** of EtherNet/IP data by unauthorized parties. • **Help prevent snooping** or data disclosure. **IMPORTANT**: This security property is optional. Some IACS network communication do not need to be secure; data integrity and authentication is typically the goal. Encryption typically affects network adapter capacity.	 Attacker cannot see the data.

Notes:

CIP Security-capable Rockwell Automation Products

This section describes the components and concepts that are part of the Rockwell Automation method of implementing CIP Security™ in an IACS.

For information on the tasks that are required to use CIP™ Security-capable products in an IACS, see:

- CIP Security Implementation Process on page 45
- CIP Security Implementation Example Architecture on page 79
- Publications listed in Additional Resources on page 8

Software and Hardware

The list of CIP Security-capable Rockwell Automation® products includes software and hardware products, for example, FactoryTalk® Policy Manager software and ControlLogix® 5580 controllers, respectively, to define the security policy.

You download software at the Rockwell Automation Product Compatibility and Download Center (PCDC).

To visit the PCDC, go to: https://compatibility.rockwellautomation.com/Pages/home.aspx

CIP Security Software Applications

Table 4 - CIP Security Software

Software Application	Description	Minimum Verion
FactoryTalk Policy Manager	FactoryTalk Policy Manager is a secure software application that you use to configure, deploy, and view the system communication security policies. The security policies are divided into different components, that is, devices, zones, and conduits. You use these components to design security models that control the permissions and usage of devices within the system. For more information, on security models and how components are used to design the models, see page 20. The security policies are distributed to the devices at once. You aren't required to make changes at the device level and face the risk of human error that results in inconsistent configuration among the devices.	6.11
FactoryTalk System Services	FactoryTalk System Services is a secure EtherNet/IP™ client that runs in the background to deploy the security policies that are configured in FactoryTalk Policy Manager. You do not take action in the client. FactoryTalk System Services provides the following in the FactoryTalk Directory to enforce security policies that are based on the ODVA CIP Security standard: • Identity/Authentication Service - Authenticates users and validates user resource requests. Validate user credentials against the FactoryTalk Directory and FactoryTalk Security policy settings to obtain privileges associated with the user. • Certificate Service - Issues and manages certificates for devices in the FactoryTalk Policy Manager model. • Deployment Service - Translates the security policy to CIP™ configurations that are delivered to endpoints. • Policy Service - Build and manages CIP network trust models and defines security policy for the CIP endpoints. • Diagnostic Service - Makes FactoryTalk audit and diagnostic logs available as a web service.	6.11
FactoryTalk Linx	FactoryTalk Linx is a secure EtherNet/IP client that initiates connections over a secure EtherNet/IP network with CIP Security-enabled devices. This server and communication service that lets devices communicate with the FactoryTalk software portfolio and Studio 5000 Logix Designer® application. **IMPORTANT**: You can't use RSLinx® Classic software to implement CIP Security in an IACS.	6.11
Studio 5000 Logix Designer	Logix Designer application is a comprehensive programming software that you use with Logix 5000™ controllers. **IMPORTANT**: Logix Designer application isn't required to implement CIP Security. However, Logix Designer application functions as CIP Security-capable software because it supports the CIP protocol and uses FactoryTalk Linx software to communicate with other devices via the CIP protocol. The Logix 5000 controller this is used in the system determines what Logix Designer application version to use. For example, to use a ControlLogix 5580 controller's Ethernet port to connect to the system, you must use software version 32.00.00 or later.	32.00.00(1)

(1) There are some configurations in which you can use Studio 5000 Logix Designer software, version 31, to connect a controller to the IACS. For more information, see Table 27 on page 111.

CIP Security-capable Hardware Devices

The following hardware devices are CIP Security-capable.

IMPORTANT

- The minimum firmware revisions that are listed for Logix 5000 controllers in Table 5 represent the first firmware revision at which you can connect the controller to an IACS with CIP Security that is implemented via a secure connection to the controller Ethernet port.
  There are some configurations in which you can use earlier firmware revisions to connect the controller to an IACS with CIP Security implemented. For more information, see CIP Security Compatibility on page 111.
- The table represents products that are CIP Security-capable at the time of this publication.
  Over time, new products will be released that are CIP Security-capable. New versions of existing products that aren't CIP Security-capable will be released in the future to make them CIP Security-capable.
  To see if a product is CIP Security-capable, see the product documentation.

Table 5 - CIP Security Hardware

Hardware Product	Description	Minimum Firmware Revision Required
Armor™ PowerFlex® Drives	Armor PowerFlex 35E and 35S drives provide high-performance variable frequency motor control 1...10 Hp in an On-Machine™ package. Armor PowerFlex drives have built-in dual Ethernet ports that let you connect the drives directly to EtherNet/IP networks. You configure the drive with Logix Designer application. CIP Security requires use of the built-in Dual EtherNet/IP ports that are provided on the Armor PowerFlex drives.	10.001
CompactLogix™ 5380 Controllers	CompactLogix 5380 controllers use a common Logix control engine and common development environment to control small to large control systems. The controllers communicate with, and can control, local and remote devices. Dual built-in Ethernet ports let the controllers connect to various EtherNet/IP network topologies, including a Device Level Ring (DLR) network. You use the Logix Designer application to configure CompactLogix 5380 controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	34.011
CompactLogix 5380 Process Controllers	CompactLogix 5380 Process controllers use a common Logix control engine and common development environment to control small to large distributed control systems. The process controller focuses on plant-wide process control. The controllers communicate with, and can control, local and remote devices. Dual built-in Ethernet ports let the controllers connect to various EtherNet/IP network topologies, including a Device Level Ring (DLR) network. You use the Logix Designer application to configure CompactLogix 5380 Process controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	34.011
Compact GuardLogix® 5380 Controllers	Compact GuardLogix 5380 controllers use a common Logix control engine and common development environment to control small to large control systems. The controllers communicate with, and can control, local and remote devices. Dual built-in Ethernet ports let the controllers connect to various EtherNet/IP network topologies, including a Device Level Ring (DLR) network. These safety controllers achieve up to SIL 2/PLd with 1oo1 architecture or up to SIL 3/PLe with 1oo2 architecture. You use the Logix Designer application to configure Compact GuardLogix 5380 controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	34.011
ControlLogix5580Controllers	ControlLogix 5580 controllers use a common Logix control engine and common development environment to control large control systems. The controllers communicate with, and can control, local and remote devices. For example, the devices can be I/O modules, network communication modules, drives, and operator interfaces. You use the Logix Designer application to configure ControlLogix 5580 controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: • The description of these controllers applies to ControlLogix 5580 standard and XT controllers. However, XT controllers can be used in environments with temperatures. • **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	32.011

Table 5 - CIP Security Hardware

Hardware Product	Description	Minimum Firmware Revision Required
ControlLogix 5580 Process Controllers	ControlLogix 5580 Process controllers use a common Logix control engine and common development environment to control large distributed control systems. The process controller focuses on plant-wide process control. The controllers communicate with, and can control, local and remote devices. For example, the devices can be I/O modules, network communication modules, drives, and operator interfaces. You use the Logix Designer application to configure ControlLogix 5580 Process controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	32.011
1756-EN4TR ControlLogix EtherNet/IP Communication Module	The 1756-EN4TR communication module performs the following functions: • Facilitate high-speed data transfer between ControlLogix 5580 and GuardLogix 5580 controllers and devices on an EtherNet/IP network. • Connect Logix 5000 control systems to multiple EtherNet/IP network topologies.	Any
GuardLogix 5580 Controllers	GuardLogix 5580 controllers use a common Logix control engine and common development environment to control large control systems. The controllers communicate with, and can control, local and remote devices. Operating as safety controllers, they provide SIL2/PLd and SIL3/PLe safety solutions. You use the Logix Designer application to configure GuardLogix 5580 controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. **IMPORTANT**: You **do not** use the Logix Designer application to define the security policy. You use FactoryTalk Policy Manager to define the security policy.	34.011
Kinetix® 5300 Drives	Kinetix 5300 drives are entry level-Integrated Motion on EtherNet/IP servo drives that are designed for small to medium machines for various motion control applications.	13.003
Kinetix 5700 Drives	Kinetix 5700 drives are single and dual-axis inverters that you can use to expand the use of Integrated Motion on EtherNet/IP to large, custom machines with high axis counts and power requirements. The drives have built-in dual Ethernet ports that let you connect the drives directly to EtherNet/IP networks.	11.001
PowerFlex 755T Drives	PowerFlex 755T drives, bus supplies, and common bus inverters provide common bus, regenerative, and high-performance variable frequency motor control 10...6000 Hp. PowerFlex 755T drives have built-in dual Ethernet ports that let you connect the drives directly to EtherNet/IP networks. CIP Security requires use of the built-in Dual EtherNet/IP ports that are provided on PowerFlex 755T Main Control Boards. This feature isn't compatible with network option cards.	10.001
PowerFlex 755TS Drives	The PowerFlex 755TS drives are scalable, next generation PowerFlex drives that are designed to meet your application needs. TotalFORCE® can now be used in a wider range of applications. This includes traditional fan, pump, and conveyor applications, and more advanced motor control processes that require high-performance features that are typically found in specialized drive solutions.	11.001
PowerFlex 6000T Drives	PowerFlex 6000T drives are medium voltage drives that use volts per Hertz, sensorless vector control, and flux vector control modes. The drives are suited for most non-regen applications. PowerFlex 6000T drives have built-in EtherNet/IP support that lets you connect the drives directly to an EtherNet/IP network.	9.001
1783-CSP CIP Security Proxy	The 1783-CSP Proxy is a standalone device that lets you connect a device that is not CIP™ Security-capable, also known as the proxied device, to an IACS that has CIP Security enabled.	Any

Use Non-CIP Security-capable Controllers with CIP Security

You can use some non-CIP Security-capable Logix controllers that aren't listed in Table 5 in IACS with CIP Security.

For more information on how to do so, see CIP Security Compatibility on page 111.

Benefits of Using Rockwell Automation Products

Implementing CIP Security with Rockwell Automation products has the following benefits:

- **Centralized System Management** - Use FactoryTalk Policy Manager software to easily create and deploy security policies to many devices at once.
- **Micro-segmentation** - Segment the automation application into smaller cell/zones, thus, reducing the attack surface.
- **HTTP ports** - You can enable or disable unsecure (HTTP) ports/protocols of devices in a system with CIP Security configured.
- **Legacy system support** - The following options are available to use for products that aren't CIP Security-capable in a specific unsecured communication network that deploys the CIP Security feature:
  - Use the 1783-CSP CIP Security Proxy to connect a device that is not CIP Security-capable to an IACS that has CIP Security™ enabled.
  - **Retrofit ControlLogix 5570-based systems** with a 1756-EN4TR communication module.
  - **AllowedList** - Authorize specific communication based on IP address.

In FactoryTalk Policy Manager, the **Authentication Method** property for a conduit uses the term Trusted IP to represent **AllowedList**.

CIP Security Communication Properties

CIP Security is comprised of a security profile, attributes, and components. These key mechanisms facilitate the security requirements for the resource that you are trying to protect.

Security Profile and Attributes

CIP Security defines the concept of a security profile. A security profile is a set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability. A security profile describes what security features a given device supports. The device enforces the security policy based on its security profile.

Understanding that security is a balance and not every CIP-connected device requires the same level of security, FactoryTalk Policy Manager lets administrators enable only the desired attributes when they create a security profile.

The Device Identity/Authentication attribute must be enabled before the options for enabling Data Integrity and Data Confidentiality can occur.

Rockwell Automation CIP Security-capable products support the following security attributes:

Property	Description
Device Identity and Authentication	Certificate base on the X.509 v3 standard is used to provide identity. Pre-shared keys are shared secrets that are shared among trusted entities that are used to provide identity. The TLS protocol facilitates mutual authentication to create trusted endpoints.
Data Integrity	Keyed-Hash Message Authentication Code (HMAC) is used as a cryptographic method of providing data integrity and message authenticity to EtherNet/IP traffic.
Data Confidentiality	Data encryption is used to encode messages or information to help prevent reading or viewing of EtherNet/IP data by unauthorized parties.

IMPORTANT	The rest of this section describes each component and, for zones and conduits, steps to create and configure them. However, the descriptions aren't exhaustive. For more detailed information on security models, including the tasks that you must complete to configure them, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

The following table describes icons that are used in this publication.

Symbol	Definition
	Represents a CIP Security connection to a device.
	Represents a trusted, but not secure, connection to a device.

CIP Security Components

FactoryTalk Policy Manager divides the system security policies into different components. The following components are used to design security models:

- Devices
- Zones
- Conduits

Devices

Devices are the modules, drives, controllers, HMI panels, computers, and servers that work together to create an IACS network. You add devices that share security requirements for a particular function to the same zone.

Considerations with devices in the security model when you use devices in an IACS network:

- The lists of current CIP Security-capable Rockwell Automation products are on page 17 and page 18.
  More CIP Security-capable Rockwell Automation products are in development.
- Just because a device is CIP Security-capable, you aren't required to enable CIP Security on that device in an IACS network.
- You can use non-CIP Security-capable devices in an IACS that includes CIP Security-enabled devices.

Zones

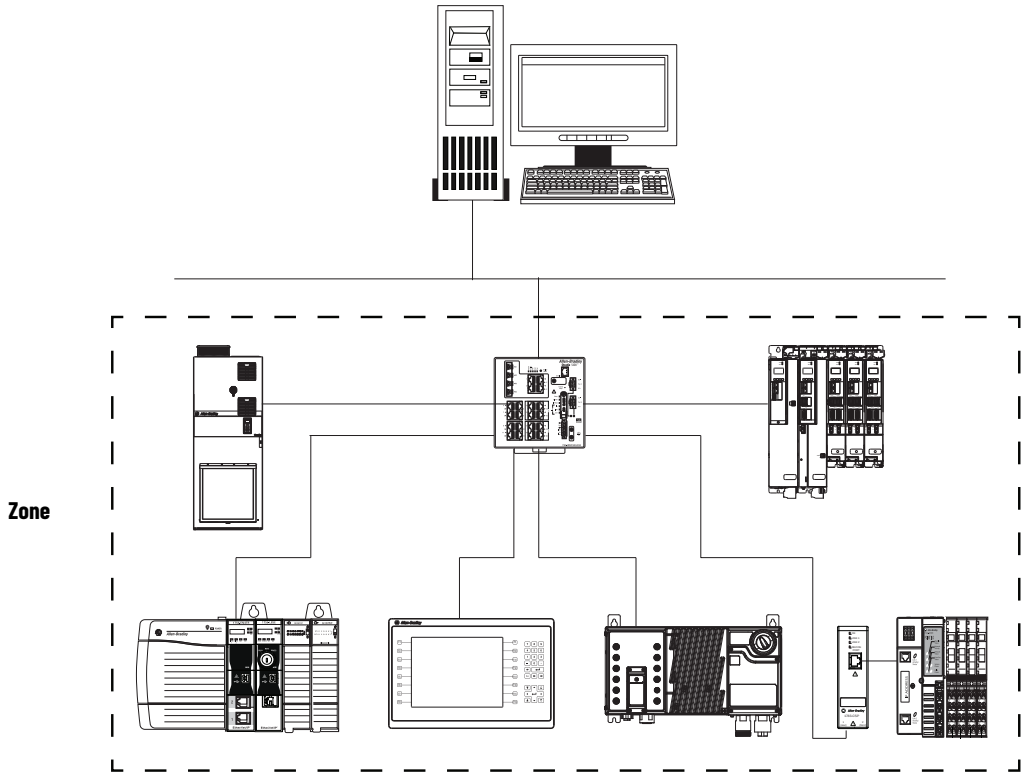
Zones are groups to which devices are added. Zones establish the rules for data integrity, data privacy, and the authentication method that is used to authenticate trusted devices.

- You can have multiple zones in a system and set security policy on a zone-by-zone basis. By using zones, you simplify management of large sets of devices in a system.
- Zones can include devices that are CIP Security-capable and devices that aren't. There can be multiple zones in an IACS network, but a device can only belong to one zone.
- Once a CIP Security-capable device is added to a zone, the device uses the policy settings of that zone.

  Communication between devices in the same zone is implied and mutually trusted. Therefore, you do not have to create conduits between devices in the same zone.

Figure 3 shows a zone that includes devices that are CIP Security-capable, for example, a ControlLogix 5580 controller, and devices that aren't, for example, a PanelView™ Plus terminal.

Figure 3 - Security Model - Zones



Conduits

Conduits create trusted communication pathways outside of zones. You must have at least two endpoints, that is, zones or devices, to create a conduit.

Conduits facilitate secure communication in the following ways:

- Zone to zone
- Device to device
- Device to zone

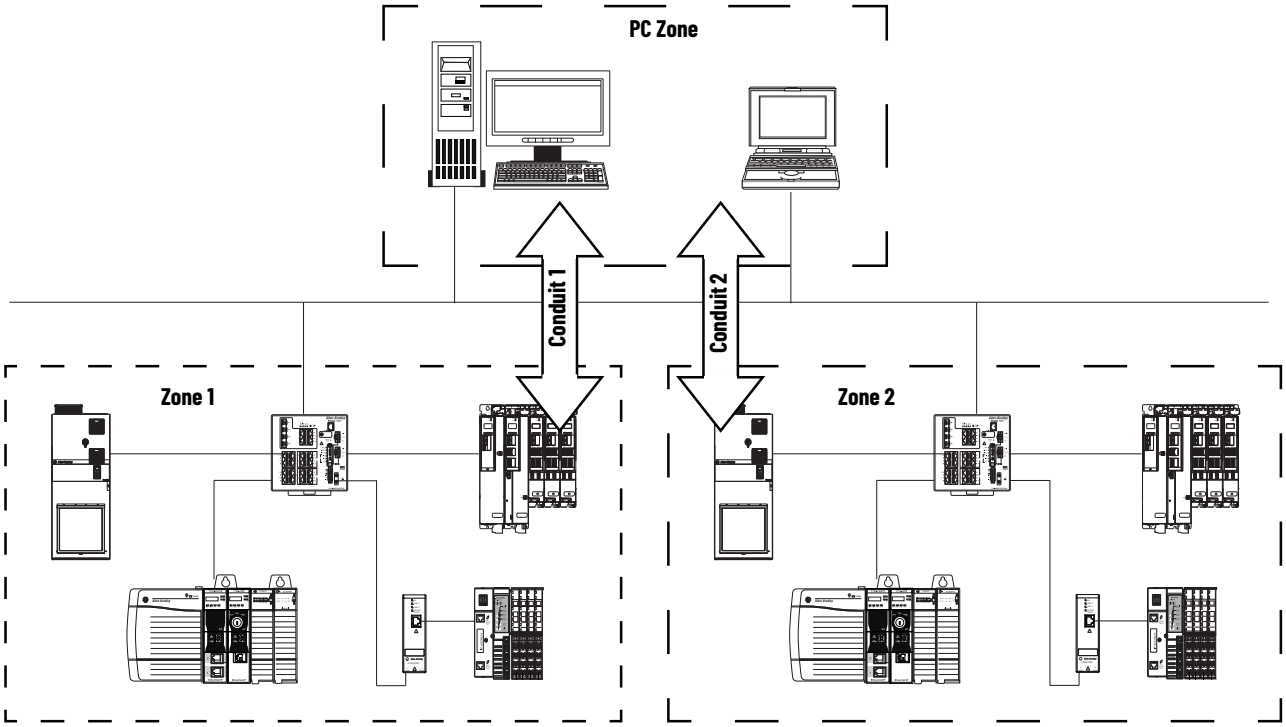
Conduits let you configure trust beyond individual zones using the following methods:

- Trusted IP authentication method - Assigns a trust relationship to an asset based on its IP address. Also known as AllowedList.
- Certificate authentication method - Establishes the identity of the device by using a certificate from a trusted authority.

IMPORTANT Currently, a device can't use multiple pre-shared keys.
If you require communication between a zone that is configured with a pre-shared key and other zones, you must configure a conduit that uses the Trusted IP authentication method to the other zones.

Figure 4 shows conduits in a system with multiple zones.

Figure 4 - Security Model - Conduits



Security Model

The security model is a fully configured instance of zones, devices, and conduits, along with their respective CIP Security properties, in FactoryTalk Policy Manager software. The zones and conduits structure the security model. The security model is deployed to the devices in the IACS via security profiles for individual devices.

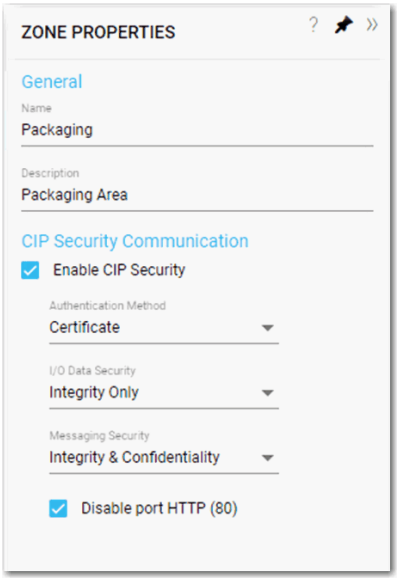
If multiple devices use the same security policies and are in the same zone, we recommend that you configure the security policies at the zone level.

The advantage to configuring security policies at the zone level is that you can configure the policies once and apply them to multiple devices. This method avoids the possibility of differences in security policies across devices that should use the same policies.

Zone Properties

Table 6 lists the configurable fields that are available when you configure zone properties.

Table 6 - Zone Security Properties

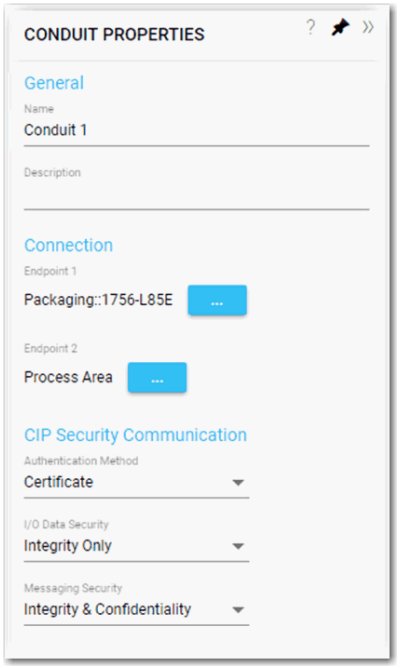
Property	Available Choices	Example FactoryTalk Policy Manager Screen
Name	User configurable	
Description	User configurable	
Enable/Disable CIP Security	• Enable • Disable	
Authentication Method	• Certificate • Pre-Shared Key	
I/O Data Security	• None • Integrity Only • Integrity + Confidentiality	
Messaging Security	• Integrity Only • Integrity + Confidentiality	
Disable Ports - HTTP (80)	• Enable • Disable	

IMPORTANT For more information on the Zone Properties, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

Conduit Properties

Table 7 lists the configurable fields that are available when you configure conduit security policy.

Table 7 - Conduit Security Properties

Property	Available Choices	Example FactoryTalk Policy Manager Screen
Name	User configurable	
Description	User configurable	
Connection Can be any of the following based on how you assign each Endpoint: • Device-to-Device • Device-to-Zone • Zone-to-Zone	• Endpoint 1 (Device or Zone) • Endpoint 2 (Device or Zone)	
Authentication Method	• Trusted IP • Certificate	
I/O Data Security	• None • Integrity Only • Integrity + Confidentiality	
Messaging Security	• Integrity Only • Integrity + Confidentiality	

IMPORTANT For more information on the Conduit Properties, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

Limitations and Considerations

The following are limitations and considerations of the solution from Rockwell Automation to implement CIP Security in an IACS:

Devices That Support DLR/Linear and Dual-IP EtherNet/IP Modes

Most CIP Security-capable devices with built-in dual Ethernet ports use one IP address for both ports and you can secure connections on both ports, for example, in a Device Level Ring network.

CIP Security-capable devices with built-in dual Ethernet ports, that is, CompactLogix 5380 and Compact GuardLogix 5380 controllers, support the following EtherNet/IP modes. The modes determine how the controllers connect to EtherNet/IP networks and how they operate on them.

- Linear/DLR
- Dual-IP

Linear/DLR

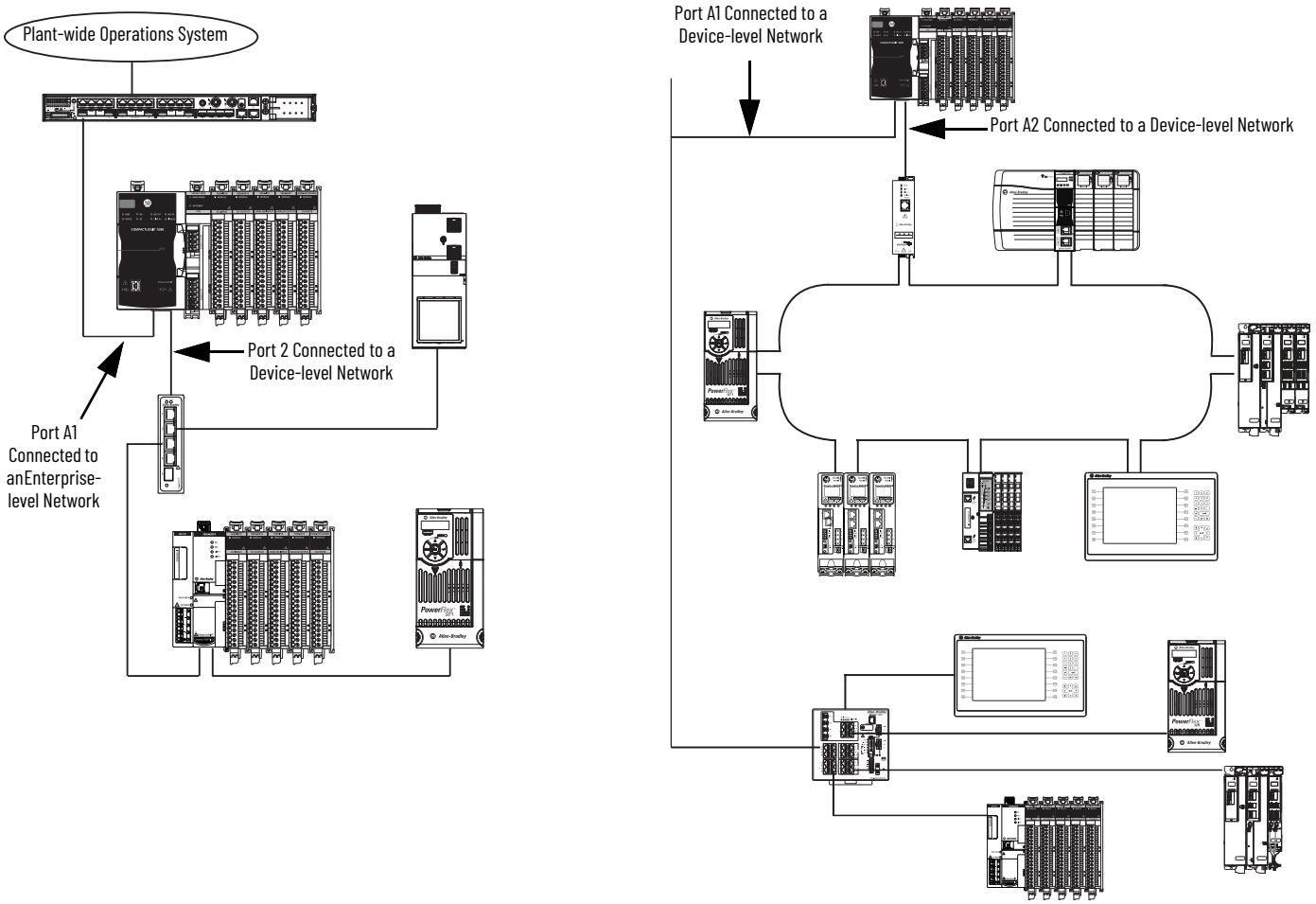
In DLR/Linear mode, the device uses one IP address for both Ethernet ports and you can secure communication on both ports.

Dual-IP Mode

In Dual-IP mode, Ethernet ports A1 and A2, respectively, can connect to separate EtherNet/IP networks. In this mode, each port requires its own network configuration.

Port A1 can connect to enterprise-level networks and device-level networks. Port A2 can only connect to device-level networks. Figure 5 shows example applications in which CompactLogix 5380 controllers use Dual-IP mode.

Figure 5 - Dual-IP Mode Examples



When you use Dual-IP mode, you can **only secure the connection on one Ethernet port** for CIP Security.

IMPORTANT	You must install FactoryTalk Policy Manager and FactoryTalk System Services software on the same server as the FactoryTalk Directory. So the network to which the secured port is connected must also have the server with this software that is connected to it. Because CIP Security does not support configuring separate security policies for the different Ethernet ports on the same device, you can only deploy a security model to one of the networks to which the controller is connected. For example, if you secure the port A1 connection to an enterprise-level network, you can't deploy a security model to the network to which port A2 is connected.

For more information on Dual-IP mode, see the CompactLogix 5380 and Compact GuardLogix 5380 Controllers User Manual, publication 5069-UM001.

Initial Security Model Deployment Fails If ControlLogix 5580 Controller is in Run Mode

If a ControlLogix 5580 controller is in Run mode, that is, the keyswitch is in the RUN position, the first time that you attempt to deploy the security model in FactoryTalk Policy Manager software, the deployment fails. The initial security model deployment is successful if the controller is in Remote Run, Remote Program, or Program mode.

IMPORTANT	This designed limitation protects the controller from a DoS attack by an attacker. The asset owner is the only party with physical access to the controller. Confirm that the controller mode is Remote Run, Remote Program, or Program so the initial security deployment is successful. If desired, you can change the controller to Run mode after the initial deployment and future security model deployments are successful.

After a ControlLogix 5580 controller has a security profile, the controller mode does not affect future security model deployments.

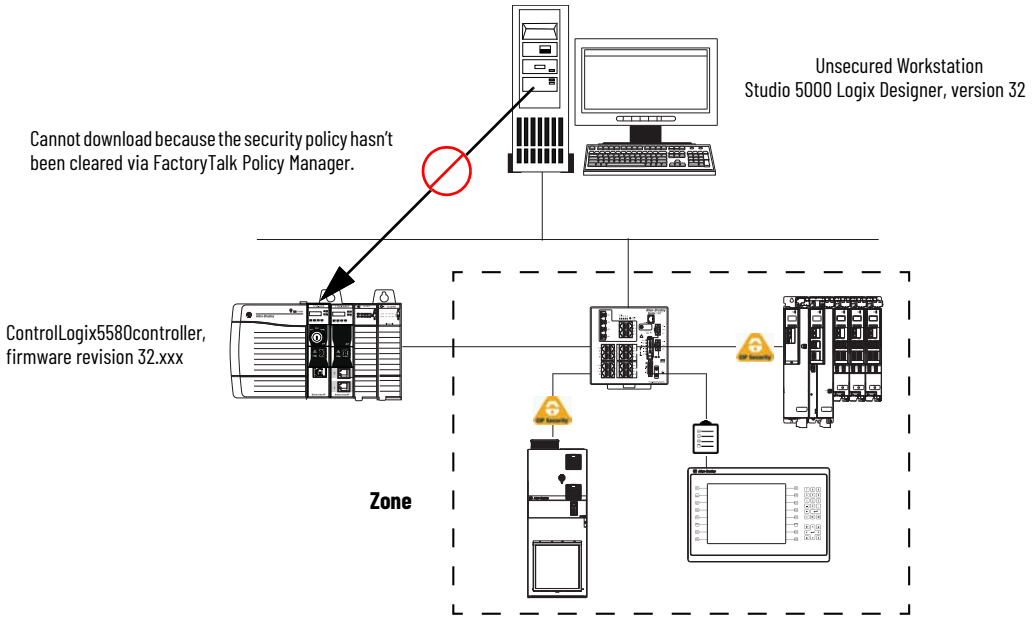
Cannot Download to ControlLogix 5580 Controller from Unsecure Workstation

This limitation is only present in the following conditions:

- FactoryTalk Policy Manager, version 6.11
- FactoryTalk System Services, version 6.11
- Logix Designer application, version 32
- ControlLogix 5580 controller, firmware revision 32.xxx

To avoid this limitation, upgrade the software and controller firmware that is listed above to the next major versions and revision, respectively.

After you enable CIP Security in the ControlLogix 5580 controller, you can't download a Logix Designer application project to the controller once it has been removed from the zone without first resetting the controller to its factory default settings.



Workstation Cannot Download to a Secured ControlLogix 5580 Controller if Security Policies Do Not Match

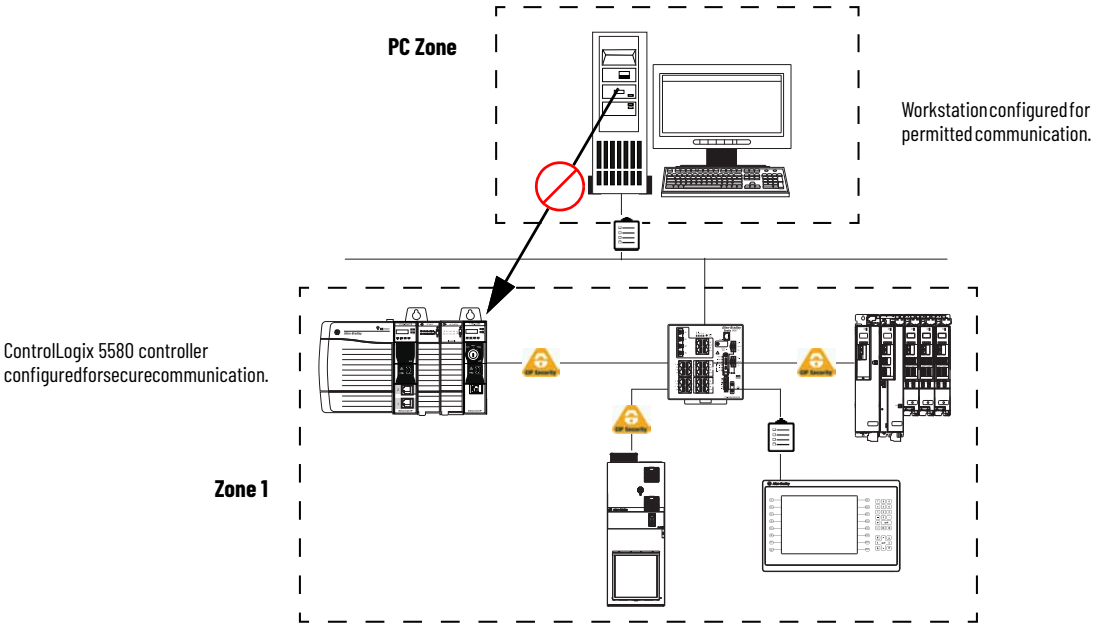
A workstation that is running Logix Designer application can't download a project to Logix 5000 controller, if the project has a different security configuration than the Logix 5000 controller.

IMPORTANT Consider the following:

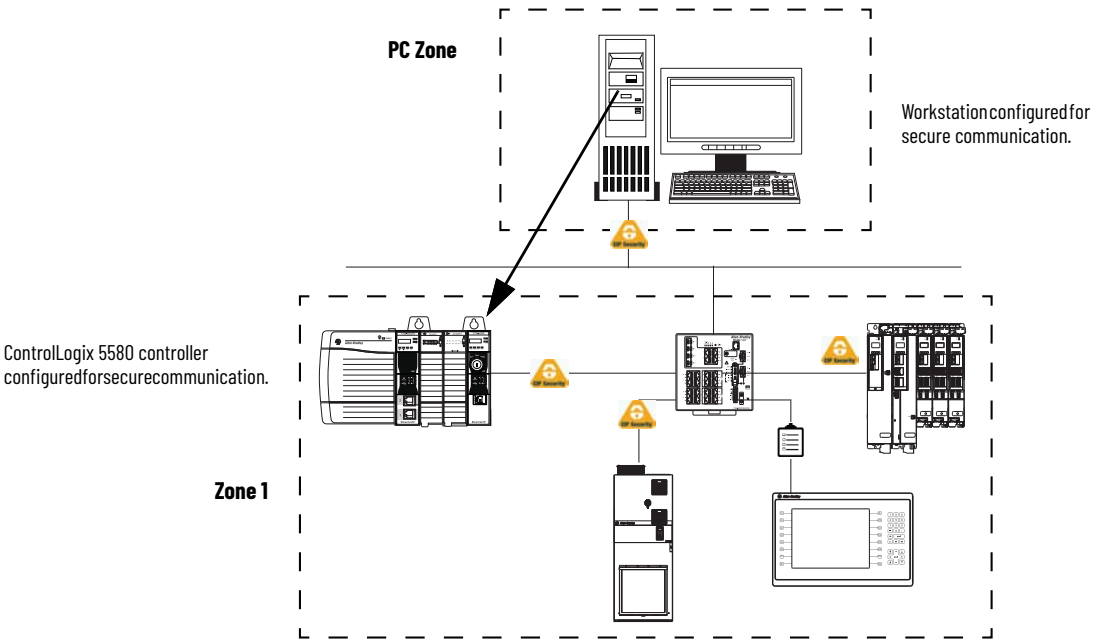
- This designed limitation enforces a high security standard to protect the controller because the controller is the most valuable asset in the IACS.
- The limitation only occurs when the workstation and the Logix 5000 controller reside in different zones.
- In this situation, the controller must connect directly to the EtherNet/IP network

The following example uses a ControlLogix 5580 controller. The following conditions exist:

- The **workstation** is configured for **permitted** communication, that is, Authentication Method = Trusted IP.
- The ControlLogix 5580 **controller** is configured for **secure** communication, that is, Authentication Method = Certificate or Authentication Method = Pre-shared Key (PSK).



To avoid this limitation, update the workstation and controller security profiles to use Authentication Method = Certificate.



Secure the Programming Connection to Redundant ControlLogix 5580 Controllers

You can secure connections between a workstation that is running a Logix Designer application and a ControlLogix 5580 controller redundant pair without the need of a 1783-CSP Proxy. The secure connection supports class 3 communications, for example, program upload or download and to monitor diagnostics.

You must use the following components:

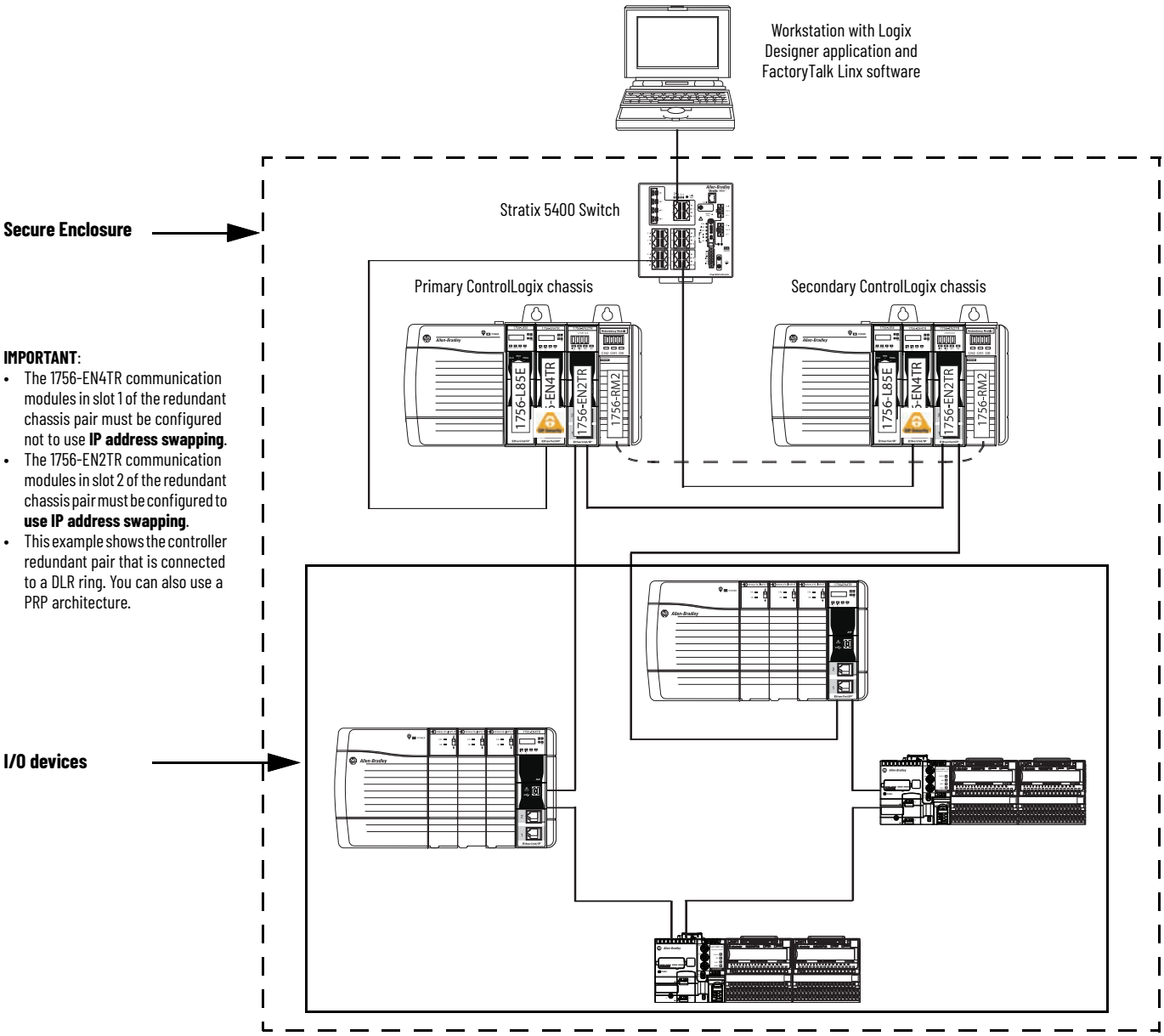
- ControlLogix 5580 controller, firmware revision 34.011 or later
- Two 1756-EN4TR communication modules, firmware revision 4.001 or later, one in each chassis

IMPORTANT	The 1756-EN4TR communication modules must be configured **not to use IP address swapping**.

- Two 1756-EN2x communication modules, one in each chassis, that connect to the I/O devices

Figure 6 on page 30 shows an application in which a workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a ControlLogix 5580 controller redundant pair.

Figure 6 - ControlLogix 5580 Controllers - Redundant Chassis Connected to I/O Network Devices



Secure the Programming Connection to the CompactLogix 5380 Controllers

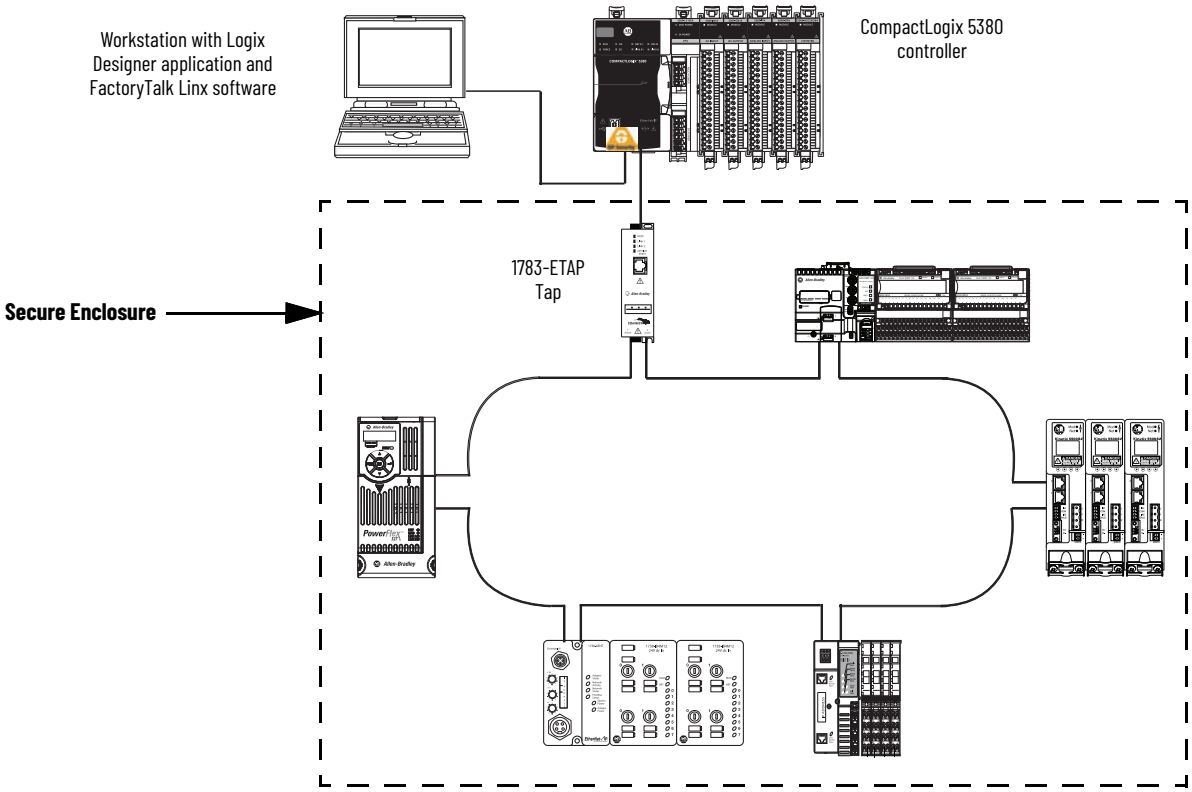
You can secure connections between a workstation that is running a Logix Designer application and a CompactLogix™ 5370 with a 1783-CSP Proxy or CompactLogix 5380 controller without the need of a 1783-CSP Proxy. The secure connection supports class 3 communications, for example, program upload or download and to monitor diagnostics.

The CompactLogix 5380 controllers must use firmware revision 34.011 or later. There is no need for the 1783-CSP Proxy because you can connect the workstation to an Ethernet port on the controller.

Figure 7 shows an application in which the workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a CompactLogix 5380 controller. The controller is operating in Linear/DLR EtherNet/IP mode.

IMPORTANT This example shows the controller that is connected to a DLR ring via a 1783-ETAP tap. The controller can be connected to any valid I/O architecture, for example, a linear topology that doesn't include a 1783-ETAP tap, and the concepts that are described in this section still apply.

Figure 7 - CIP Security with CompactLogix 5380 Controllers Connected to the I/O Network



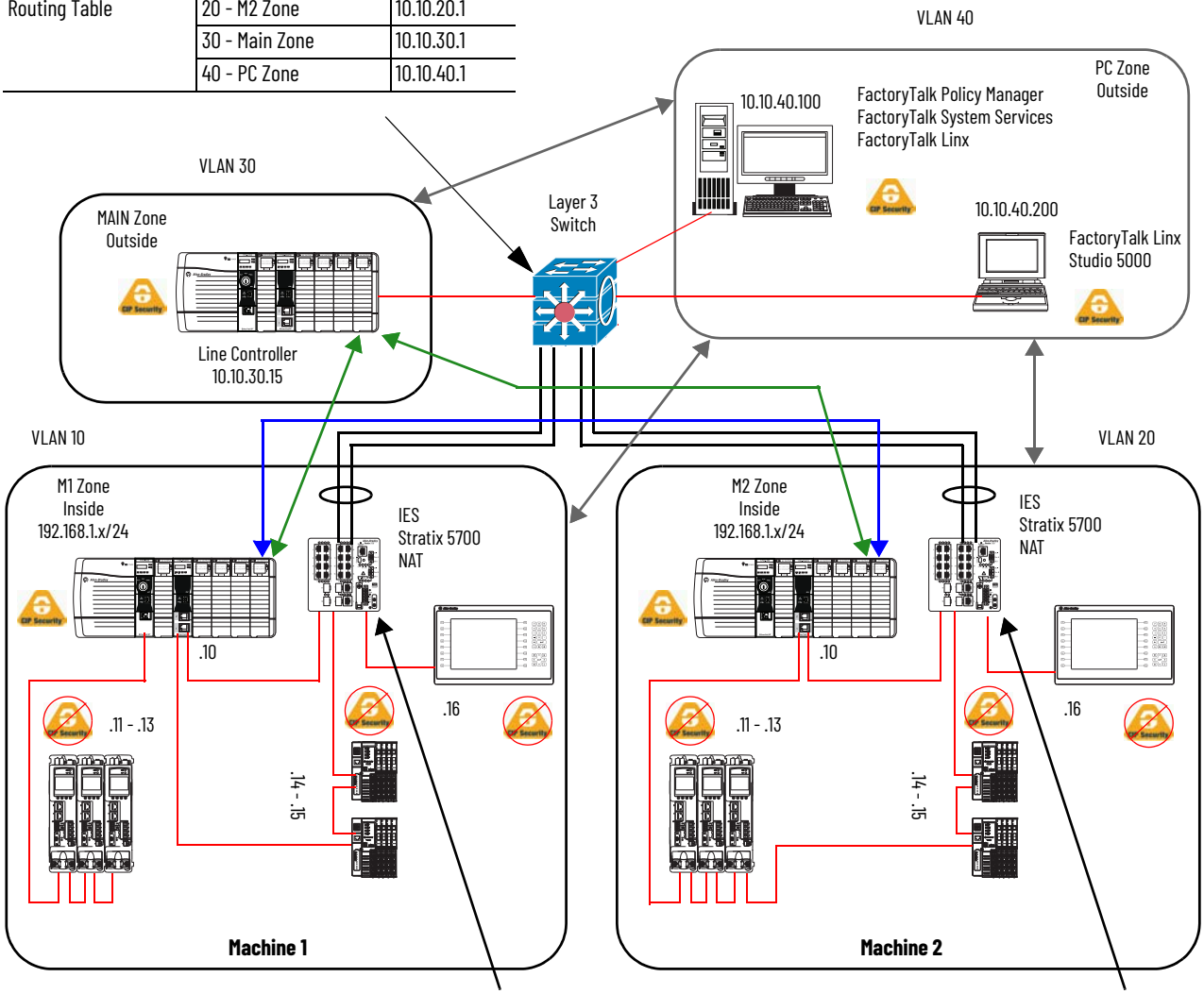
Network Address Translation

Network Address Translation (NAT) is supported with CIP Security only if the computer/server with FactoryTalk Policy Manager can access the CIP Security endpoint via an IP address. That is, the devices behind the NAT have IP addresses that are accessible from devices on the outside.

In this example, the 1756-EN4TR in M1 Zone (Machine 1) can use CIP Security because the Stratix® 5700 switch performing the NAT contains a NAT translation for the 1756-EN4TR and a Gateway Translation. When NAT with routing is configured correctly, the outside computer/server with FactoryTalk Policy Manager can access the CIP Security endpoint via the Outside translated IP address that is configured in the Stratix 5700 switch.

It's important that NAT is properly configured before you apply any CIP Security implementation. For more information, see Deploying Network Address Translation within a CPwE Architecture Design and Implementation Guide, publication ENET-TD007.

	VLAN ID - Description	IP Address
Routing Table	10 - M1 Zone	10.10.10.1
	20 - M2 Zone	10.10.20.1
	30 - Main Zone	10.10.30.1
	40 - PC Zone	10.10.40.1



	Device	Inside	Outside
Inside to Outside NAT Table	M1 1756-EN4TR	192.168.1.10	10.10.10.10
Gateway Transition		Outside	Inside
		10.10.10.1	192.168.1.1

	Device	Inside	Outside
Inside to Outside NAT Table	M2 1756-EN4TR	192.168.1.10	10.10.20.10
Gateway Transition		Outside	Inside
		10.10.20.1	192.168.1.1

Conduit Types

- (Outside) Device to (Inside) Device
- (Inside) Device to (Inside) Device
- (Outside) Device to (Inside) Device and (Outside) Zone to (Outside) Zone

Policy Provisioning

CIP Security protocol policies can only be deployed over an EtherNet/IP network. A device must reside on the same physical Ethernet network as FactoryTalk Policy Manager server or on a different network that is connected with a router. Policy deployment over multiple different networks and platforms using CIP Bridging is not supported.

For example, in Figure 8 on page 34, you can deploy CIP Security policies to Kinetix 5700 Drives_1 and Kinetix 5700 Drives_2 because they are on the same physical Ethernet network.

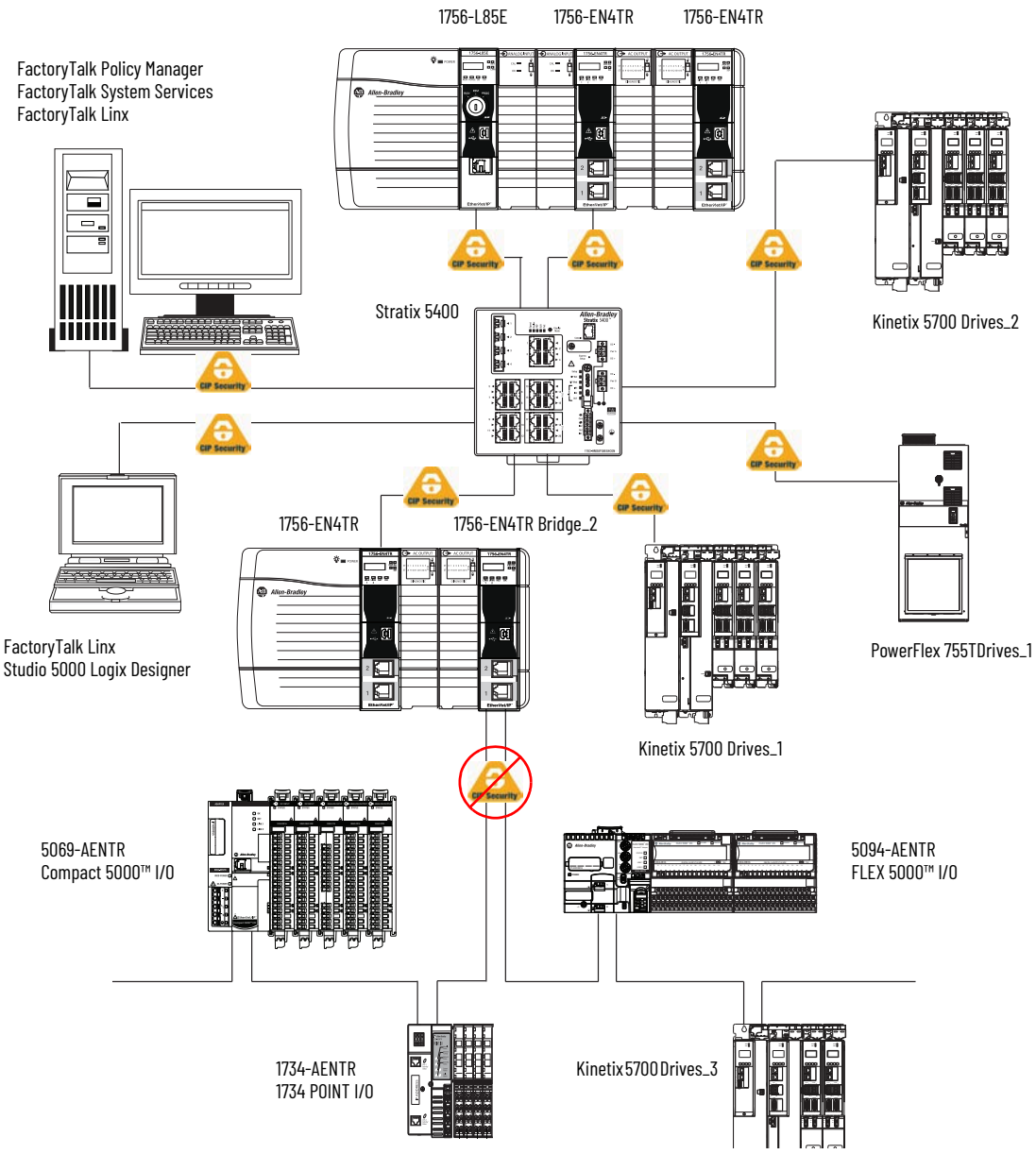
You can't provision the policy to Kinetix 5700 Drives_3 because it is on a different physical network. Even though CIP allows communication bridging over multiple networks and backplanes, CIP Security is effective only on one (or multiple-routed) network and FactoryTalk Policy Manager software does deploy policies accordingly.

To provision CIP Security policies to devices connected to 1756-EN4TR Bridge_2, like 5069-AENTR, 5094-AENTR and Kinetix 5700 Drives_3, you must have a second instance of FactoryTalk Policy Manager connected directly on that physical Ethernet network.

CIP Security is easier to deploy and manage in flat EtherNet/IP networks that are designed and implemented according to Connected Plant-wide Ethernet principles. For more information, see Deploying CIP Security within a Converged Plantwide Ethernet Architecture document.

For more information, see Deploying CIP Security within a Converged Plantwide Ethernet Architecture, publication ENET-TD022.

Figure 8 - Policy Provisioning



CIP Bridging Control

IMPORTANT CIP Bridging Control is only available with FactoryTalk Policy Manager software, version 6.30 and later.

CIP Security policies define which EtherNet/IP-enabled devices can communicate securely with each other, for example, whether a ControlLogix 5580 controller can communicate securely with a 1756-EN4TR communication module. CIP Bridging Control compliments those policies.

The following device families support CIP Bridging Control:

- CompactLogix 5380 controllers, firmware revision 34.011 or later
- ControlLogix 5580 controllers, firmware revision 32.011 or later
- ControlLogix 1756 EN4TR EtherNet/IP communication modules, any firmware revision

The following are the benefits of using CIP Bridging Control:

- Prevent someone from accessing a secured network from an unsecured network via backplane, for example, via a 1756-EN2TR EtherNet/IP communication module.
- Prevent someone from accessing a secured network from a USB port either directly via a CIP Security-enabled device, for example, ControlLogix 5580 controller, or indirectly via a non-CIP Security-capable device, for example, a 1756-EN2TR EtherNet/IP communication module over a backplane.

CIP Bridging Control Example

This example describes how you can use CIP Bridging Control to isolate secure and unsecure communication.

It's common for modern devices to be part of a larger platform connected via a backplane. Some of them, for example, ControlLogix systems, let you combine many communication modules for network-to-network connectivity.

With the introduction of CIP Security, many existing control system owners are challenged by the requirement to define an adoption strategy that becomes a multi-step process that secures only certain parts of IACS in each step. This scenario can create a backdoor to secure networks. Controlling CIP bridging can help to close that backdoor.

In Figure 9 on page 36, there are two parts to the application:

- The ControlLogix chassis is configured to segment EtherNet/IP network traffic so that each of the three 1756-EN2TR EtherNet/IP communication modules connect to a different physical Ethernet network.

  In this case, CIP communication can occur using CIP bridging between the two I/O networks or between an I/O network and the HMI/supervisory network.
- In the second diagram, CIP Security is implemented so that you can make a secure connection to the ControlLogix 5580 controller from either workstation and prevent access to the secured network via the other EtheNet/IP communication modules in the chassis.

  To implement CIP Security, you complete the following steps.

  a. You replace the 1756-EN2TR EtherNet/IP communication module in slot 1 with a 1756-EN4TR EtherNet/IP communication module.

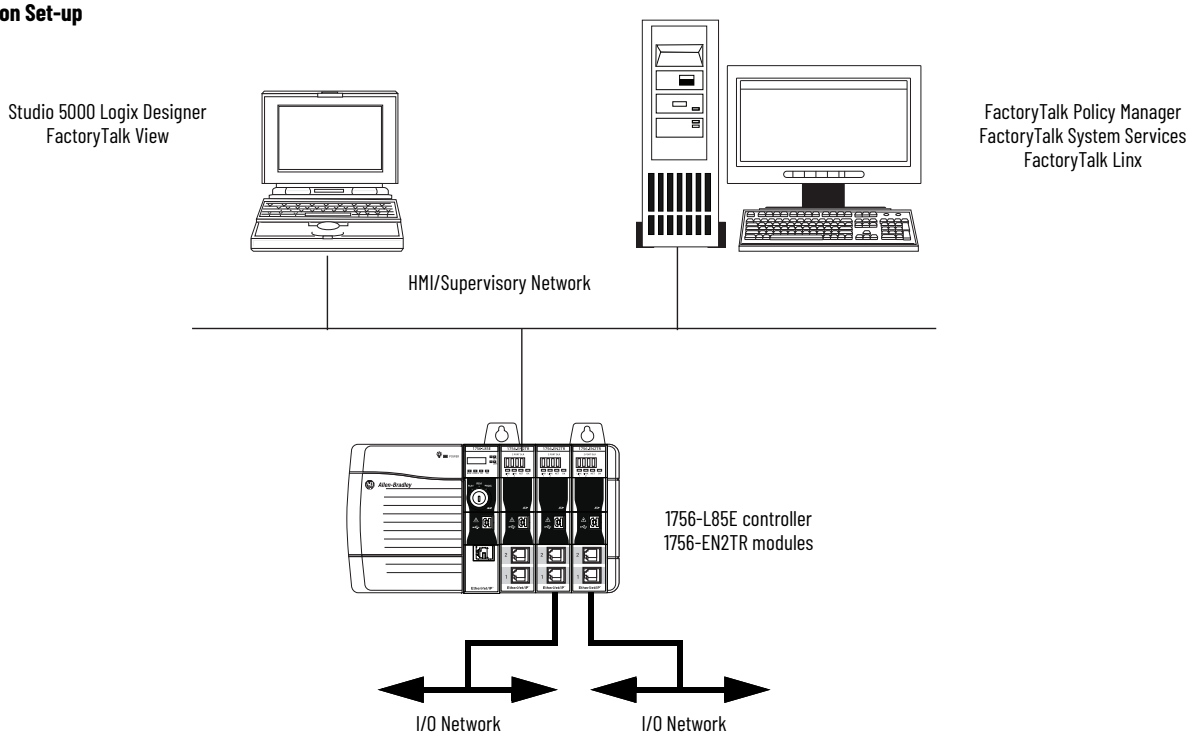
  b. In FactoryTalk Policy Manager software, you update, and deploy, the security model so that the connection to the 1756-EN4TR EtherNet/IP communication module is secured.

  c. In FactoryTalk Policy Manager software, you use CIP Bridging Control on the 1756-EN4TR EtherNet/IP communication to prevent communication to and from the 1756-EN4TR EtherNet/IP communication module and either of the 1756-EN2TR EtherNet/IP communication modules.

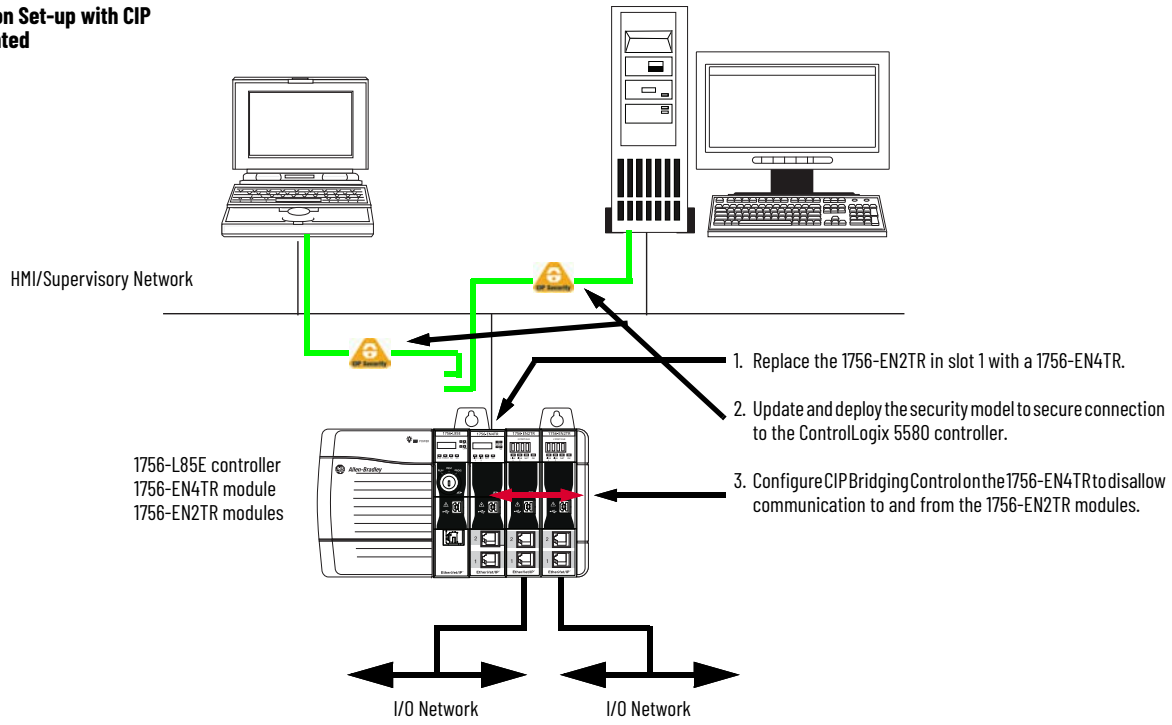
     By doing so, no device on the networks that is connected to the 1756-EN2TR EtherNet/IP communication modules can access the secured network.

Figure 9 - CIP Bridging Control Example

Initial Application Set-up



Updated Application Set-up with CIP Security Implemented



Implementing CIP Bridging Control

For information on how to implement CIP Bridging Control, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

Use of I/O Connections in Redundancy Configuration

Currently, you **can't** establish secure connections with I/O devices in a ControlLogix Redundancy system.

However, you can establish CIP Security Class 3 connections to a 1756-EN4TR communication module in a redundant configuration to secure Studio 5000 Logix Designer connections.

For information on how to secure programming connections to ControlLogix Redundancy systems, see the CIP Security Proxy User Manual, publication 1783-UM013.

Automatic Device Configuration (ADC)

ADC is a feature in Logix Designer application supports the automatic download of configuration data once a Logix 5000 controller establishes a connection to a drive and its associated peripherals.

After device configuration is downloaded, you must add the drive to the security model and deploy it to establish secure connections with the drive.

This applies whether the drive is CIP Security-capable and connected directly to the network or non-CIP Security-capable and connected via a 1783-CSP CIP Security Proxy.

Disable CIP Security

You can use FactoryTalk Linx software, version 6.30.00 or later, to disable CIP Security on a device. The following are examples of why you would disable CIP Security on a device:

- To eliminate unwanted notifications from IT port scanning applications for devices that are CIP Security-capable but do not have CIP Security implemented
- To prevent a malicious actor with access to the local network from configuring CIP Security on the device. Such an action by a malicious actor will prevent legitimate users and devices from communicating with the device.
- By disabling CIP Security, you also disable Automatic Policy Deployment.

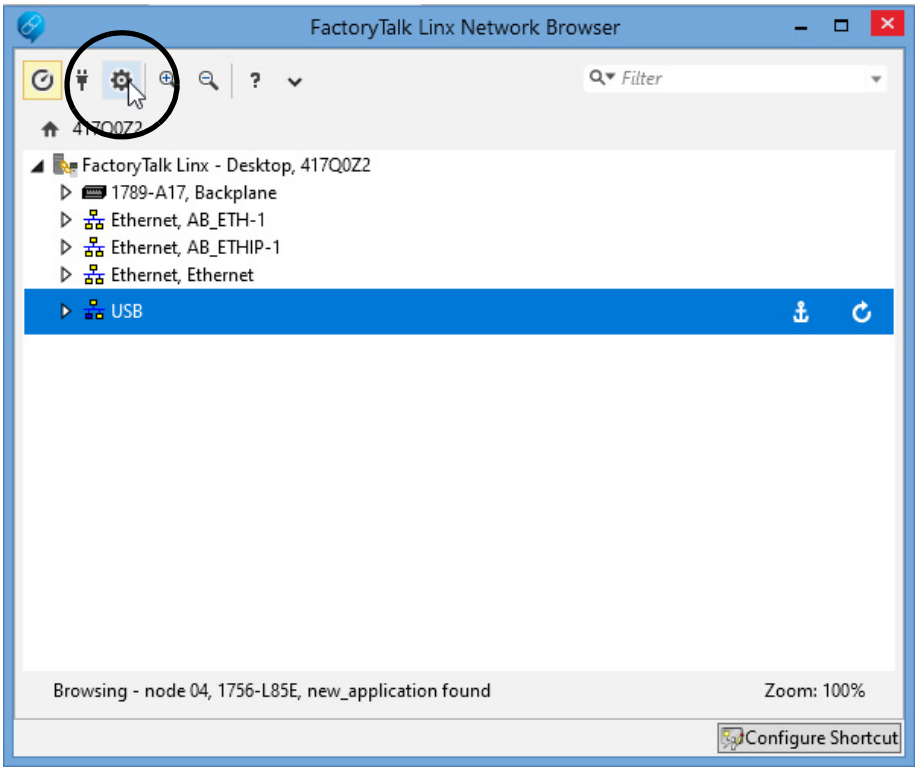
To disable CIP Security in FactoryTalk Linx software, you must disable Port 2221. If you disable CIP Security on a device, you must re-enable the port before you can implement CIP Security on the device again.

IMPORTANT	To re-enable Port 2221, you must reset the device to its factory default settings. Before you reset a device to its factory default settings, consider the impact on your control system. For example, if you reset a ControlLogix 5580 controller to its factory default state, it clears the application program from the controller, requiring you to download it again.

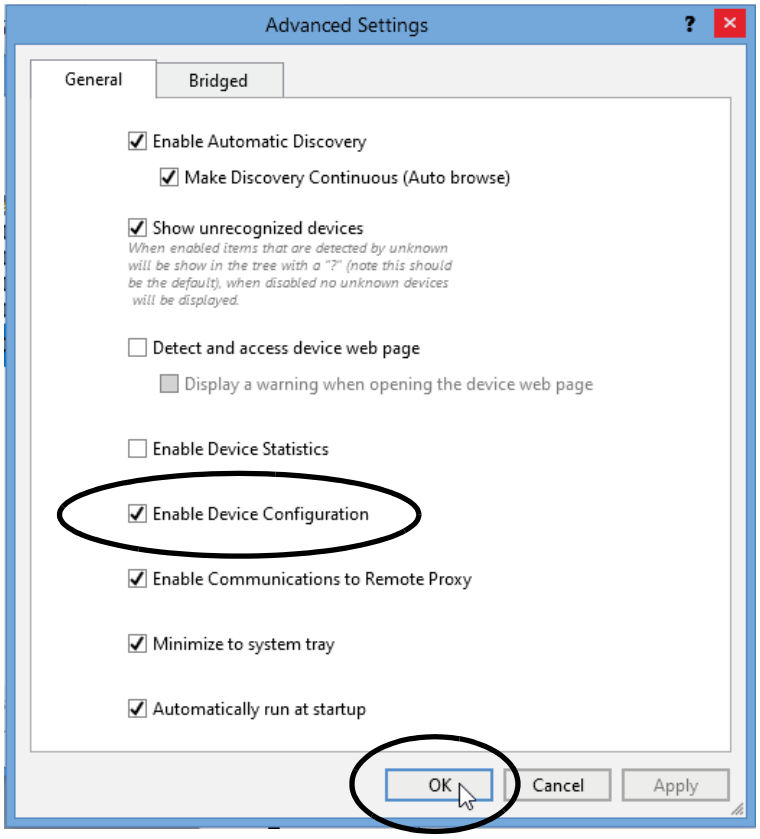
Complete the following steps.

These steps were completed with FactoryTalk Linx software, version 6.40. If you are using a different version, the screens can appear differently. The tasks that are described might vary slightly but accomplish the same goal of disabling CIP Security on a device.

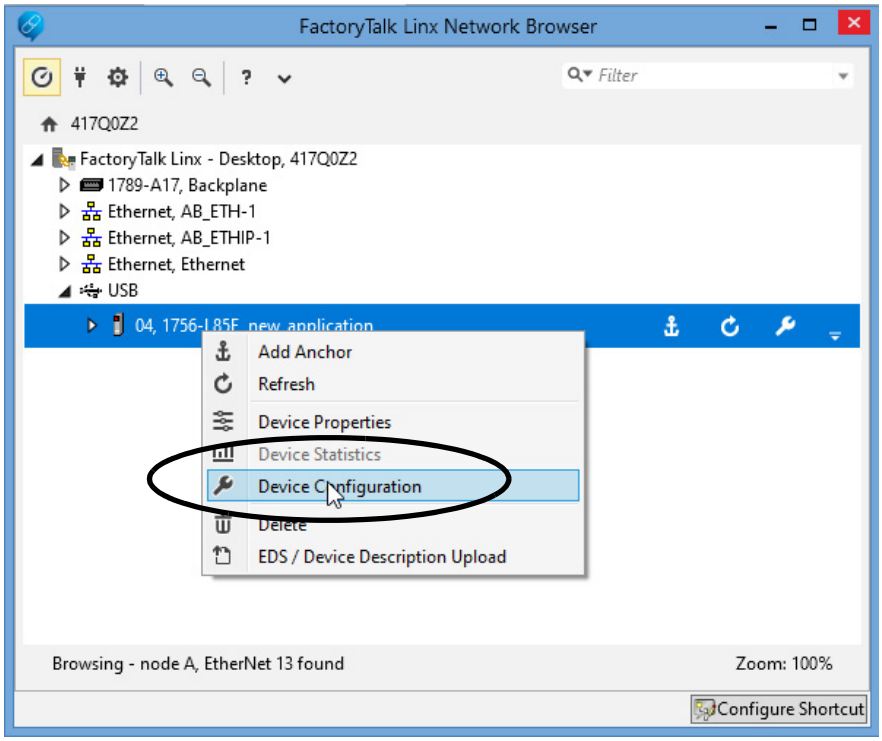
1. Click the Advanced Settings icon.



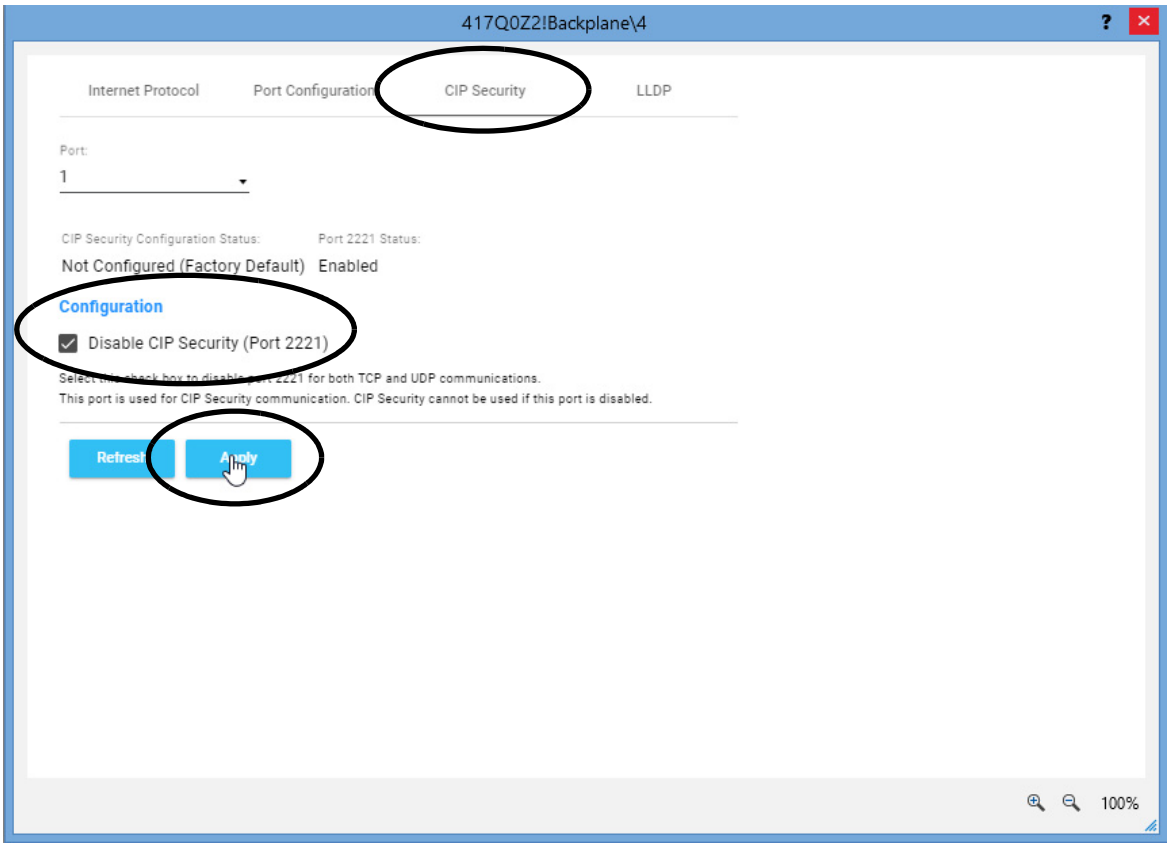
2. On the General tab of the Advanced Settings dialog box, enable Enable Device Configuration if it's not already enabled, and click OK.



3. On the FactoryTalk Linx Network Browser dialog box, navigate to the device.
4. Right-click on the device, and choose Device Configuration.



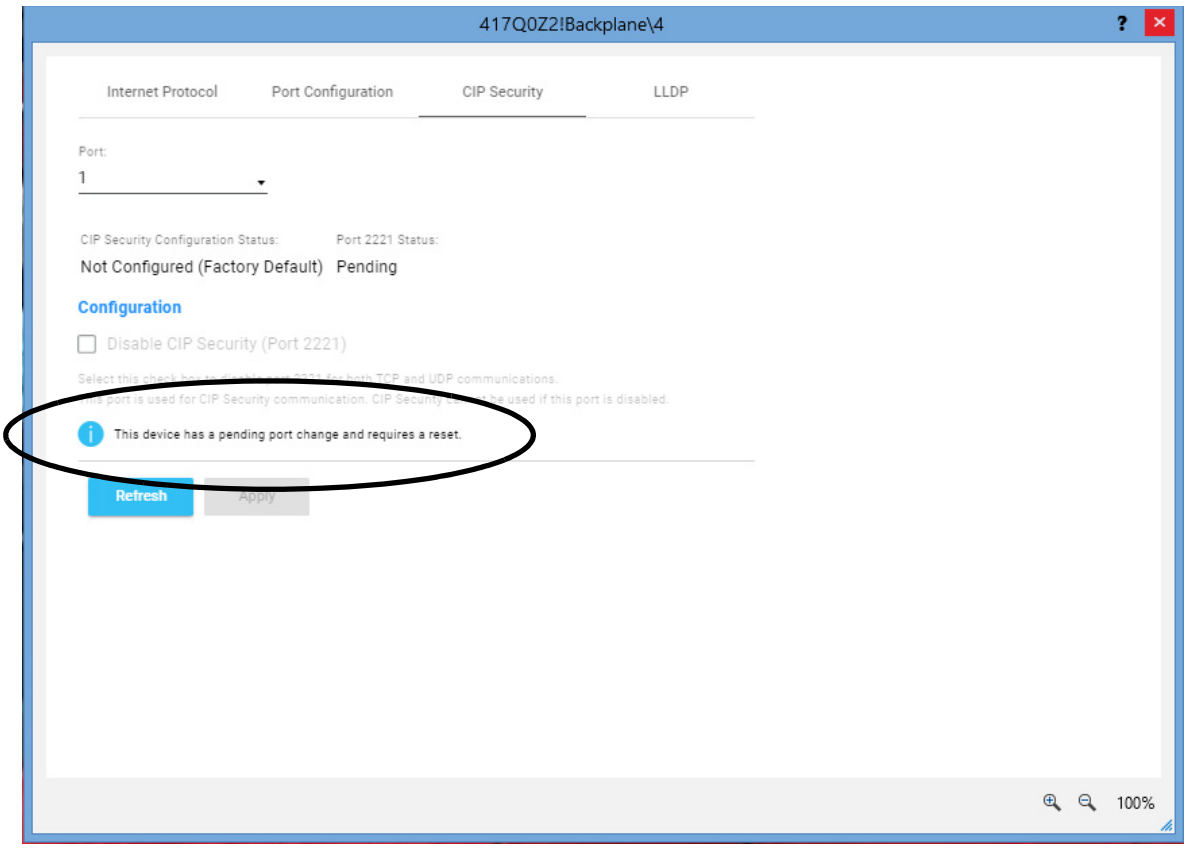
5. On the next dialog box, complete the following steps.
   a. Click the CIP Security tab.
   b. Select the Disable CIP Security (Port 2221) checkbox.
   c. Click Apply.



6. When the warning dialog box appears prompting you to continue the process, click Yes.

7. When the dialog box indicates that CIP Security was successfully disabled, click Close.

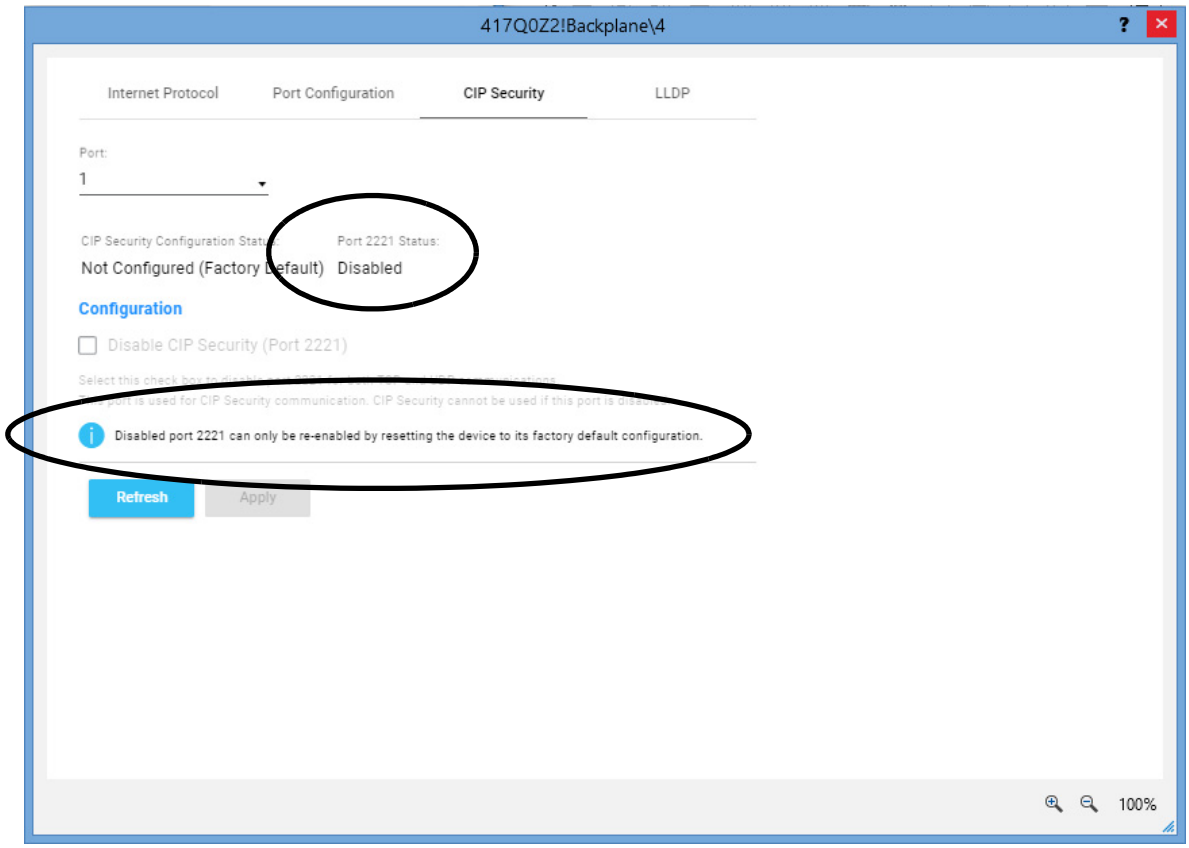
The dialog box appears that indicates the port status is pending and that a device reset is required for the change to take effect.



8. Reset the device.

   For example, if you need to disable Port 2221 on a ControlLogix 5580 controller, you can remove it from the chassis and reinsert it in the chassis to reset it.

   If you navigate to the device's configuration in FactoryTalk Linx software as described in this section, you see that Port 2221 is disabled and, thus, CIP Security is disabled on the device.



IMPORTANT To re-enable Port 2221, you must reset the device to its factory default settings. Before you reset a device to its factory default settings, consider the impact on your control system.

For example, if you reset a ControlLogix 5580 controller to its factory default state, it clears the application program from the controller, requiring you to download it again.

This is also true for re-enabling Automatic Policy Deployment (APD).

Add Legacy Devices to the Security Model

You can add legacy devices to the security model and use Trusted IP to communicate with other devices in IACS.

However, because such a configuration can result in an unauthorized device, for example, a hijacked device, or a spoofed IP address, we recommend that you do not connect legacy devices to the IACS.

We recommend that you consider adding legacy devices to security model only if they are intended to initiate connections with secured devices and you accept the associated risk.

RSLinx Classic Software

You **can't** use RSLinx® Classic software to implement CIP Security in an IACS network. You must use FactoryTalk Linx, version 6.11 or later.

Subject Alternative Name

If the certificates used to establish CIP Security are not complete, an attacker can effect packet routing through TCP/IP based attacks on network traffic, for example, via spoofing. This can let an attacker redirect legitimate communication from an intended target to a different one.

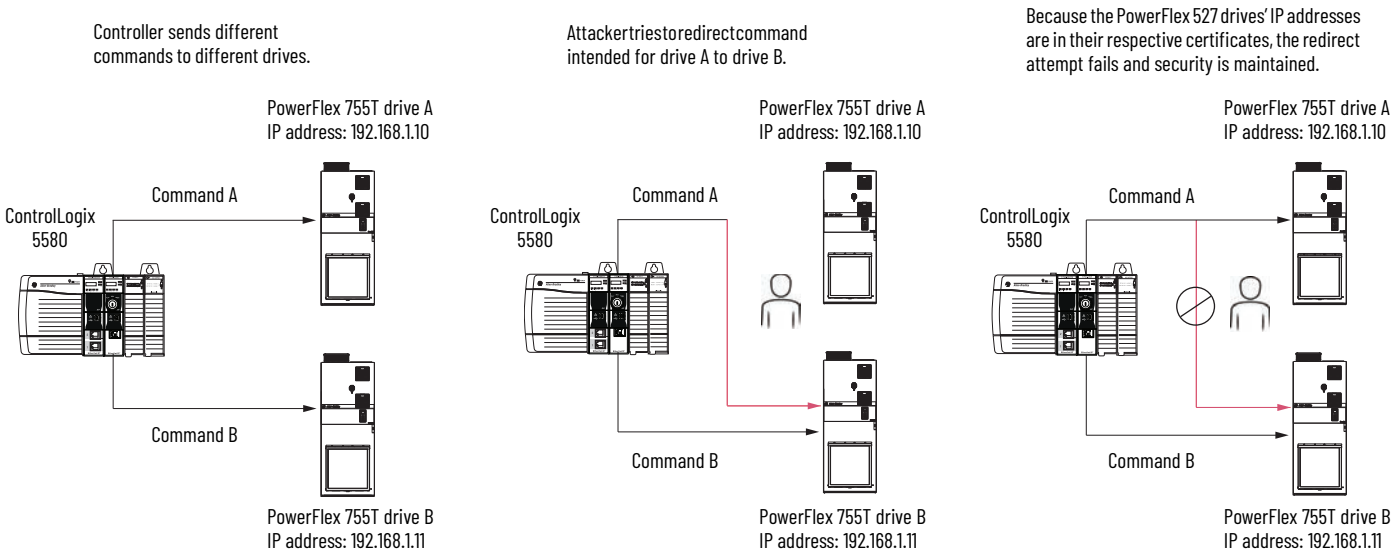
Subject Alternative Name increases the degree of security on a connection to a trusted device. The feature confirms that not only is the target device a trusted device but also that it is the actual device to which the connection must be made. It helps prevent against specific communication redirect attacks.

With Subject Alternative Name configured, the device's IP address is used as a unique identifier and added to the Subject Alternative Name field in the trusted device's certificate. A connection attempt between devices is successful if the IP address in the Subject Alternative Name field of the certificate matches the IP address of the intended target device in the connection. Connection originators, for example, a ControlLogix 5580 controller or 1756-EN4TR communication module, check the trusted device's certificate for the IP address before establishing a secure connection.

For example, Figure 10 shows a ControlLogix 5580 controller that sends commands to trusted PowerFlex 755T drives. The commands are unique to each drive, including the drive's IP address in its trusted certificate. An attacker intercepts command A that is intended for PowerFlex 755T drive A in an attempt to redirect it to PowerFlex 755T B.

Because the command includes drive A IP address = 192.168.1.10, and PowerFlex 755T drive B has an IP address = 192.168.1.11, the command is not sent to PowerFlex 755T drive B.

Figure 10 - Subject Alternative Name Example



IMPORTANT Subject Alternative Name is enabled by default with FactoryTalk® Policy Manager software, version 6.40.00 or later, and only connection originators can verify the Subject Alternative Name in a target device when making a secure connection.

If you change a device's IP address, you must redeploy the security model. Subject Alternative Name updates the IP address in the trusted certificate to match the new IP address on the device.

The following support Subject Alternative Name:

- ControlLogix 5580 controllers
- GuardLogix 5580 controllers, firmware revision 35.011 or later
- CompactLogix 5380 controllers, firmware revision 35.011 or later
- Compact GuardLogix 5380 controllers, firmware revision 35.011 or later

CIP Security Implementation Process

This section describes the overall process of implementing CIP Security™ with Rockwell Automation® products in a simple IACS.

For information on a more complex IACS, see CIP Security Implementation Example Architecture on page 79.

You can use the security assessment process to assign security levels to zones and conduits. We recommend that you assign zone and conduit security levels based on the potential consequences if an attack objective be achieved in that zone.

For more information, see Security Assessment on page 11.

Design and Install the System

You must install software on specific computers and connect hardware devices to EtherNet/IP™ networks. You download software at the Rockwell Automation Product Compatibility and Download Center (PCDC).

At a minimum, the IACS design should include the following information:

- Verification of the system components required to implement CIP Security into the IACS network.
- Inventory of existing devices and software, including firmware revisions.
- Detailed observation and documentation of intended system functions and operation.
- Detailed observation and documentation of required data flows between devices.

Remember, the system can include products that are CIP™ Security-capable and products that aren't. The list of CIP Security-capable products that are currently available from Rockwell Automation are listed at the following:

- CIP Security Software Applications on page 17
- CIP Security-capable Hardware Devices on page 18

IMPORTANT	We generally recommend that you design and implement your CIP Security model before you download your Logix Designer application project to a Logix 5000 controller. However, there are some systems in which it is more appropriate to download a project to the system before you implement CIP Security.

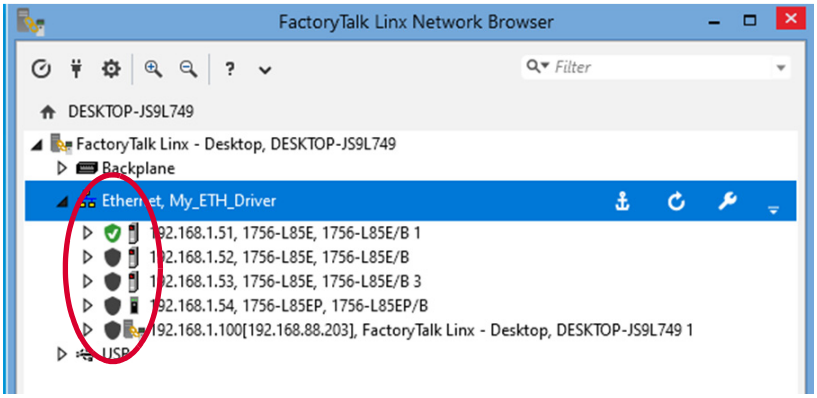
Identify CIP Security-capable and CIP Security-enabled Devices

In FactoryTalk Policy Manager software, version 6.20 or later, and FactoryTalk Linx software, version 6.20 or later, icons next to devices in browsed lists indicate the CIP Security-capable state. This functionality is disabled in FactoryTalk Linx software by default. You must enable it.

Table 8 - CIP Security Device State Icons

Icon	Description
	The device is CIP Security-capable, but no configuration action has been taken yet.
	The device is CIP Security-capable and is in the CIP Security configuration process.
	The device is CIP Security-capable and is active.
	The device is CIP Security-capable but CIP Security is disabled.
	The device is CIP Security-capable, but there is an error in the configuration.

The following example shows the CIP Security status of ControlLogix 5580 controllers in FactoryTalk Linx Network Browser.



 If a device does not support CIP Security, there is no icon in front of it.

Unsecure Device Management

You can connect unsecure devices to an IACS with CIP Security implemented. In this case, the unsecure device is a target device and is not in the CIP Security model. Devices in the CIP Security model can transmit data to the unsecure device. The unsecure device, however, cannot transmit data to the devices in the model.

Identify, Organize, and Create Zones

Zones are groups to which devices are added. Devices that share security requirements for a particular function, and you want to trust each other, can be added to the same zone.

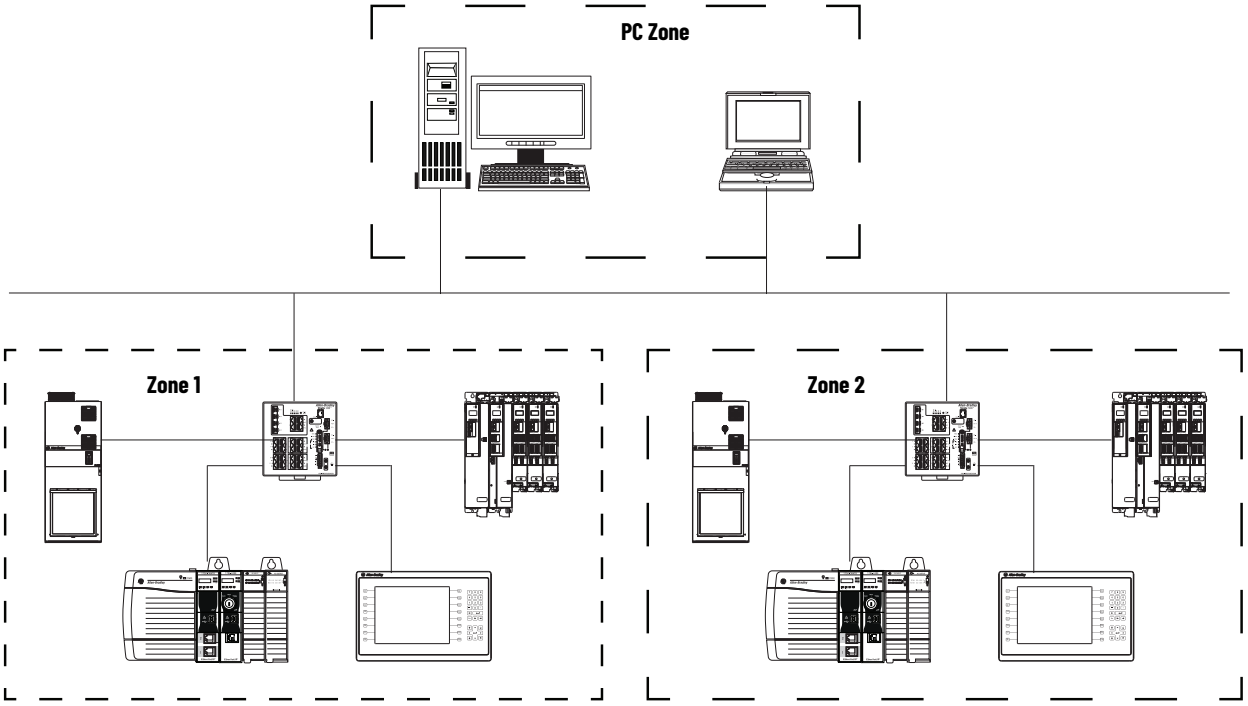
When devices are added to the zone, communication between the devices is implied while still letting mutual trust be established through an exchange of certificates or pre-shared keys. It's worth noting that any device in a zone that is deemed to be 'trusted' is only trusted by other devices in the same zone, not all devices in the IACS.

For example, if a ControlLogix® 5580 controller and Kinetix® 5700 drives are added to Zone 1 and certificates are used with integrity, the devices are authenticated by exchanging certificates with each other.

If a zone includes devices that are non-CIP Security-capable and CIP Security-enabled devices, connections to the non-CIP Security-capable devices are **not secured** using standard ports.

You can create zones and add other computers/servers that do not use FactoryTalk Linx software but still require communications to IACS devices. The devices that do not use FactoryTalk Linx are added as generic devices. This lets you easily create Trusted IP conduits between the computers/servers to the IACS devices.

Figure 11 - System Implementation - Zones



After you identify and organize the zones, create a detailed security matrix that lists what devices occupy each zone. Table 9 is a security matrix with zones and devices.

Table 9 - Security Matrix - Zones and Devices

PC Zone	Zone 1	Zone 2
FactoryTalk Linx[1] FactoryTalk Policy Manager FactoryTalk System Services	ControlLogix® 5580 controller	ControlLogix 5580 controller
Studio 5000 Logix Designer®[2] FactoryTalk Linx FactoryTalk View	1756-EN4TR EtherNet/IP communication module	1756-EN4TR EtherNet/IP communication module
	Kinetix 5700 servo drives	Kinetix 5700 servo drives
	PowerFlex® 755T drive	PowerFlex 755T drive
	PanelView™ Plus terminal[3]	PanelView Plus terminal[3]

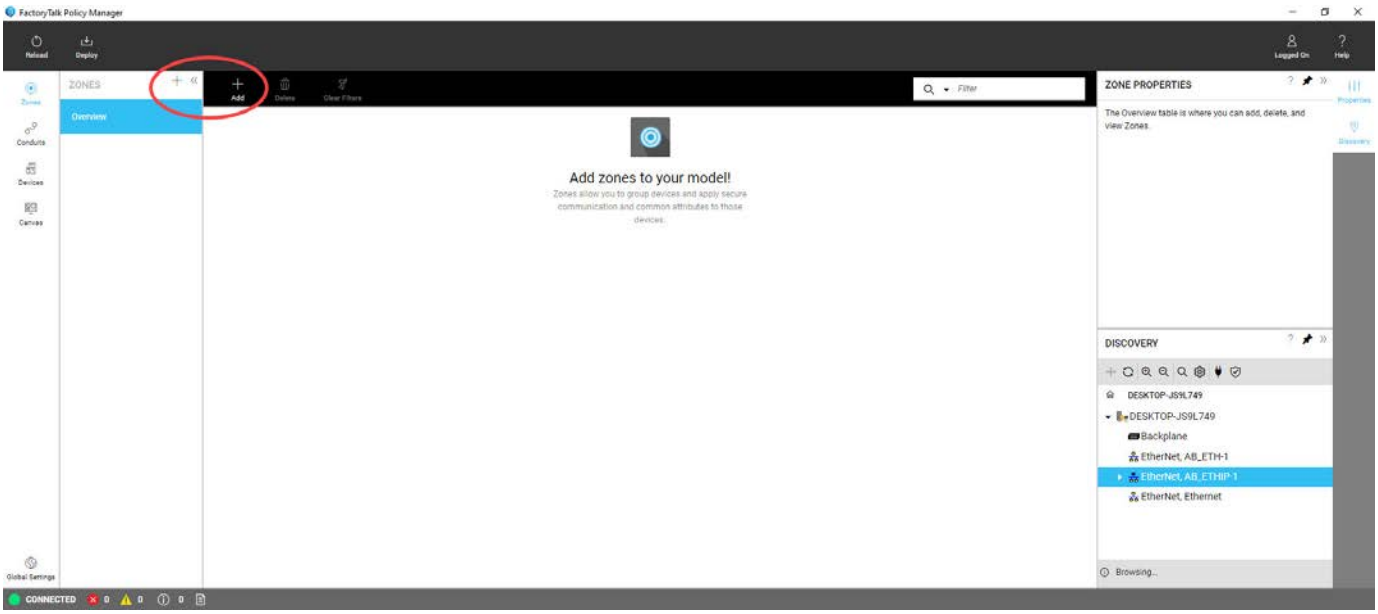
(1) This group of software is installed on the same server/computer.

(2) This group of software is installed on the same computer. It's a second computer, that is, another one from the server/computer on which FactoryTalk Linx, FactoryTalk Policy Manager, and FactoryTalk System Services is installed.

(3) This device is not CIP Security-capable.

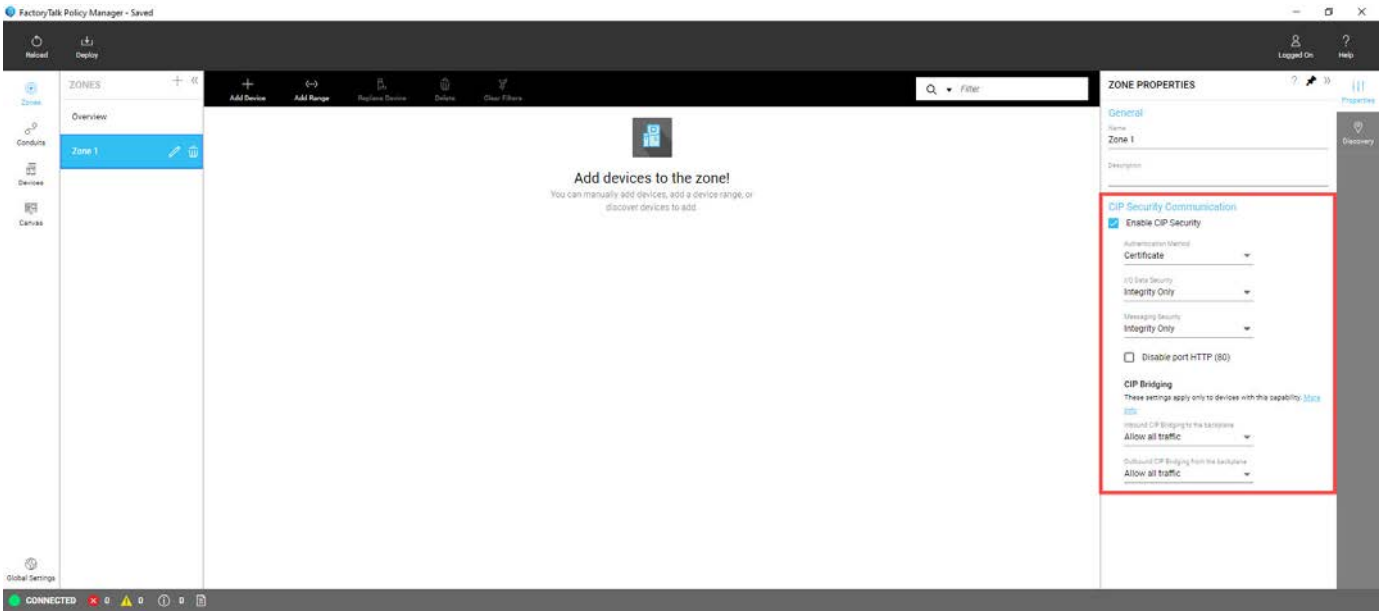
Create a Zone

1. In the FactoryTalk Policy Manager navigation bar, choose **Zones**.
2. On the toolbar next to **ZONES**, click [+].

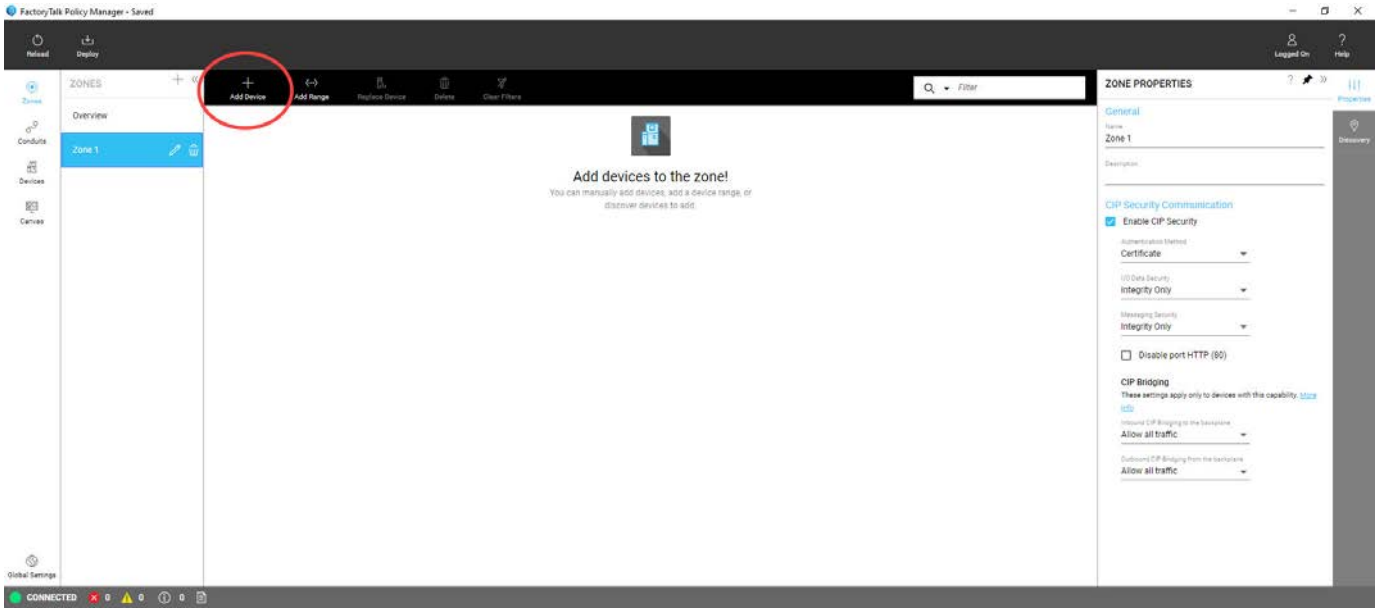


A zone is added to the list with the following default values:

- **Name** - Zone #
- **Description** - None
- **Enable CIP Security** - Not selected by default. Check Enable CIP Security to configure CIP Security-related settings.

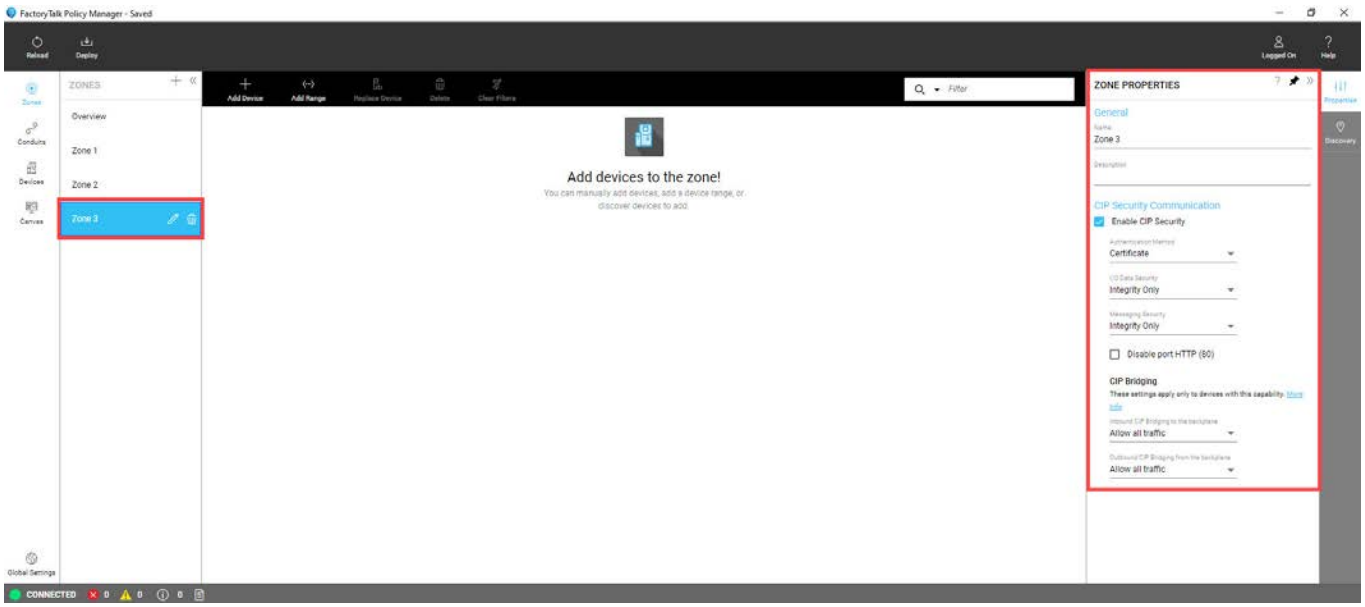


3. Add devices to the zone. You can add devices in three ways:
   - Discover devices via FactoryTalk Linx.
   - Manually add devices.

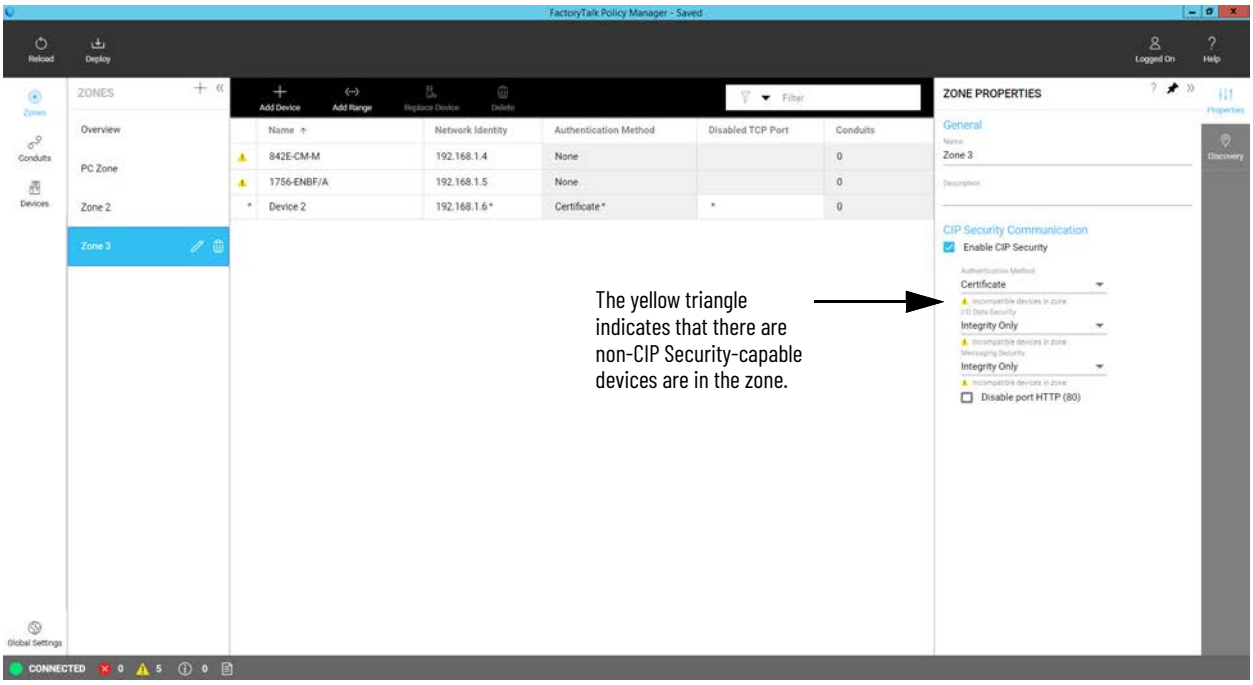


Configure the Zone

1. In the FactoryTalk Policy Manager navigation bar, choose **Zones**.
   The **ZONES** column displays a list of the configured zones.
2. In the **ZONES** column, choose a zone.
3. Change the properties of the zone as appropriate.



If a zone includes devices that aren't CIP Security-capable, a warning notification appears in the zone properties. An AllowedList isn't needed, however. All CIP Security-capable devices in the zone automatically allow this device.



For more information on zones, see the following:

- FactoryTalk Policy Manager software online help
- FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001

Identify, Organize, and Create Conduits

Conduits create explicit trusted communication pathways between zones, zones and devices, and between devices in separate zones. After you create, identify, and organize the conduits, update the security matrix to detail the conduits.

Figure 12 - System Implementation - Conduits

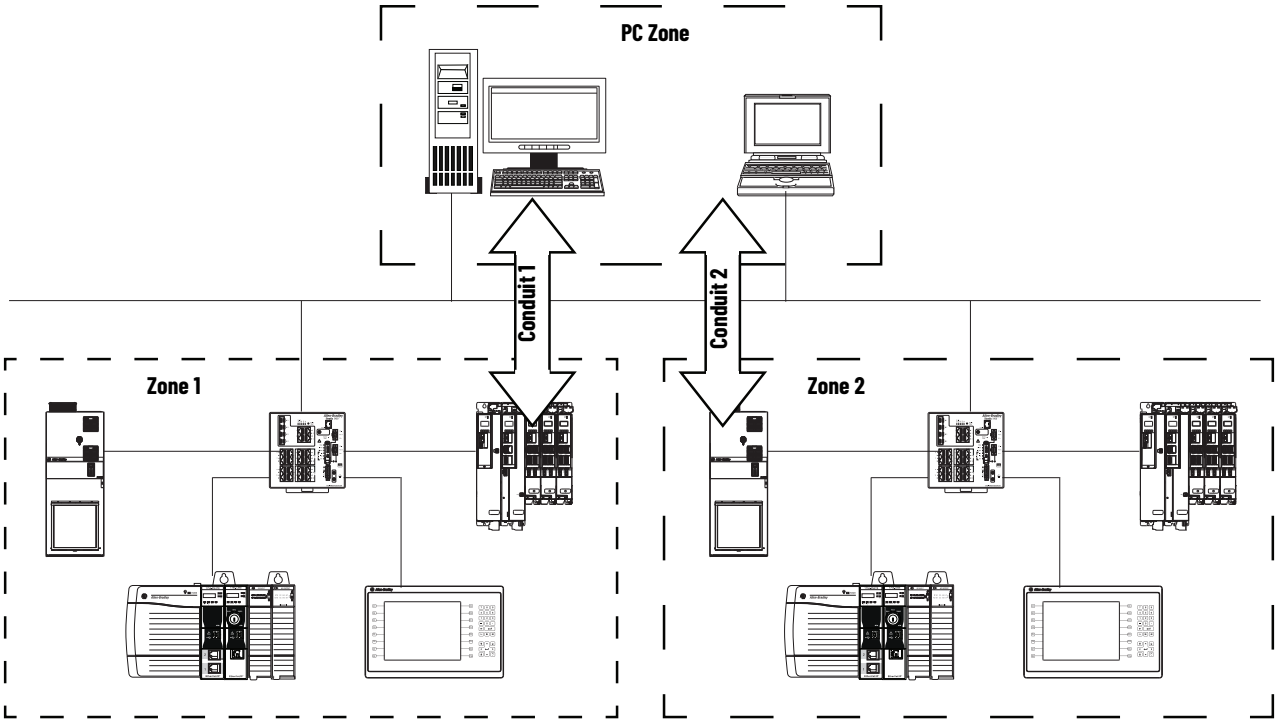


Table 10 is an example of an updated security matrix after conduits are identified and organized.

In the table, the Source row and Destination column cell intersections represent the endpoints of the Conduit between the zones. For example, cell at column 2/row 3 indicates that Conduit 2 uses a Zone-to-Zone pathway between PC Zone and Zone 2.

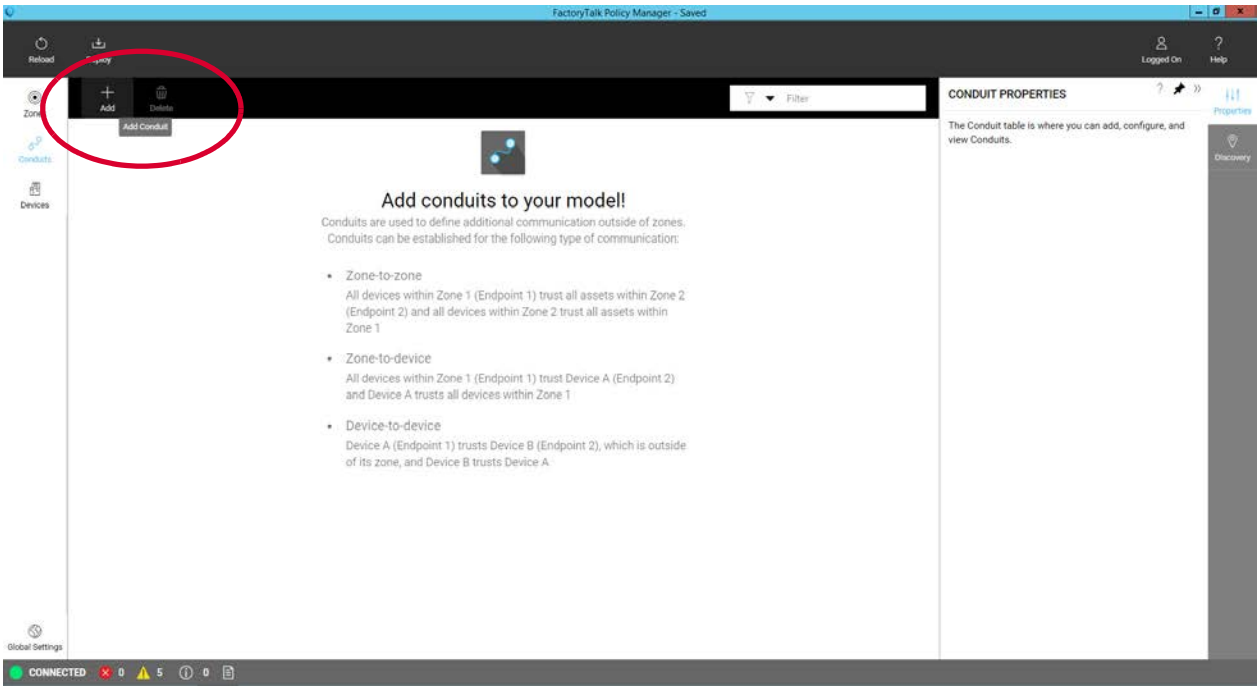
Table 10 - Security Matrix - Conduits

Source	Destination		
	PC Zone	**Zone 1**	**Zone 2**
PC Zone	Permit(1)	Conduit 1: Zone-to-Zone	Conduit 2: Zone-to-Zone
Zone 1	Conduit 1: Zone-to-Zone	Permit	Denied
Zone 2	Conduit 2: Zone-to-Zone	Denied	Permit

(1) Default permits pathway.

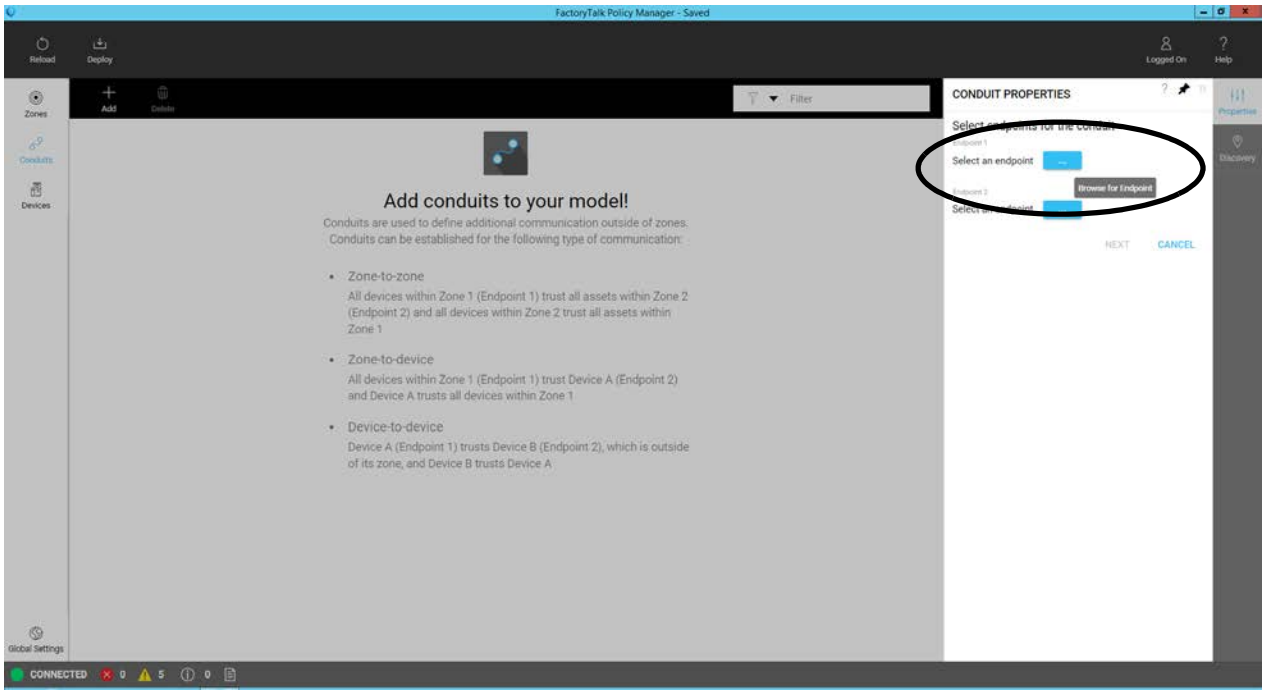
Create a Conduit

1. In the FactoryTalk Policy Manager navigation bar, choose Conduits.
2. On the toolbar, click [+].



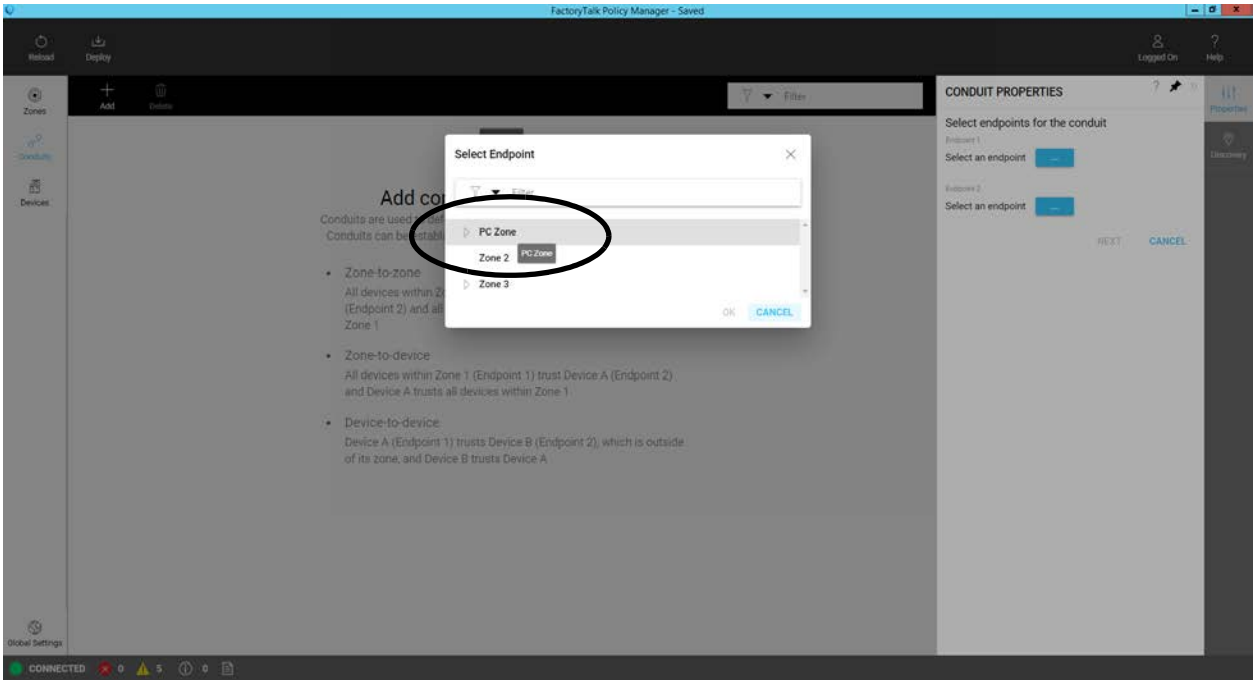
The **CONDUIT PROPERTIES** pane opens.

3. In **Endpoint 1**, next to **Select an endpoint**, choose **Browse for Endpoint [...]**.

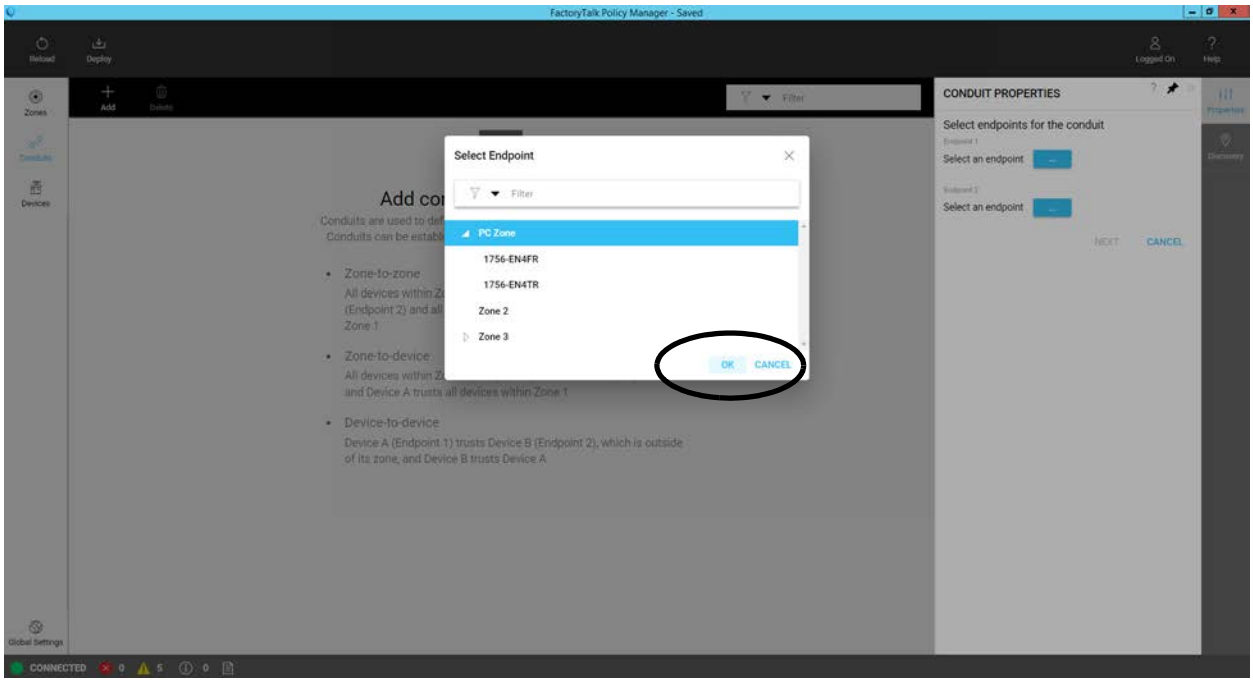


4. Select the **endpoint**.
   You can choose a zone or device to assign as the first endpoint of the conduit.

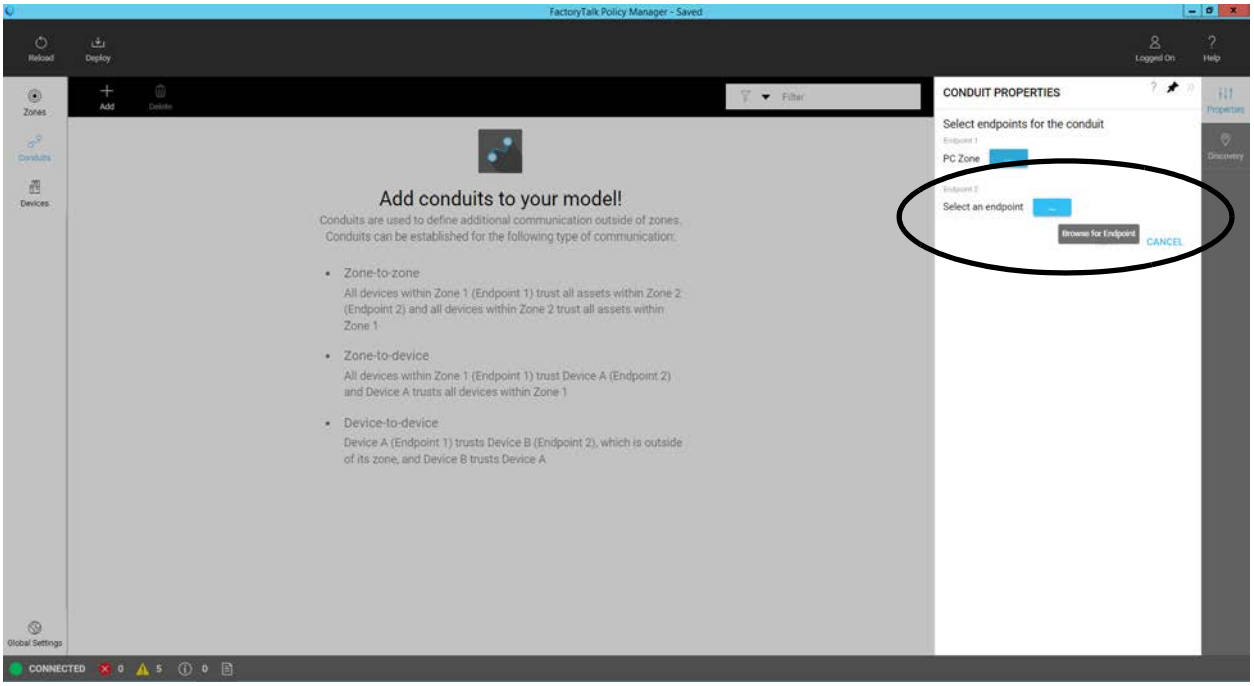
In Filter, you can type part of the name to list only endpoints that match that criteria.



5. Click OK.

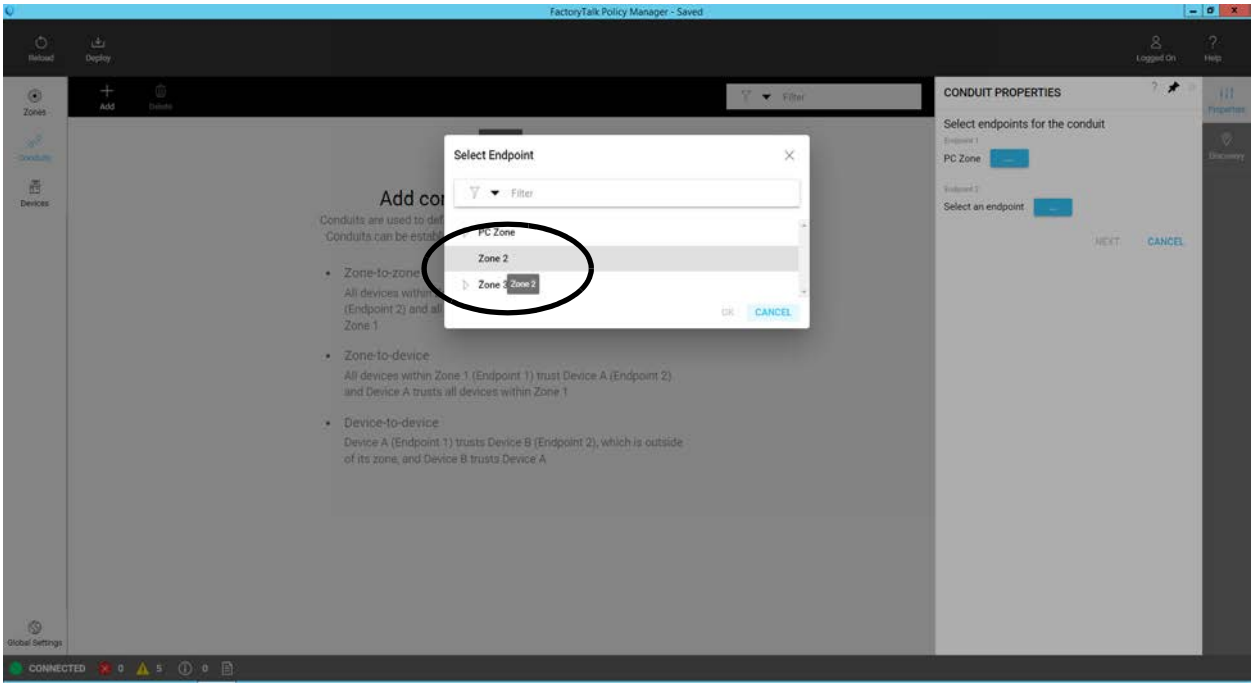


6. In **Endpoint 2**, next to **Select an endpoint**, choose **Browse for Endpoint [...]**.

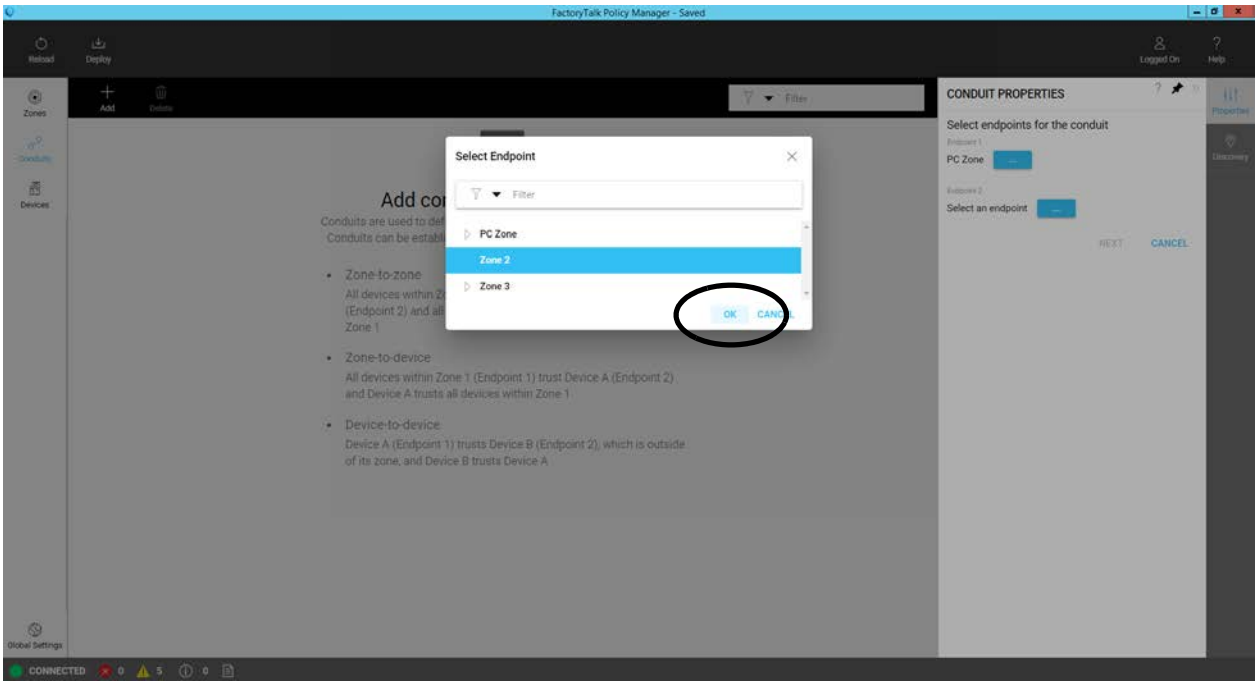


7. To assign as the second endpoint of the conduit, choose a zone or device.
   You can choose a zone or device to assign as the second endpoint of the conduit.

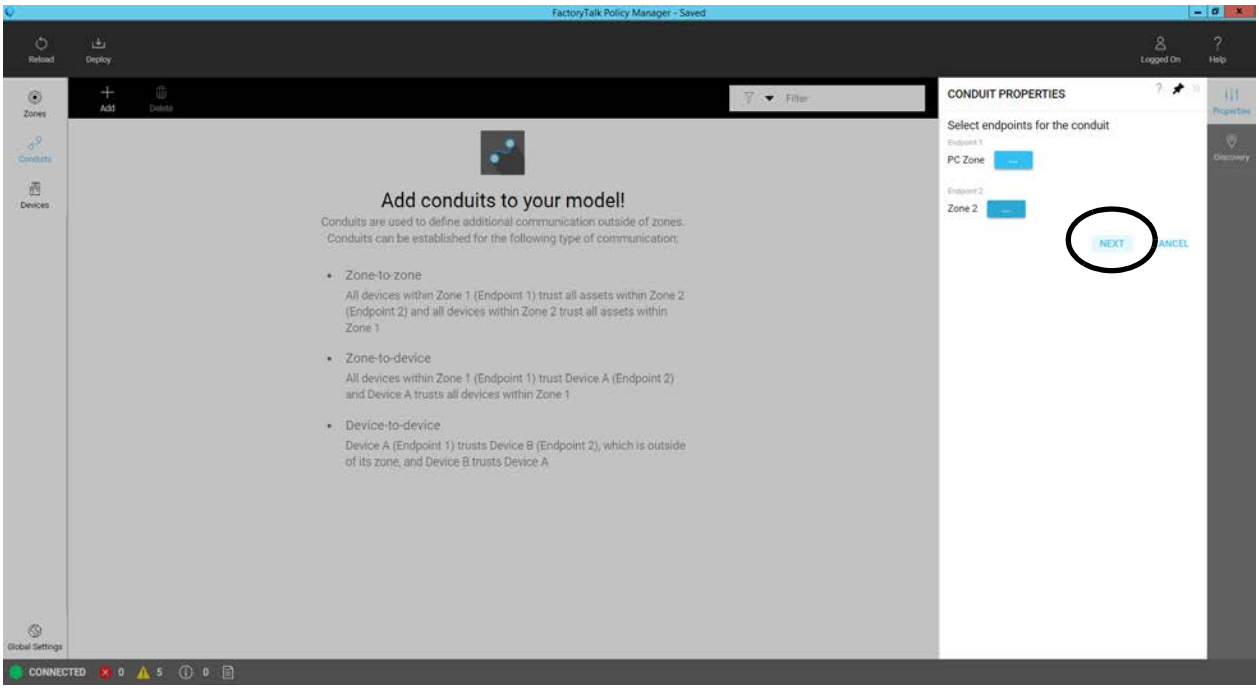
In Filter, you can type part of the name to list only endpoints that match that criteria.



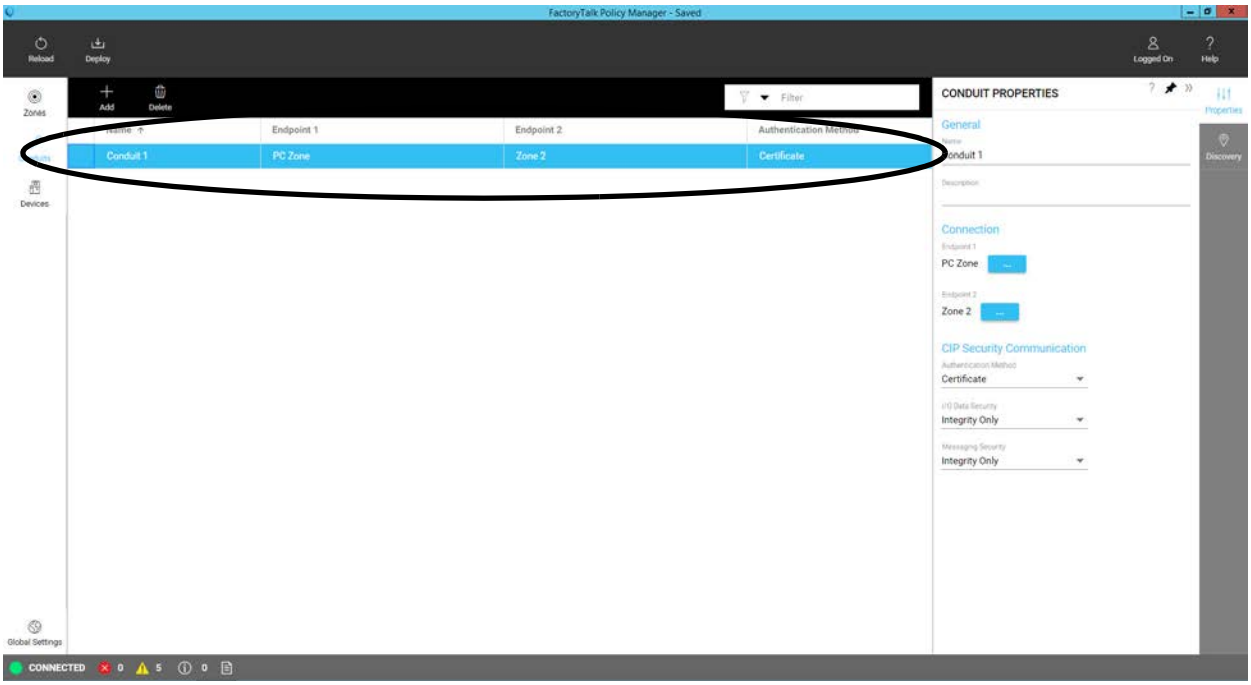
8. Click OK.



9. Click Next.



The first conduit appears in the Conduits list.

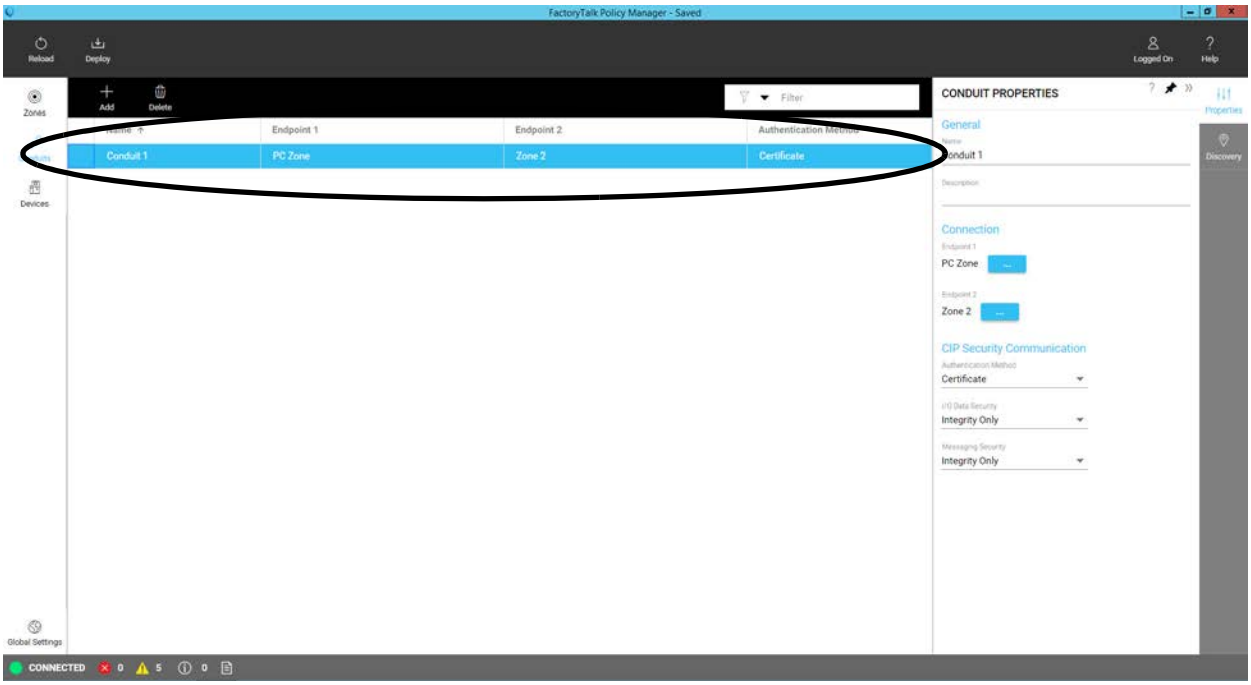


If you must create another conduit, repeat the process, starting at step 2 on page 52.

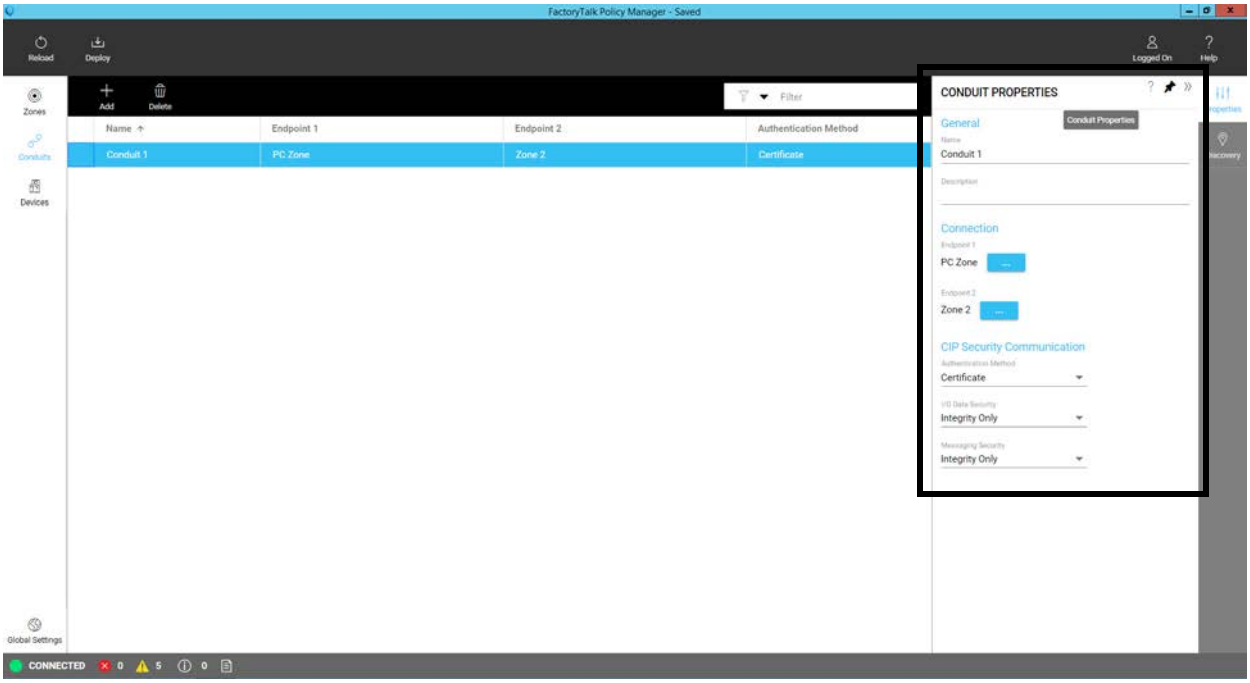
Configure the Conduit

1. In the FactoryTalk Policy Manager navigation bar, choose **Conduits**, and choose the conduit that you want to configure.

CONDUIT PROPERTIES is automatically opened to the most recently configured conduit.
To edit another conduit, select a conduit from the list to display its properties.



2. Change the conduit properties as needed.



If both endpoints are CIP Security capable, configure **CIP Security Communication**.

- In **I/O Data Security and Messaging Security** choose one of the following:
  - Integrity only - Use to check if the data or message was altered and reject altered information.
  - Integrity & Confidentiality - Use to check integrity plus encrypt the data or message so the corresponding decryption key is required to read the information. Rejects altered and/or untrusted information while also protecting the confidentiality of the information.
  - In **I/O Data Security**, click None to stop using additional security checks on I/O data.

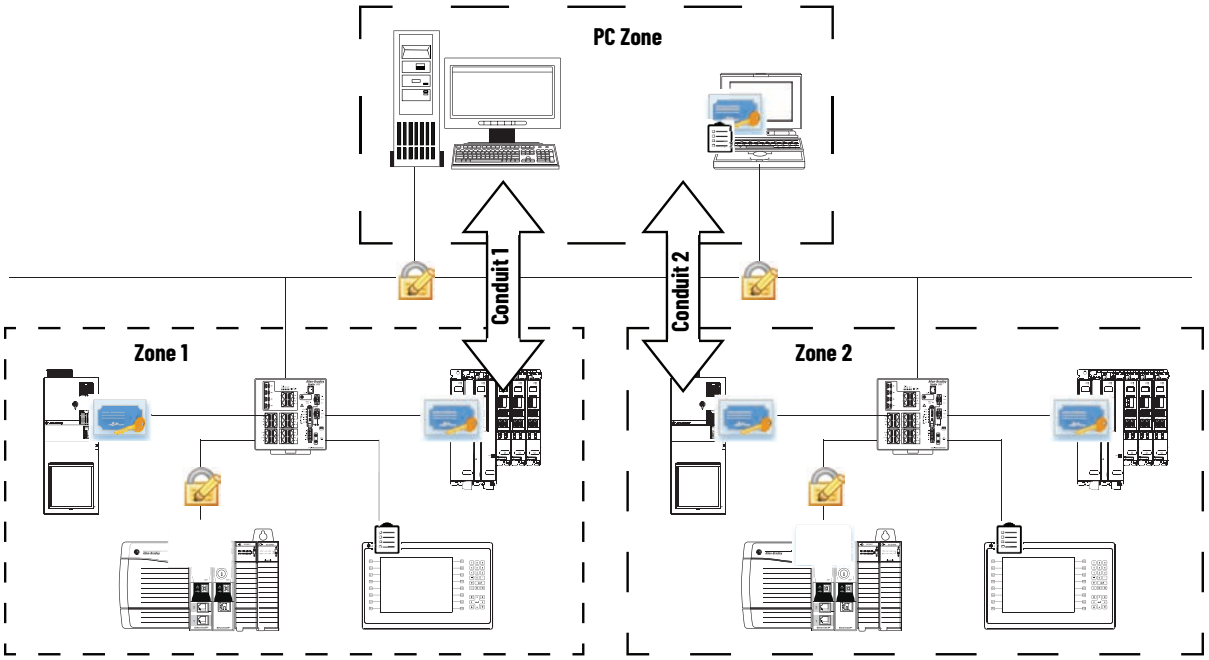
For more information on conduits, see the following:

- FactoryTalk Policy Manager software online help
- FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001

Identify and Create Security Features/Policies

Security policies are created based on device capabilities and operational functions of automation applications.

Figure 13 - System Implementation - Security Policies



After you identify and create security features/policies, update the security matrix that details applicable security policies between conduits. For example, enable certificates or pre-shared keys, enable/disable confidentiality and AllowedList.

Table 11 is an updated security matrix with security features and policies defined.

Table 11 - Security Matrix - Security Features and Policies

Conduit 1 **Secure FactoryTalk Linx Communication**	**Zone to Zone**		**Security Policy**
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Zone 1	• Certificates • Integrity • Confidentiality

Conduit 2 **Secure FactoryTalk Linx Communication**	**Zone to Zone**		**Security Policy**
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Zone 2	• Certificates • Integrity • Confidentiality

Trusted IP (AllowedList)	**Zone/Device to Zone/Device**		
(Non-CIP Security-capable devices)	PC Zone Device - FactoryTalk Network Manager (IP address: xxx.xxx.xxx.xxx)	Zone 1 - Devices	• Kinetix 5700 drive (IP address: xxx.xxx.xxx.xxx) • ControlLogix 5580 controller (IP address: xxx.xxx.xxx.xxx0 • 1756-EN4TR module (IP address: xxx.xxx.xxx.xxx) • PanelView Plus terminal: (IP address: xxx.xxx.xxx.xxx) • PowerFlex 755T drive (IP address: xxx.xxx.xxx.xxx)
		Zone 2 - Devices	• Kinetix 5700 drive (IP address: xxx.xxx.xxx.xxx) • ControlLogix 5580 controller (IP address: xxx.xxx.xxx.xxx0 • 1756-EN4TR module (IP address: xxx.xxx.xxx.xxx) • PanelView Plus terminal: (IP address: xxx.xxx.xxx.xxx) • PowerFlex 755T drive (IP address: xxx.xxx.xxx.xxx)

Deploy Security Model

After the zones, conduits, and devices security policies have been configured, the resulting security model can be deployed.

You click the Deploy button in FactoryTalk Policy Manager software to trigger FactoryTalk System Services to deploy the security model. FactoryTalk System Services runs in the background. You do not take action in the client.

IMPORTANT	Before a deployed security model becomes active, communication must be reset to all configured devices, resulting in a short loss of connectivity.

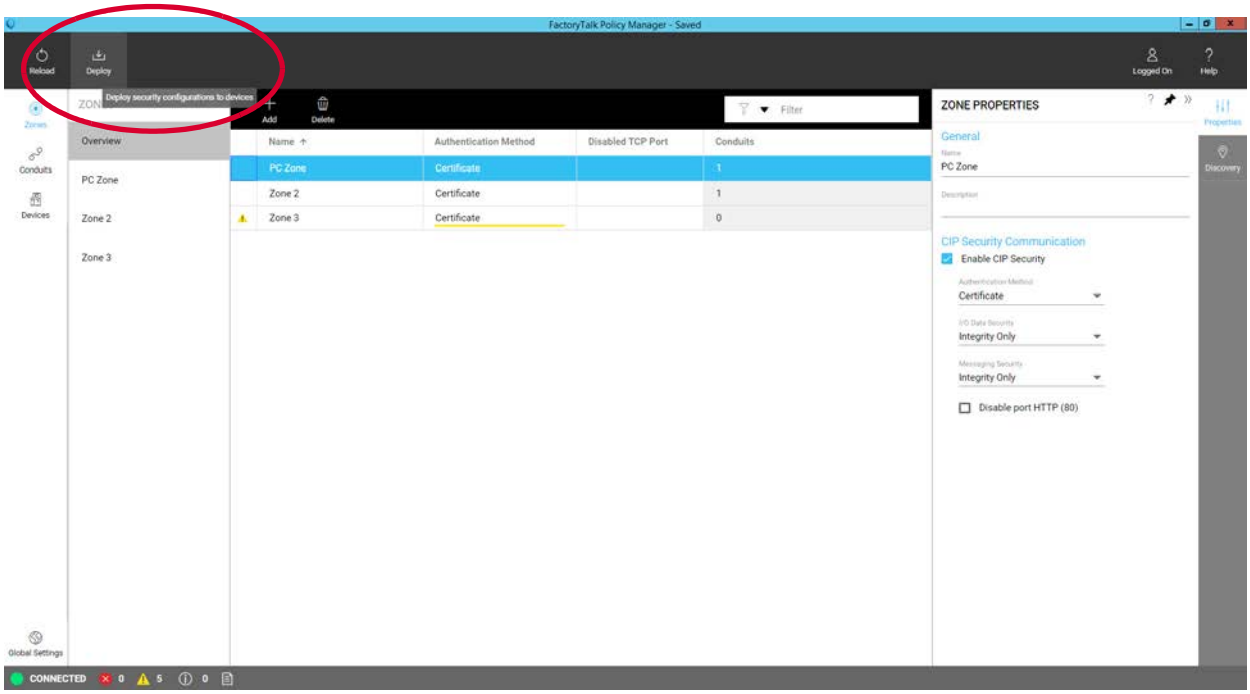
Once the security model is deployed and active, that is, communication is reset on a device, the device only accepts communication from other devices in the same zone or using conduits that are configured to enable communication with other security zones or devices.

Before deploying a security model, make sure that all devices are operational and have network access.

After the security model is deployed and active on all affected devices, FactoryTalk Policy Manager and FactoryTalk System Services are no longer required for real-time operations. They're required again if changes to the security model must be deployed.

To deploy the model, complete the following steps.

1. On the FactoryTalk Policy Manager toolbar, select Deploy.

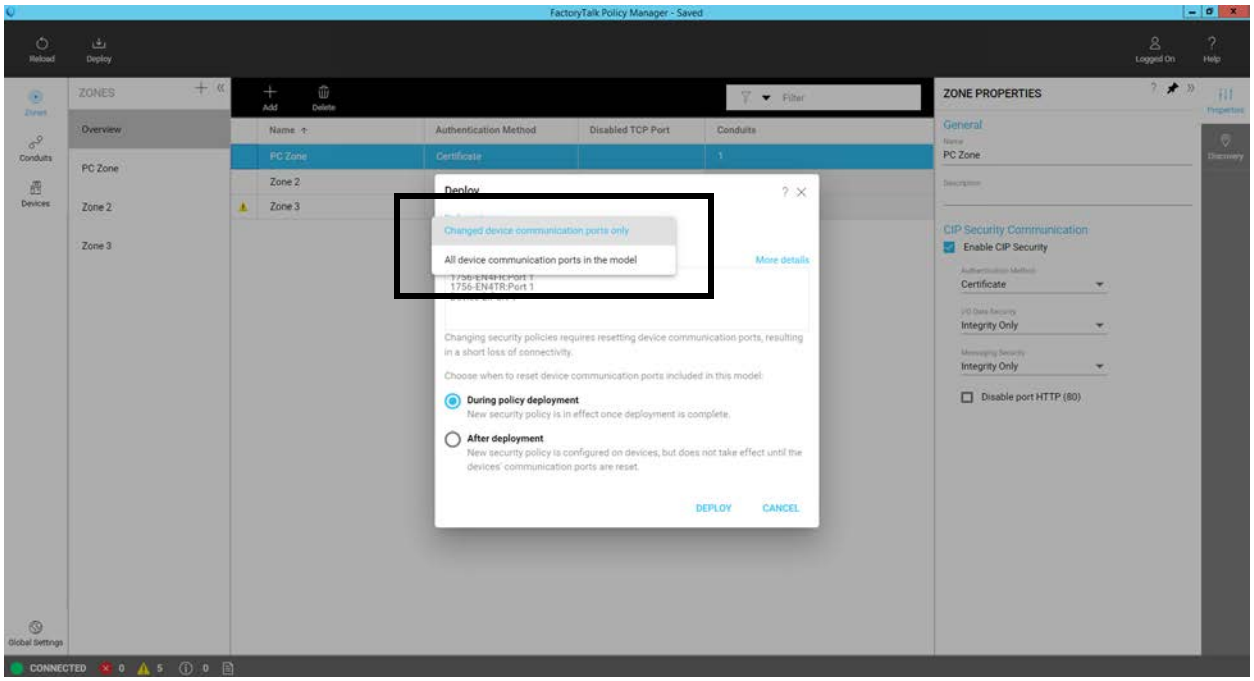


2. Review the **Deploy** dialog box.
   The list of devices identifies the devices to be configured when this model is deployed.

IMPORTANT	If the list contains unexpected devices, click CANCEL and then change the model as needed.

3. Complete the following steps.
   a. Choose the Deployment scope based on your application.
      - Select Changed device communication ports only for differential deployment.
      - Select All device communication ports in the model for full deployment.

      We recommend that you use the default option. That is, Changed device communication ports only.



   b. Choose one of the following options for when to reset the communication channels for the items included in the security model.

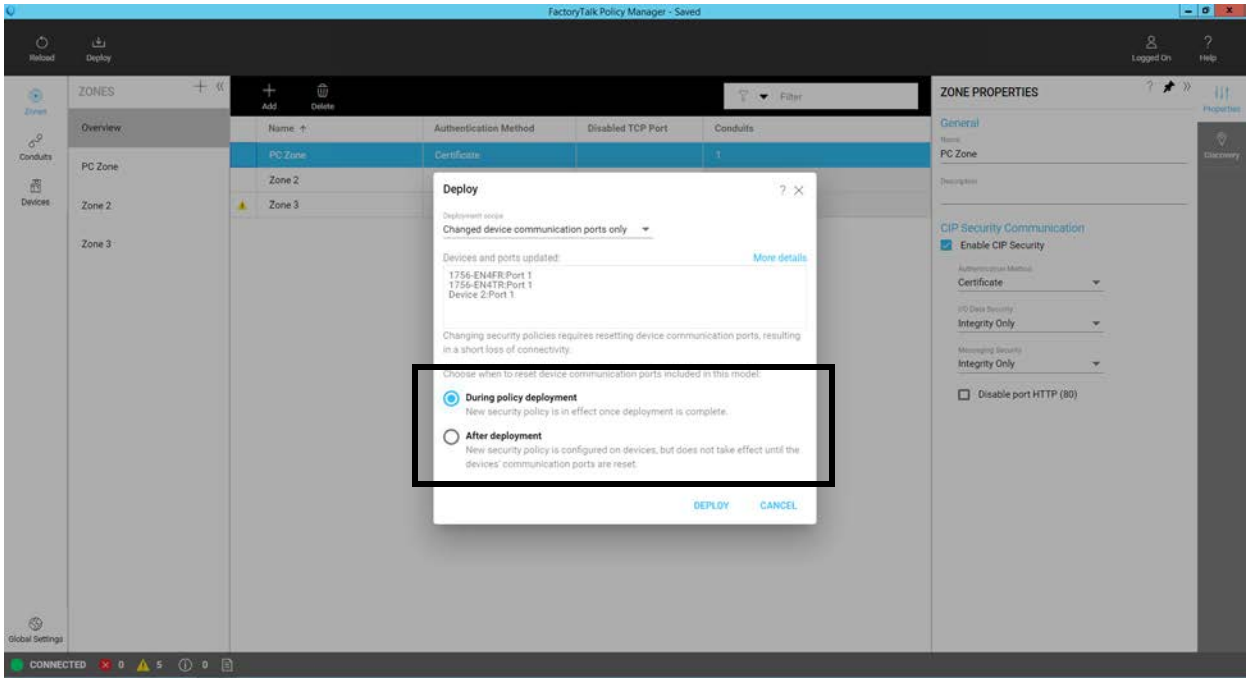
The following types of deployment are available:

- During deployment - The CIP connection is closed and reopened on the device during the deployment process.

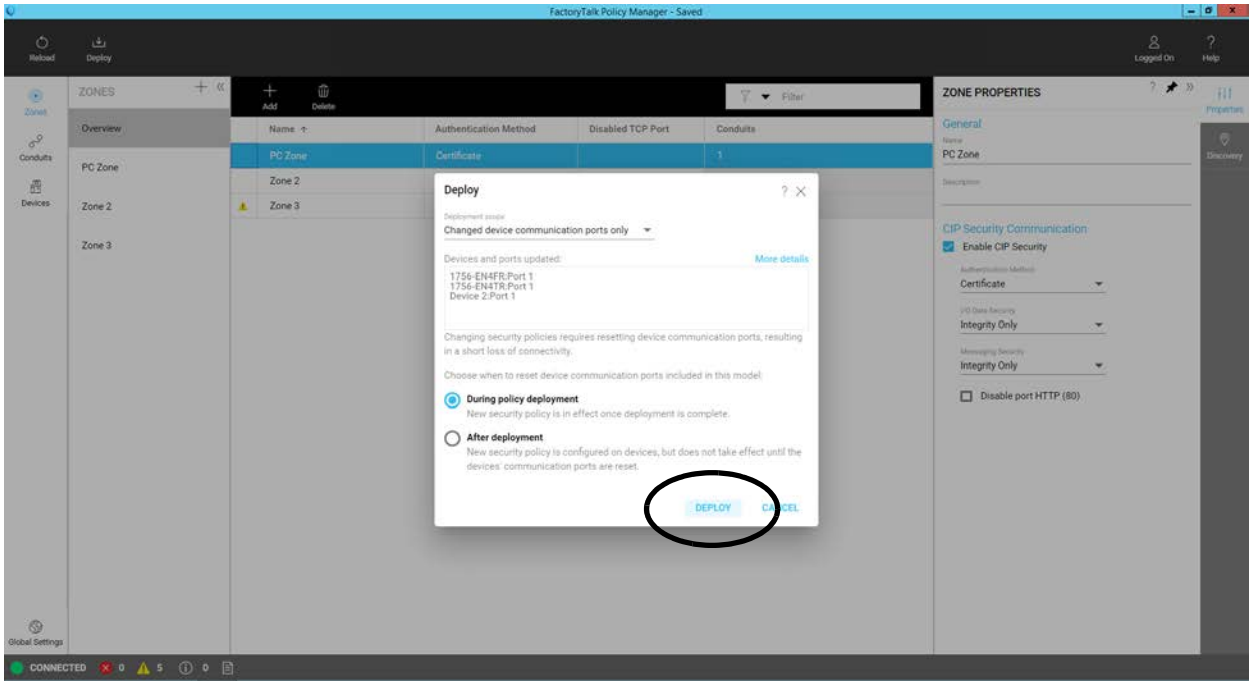
  Similar to when the network card on a computer is reset, the device stays functional but is disconnected from the network for a few moments. This option applies the new policy to the device when the policy is deployed.
- After deployment - Security policy changes are applied to devices with existing connections only after those connections are closed and reopened. For example, you can close and reopen existing connections by cycling power to a device, or by inhibiting and uninhibiting the connection.

IMPORTANT	With the After deployment option, the security policy is applied to each connection individually. If the connection reset is postponed and an unexpected connection drop occurs, the system can enter a state in which the security policy operates only in parts of the system. In this case, unexpected connection outages can occur. Connection outages are difficult to track. We recommend that you use extreme caution when using the After deployment option.

This option is useful if there's a scheduled maintenance reset process in your environment that can be relied upon to perform this function.



4. Click DEPLOY.



The Results pane updates with the results of the deployment as it occurs. After deployment is complete a summary report is provided listing the successes, failures, and errors encountered during the process.

For information on how to deploy a security model, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

Back Up the Security Model

You aren't required to back up the security model. However, we **strongly recommend** that you back it up after each policy deployment to keep the backup files synchronized with the current security policy.

Back up FactoryTalk System Services to save a copy of the security model and its associated certificates. After the model has been created, the FactoryTalk System Services backup file is included with the FactoryTalk Services Platform backup when it's performed.

IMPORTANT You must have Administrator privileges to back up FactoryTalk System Services.

To back up the security model, complete the following steps.

1. Open a command prompt as an Administrator.
2. In the command prompt window type:

   cd C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services
3. Run the backup utility by typing one of the following commands:
   - FTSSBackupRestore -B -PW "password" (FactoryTalk System Services, version 6.11)
   - FtssBackupRestore -B -P "password" (FactoryTalk System Services, version 6.20 or later)

     Creates an encrypted backup of the data using the password that is supplied in quotation marks. This password must be supplied to restore the data.

     The backup uses 7-zip to password-encrypt the archive file with AES-256. The headers are also encrypted so the names of the files within the archive are encrypted.
4. The password-protected backup file that is named *FTSS_Backup.7z* is created. The file is included in the FactoryTalk Services Platform Backup.

   Verify that the file is present in the following location:

   C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTSS_Backup

The ProgramData folder is hidden by default in Windows File Explorer.

Save Security Model Backup to Another Secure Location

We **recommend** that you save the backup.zip file to another secure location and the *FTSS_Backup* folder described previously.

Different From FactoryTalk Directory Backup File

FactoryTalk Directory provides a central lookup service for all products participating in an application, including FactoryTalk System Services application. We recommend that you create FactoryTalk backup files to preserve and restore a FactoryTalk system if there's a systems failure.

To be clear, a FactoryTalk Directory backup excludes product backup files. You must back up individual applications separately from a FactoryTalk Directory backup. However, once you create a backup of the Security Model (FTSS_Backup folder), this folder is included in the FactoryTalk Directory Backup when performed.

For more information on how to back up the FactoryTalk Directory, see the FactoryTalk Security System Configuration Guide, publication FTSEC-QS001.

Restore FactoryTalk System Services

Restore FactoryTalk System Services to return the FactoryTalk System Services databases to a known good state.

IMPORTANT Consider the following:

- If you restore FactoryTalk System Services, the security model backup folder is automatically deleted. For this reason, we recommend that you save the security model backup file in a separate location, as described on page 62.
- Restoring FactoryTalk System Services requires administrator privileges.

To restore a FactoryTalk System Services database, complete the following steps.

1. Verify the backup.zip file is present in the following location:

   C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTSS_Backup
2. Open a command prompt as an Administrator.
3. In the command prompt window type:

   cd C:\Program Files (x86)\RockwellSoftware\FactoryTalk System Services.
4. Run the FactoryTalk System Services Backup & Restore Utility by typing one of these commands:
   - FTSSBackupRestore -R -PW "password" (FactoryTalk System Services, version 6.11)

     or
   - FTSSBackupRestore -R -P “password” (FactoryTalk System Services, version 6.20 or later)

     Restores an encrypted backup of the databases that is decrypted using the password that is supplied after the -P parameter. Quotation marks are optional.

You can restore a FactoryTalk System Services database backup in a later revision of software. For example, you can open a backup of a FactoryTalk System Services database, version 6.11 with version 6.20 or later.

IMPORTANT Before you migrate from version 6.11 to version 6.20 or later, we recommend that you see the following Rockwell Automation Knowledgebase articles that are available at https://rockwellautomation.custhelp.com/app/home:

- Backup and restore CIP Security models of FactoryTalk Policy Manager and FactoryTalk System Services, click here.
- Fail to migrate existing FactoryTalk System Service data with CIP Security policy models, click here.
- FactoryTalk Policy Manager download and install, click here.

We recommend that you use the latest version of FactoryTalk Policy Manager.

Remove the Security Policy

If necessary, you can remove the security policy from software applications and hardware devices.

Remove the Security Policy From a Software Application

You can use the following to remove the security policy from FactoryTalk Linx:

- FactoryTalk Policy Manager

  When you use the FactoryTalk Policy Manager method, you not only remove the security policy from FactoryTalk Linx. The computer with FactoryTalk Linx on it also no longer appears in FactoryTalk Policy Manager.

  The FactoryTalk Policy Manager **method only works** if the computer with FactoryTalk Policy Manager is accessible to the computer with FactoryTalk Linx on it.

- FactoryTalk Administration Console

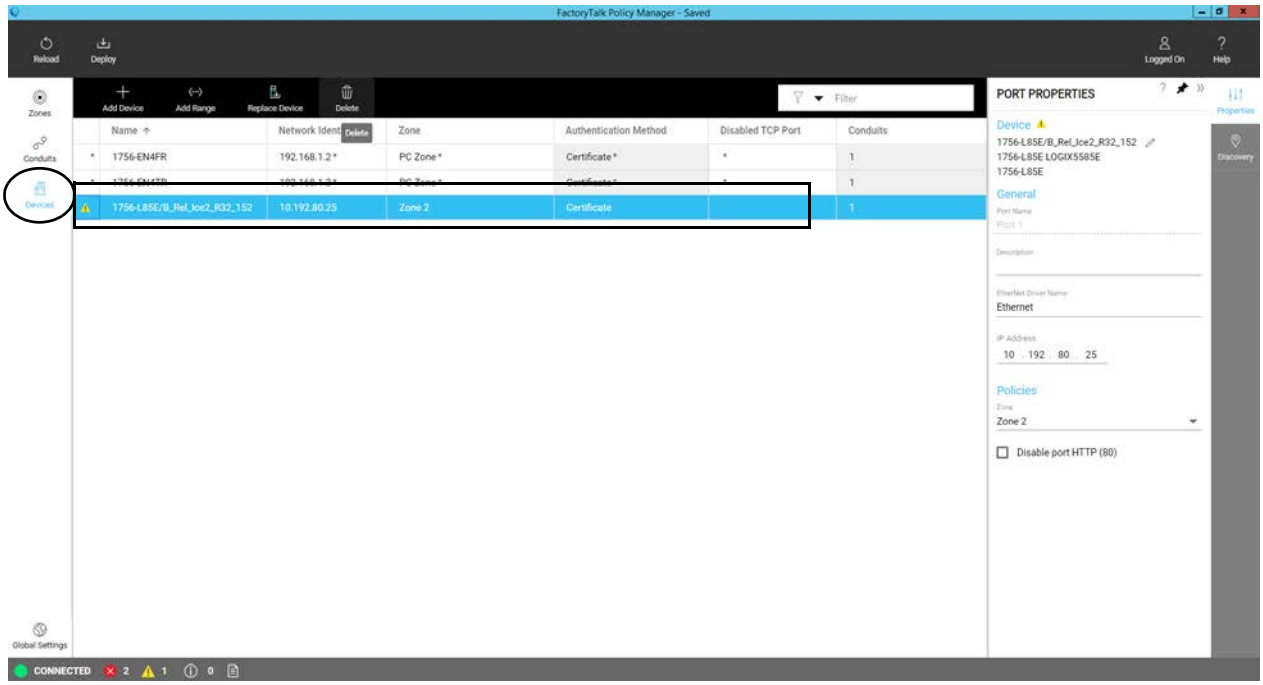
  If the computer with FactoryTalk Policy Manager isn't accessible to the computer with FactoryTalk Linx on it, you must use the FactoryTalk Administration Console method.

  When you use the FactoryTalk Administration Console method, you remove the security policy from FactoryTalk Linx.

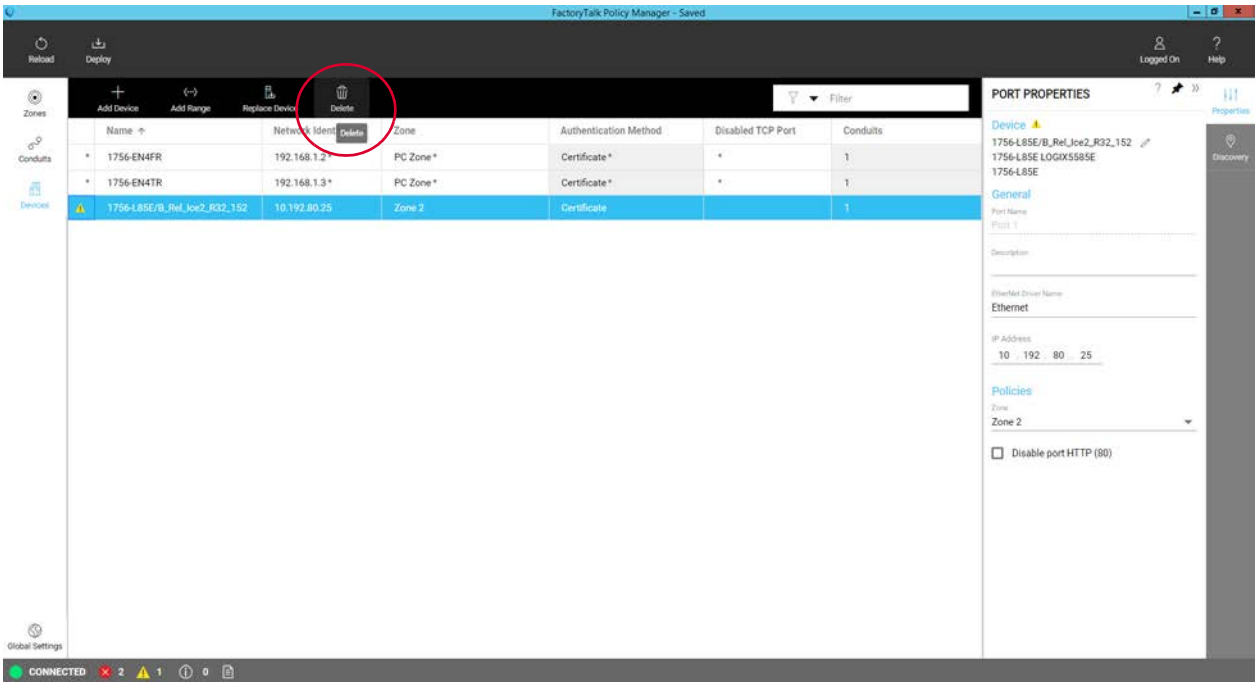
  You must then return to FactoryTalk Policy Manager to delete the computer with FactoryTalk Linx, and then you redeploy the model so that other devices can update their trust models.

Remove Security Policy From FactoryTalk Linx Via FactoryTalk Policy Manager

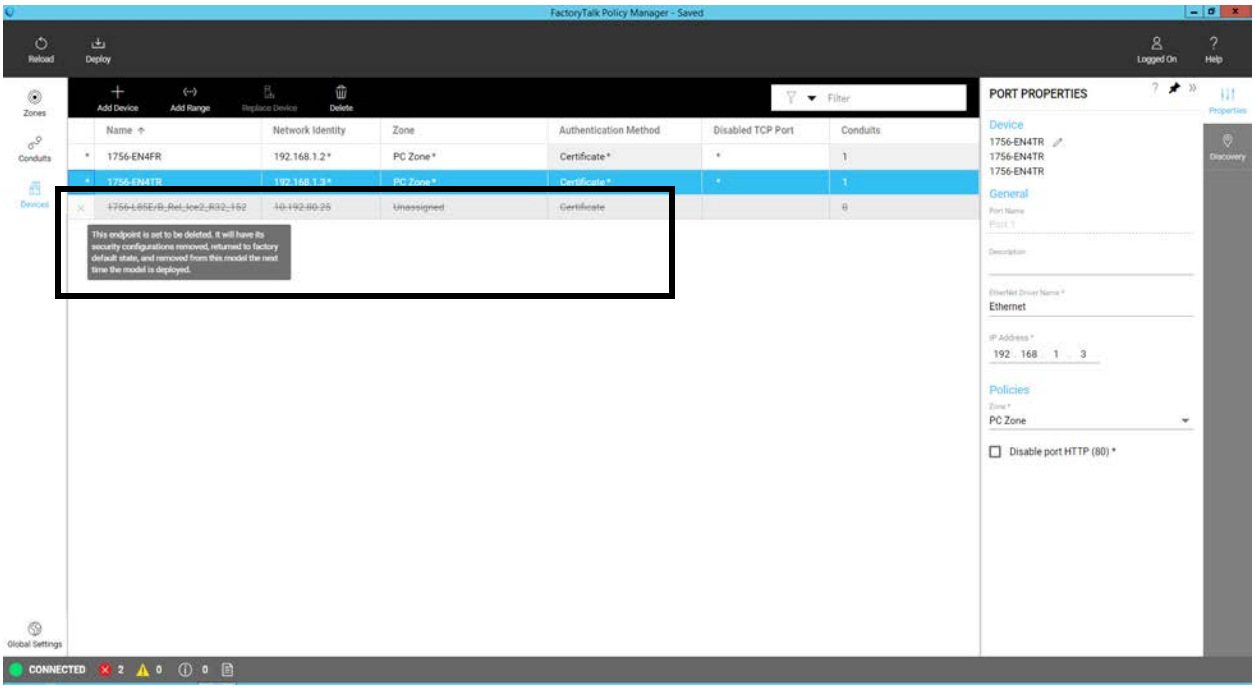
1. In the FactoryTalk Policy Manager navigation bar, select **Devices**, and then select the device.



2. Above the list of devices, click **Delete**.



After you click Delete, the device stays in the table but is crossed out. The device no longer appears in the list after you deploy the updated security model and state in the next step.

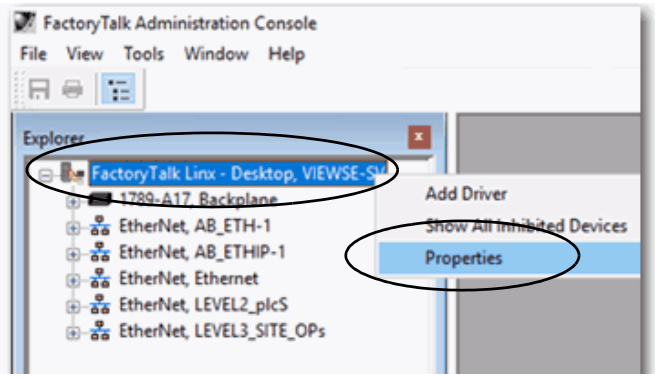


3. Deploy the security model as described starting on page 59, and choose to reset the communication channels During deployment.

Remove Security Policy From FactoryTalk Linx Via FactoryTalk Administration

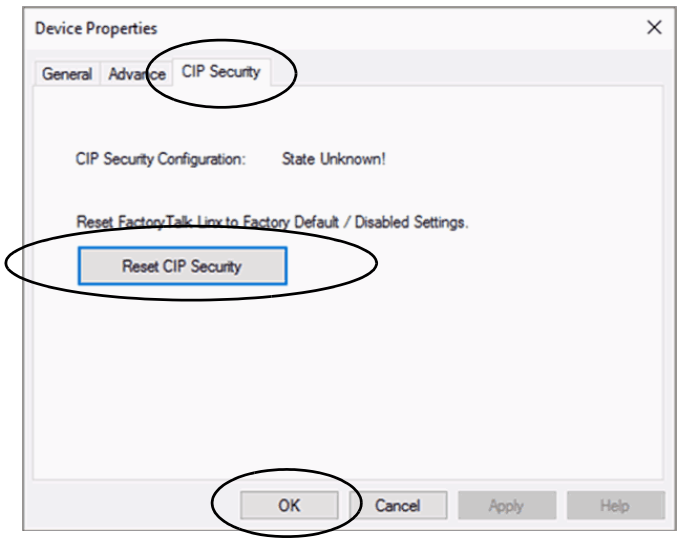
1. Start FactoryTalk Administration Console for an IACS that is online and has a security policy in place.
2. At the bottom of the Explorer pane, click the Communications tab.

3. Right-click the FactoryTalk Linx and choose Properties.



The Device Properties dialog box appears.

4. Complete the following steps.
   a. Click the CIP Security tab.
   b. Click the Reset CIP Security.
   c. Click OK.



For more information on how to use FactoryTalk Administration Console, see the software online help.

Remove the Security Policy From a Device

You can use the following ways to remove the security policy from a device:

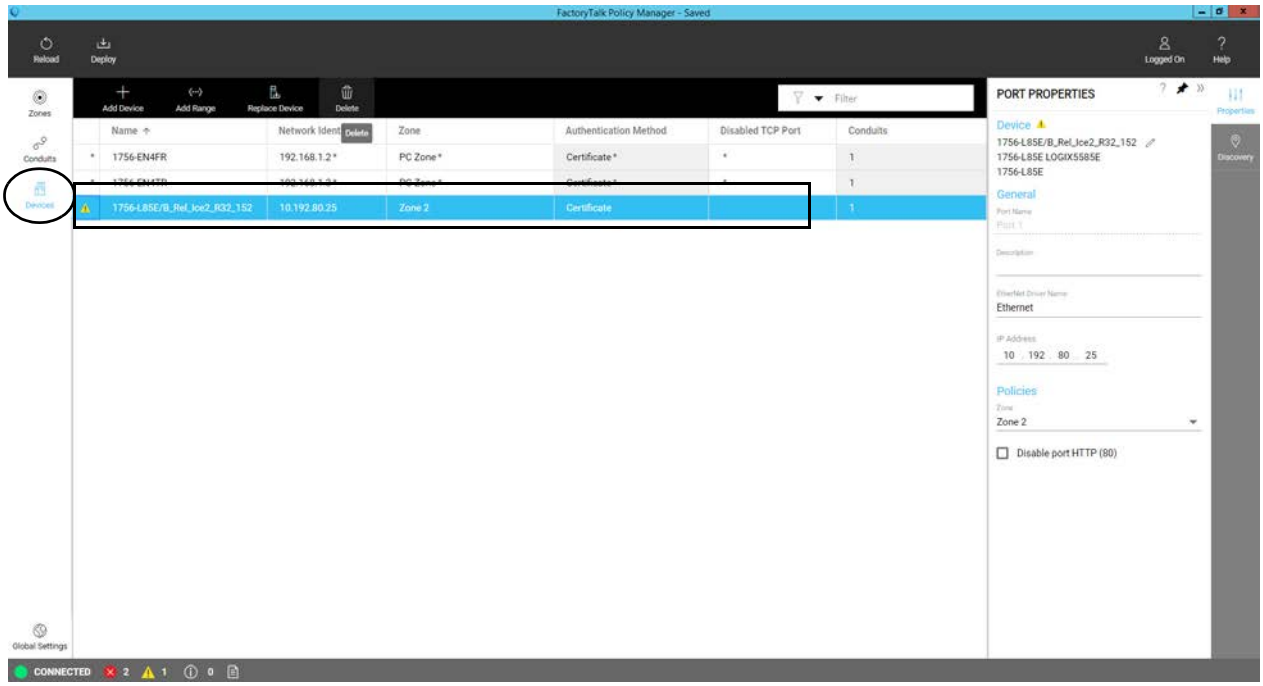
- Via FactoryTalk Policy Manager - Two methods with this option.
  - Option 1 - Change the device security policy.
  - Option 2 - Delete the device from the security model.

  The FactoryTalk Policy Manager **methods only work** if the computer with FactoryTalk Policy Manager is accessible to the device.
- Reset device to factory default settings

  If the computer with FactoryTalk Policy Manager is not accessible to the device, you can use this method.

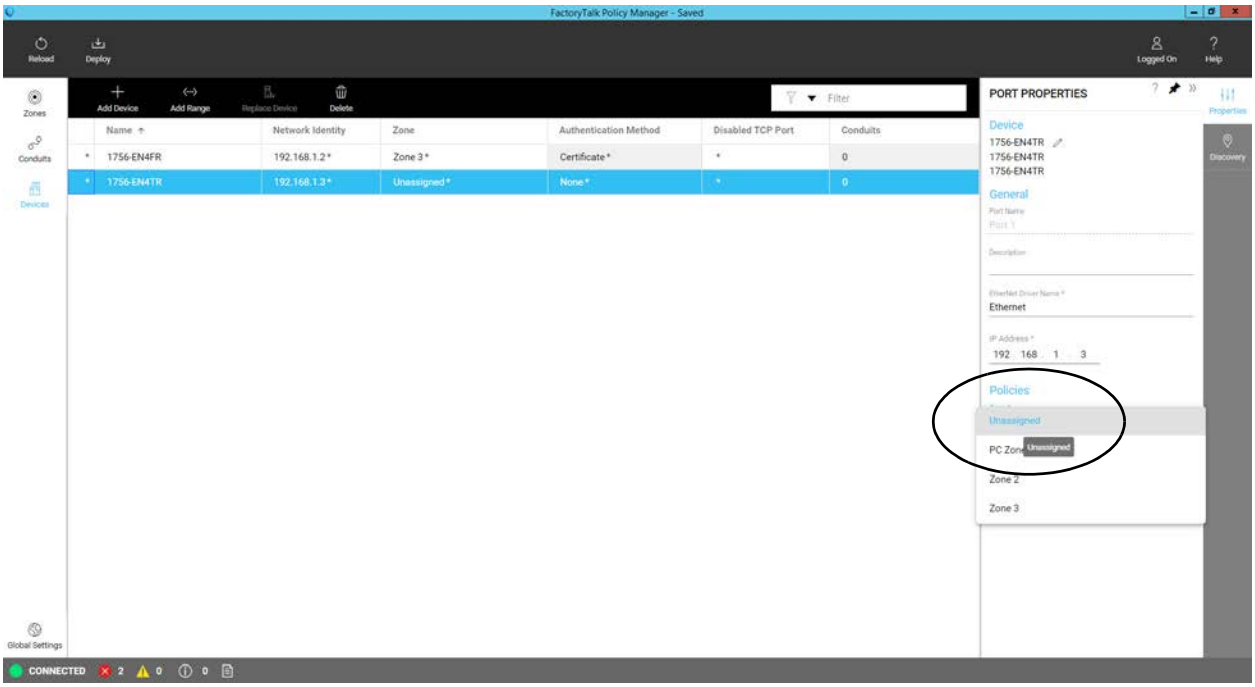
Remove Security Policy From a Device Via FactoryTalk Policy Manager - Option 1

1. In the FactoryTalk Policy Manager navigation bar, select **Devices**, and then select the device.



PORT PROPERTIES are displayed.

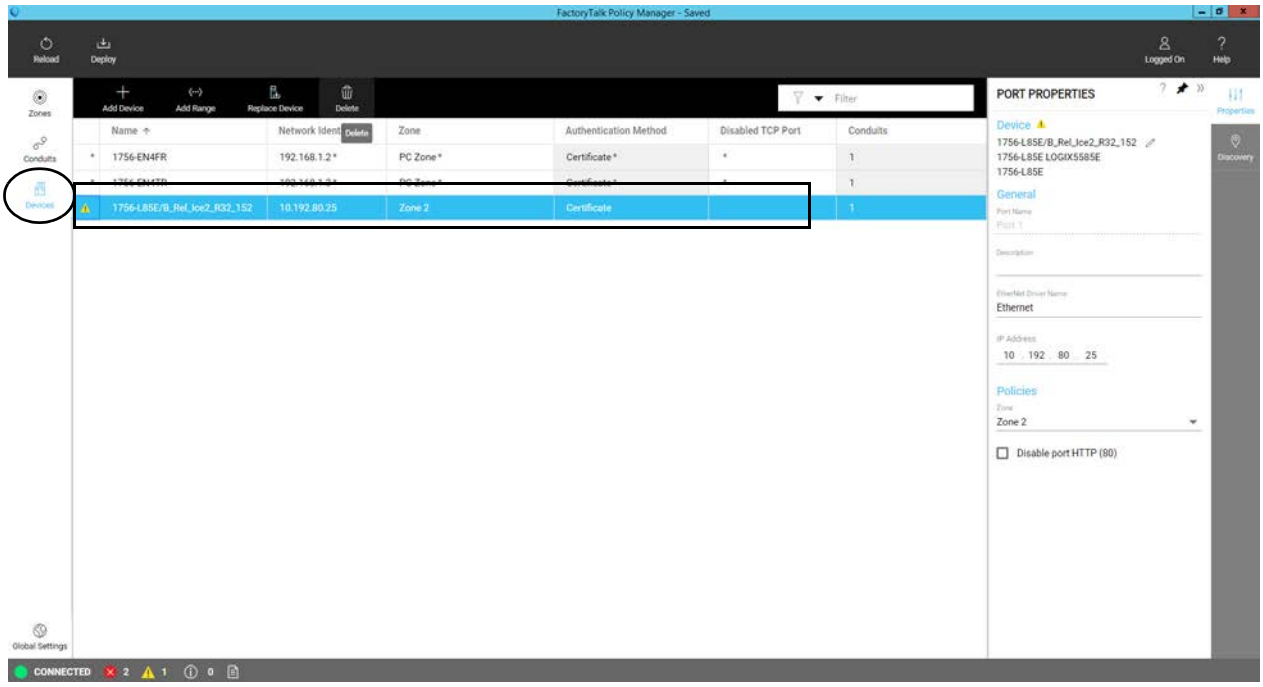
2. In the **Policies** area, change the security policies for the device.
   In **Zone**, choose either **Unassigned** or a zone that is not CIP Security enabled.



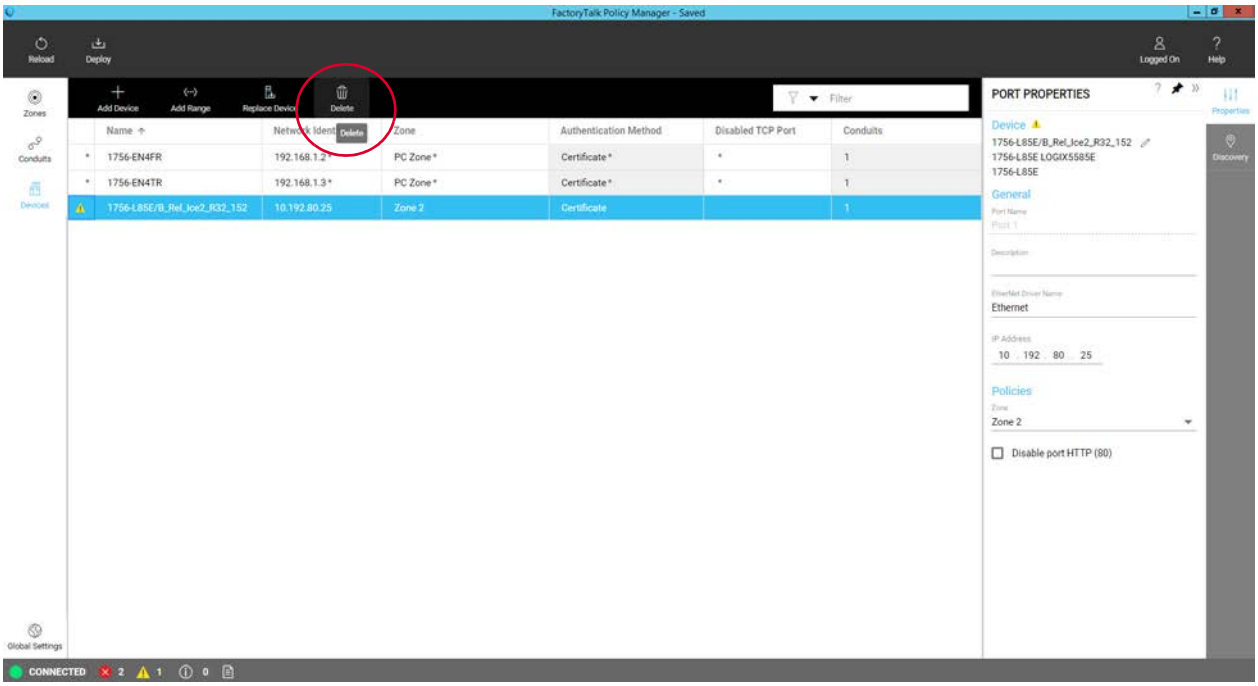
3. Deploy the security model as described starting on page 59, and choose to reset the communication channels During deployment.
   The device security policy is reset to none.

Remove Security Policy From a Device Via FactoryTalk Policy Manager - Option 2

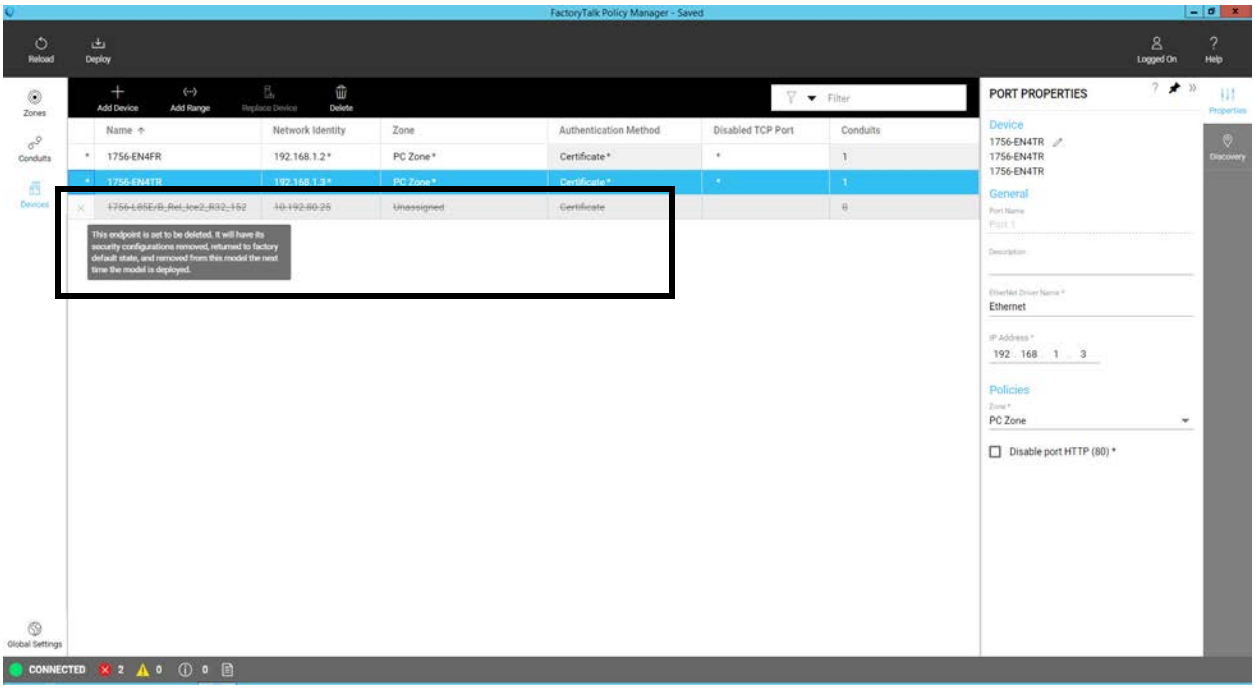
1. In the FactoryTalk Policy Manager navigation bar, select **Devices**, and then select the device.



2. Above the list of devices, click **Delete**.



After you click Delete, the device stays in the table but is crossed out. After you deploy the updated security model and state, the device no longer appears in the list.



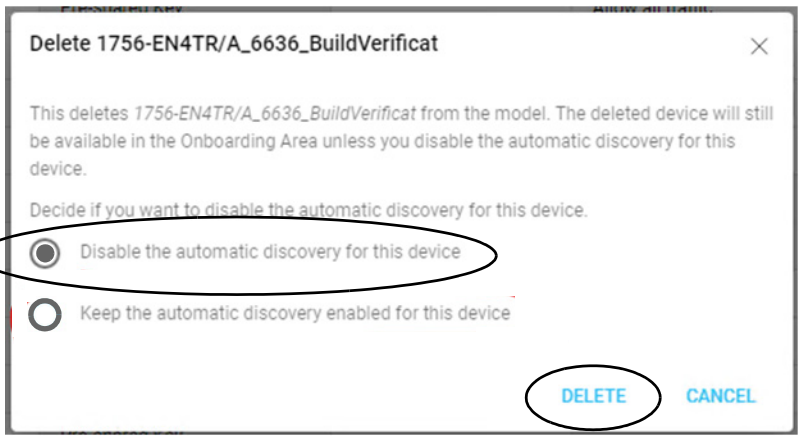
3. Deploy the security model as described starting on page 59, and choose to reset the communication channels During deployment.

IMPORTANT If the device can't be reached when the Deploy attempts to clear the security policy from the device, the attempt fails and the security policy remains in the device.

When you remove the security policy from a device, if APD is enabled, the device automatically re-enrolls in the model in the onboarding zone. To avoid this, you can disable APD on the device itself.

To disable APD for a device with FactoryTalk Policy Manager software, complete the following steps.

1. Remove the device from the model.
2. When prompted, choose to disable the automatic discovery for this device and click Delete.



3. Deploy the security model.

Remove Security Policy From a Device By Resetting the Device to Factory Default State

You can remove the security policy from a device by resetting the device to its factory default state.

IMPORTANT	The methods by which you reset devices to their factory default, and the conditions of each device when it is in its factory default state, vary. Before you reset a device to its factory default state to remove the security policy, be aware of the impact the reset can have on your IACS in general. Resetting a device to its factory default state can affect the overall system in ways unrelated to CIP Security.

For information on how to reset a device to its factory default state, see the technical documentation for the device.

Set Mask Parameters on PowerFlex 755T and PowerFlex 6000T Drives to Maintain Security

You can only apply CIP Security to the built-in EtherNet/IP interface on PowerFlex 755TL/TM/TR/TS and PowerFlex 6000T drives. There are ports in addition to the built-in EtherNet/IP interface that you should secure.

There are ports on these products where Human Interface Modules (HIMs) and communication option cards can connect. You can secure these ports by configuring mask parameters in the host PowerFlex product.

Device Peripheral Interface (DPI) Ports

HIMs and serial communication devices can connect to PowerFlex 755TL/TM/TR/TS products and PowerFlex 6000T drives at DPI™ ports 1...3. These include the following devices:

- 20-HIM-A6
- 20-HIM-C6S
- 1203-USB (Ports 2 and 3 only when used with PowerFlex 6000T)
- 1203-SSS (PowerFlex 6000T only; ports 2 and 3 only)

Port 1 is the HIM cradle on the control pod. Ports 2 and 3 are accessible through the DPI connector on the back of the HIM cradle on the control pod.

Communication option cards can connect to **DPI ports 4...6**. The cards include the following devices:

Drives	Possible Devices
PowerFlex 755T	• 20-750-CNETC • 20-750-DNET • 20-750-ENETR • 20-750-PBUS • 20-750-PNET • 20-750-PNET2P
PowerFlex 6000T	• 20-750-DENC • 20-750-ENC • 20-750-ENETR • 20-750-PBUS • 20-750-PNET • 20-750-PNET2P • 20-750-UFB

These ports are optional card slots in the control pod.

Drives	DPI Port	Possible Devices
PowerFlex 755T	1	20-HIM-A6
	2 and 3	• 20-HIM-A6 • 20-HIM-C6S • 1203-USB
	4...6	• 20-750-CNETC • 20-750-DNET • 20-750-ENETR • 20-750-PBUS • 20-750-PNET • 20-750-PNET2P
PowerFlex 6000T	1...3	20-HIM-C6S
	2...6	• 20-WIM-Nx • 1203-SSS • 1203-USB
	4...6	• 20-750-DENC • 20-750-ENC • 20-750-ENETR • 20-750-PBUS • 20-750-PNET • 20-750-PNET2P • 20-750-UFB

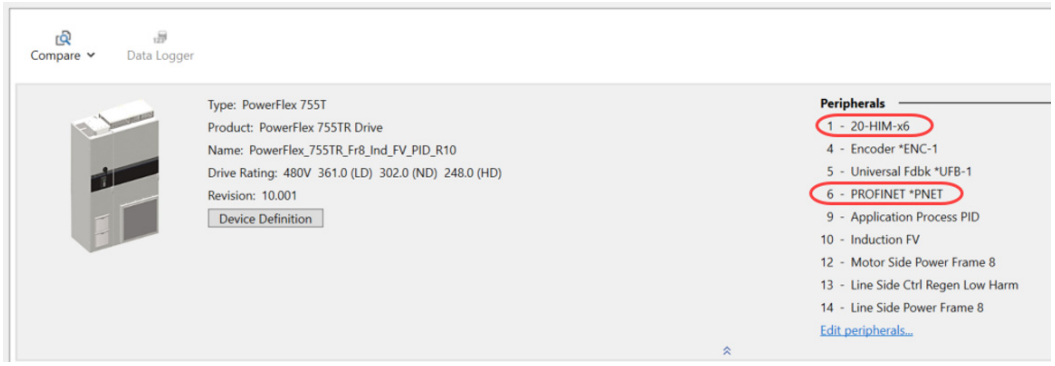
Setting Masks to Secure the DPI Ports

Perform the following configurations from a tool such as Connected Components Workbench™ software or Logix Designer application. You must understand the following parameters

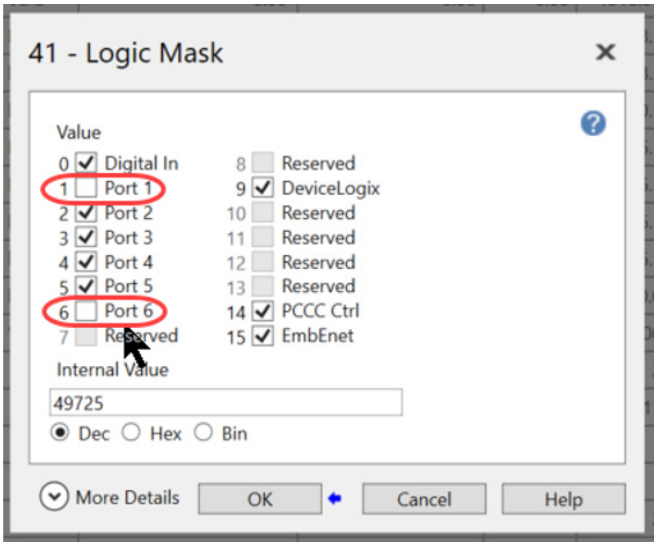
- 0:41 [Logic Mask]
- 0:230 [Write Mask Cfg]
- 0:231 [Write Mask Act].

For more information, see the PowerFlex Drives with TotalFORCE Control Programming Manual, publication 750-PM101.

1. Identify which ports contain HIMs, serial communication devices and communication option cards.
   For example, this drive has a HIM at port 1 and a PROFINET option card in port 6.

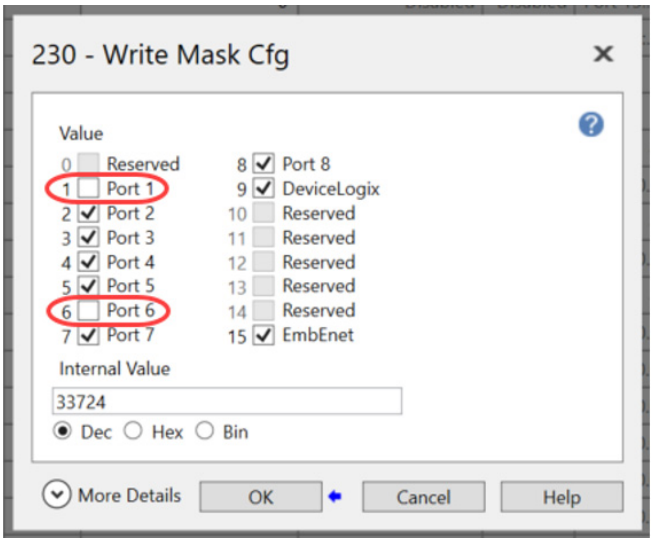


2. Clear the corresponding bits in the parameter 0:41 [Logic Mask].
   In the example, you must disable port 1 and port 6. You must clear the corresponding bits 1 and 6.



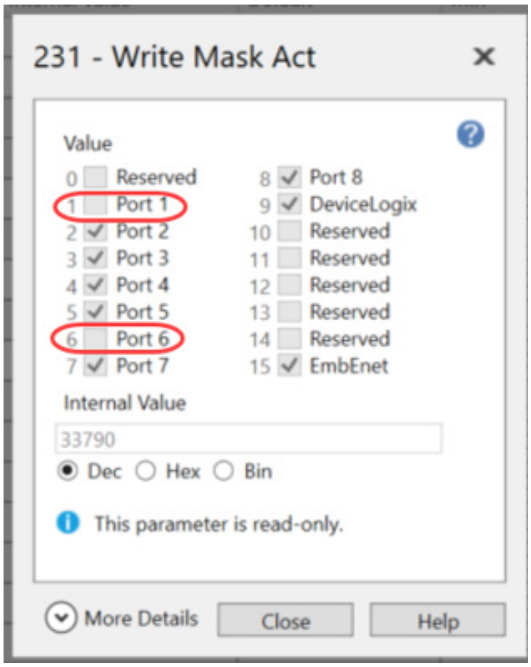
Clearing the bit that corresponds to the port helps prevent a device at that port from controlling the start and logic command (such as direction) of the host product.

3. Clear the corresponding bits in the parameter 0:230 [Write Mask Cfg].
   In this example, port 1 and port 6 are disabled. You must clear the corresponding bits 1 and 6.



Clearing the bit that corresponds to the port helps prevent a device at that port from writing values to any of the parameters in the host product.

4. Cycle power or perform a reset to allow the configuration in parameter 0:230 [Write Mask Cfg] to take effect.
5. Verify that the corresponding bits are properly set in parameter 0:231 [Write Mask Act].



Use Syslog with CIP Security

IMPORTANT The following products support Syslog:

- FactoryTalk Linx, version 6.21 or later
- ControlLogix 5580 controllers, firmware revision 34.011 or later
- GuardLogix® 5580 controllers, firmware revision 34.011 or later
- 1756-EN4TR EtherNet/IP communication module, firmware revision 4.001 or later
- 1783-CSP CIP Security Proxy, firmware revision 1.001 or later
- PowerFlex 755T drives, firmware revision 10.001 or later

Syslog is a standardized and widely used event message logging technology. Syslog is a standard for event logging. You use Syslog to generate, store, report, and analyze security-related events.

When syslog operates over a network, it uses a client-server architecture in which a syslog server monitors for, and logs, messages that are coming from clients.

CIP Security-capable devices are syslog-capable. To enable and configure syslog in certified security applications, you must implement CIP Security.

Syslog Collector

A Syslog collector stores event messages that are sent from the generating device to the collector.

IMPORTANT The syslog collector and the generating device must be connected to the same Ethernet network.

If you use another tool as the Syslog collector, it must support the following:

- RFC-5424 syslog protocol
- Ability to receive messages from CIP Security-enabled devices

You must configure an IP address for the Syslog Collector in FactoryTalk Policy Manager software.

Define Event Policy in FactoryTalk Policy Manager

Administrators use FactoryTalk Policy Manager software to define the event generation policy for Rockwell Automation endpoints with no separate tools, no custom UIs, no setting up individual devices.

Also known as Secure Eventing, this service uses the following communication protocols to log messages:

- UDP - A protocol that gives good performance for a high volume of messages, however, it can lose data during network issues.
- TCP - A protocol that is best suited for high-priority messaging.

To use syslog in FactoryTalk Policy Manager software, complete the following tasks.

1. Enable Security Eventing.
2. Configure the IP address of the syslog collector.
3. Configure endpoint filtering based on the following:
   - Severity Level of Information based on the descriptions in Table 13 on page 77.
   - Log failures - Select whether only failures or both successes and failures are logged.
4. Change the port of the syslog server.
5. Set the protocol - TCP or UDP.
6. Enable Sequence ID and Time Quality.
7. Select what details are included in events, that is, Sequence ID and/or Time Quality.

When an event occurs, the syslog generates an event that includes metadata that is related to the syslog configuration.

For example, if an unauthorized device that uses IP address 192.168.1.102 tries to make a connection to a device in the system. The connection attempt is denied and the syslog generates an event that indicates that an unauthorized device tried to make the connection.

In this case, the event ID = cipsec_tls_srv_session_failed, event=13. The syslog indicates the time, in milliseconds or nanoseconds, when the event occurred.

Facility Codes and Severity Levels

When detected, each message is labeled with a facility code and is assigned a severity level.

Facility Codes

Table 12 describes the facility codes that syslog uses to label events.

Table 12 - Syslog Event Facility Codes

Category	ID	Facility Code	Definition
null	0	local0(16)	For future use, no events belong to this category.
comms	1	local0(16)	A general communications-related event
config	2	local0(16)	A general configuration-related event
diag	3	syslog(5)	A general fault or error diagnostic
stat	4	local0(16)	A general event providing statistical data
alert	5	syslog(5)	A general event-related to a potential threat
control	6	local0(16)	A general control system-related event
audit	7	local0(16)	A general audit log-related event
backup	8	local0(16)	A general backup or restore-related event
security	9	auth(4)	A general security-related event
cip	10	local0(16)	A CIP-related event
http	11	local0(16)	A web server or client-related event
opc	12	local0(16)	An OPC or OPC-UA-related event
log	13	local0(16)	A log-related event
cert	14	local0(16)	A certificate-related event
discovery	15	local0(16)	A system discovery-related event
auth	16	auth(4)	An account management-related event
sys	17	local7(23)	A general system-related event
cipsec	18	auth(4)	A CIP Security-related event
ra-wks	19	local0(16)	A workspace-related event (frontend and backend)
ra-comms	20	local0(16)	An automation device communication-related event
ra-top	21	local0(16)	A topology-related event
ra-cat	22	local0(16)	A category-related event
ra-ns	23	local0(16)	A Namespace-related event
ra-authc	24	local0(16)	An authentication-related event
ra-authz	25	local0(16)	An authorization-related event
ra-cert	26	local0(16)	A certificate-related event
ra-secret	27	local0(16)	A secret-related event
ra-log	28	local0(16)	A logging management-related event
ra-vcs	29	local0(16)	A version control system management-related event
ra-sys	30	local0(16)	A general system management-related event
safety	31	local0(16)	A safety-related event
ctlr	32	local0(16)	A Programmable Automation Controller-related event

Severity Levels

Events can have security risks that can take many forms, for example:

- Threat actors that try to gain unauthorized, and undetected, access to an IACS network with the intention to commit malicious acts.
- Well-intentioned personnel with no malicious intention but who make mistakes that can result in unintended consequences.

Table 13 describe the severity levels as defined by The Syslog Protocol, RFC 5424, standard.

Table 13 - Event Security Risk Severity Levels

Severity Name	Severity Level		Definition
emrg	0	Emergency	System is unusable.
alrt	1	Alert	Should be corrected immediately
crit	2	Critical	Critical condition
err	3	Error	Error condition
warn	4	Warning	Error may occur if action is not taken.
note	5	Notice	Events are unusual.
info	6	Informational	Normal operations, no action required.
dbg	7	Debug	Information for developers
audit	8	Audit	Information for the audit system
time	9	Time	Timestamp value to format according to RFC 3339
causeid	10	Cause Identification	Uniquely identifies a transaction of operations (by UUID)

Syslog Message List

For a complete list of syslog messages, see the Logix 5000 Controller and I/O Fault Codes and Syslog Messages Reference Data, publication 1756-RD001.

Notes:

CIP Security Implementation Example Architecture

This section describes example ControlLogix® 5580 and CompactLogix™ 5380 IACS with CIP Security™ implemented.

ControlLogix 5580 Controllers Example Architecture

This example shows how to use ControlLogix 5580 controllers in an example architecture.

Phase One of Implementation

In the first phase of the CIP™ Security implementation, you secure communication between the Computer (PC) zone and each IACS zone. The degree to which you secure communication depends on your system needs.

For more information on the CIP Security properties that you can use to secure communication, see Secure Data Transport on page 14.

We **recommend** that you secure communication between the PC Zone to each IACS zone because it has the most vulnerabilities from Windows-based operating systems when it is not secured.

In this phase, you complete the following tasks:

- Create Zones
- Create Zone-to-Zone Conduits
- Deploy Security Policies

Create Zones

Create zones and all applicable devices including CIP Security-capable and non-CIP Security-capable devices.

- PC Zone (FactoryTalk® Site servers and engineering workstations [EWS])
- Cell Zone A (Controller zone)
- Cell Zone B (I/O zone)
- Cell Zone C (Controller zone)

IMPORTANT The example zones that are shown in this section are all in the same subnet/VLAN.

Figure 14 - CIP Security Architecture - Zones

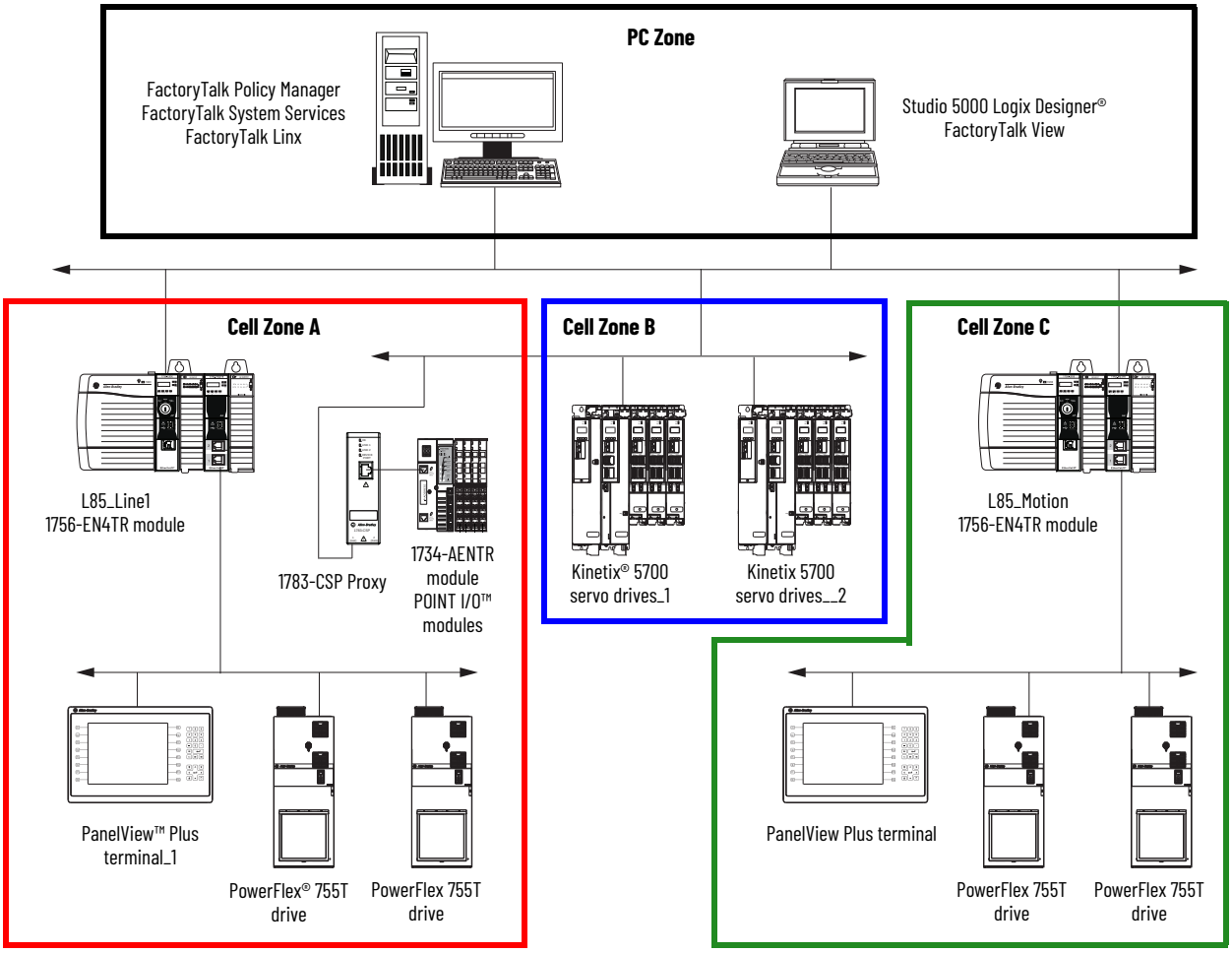


Table 14 is a security matrix with zones and devices.

Table 14 - Security Matrix - Zones

PC Zone Software	Cell Zone A	Cell Zone B	Cell Zone C
FactoryTalk Linx(1) FactoryTalk Policy Manager FactoryTalk System Services	L85_Line1	Kinetix 5700 servo drives_1	L85_Motion
Studio 5000 Logix Designer(1) FactoryTalk View	1756-EN4TR module	Kinetix 5700 servo drives_2	1756-EN4TR module
	1783-CSP proxy		PanelView Plus terminal(2)
	1734-AENTR module(2)		PowerFlex 755T drive
	PanelView Plus terminal_1(2)		PowerFlex 755T drive
	PowerFlex 755T drive		
	PowerFlex 755T drive		

(1) This group of software is installed on the same server/computer.

(2) This device is not CIP Security-capable.

Create Zone-to-Zone Conduits

1. Create zone-to-zone conduits for secure CIP-connection from the FactoryTalk Linx data server and engineering workstation in the PC zone to each of the respective Controller zones named Cell Zone A, B, and C.
   - PC Zone to Cell Zone A
   - PC Zone to Cell Zone B
   - PC Zone to Cell Zone C

Figure 15 - CIP Security Architecture - Conduits

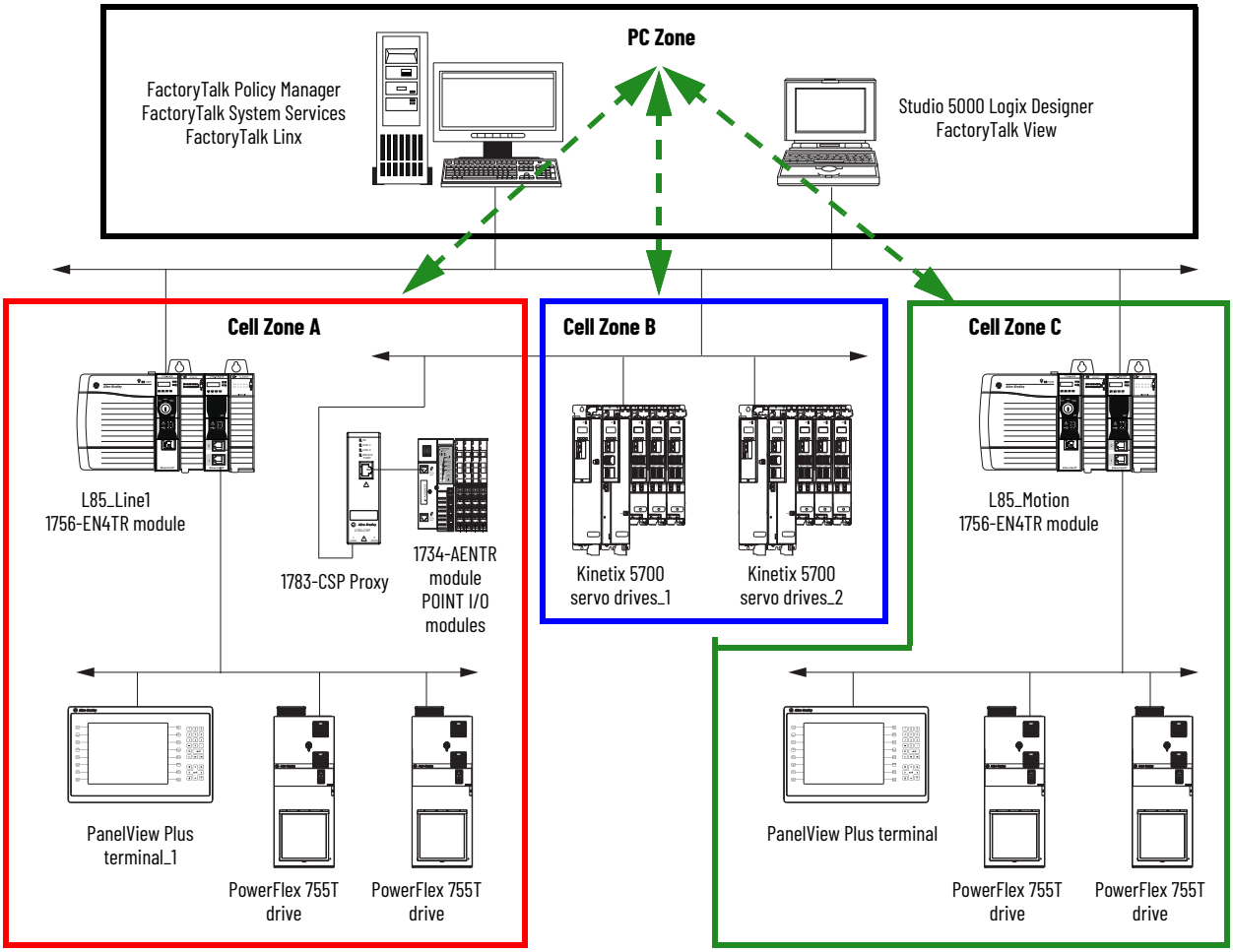


Table 15 is an example of an updated security matrix after conduits are identified and organized.

Table 15 - Security Matrix - Conduits

Source	Destination			
	PC Zone	**Cell Zone A**	**Cell Zone B**	**Cell Zone C**
PC Zone	Permit(1)	Conduit 1: Zone-to-Zone	Conduit 2: Zone-to-Zone	Conduit 3: Zone-to-Zone
Cell Zone A	Conduit 1: Zone-to-Zone	Permit	Denied	Denied
Cell Zone B	Conduit 2: Zone-to-Zone	Denied	Permit	Denied
Cell Zone C	Conduit 3: Zone-to-Zone	Denied	Denied	Permit

(1) Default pathway.

Configure Conduit Security Policies

Configure the conduit security policies that use certificates and message integrity in the following ways:

- Between the FactoryTalk Linx software to the ControlLogix® 5580 controller in Cell Zone A (Controller zone).
- Between the FactoryTalk Linx software and the Kinetix 5700 drives in Cell Zone B (I/O zone).
- From the FactoryTalk Linx software to the ControlLogix 5580 controller in Cell Zone C (Controller zone) through a 1756-EN4TR communication module.

Optionally, you can establish an allowed list from the PC zone to each IP address of the non-CIP Security-capable devices.

Figure 16 - CIP Security Architecture - Conduit Security Policies

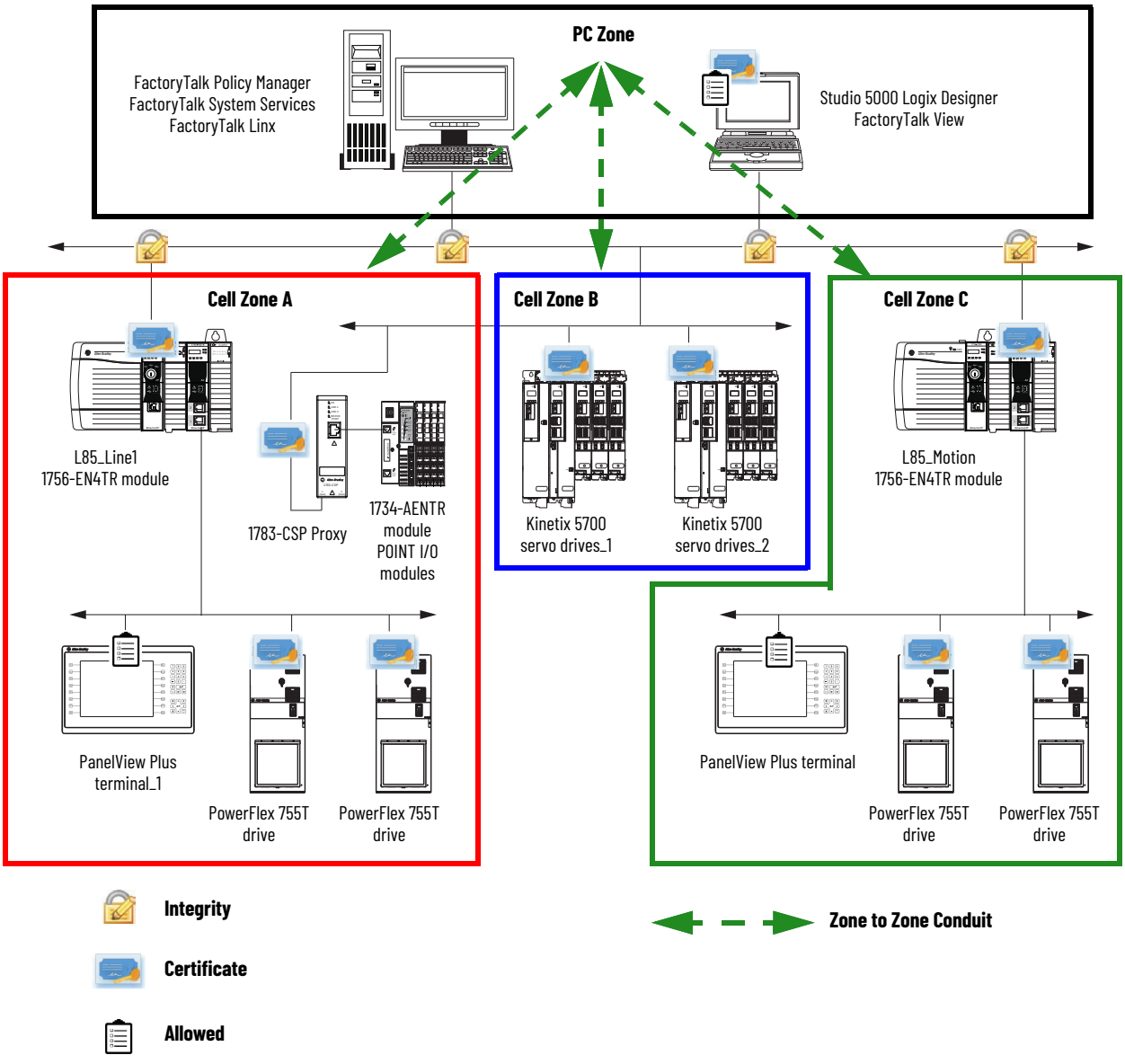


Table 16 is an example of an updated security matrix after the conduit security policies are configured.

Table 16 - Security Matrix - Conduit Security Policies Matrix

Secure Linx Communication: Conduits 1, 2, and 3	Zone to Zone		Security Policy
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Cell Zone A	• Certificates • Integrity • Confidentiality
	PC Zone	Cell Zone B	
	PC Zone	Cell Zone C	

Trusted IP (allowed)	Zone Device-to-Zone Device		
(Non-CIP Security-capable devices)	PC Zone Device:FactoryTalkNetwork Manager IP address: 192.168.1.100	Cell Zone A - Devices	• L85_Line1 (192.168.1.8) • 1756-EN4TR module (192.168.1.9) • 1783-CSP proxy (192.168.1.10) • 1734-AENTR module (192.168.11) • PanelView Plus terminal_1 (192.168.1.12) • PowerFlex 755T drive (192.168.1.13) • PowerFlex 755T drive (192.168.1.14)
		Cell Zone C - Devices	• L85_Motion (192.168.3.8) • 1756-EN4TR module (192.168.3.9) • PanelView Plus terminal (192.168.3.10) • PowerFlex 755T drive (192.168.3.11) • PowerFlex 755T drive (192.168.3.12)

Deploy Security Policies

Deploy the security policies to the devices as described on page 59.

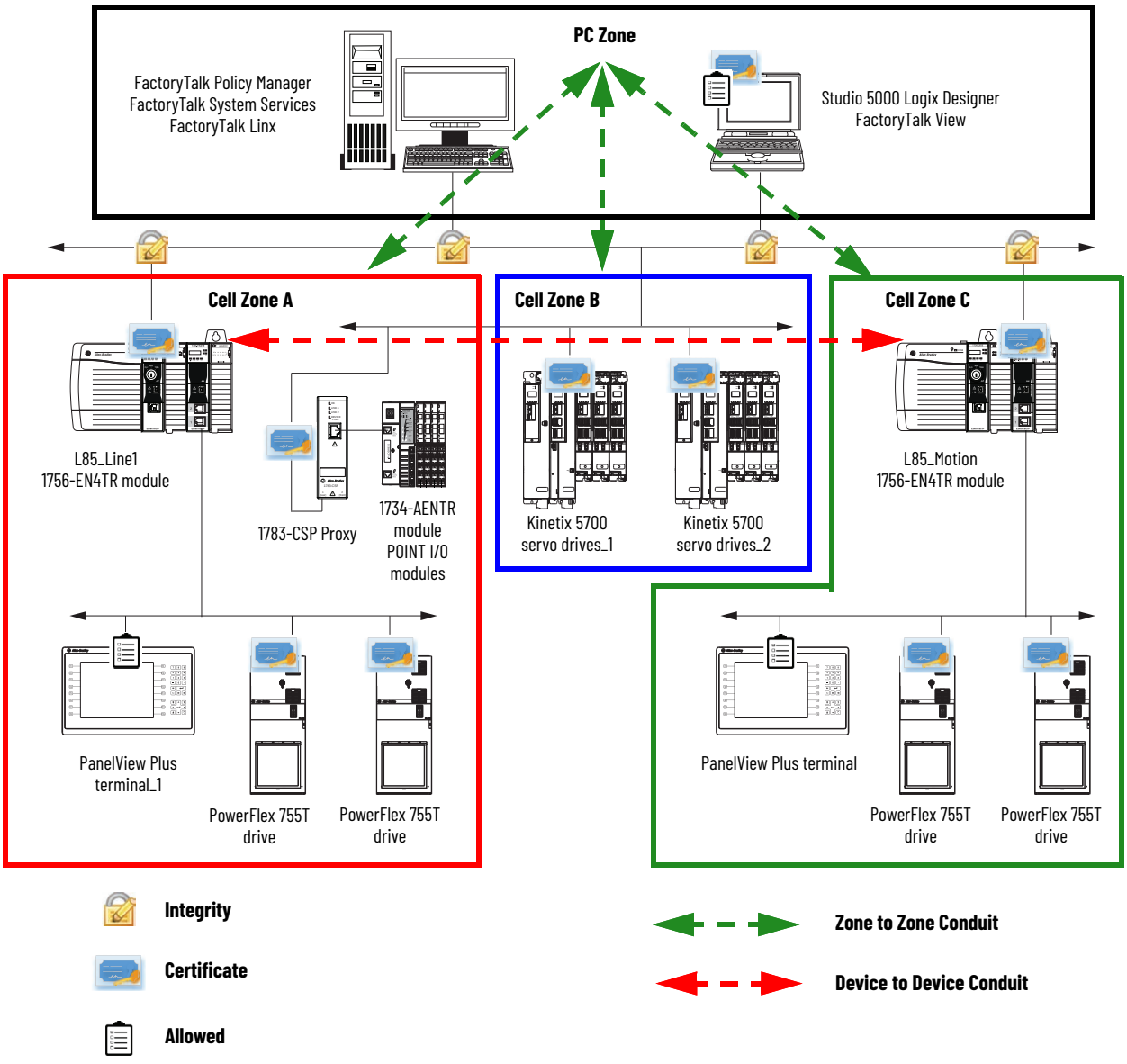
Phase Two of Implementation

In the second phase of the CIP Security implementation, you secure communication between device-to-device for micro-segmentation. You use the existing zones that are created in the first phase.

Create a Device-to-Device Conduit

Create a device-to-device conduit for secure CIP-connection from the ControlLogix 5580 controller in Cell Zone A (Controller zone) to the ControlLogix 5580 controller in Cell Zone C (Controller zone).

Figure 17 - CIP Security Architecture - Device-to-Device Conduit Added



Create a Zone-to-Device Conduit

Create a zone-to-device conduit from the Kinetix 5700 drives in Cell Zone B (I/O zone) to the ControlLogix 5580 controller in Cell Zone C (Controller zone).

Figure 18 - CIP Security Architecture - Zone-to-Device Conduit Added

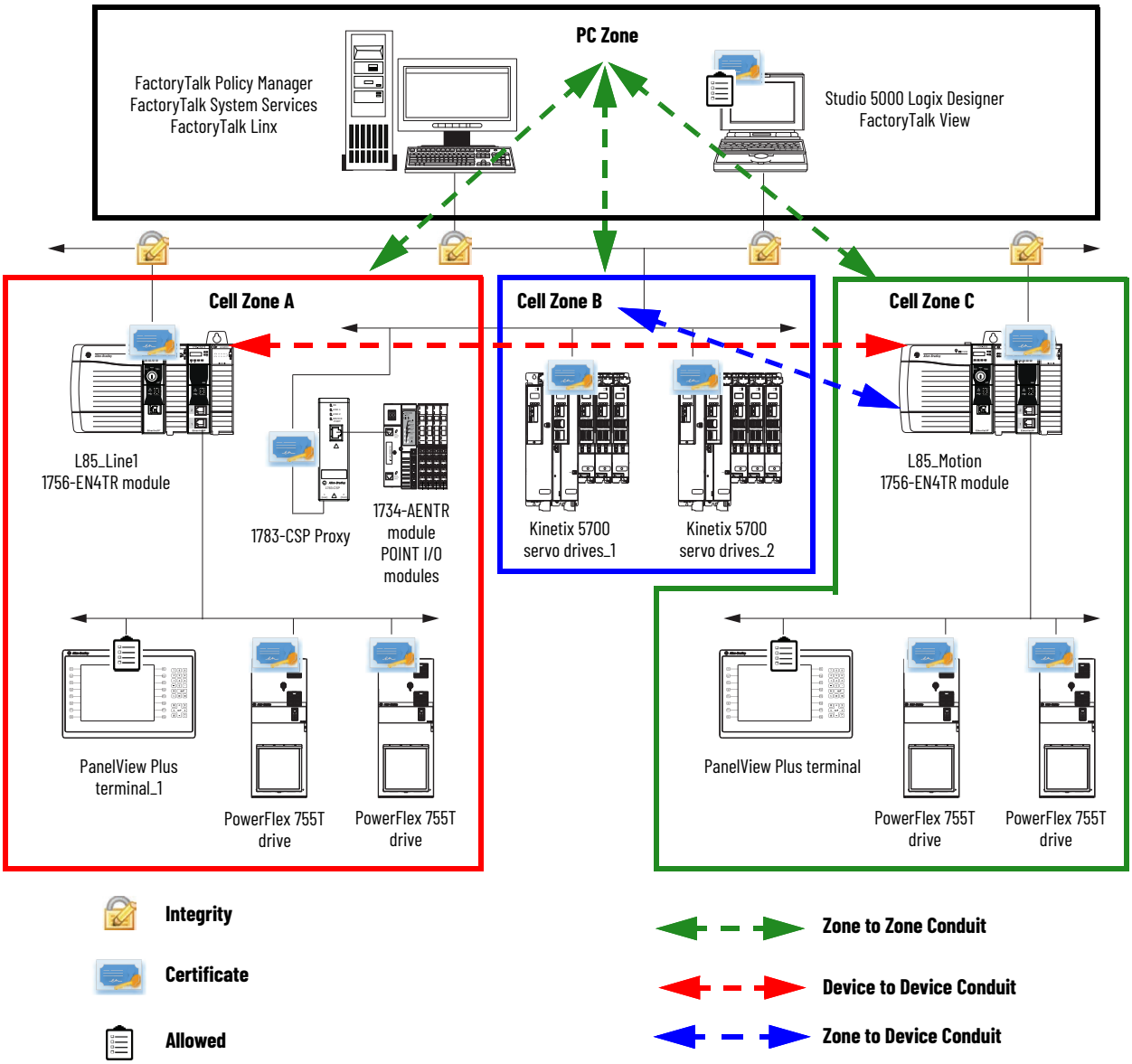


Table 17 is an example of an updated security matrix after conduits are identified and organized.

Table 17 - Security Matrix - Device-to-Device and Zone-to-Zone Conduits Added

Source	Destination			
	PC Zone	Cell Zone A	Cell Zone B	Cell Zone C
PC Zone	Permit(1)	Conduit 1: Zone-to-Zone	Conduit 2: Zone-to-Zone	Conduit 3: Zone-to-Zone
Cell Zone A	Conduit 1: Zone-to-Zone	Permit	Denied	Conduit 4: Device-to-Device
Cell Zone B	Conduit 2: Zone-to-Zone	Denied	Permit	Conduit 5: Zone-to-Device
Cell Zone C	Conduit 3: Zone-to-Zone	Denied	Denied	Permit

(1) Default pathway.

Create Conduit Security Policies

Create the conduit security policies that use certificates, message integrity, and data encryption between endpoints in Conduit 4 and Conduit 5.

Figure 19 - CIP Security Architecture - Conduit Security Policies

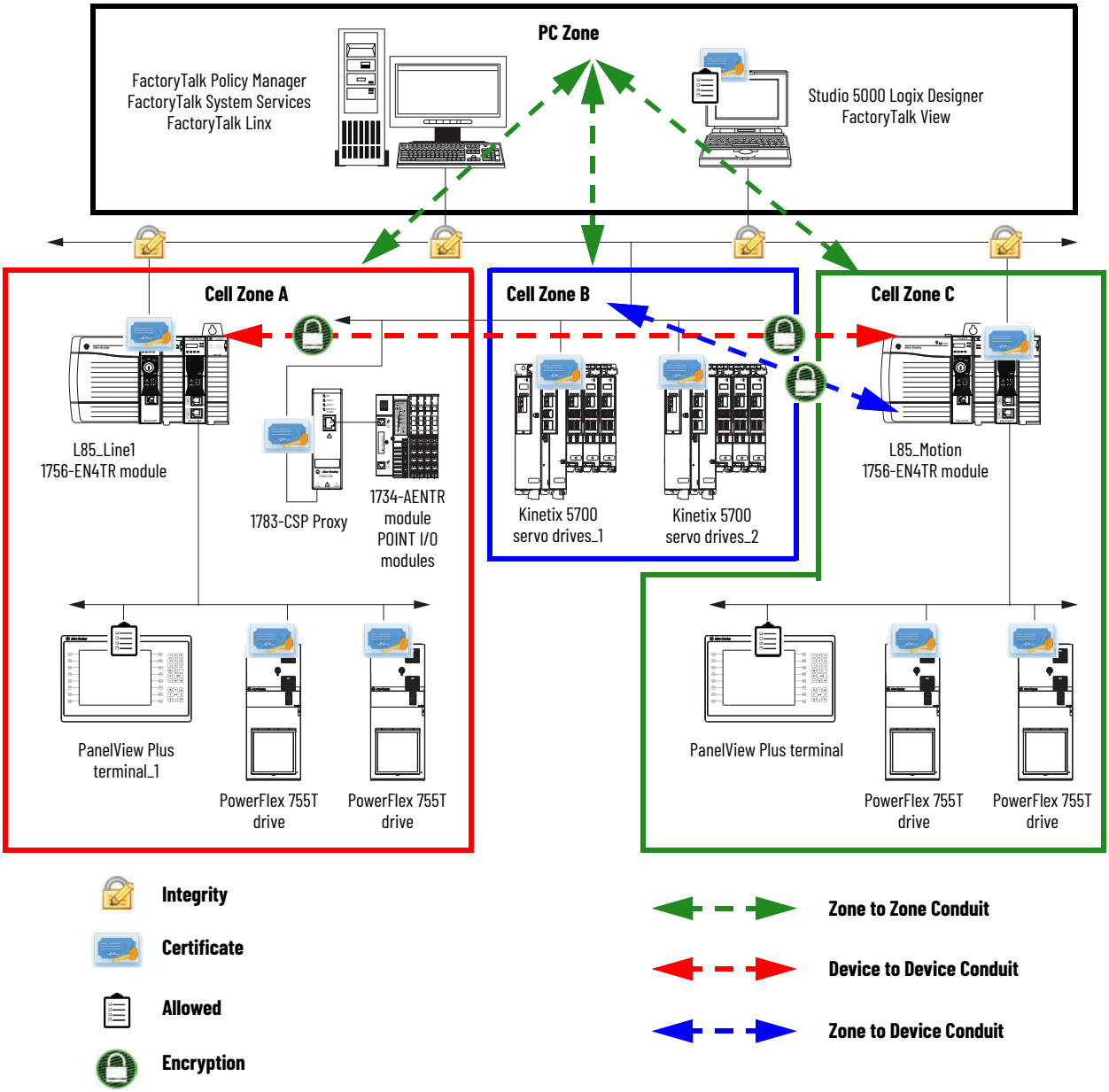


Table 18 is an example of an updated security matrix after the conduit security policies are configured.

Table 18 - Security Matrix - Conduit Security Policies Matrix

Secure Linx Communication: Conduits 1, 2, and 3	**Zone-to-Zone**		**Security Policy**
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Cell Zone A	• Certificates • Integrity • Confidentiality
	PC Zone	Cell Zone B	
	PC Zone	Cell Zone C	

Secure Controller Communication: Conduit 4	**Device-to-Device**		**Security Policy**
(Secure communication with originator and target)	L85_Line1	L85_Motion	• Certificates • Integrity • Confidentiality

Secure I/O Communication: Conduit 5	**Zone-to-Device**		**Security Policy**
(Secure communication with originator and target)	L85_Motion	Cell Zone B	• Certificates • Integrity • Confidentiality

Trusted IP (allowed)	**Zone Device to Zone Device**		
(Non-CIP Security-capable devices)	PC Zone Device:FactoryTalkNetwork Manager IP address: 192.168.1.100	Cell Zone A - Devices	• L85_Line1 (192.168.1.8) • 1756-EN4TR module (192.168.1.9) • 1783-CSP proxy (192.168.1.10) • 1734-AENTR module (192.168.11) • PanelView Plus terminal_1 (192.168.1.12) • PowerFlex 755T drive (192.168.1.13) • PowerFlex 755T drive (192.168.1.14)
		Cell Zone C - Devices	• L85_Motion (192.168.3.8) • 1756-EN4TR module (192.168.3.9) • PanelView Plus terminal (192.168.3.10) • PowerFlex 755T drive (192.168.3.11) • PowerFlex 755T drive (192.168.3.12)

Deploy Security Policies

Deploy the updated security policies to the devices as described on page 59.

CompactLogix 5380 Controllers Example Architecture

This example shows how to use CompactLogix 5380 and Compact GuardLogix 5380 controllers in an example architecture. CompactLogix 5380 and Compact GuardLogix 5380 controllers have dual built-in Ethernet ports and support the following modes:

- Linear/DLR - The controller uses one IP address for both Ethernet ports and you can secure communication to both ports.
- Dual-IP Mode - Ethernet ports A1 and A2 can connect to separate EtherNet/IP™ networks, and each port requires its own network configuration. Port A1 can connect to enterprise-level networks and device-level networks. Port A2 can only connect to device-level networks.

IMPORTANT	You can only apply CIP Security to one of the ports in Dual-IP mode. Typically, CIP Security is applied to port A1 because it can connect to enterprise-level and device-level networks.

In this example architecture, one controller is configured for Dual-IP mode, and the other controller is configured for Linear mode. On the controller that uses Dual-IP mode, Port A1 is configured for CIP Security.

Phase One of Implementation

In the first phase of the CIP Security implementation, you secure communication between the PC Zone and each IACS zone. The degree to which you secure communication depends on your system needs.

For more information on the CIP Security properties that you can use to secure communication, see Secure Data Transport on page 14.

We **recommend** that you secure communication between the PC Zone to each IACS zone because it has the most vulnerabilities from Windows-based operating systems when it is not secured.

In this phase, complete the following tasks:

- Create Zones
- Create Zone-to-Zone Conduits
- Deploy Security Policies

Create Zones

Create zones and all applicable devices including CIP Security-capable and non-CIP Security-capable devices.

- PC Zone (FactoryTalk Site servers and EWS)
- Cell Zone A (Controller zone)
- Cell Zone B (I/O zone)
- Cell Zone C (Controller zone)

IMPORTANT	The example zones that are shown in this section are all in the same subnet/VLAN.

Figure 20 - CIP Security Architecture - Zones

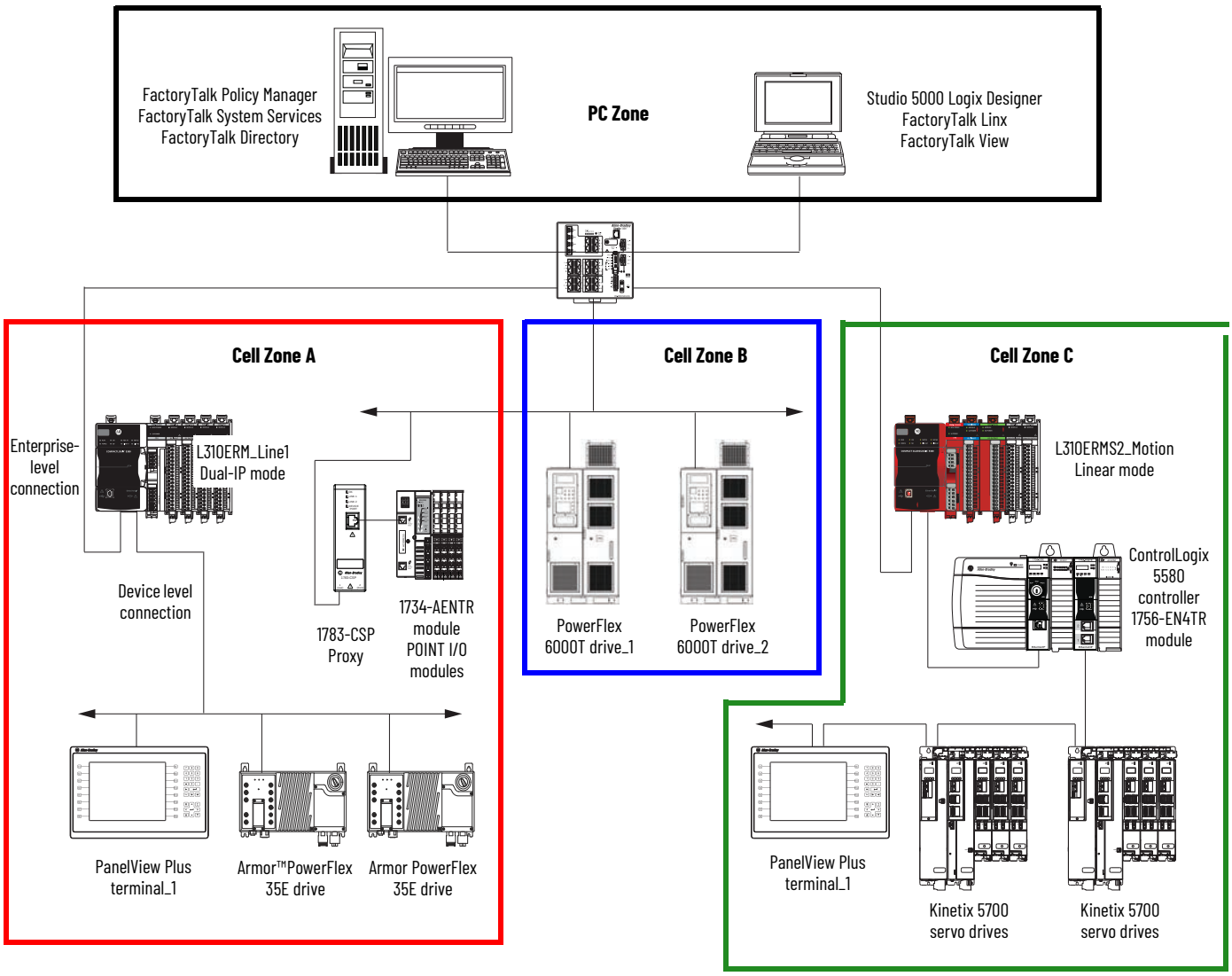


Table 19 is a security matrix with zones and devices.

Table 19 - Security Matrix - Zones

PC Zone Software	Cell Zone A	Cell Zone B	Cell Zone C
FactoryTalk Linx(1) FactoryTalk Policy Manager FactoryTalk System Services	L310ERM_Line1(2)	PowerFlex 6000T drive_1	L310ERMS2_Motion(3)
Studio 5000 Logix Designer(1) FactoryTalk View	1783-CSP proxy	PowerFlex 6000T drive_2	ControlLogix 5580 controller
	1734-AENTR module(4)		1756-EN4TR module
	PanelView Plus terminal_1(2)		PanelView Plus terminal(2)
	Armor PowerFlex 35E drive		Kinetix 5700 servo drives
	Armor PowerFlex 35E drive		Kinetix 5700 servo drives

(1) This group of software is installed on the same server/computer.
(2) This controller is configured for Dual-IP mode.
(3) This controller is configured for Linear/DLR mode.
(4) This device is not CIP Security-capable.

Create Zone-to-Zone Conduits

1. Create zone-to-zone conduits for secure CIP-connection from the FactoryTalk Linx data server and engineering workstation in the PC zone to each of the respective Controller zones named Cell Zone A, B, and C.
   - PC Zone to Cell Zone A
   - PC Zone to Cell Zone B
   - PC Zone to Cell Zone C

Figure 21 - CIP Security Architecture - Conduits

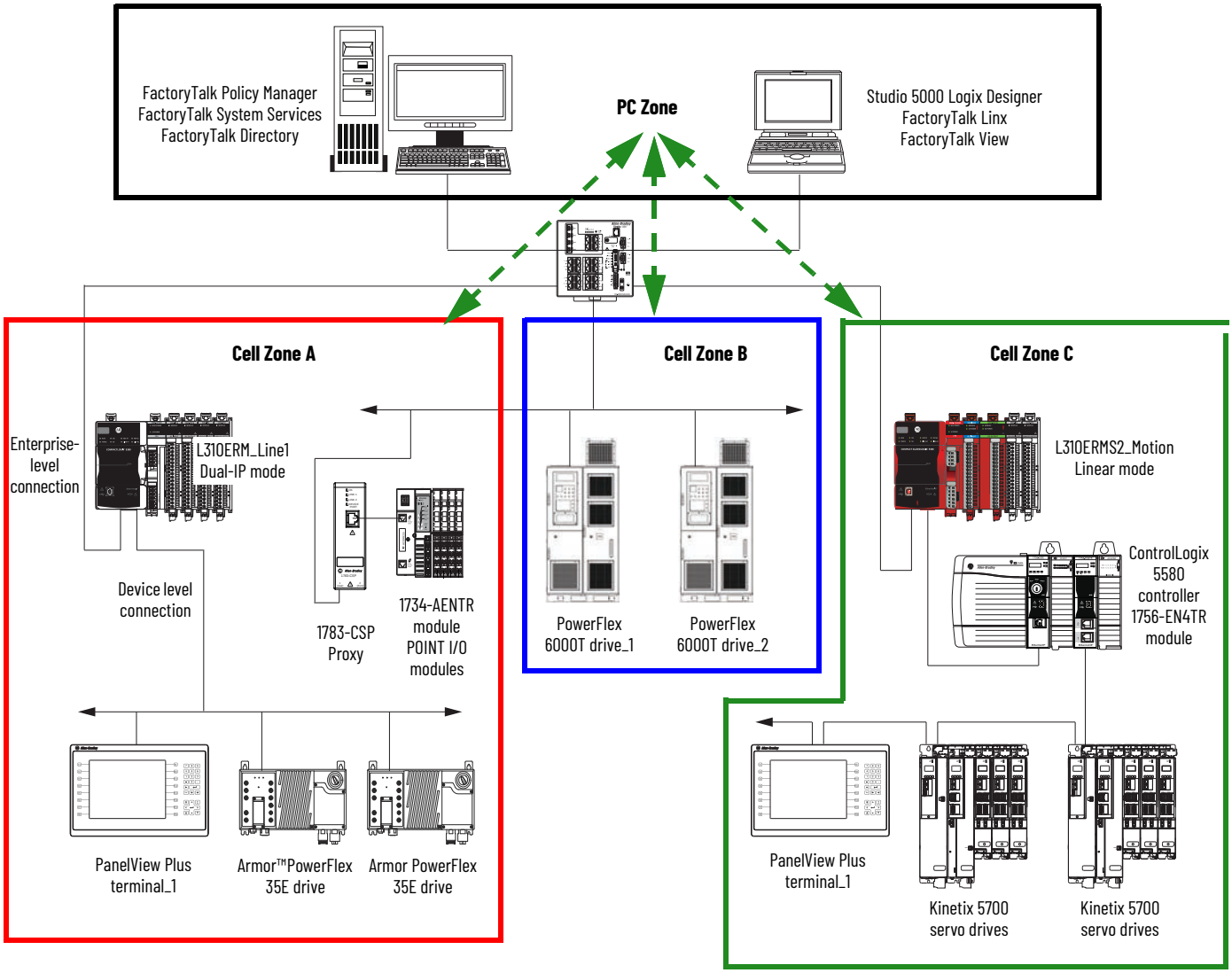


Table 20 is an example of an updated security matrix after conduits are identified and organized.

Table 20 - Security Matrix - Conduits

Source	Destination			
	PC Zone	**Cell Zone A**	**Cell Zone B**	**Cell Zone C**
PC Zone	Permit(1)	Conduit 1: Zone-to-Zone	Conduit 2: Zone-to-Zone	Conduit 3: Zone-to-Zone
Cell Zone A	Conduit 1: Zone-to-Zone	Permit	Denied	Denied
Cell Zone B	Conduit 2: Zone-to-Zone	Denied	Permit	Denied
Cell Zone C	Conduit 3: Zone-to-Zone	Denied	Denied	Permit

(1) Default pathway.

Configure Conduit Security Policies

Configure the conduit security policies that use certificates and message integrity in the following ways:

- Between the FactoryTalk Linx software to the CompactLogix 5380 controller in Cell Zone A (Controller zone).
- Between the FactoryTalk Linx software and the PowerFlex 6000T drives in Cell Zone B (I/O zone).
- From the FactoryTalk Linx software to the Compact GuardLogix 5380 controller in Cell Zone C (Controller zone).

Optionally, you can establish an allowed list from the PC zone to each IP address of the non-CIP Security-capable devices.

Figure 22 - CIP Security Architecture - Conduit Security Policies

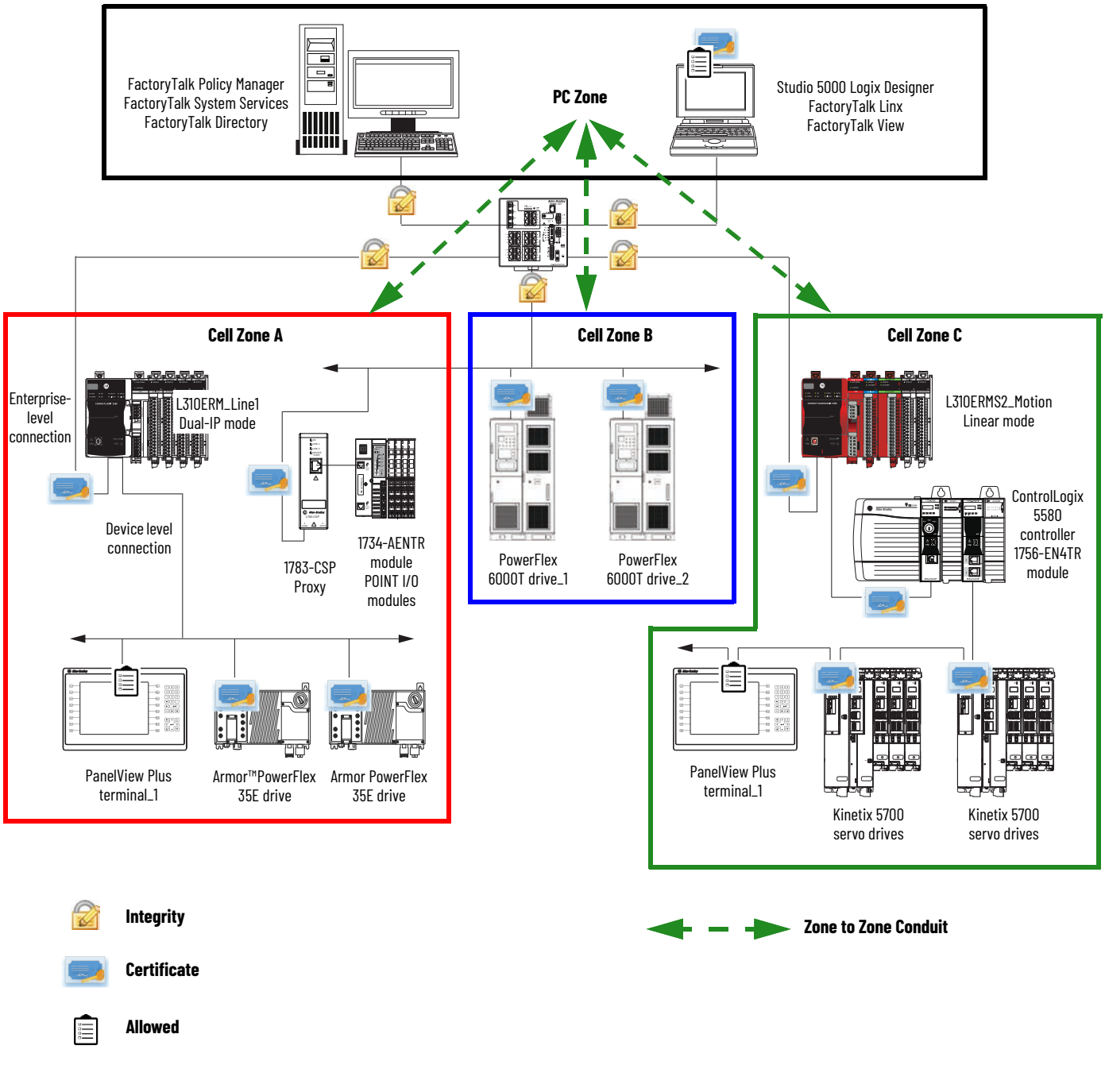


Table 21 is an example of an updated security matrix after the conduit security policies are configured.

Table 21 - Security Matrix - Conduit Security Policies Matrix

Secure Linx Communication: Conduits 1, 2, and 3	Zone to Zone		Security Policy
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Cell Zone A	• Certificates • Integrity • Confidentiality
	PC Zone	Cell Zone B	
	PC Zone	Cell Zone C	

Trusted IP (allowed)	Zone Device-to-Zone Device		
(Non-CIP Security-capable devices)	PC Zone Device: FactoryTalk Network Manager IP address: 192.168.1.100	Cell Zone A - Devices	• L310ERM_Line1 – Port A1 (192.168.2.2) – Port A2 (192.168.1.8) • 1783-CSP proxy (192.168.1.9) • 1734-AENTR module (192.168.10) • PanelView Plus terminal_1 (192.168.1.11) • Armor PowerFlex 35E drive (192.168.1.12) • Armor PowerFlex 35E drive (192.168.1.13)
		Cell Zone C - Devices	• L310ERMS2_Motion (192.168.3.8) • ControlLogix 5580 controller (192.168.3.9) • 1756-EN4TR module (192.168.3.10) • PanelView Plus terminal (192.168.3.11) • Kinetix 5700 drive (192.168.3.12) • Kinetix 5700 drive (192.168.3.13)

Deploy Security Policies

Deploy the security policies to the devices as described on page 59.

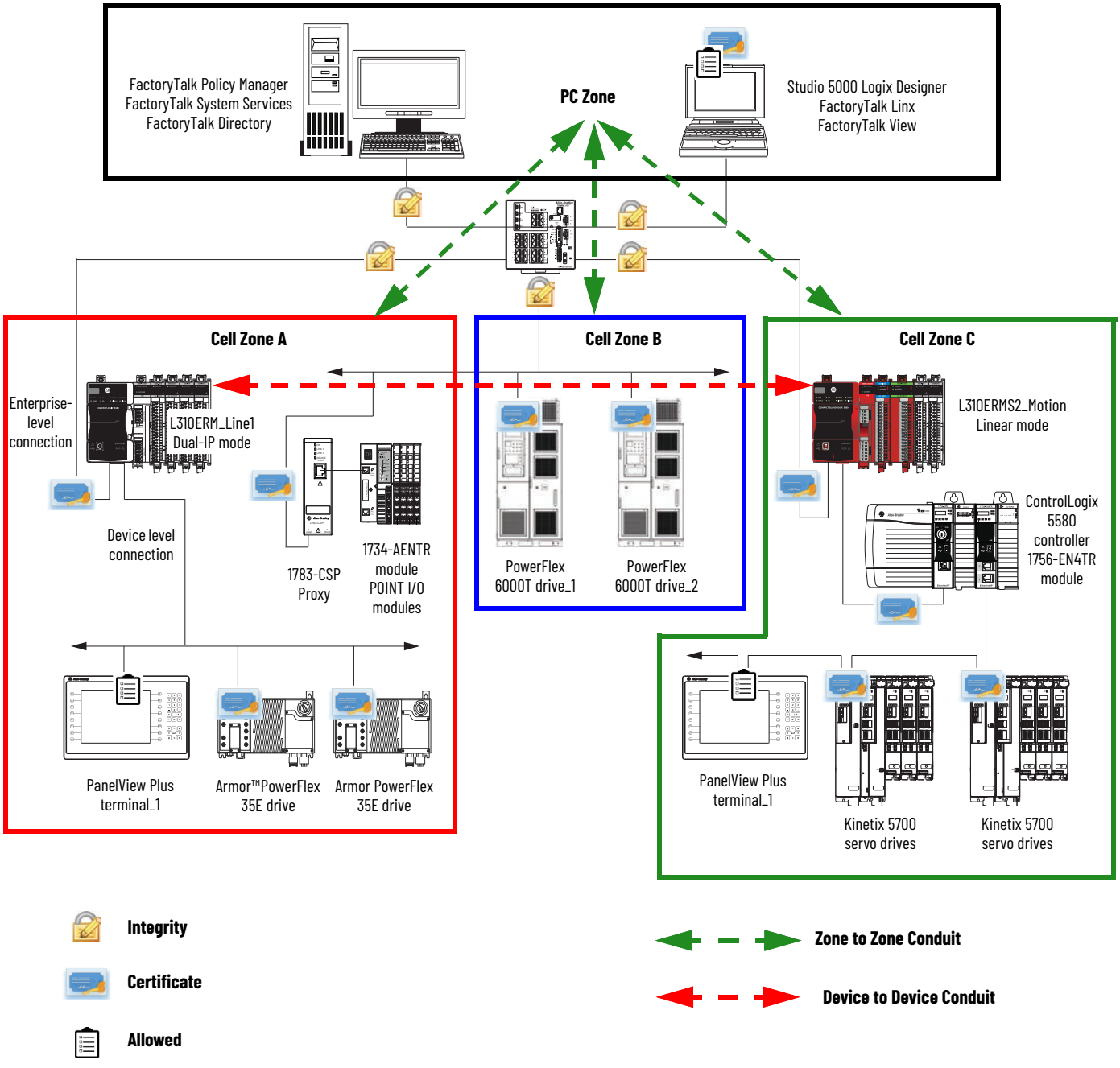
Phase Two of Implementation

In the second phase of the CIP Security implementation, you secure communication between device to device for micro-segmentation. Use the existing zones that are created in the first phase.

Create a Device-to-Device Conduit

Create a device-to-device conduit for secure CIP-connection from the CompactLogix 5380 controller in Cell Zone A (Controller zone) to the Compact GuardLogix 5380 controller in Cell Zone C (Controller zone).

Figure 23 - CIP Security Architecture - Device-to-Device Conduit Added



Create a Zone-to-Device Conduit

Create a zone-to-device conduit from the PowerFlex 6000T drives in Cell Zone B (I/O zone) to the Compact GuardLogix 5580 controller in Cell Zone C (Controller zone).

Figure 24 - CIP Security Architecture - Zone-to-Device Conduit Added

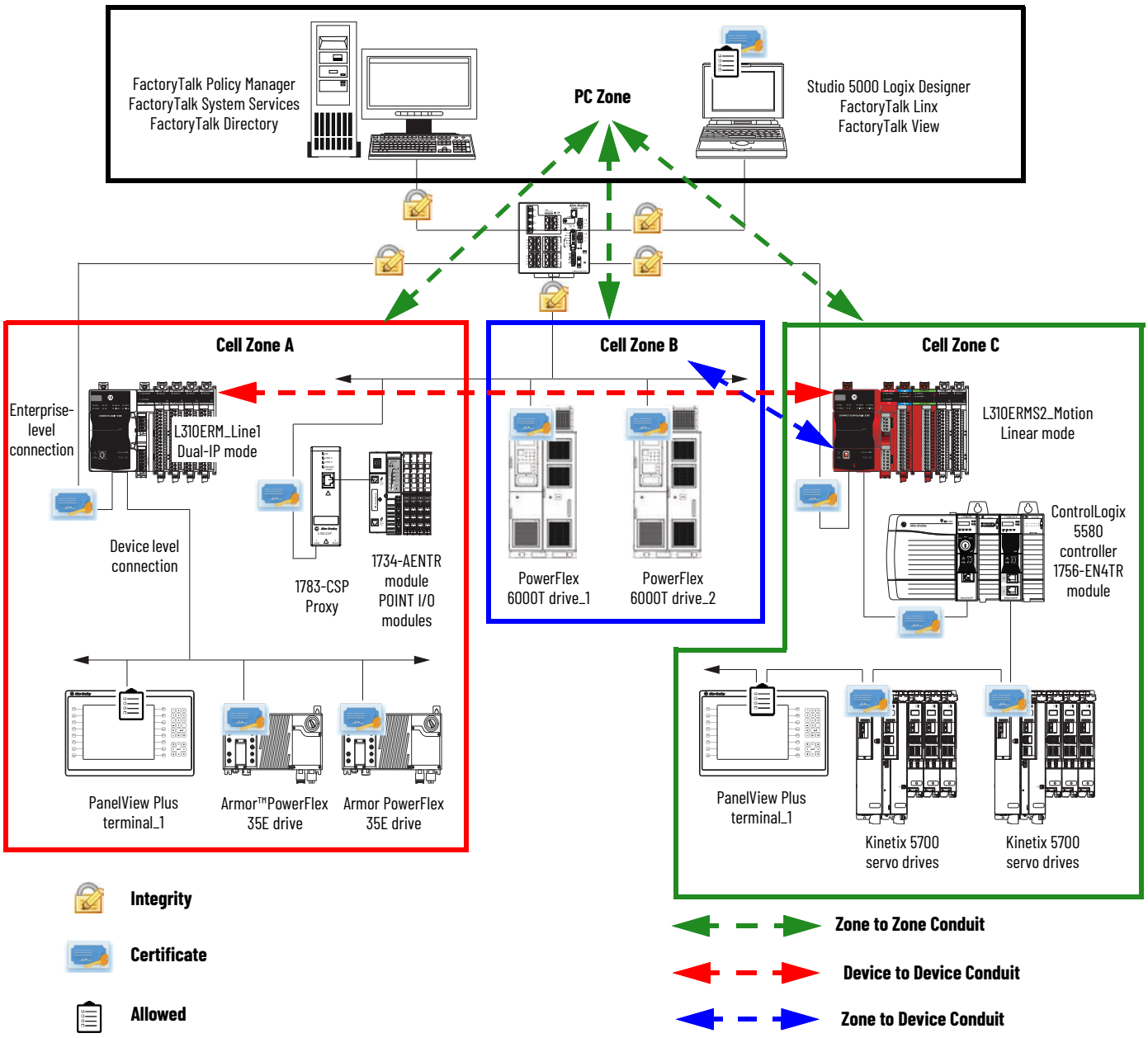


Table 22 is an example of an updated security matrix after conduits are identified and organized.

Table 22 - Security Matrix - Device-to-Device and Zone-to-Zone Conduits Added

Source	Destination			
	PC Zone	**Cell Zone A**	**Cell Zone B**	**Cell Zone C**
PC Zone	Permit(1)	Conduit 1: Zone-to-Zone	Conduit 2: Zone-to-Zone	Conduit 3: Zone-to-Zone
Cell Zone A	Conduit 1: Zone-to-Zone	Permit	Denied	Conduit 4: Device-to-Device
Cell Zone B	Conduit 2: Zone-to-Zone	Denied	Permit	Conduit 5: Zone-to-Device
Cell Zone C	Conduit 3: Zone-to-Zone	Denied	Denied	Permit

(1) Default pathway.

Create Conduit Security Policies

Create the conduit security policies that use certificates, message integrity, and data encryption between endpoints in Conduit 4 and Conduit 5.

Figure 25 - CIP Security Architecture - Conduit Security Policies

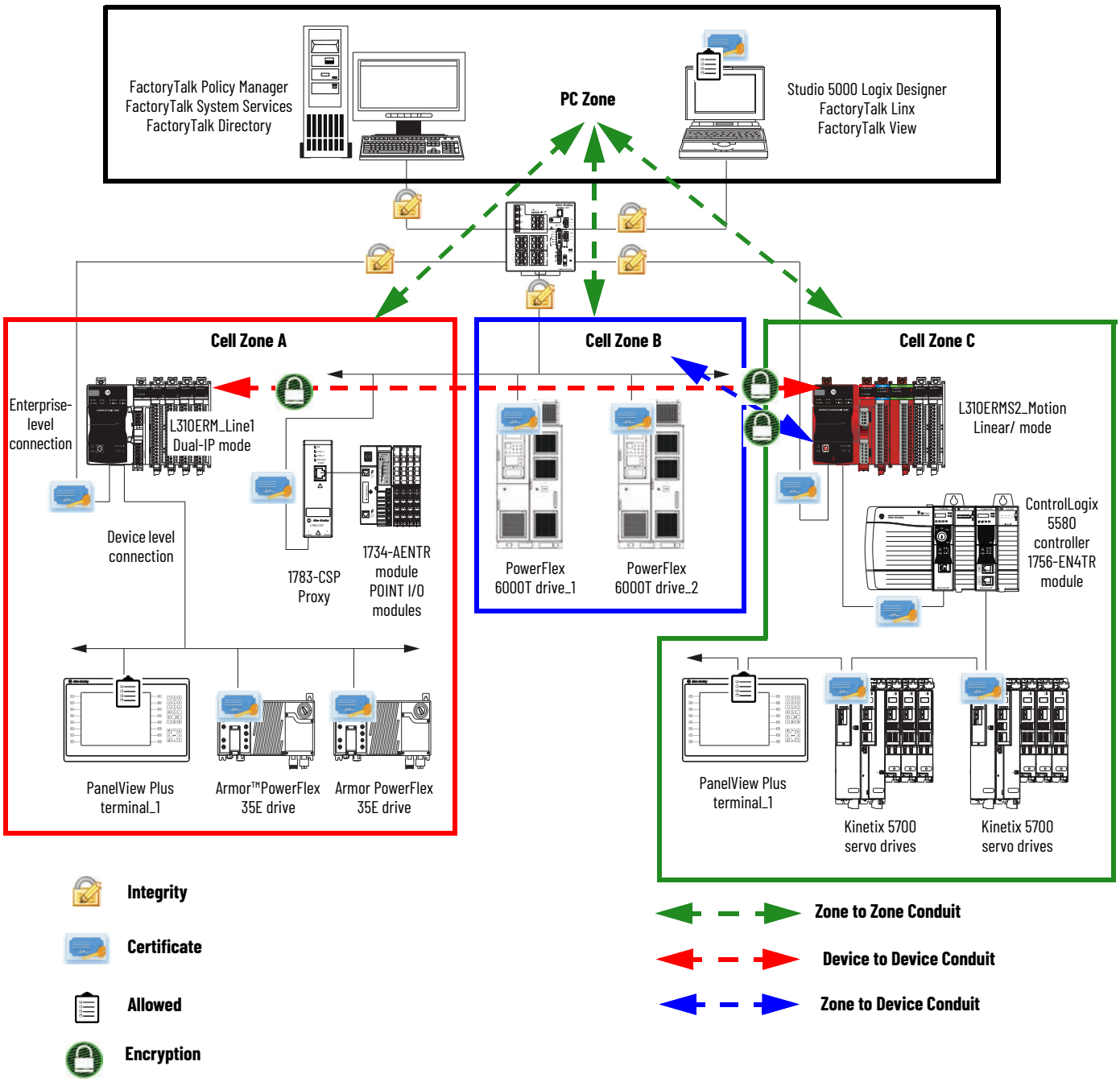


Table 23 is an example of an updated security matrix after the conduit security policies are configured.

Table 23 - Security Matrix - Conduit Security Policies Matrix

Secure Linx Communication: Conduits 1, 2, and 3	**Zone-to-Zone**		**Security Policy**
Zone to Zone (Secure communication with FactoryTalk Linx.)	PC Zone	Cell Zone A	• Certificates • Integrity • Confidentiality
	PC Zone	Cell Zone B	
	PC Zone	Cell Zone C	

Secure Controller Communication: Conduit 4	**Device-to-Device**		**Security Policy**
(Secure communication with originator and target)	L310ERM_Line1	L310ERMS2_Motion	• Certificates • Integrity • Confidentiality

Secure I/O Communication: Conduit 5	**Zone-to-Device**		**Security Policy**
(Secure communication with originator and target)	L310ERMS2_Motion	Cell Zone B	• Certificates • Integrity • Confidentiality

Trusted IP (allowed)	**Zone Device to Zone Device**		
(Non-CIP Security-capable devices)	PC Zone Device:FactoryTalkNetwork Manager IP address: 192.168.1.100	Cell Zone A - Devices	• L310ERM_Line1 – Port A1 (192.168.2.2) – Port A2 (192.168.1.8) • 1783-CSP proxy (192.168.1.9) • 1734-AENTR module (192.168.10) • PanelView Plus terminal_1 (192.168.1.11) • Armor PowerFlex 35E drive (192.168.1.12) • Armor PowerFlex 35E drive (192.168.1.13)
		Cell Zone C - Devices	• L310ERMS2_Motion (192.168.3.8) • ControlLogix 5580 controller (192.168.3.9) • 1756-EN4TR module (192.168.3.10) • PanelView Plus terminal (192.168.3.11) • Kinetix 5700 drive (192.168.3.12) • Kinetix 5700 drive (192.168.3.13)

Deploy Security Policies

Deploy the updated security policies to the devices as described on page 59.

Add or Replace A Device In a CIP Security System

This section describes how to perform the following tasks in an IACS with CIP Security™ implemented:

- Add a new device
- Replace a device

The processes for adding or replacing a device differ based on whether the device supports Automatic Policy Deployment (APD).

APD lets EtherNet/IP™ endpoints, for example, field devices, initiate deployment of security policies that are defined on a system server. This feature makes it easier to add and replace CIP™ Security-capable devices that support APD to an IACS with CIP Security implemented.

Automatic Policy Deployment

APD leverages ODVA's CIP Security Pull Model concept that enables EtherNet/IP endpoints, for example, field devices, to initiate deployment of policies defined on a system server. That is, a CIP Security-capable endpoint can obtain a certificate from the certificate authority.

During the onboarding process, the devices are discovered, identified, and provisioned with identities and temporary policies. The onboarded devices can then be merged into the security model and have their policies deployed automatically.

By using APD, you can improve the system:

- Operational readiness level
- Uptime
- Security (by provisioning security policies to field devices as soon as they power up)

Table 24 lists the products that support APD.

Table 24 - Automatic Policy Deployment Requirements

Software or Component	Minimum Software Version	Minimum Firmware Revision
FactoryTalk Policy Manager	6.30	–
FactoryTalk System Services	6.30	–
FactoryTalk Linx	6.30	–
CompactLogix 5380 Controllers	–	34.011
CompactLogix 5380 Process Controllers	–	34.011
Compact GuardLogix™ 5380 Controllers	–	34.011
ControlLogix 5580 Controllers(1)	–	34.011
ControlLogix 5580 Process Controllers	–	34.011
1756-EN4TR ControlLogix EtherNet/IP Communication Module	–	4.001
GuardLogix 5580 Controllers	–	34.011

(1) This includes ControlLogix 5580 standard and XT controllers.

APD requires a system server with FactoryTalk Policy Manager installed and FactoryTalk System Services running.

After the FactoryTalk Policy Manager installation, FactoryTalk System Services start automatically with Windows® and run independently from FactoryTalk Policy Manager. FactoryTalk System Services operate in the background even if the FactoryTalk Policy Manager application is closed.

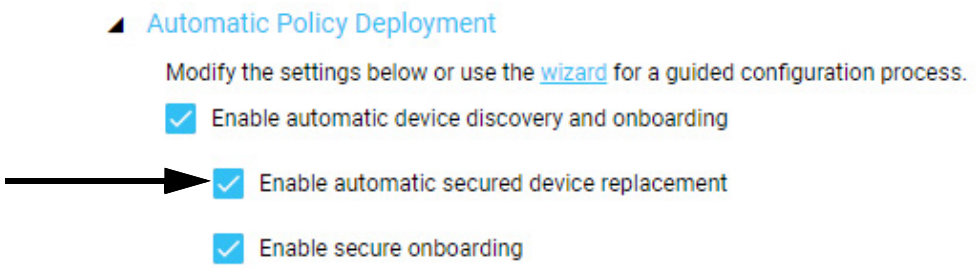
Enable Automatic Policy Deployment

By default, APD is **enabled in the products** that support it, that is, those listed in Table 24.

However, by default, APD is **disabled in FactoryTalk Policy Manager** software.

To enable APD, you must check the boxes in the Automatic Policy Deployment section of FactoryTalk Policy Manager software. The Automatic Policy Deployment section is in the software's global settings.

IMPORTANT: If Enable automatic secured device replacement is not enabled, the security policy is not automatically deployed to a new device. In this case, you must manually start the deployment process.



Deployment Operation

APD discovers the device on the network that you can add to the security model.

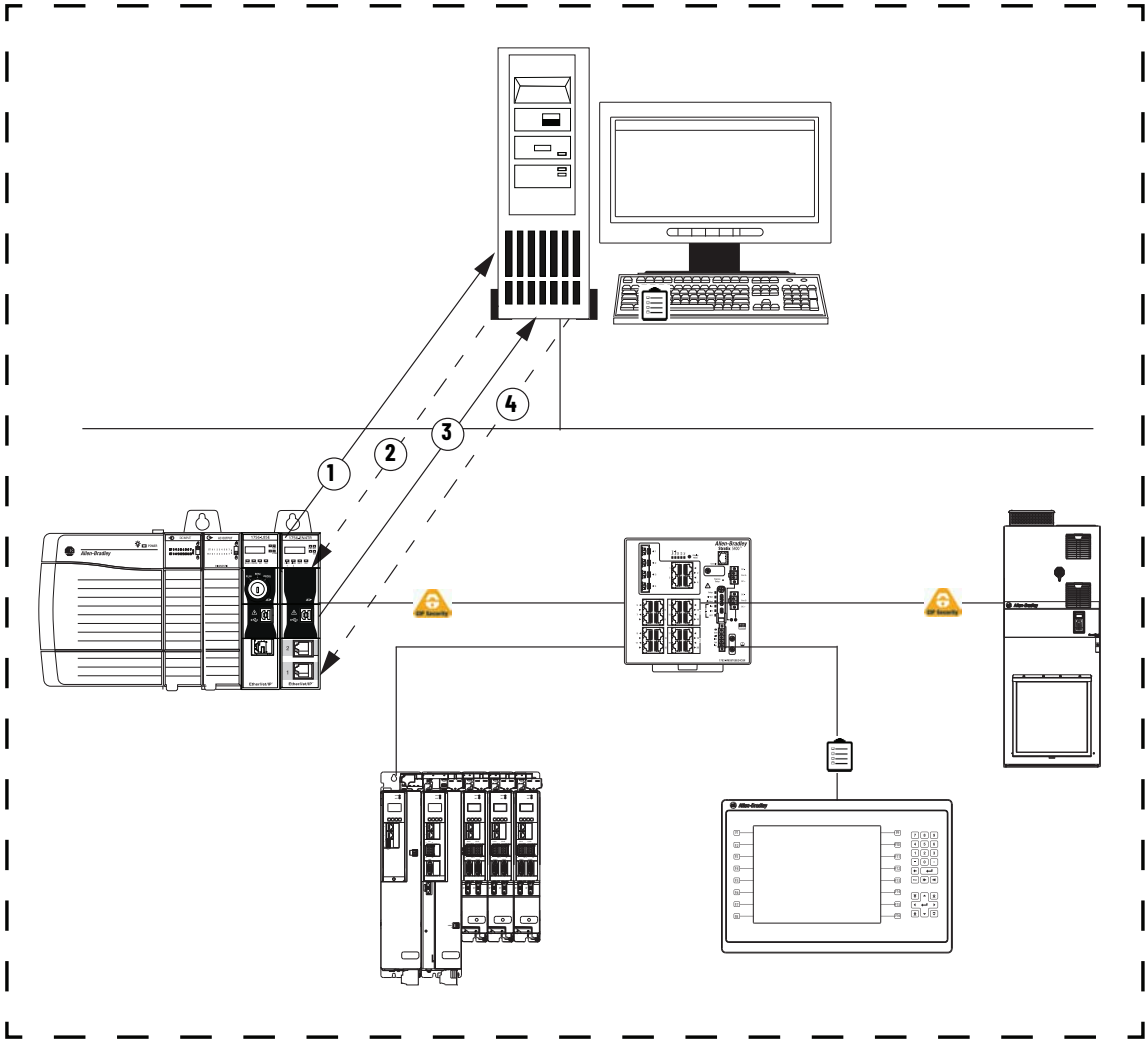
IMPORTANT
- The server with the certificate authority, that is, FactoryTalk System Services, must be turned on and connected to the EtherNet/IP network.
- APD can onboard and merge only one EtherNet/IP device interface. This applies to CompactLogix 5380 and Compact GuardLogix 5380 controllers when they're configured for Dual-IP mode.

The following steps occur when an endpoint uses APD:

1. The endpoint uses the Domain Name Server-based Service Discovery (DNS-SD) technology to discover the server.

   If FactoryTalk System Services and FactoryTalk Policy Manager are on another subnet or VLAN, you need an external DNS-SD server or a switch with technology that bridges mDNS over subnets.
2. The server acknowledges the endpoint via FactoryTalk System Services.
3. The endpoint uses the Enrollment over Secure Transport (EST) technology to request a certificate from that server.
4. The server sends the endpoint a certificate and temporary policy.

Figure 26 - Steps to Using APD



Depending on your requirements, you can set APD to:

- Automatically or manually deploy the configuration of discovered devices that match the devices in the security model.
- Allow or restrict the devices in the Onboarding Area from connecting with other devices in the network.

The APD process is independent from the manual security policy deployment process.
The manual security policy model deployment process can interrupt the APD process. Once the security model is deployed, APD continues adding and merging the discovered devices.

For auditing and troubleshooting purposes, APD indicates changes to the security model with:

- The Results pane updates.
- Toast notifications for onboarding devices and merged devices.
- The following icons throughout the FactoryTalk Policy Manager interface:

Icon	Event
	Devices newly added to the Onboarding Area.
	Automatically merged and deployed devices.
	Automatically merged devices.

Onboarding

The onboarding process automatically identifies EtherNet/IP endpoints and provisions certificates and temporary policies. Once the onboarding process finishes, the identified devices are placed in the Onboarding Area.

The devices in the Onboarding Area aren't a part of the security model. You can't add a conduit to the Onboarding Area or to any onboarding device. Depending on the onboarding policy, you can allow or restrict the onboarding devices from connecting with other devices in the network.

While you can restrict communication over the EtherNet/IP network, you cannot restrict communication over the backplane. For example, you can restrict connections to a ControlLogix 5580 controller via its Ethernet port. However, a module in the same chassis can still communicate with the controller via the backplane.

When the device is in the Onboarding area, there is security because other devices can't communicate with the device. You must add the device to the FactoryTalk Policy Manager security model for other devices to communicate with it.

You can manually move the devices from the Onboarding Area into the security model.

IMPORTANT	When you move a device from the Onboarding Area to a zone or make the device unassigned, you can't assign the device to the Onboarding Area again.

If you delete a device that can be discovered by APD, FactoryTalk Policy Manager prompts you to:

- Disable the automatic discovery for the endpoint to help prevent the device from reappearing in the Onboarding Area.
- Keep the automatic discovery enabled to restore the device in the Onboarding Area.

Device Does Not Appear in Onboarding Area

It is possible that a device that supports APD is connected to the network and doesn't appear in the Onboarding area of FactoryTalk Policy Manager software.

If the APD function is disabled on the device, it does not appear in the Onboarding Area. You can enable APD by resetting the device to the out-of-the-box state.

FactoryTalk System Services starts the Multicast DNS (mDNS) server.

Initially, a CIP Security-capable device sends a DNS-SD query to the DNS server (if its address is entered in the device's network parameters) to discover an EST server.

If no DNS server is configured or anything goes wrong, then the CIP Security-capable device sends a mDNS request and waits for response from any mDNS responder.

Once the EST server has been discovered then the device interacts with it to request an identity and trust information.

The following issues can prevent devices from appearing in Onboarding Area:

- For some reason, a firewall is preventing communication to mDNS and/or EST servers, therefore FactoryTalk System Services cannot respond to requests.

  To resolve this issue, you must add or modify the firewall rules to allow the communication between the CIP Security-capable device and the mDNS and/or EST servers.

  The ports that must be enabled are:

  - mDNS: UDP 5353
  - EST: TCP 40014

  If this issue exists in your application, we **recommend** that you use resources available with the company that designed your firewall to resolve the issue.
- If multiple network interfaces are used in the workstation, there are two IP addresses that are used in the same workstation, one for each interface.

  In this case, FactoryTalk System Services software can fail to identify, and use, the correct IP addresses. That is, the EST server uses one IP address. But the mDNS-SD functions as if the EST server is using the other IP address.

  As a result, the request for a certificate is not responded to, and the device is not onboarded.

  For more information, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

Use Switch to Respond to mDNS-SD Requests

If the device is connected to a switch that knows the location of the server with FactoryTalk System Services installed on it, you can configure the switch to respond to the mDNS requests on behalf of the server with FactoryTalk System Services.

In this case, the switch functions more like a proxy. When the device makes the request for the EST server, the switch responds with the location of the EST server.

However, you must configure the switch to respond with the location of the EST server. If the switch is not properly configured, the device can't obtain the IP address of the EST server.

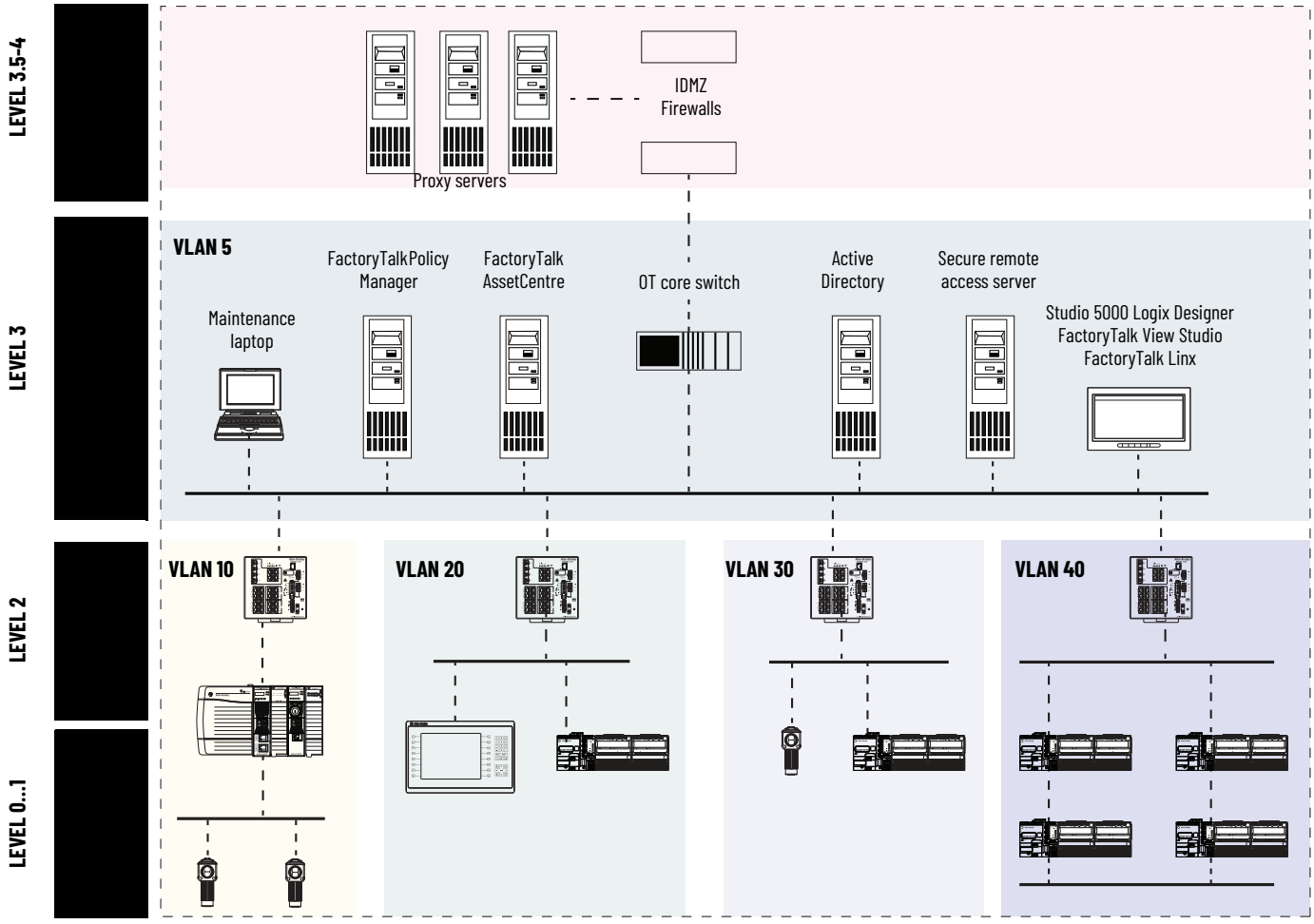
IMPORTANT Remember the following:

- If the server with FactoryTalk System Services installed on it is on the same subnet as the device that is being onboarded, mDNS support is not required in any switch.
- If the server with FactoryTalk System Services installed on it is on another subnet than the device that is being onboarded, your application must use one of the following:
  - External DNS-SD server
  - Switch that can bridge mDNS over subnets

Automatic Policy Deployment Example

The following is an example of a system in which FactoryTalk System Services and FactoryTalk Policy Manager are on different subnets.

The application requires an external DNS-SD server or a switch with technology that bridges mDNS over subnets.



Merging

Depending on the security model and the devices available in the network, the merging process can be automatic or manual.

Automatic Merging

The merging process is automatic if the onboarding device has the same IP address as the matching device in the security model.

The onboarding device does not need to be identical with the matching device in the security model. During the merging process, the newer device properties overwrite the older device properties.

IMPORTANT The automatic merging process never overwrites the following properties:

- IP address
- Device name
- Device description

Manual Merging

The merging process is manual if the onboarding device can't be associated with any device in the security model.

An administrator can manually move the discovered device from the Onboarding Area to the security model.

Firmware Revision Updates

Some components have a minimum required firmware revision to operate in an IACS with CIP Security that is less than the minimum required firmware revision to use Automatic Policy Deployment. You can update the firmware revision to use Automatic Policy Deployment.

For example, if you can use a 1756-EN4TR ControlLogix EtherNet/IP communication module, firmware revision 3.002, in an IACS with CIP Security. You can replace the communication module with another of the same firmware revision level, that is, revision 3.002. But the replacement communication module does not support Automatic Policy Deployment.

In this example, for the replacement communication module to support Automatic Policy Deployment, updates the communication module from revision 3.002 to revision 4.001 or later.

Benefits of Automatic Policy Deployment

The following benefits exist with the APD

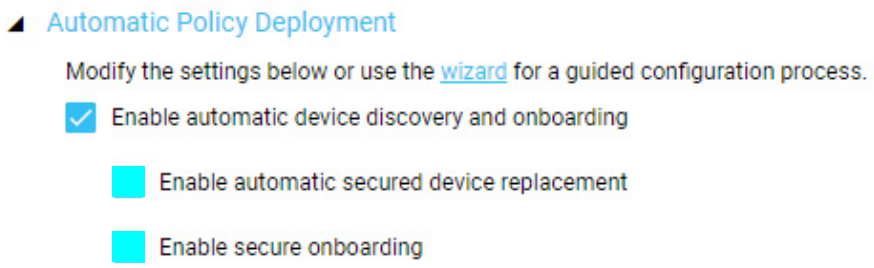
- Easier device replacement - Certificates are unique to each device. With APD, once the replacement device receives the new certificate, it can communicate securely with the server.
- Initial commissioning - When you set up a system, APD lets identity distribution be more automated.
- Reduced risk for a device on the network - By using a staging area, the trust-on-first-use (TOFU) window is shortened.

Disable Automatic Policy Deployment in FactoryTalk Policy Manager

To disable APD in FactoryTalk Policy Manager software, you must clear the boxes in the Automatic Policy Deployment section of FactoryTalk Policy Manager software.

When you disable APD in the software, you disable the EST services and the queries from any APD-capable devices are not responded to.

The Automatic Policy Deployment section is in the software's global settings.



Add a New Device That Supports Automatic Policy Deployment

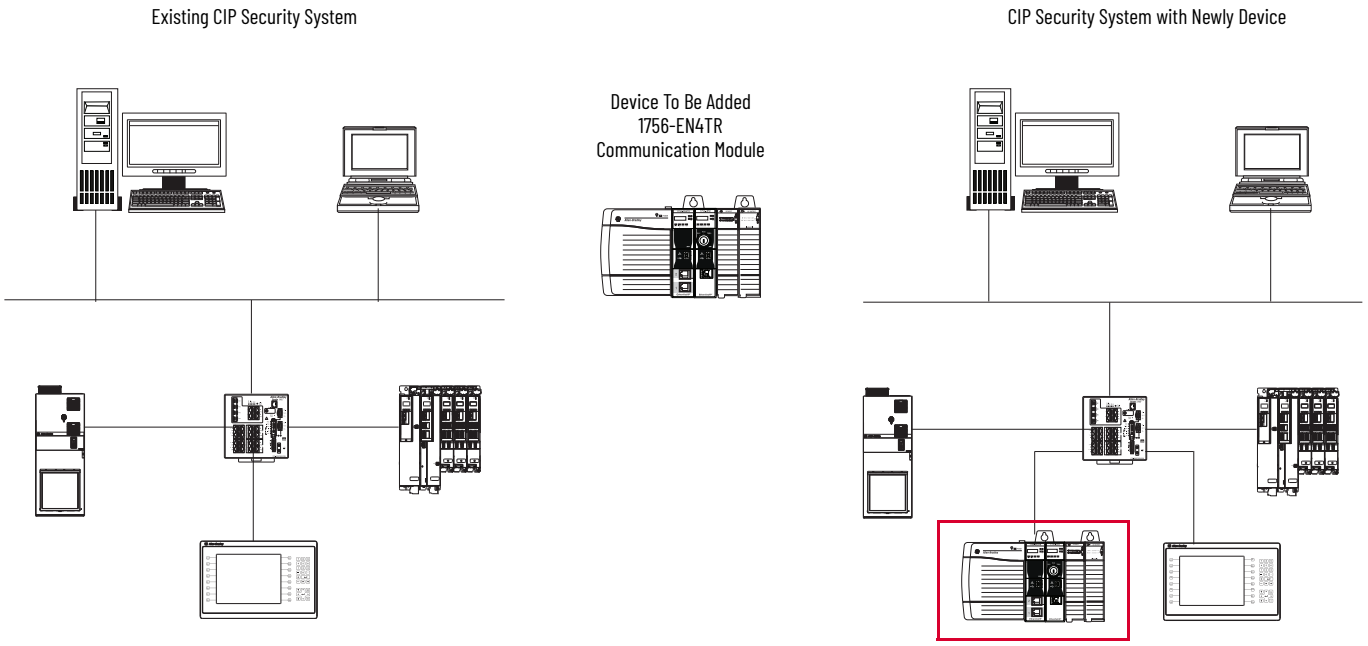
There are two scenarios in which a device that supports APD is added to an IACS with CIP Security implemented:

- New Device is Not in the Security Policy Model
- New Device is in the Security Policy Model

New Device is Not in the Security Policy Model

In this scenario, you add a device that wasn't previously in the FactoryTalk Policy Manager security policy model.

Figure 27 - Add a New Device When the Device is Not in the Security Policy Model



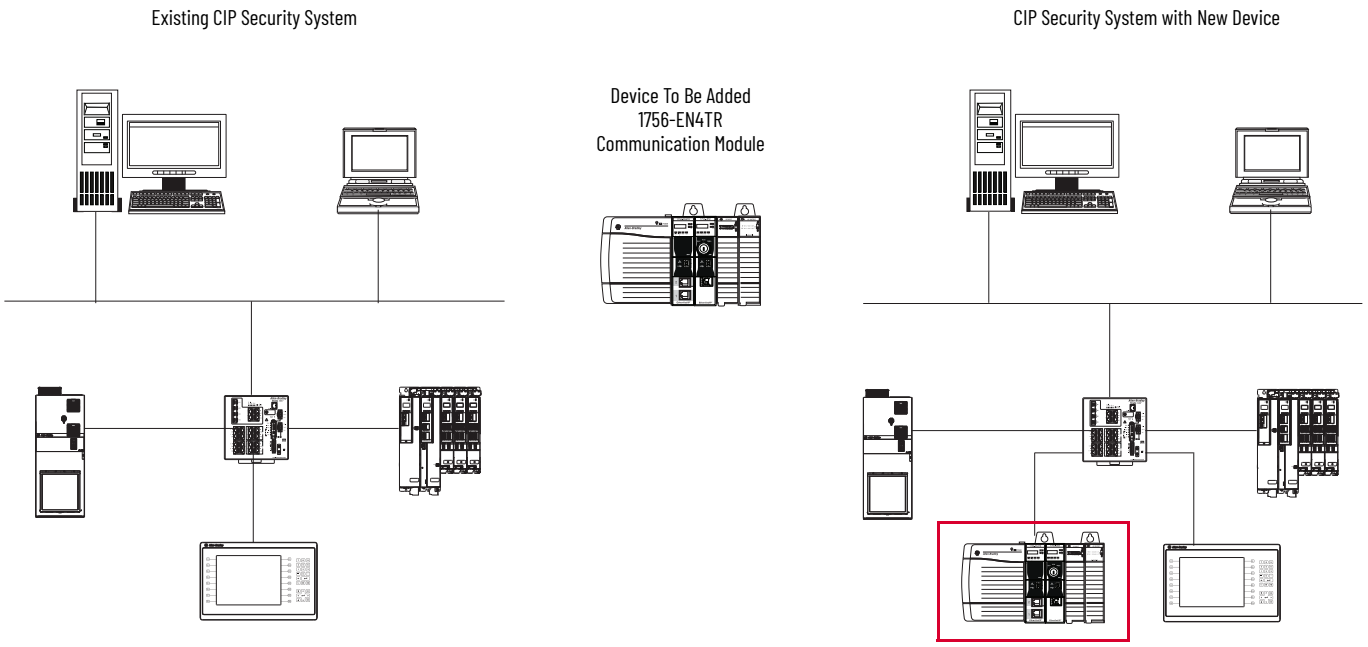
Complete the following steps.

1. Connect the 1756-EN4TR communication module to the network.
2. When the 1756-EN4TR communication module appears in the Onboarding area of FactoryTalk Policy Manager software, merge the 1756-EN4TR communication module into the security policy model.
3. Deploy the updated security model as described in Deploy Security Model on page 59.

New Device is in the Security Policy Model

In this scenario, you add a device that is in the FactoryTalk Policy Manager security policy model but the policy wasn't deployed to that device yet.

Figure 28 - Add a New Device When Device is in the Security Policy Model



Complete the following steps.

1. Connect the 1756-EN4TR communication module to the network.

   The communication module appears in the Onboarding area of FactoryTalk Policy Manager software and is automatically merged into the security model.
2. Deploy the updated security model as described in Deploy Security Model on page 59.

Replace a Device That Supports Automatic Policy Deployment

There are two scenarios in which a device that supports APD replaces a device:

- Replacement Device is Not Identical to the Existing Device
- Replacement Device is Identical to the Existing Device

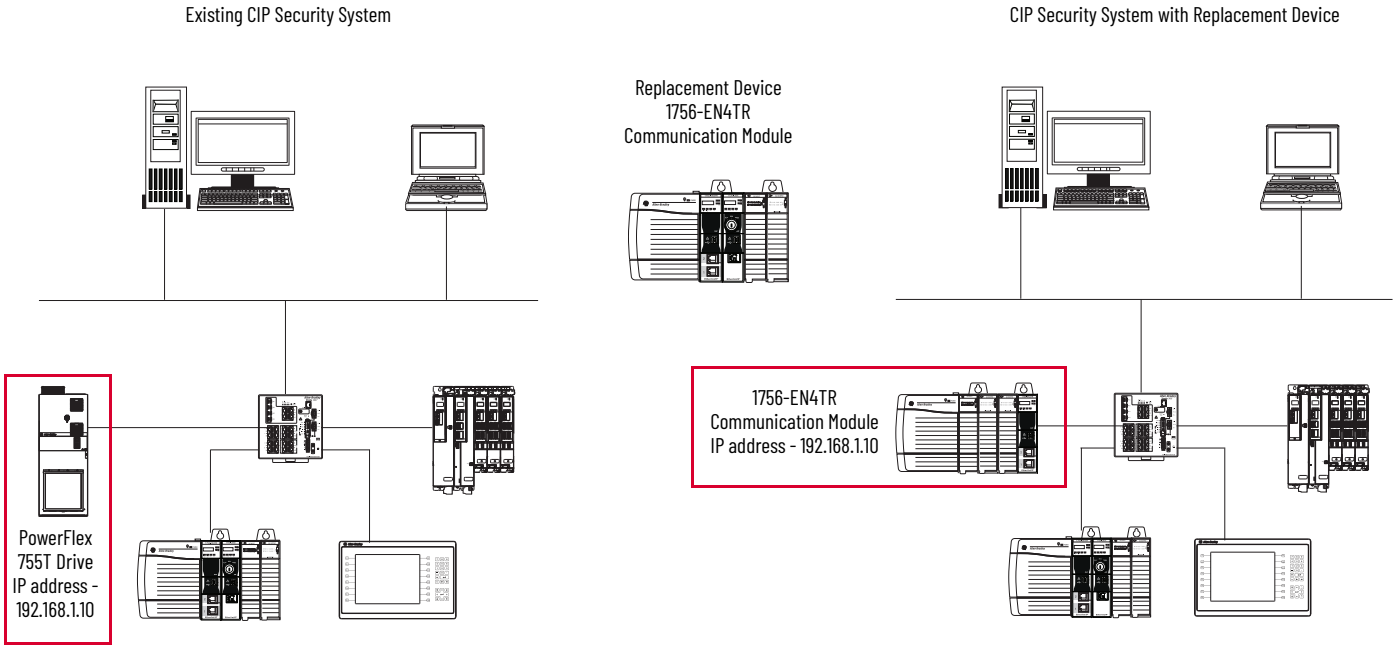
Replacement Device is Not Identical to the Existing Device

In this scenario, you replace a device that is in the FactoryTalk Policy Manager security policy model and has the same IP address. However, the replacement device isn't the same as the existing device.

IMPORTANT When you replace a device with another device that uses the same IP address, the new device's properties overwrite the existing device's properties.

Figure 29 shows an example in which the PowerFlex 755T drive with IP address 192.168.1.10 is replaced by a 1756-EN4TR communication module with the same IP address.

Figure 29 - Replace a Device With a New Device That Only Uses the Same IP Address Only



Complete the following steps.

1. Disconnect the PowerFlex 755T drive from the network.
2. Connect the 1756-EN4TR communication module to the network.

   The communication module appears in the Onboarding area of FactoryTalk Policy Manager software and is automatically merged into the security model.

   You can access the Onboarding area via the following in FactoryTalk Policy Manager:
   - Canvas tab - When devices are set up, they automatically appear in the Canvas tab.
   - Devices tab and finding the device
3. Deploy the updated security model as described in Deploy Security Model on page 59.

Replacement Device is Identical to the Existing Device

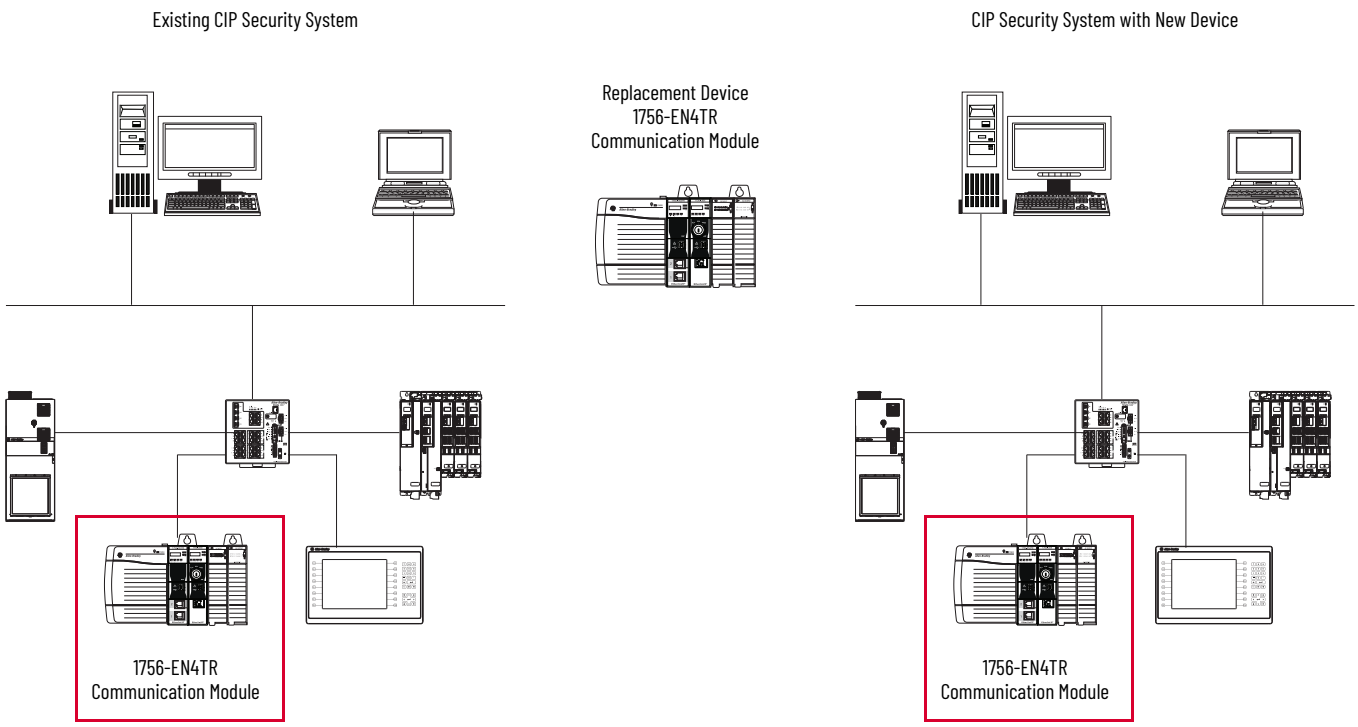
In this scenario, you replace a device that is in the FactoryTalk Policy Manager security policy model. The replacement device is identical to the existing device. That is, the following properties match between the devices:

- IP address
- Vendor
- Product type
- Product code

IMPORTANT This process is known as **Secured Device Replacement**.

Figure 30 shows an example in which a 1756-EN4TR communication module is replaced by a 1756-EN4TR communication module with the same properties.

Figure 30 - Replace a Device With An Identical Device



Complete the following steps.

1. Disconnect the 1756-EN4TR communication module from the network.
2. Connect the replacement 1756-EN4TR communication module to the network.

   The communication module appears in the Onboarding area of FactoryTalk Policy Manager software and is automatically merged into the security model.

The security policy is automatically deployed to the new communication module using APD.

Devices That Do Not Support Automatic Policy Deployment

Table 25 lists CIP Security-capable devices that do not support APD.

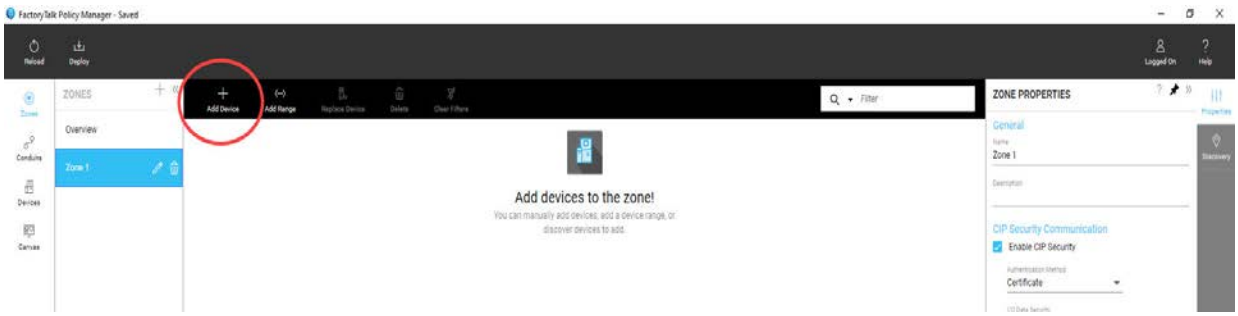
Table 25 - CIP Security-capable Devices That Do Not Support APD

Software or Component	Software Version	Firmware Revision
FactoryTalk® Policy Manager	6.21 or later	–
FactoryTalk System Services		–
FactoryTalk Linx		–
ControlLogix® 5580 Controllers	–	33.xxx or earlier
Armor™ PowerFlex Drives	–	10.001
Kinetix® 5300 Drives	–	13.003
Kinetix 5700 Drives	–	11.001
PowerFlex 755T Drives	–	10.001
PowerFlex 755TS Drives	–	11.001
PowerFlex 6000T Drives	–	9.001

Add a Device That Does Not Support APD to an Existing CIP Security System

Complete the following steps to add a CIP Security-capable device that does not support APD to an existing CIP Security system.

1. Connect the device to the network.
2. In FactoryTalk Policy Manager software, add devices to the zone. You can add devices in the following ways:
   - Discover devices via FactoryTalk Linx.
   - Manually add devices from the catalog.



3. Deploy the updated security model as described in Deploy Security Model on page 59.

Replace a Secured Device That Does Not Support APD in an Existing System

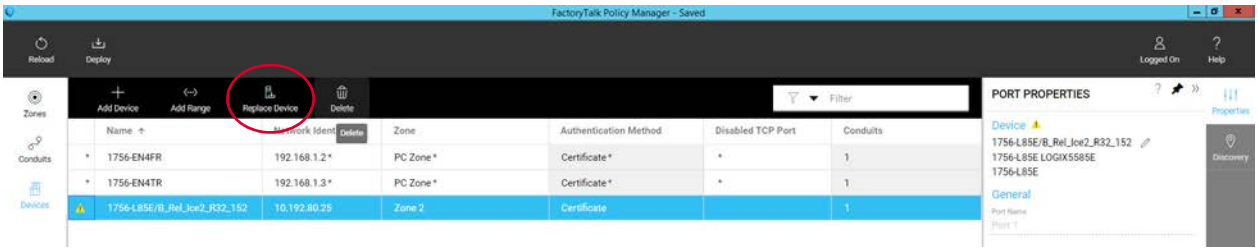
When you replace a CIP Security-enabled device that does not support APD, it can't function in a secured IACS as before without a policy redeployment.

IMPORTANT	This restriction does not apply when you use a 1783-CSP Proxy to connect a proxied device to an IACS that uses CIP Security. If you replace a proxied device that is connected to a 1783-CSP Proxy with an identical device, that is, same device type, catalog number, firmware revision, and IP address, you aren't required to redeploy the security model. For more information on how to use a 1783-CSP Proxy in an IACS that has CIP Security implemented, see the CIP Security Proxy User Manual, publication 1783-UM013.

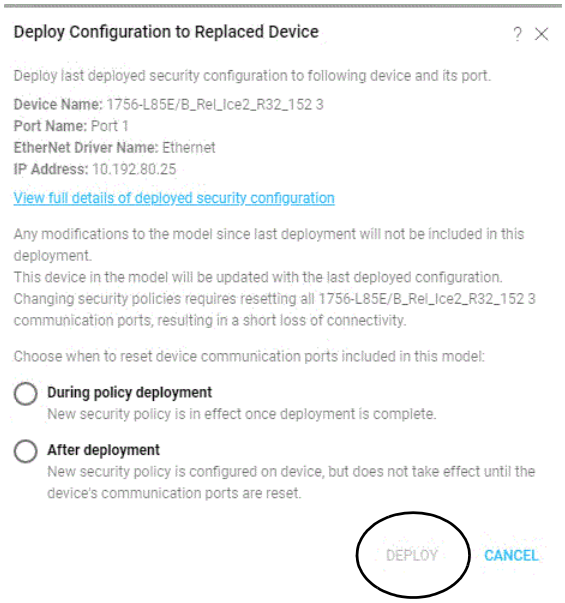
Complete the following steps to replace a CIP Security-enabled device that does not support APD.

Complete the following steps.

1. Disconnect the original device from the network.
2. Connect the new device to the network.
3. In FactoryTalk Policy Manager software, select a particular device and click Replace Device.



4. When the following dialog box appears, choose when to reset device communication on ports included in the model, and click Deploy.



Notes:

CIP Security Compatibility

This section describes the software and the devices that you can use in an IACS with CIP Security™ implemented. The devices that are listed in the section can be connected directly to the IACS or via a CIP™ Security-capable device, for example, a 1756-EN4TR EtherNet/IP™ communication module or a 1783-CSP CIP Security Proxy.

Software

Table 26 lists the software that is used to implement CIP Security.

Table 26 - Software That Is Used to Implement CIP Security

Software	Version	Required
FactoryTalk® Policy Manager	6.11 or later	Yes
FactoryTalk System Services	6.11 or later	Yes
FactoryTalk Linx	6.11 or later	Yes
Studio 5000 Logix Designer®	31.00.00 or later	Not required but commonly used with CIP Security.

Logix Controllers

Table 27 lists how you can use CIP Security with Logix 5000 controllers that are used in Logix Designer application projects, versions 31 or later.

Table 27 - CIP Security With Logix Controllers in Logix Designer Applications

Controller	Studio 5000 Logix Designer Application					
	V31	V32	V33	V34	V35	V36
ControlLogix® 5580	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)	CIP Security is supported by using one of the following: • The controller Ethernet port. • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)				
ControlLogix 5570	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)					
GuardLogix® 5580	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)			CIP Security is supported by using one of the following: • The controller Ethernet port. • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)		
GuardLogix 5570	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)					
CompactLogix™ 5380	CIP Security is supported by using a CIP Security Proxy. (1)			CIP Security is supported by using one of the following: • Either controller Ethernet port. • A CIP Security Proxy.(1)		
CompactLogix 5370	CIP Security is supported by using a CIP Security Proxy. (1)					

Table 27 - CIP Security With Logix Controllers in Logix Designer Applications

Controller	Studio 5000 Logix Designer Application					
	V31	V32	V33	V34	V35	V36
Compact GuardLogix SIL 2 5380	CIP Security is supported by using a CIP Security Proxy. (1)			CIP Security is supported by using one of the following: • Either controller Ethernet port. • A CIP Security Proxy.(1)		
Compact GuardLogix SIL 3 5380	Not available	CIP Security is supported by using a CIP Security Proxy.(1)		CIP Security is supported by using one of the following: • Either controller Ethernet port. • A CIP Security Proxy.(1)		
Compact GuardLogix 5370	CIP Security is supported by using a CIP Security Proxy.(1)					

(1) **IMPORTANT**: This is only for workstation programming, upload/download, and data collection, not for I/O. For more information, see the CIP Security Proxy User Manual, publication 1783-UM013.

CIP Security is not available with any of the following controllers in any programming software version:

- ControlLogix 5560
- ControlLogix 5550
- GuardLogix 5560
- CompactLogix 5480
- 1768 CompactLogix
- 1768 Compact GuardLogix
- 1769 CompactLogix
- FlexLogix™ L34
- DriveLogix™ 5370
- SoftLogix™ 5800

ControlLogix 5580 and 5570 Controller Redundancy

Table 28 lists how you can use CIP Security ControlLogix 5570 and 5580 controller redundancy in Logix Designer application projects, versions 31 or later.

Table 28 - ControlLogix 5580 and 5570 Controller Redundancy With a CIP Security System

Controller	Studio 5000 Logix Designer® Application					
	V31	V32	V33	V34	V35	V36
ControlLogix® 5580 controllers	Redundancy not available		CIP Security is supported by using one CIP Security Proxy through an Ethernet switch to 1756-EN2x communication modules in a redundant chassis pair. (1)	CIP Security is supported by using one of the following: • One CIP Security Proxy through an Ethernet switch to 1756-EN2x EtherNet/IP communication modules in a redundant chassis pair. (1) • A pair of 1756-EN4TR communication modules, firmware revision 4.001 or later. (2)		
ControlLogix 5570 controllers	CIP Security is supported by using one CIP Security Proxy through an Ethernet switch to 1756-EN2x EtherNet/IP communication modules in a redundant chassis pair.(1)					

(1) **IMPORTANT**: This is only for workstation programming, upload/download, and data collection, not for I/O. For more information, see the CIP Security Proxy User Manual, publication 1783-UM013.

(2) **IMPORTANT**: This is only for workstation programming, upload/download, and data collection, not for I/O. For more information, see the High Availability Systems Reference Manual, publication HIGHAV-RM002.

Other Devices

Table 29 lists other devices that you can use with CIP Security.

Table 29 - Other Devices Used With a CIP Security System

Device	Firmware Revision
1756-EN4TR EtherNet/IP communication module	Any
Armor™ PowerFlex® drives	10.001 or later
Kinetix® 5300 drives	13.003 or later
Kinetix 5700 drives	11.001 or later
PowerFlex 755T drives	10.001 or later
PowerFlex 755TS drives	11.001 or later
PowerFlex® 6000T drives	9.001 or later
1783-CSP CIP Security Proxy	Any
Proxied devices that have been tested with the 1783-CSP CIP Security Proxy	For information on the devices that have been tested with a CIP Security Proxy and can be used in a system with CIP Security implemented, see the CIP Security Proxy User Manual, publication 1783-UM013.

Notes:

History of Changes

This section contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

SECURE-AT001C-EN-P, August 2022

This revision:

- Added information about the following products that you can use with CIP Security:
  - Armor™ PowerFlex® Variable Frequency Drives (VFD)
  - CompactLogix™ 5380 Controllers
  - Compact GuardLogix® 5380 Controllers
  - ControlLogix 5580 Process Controllers
  - GuardLogix 5580 Controllers
  - PowerFlex 755TS Drives
- Added section Use Non-CIP Security-capable Controllers with CIP Security
- Change Allowed to AllowedList as appropriate
- Added a table to define icons that had not previously been defined
- Changed section Dual-port Devices to Devices That Support DLR/Linear and Dual-IP EtherNet/IP Modes and added content
- Added information on how to Secure the Programming Connection to Redundant ControlLogix 5580 Controllers
- Added information on how to Secure the Programming Connection to the CompactLogix 5380 Controllers
- Updated the description of CIP Bridging, including changing the name to Policy Provisioning
- Added information on CIP Bridging Control
- Updated the description of how to use I/O connections in Redundancy Systems
- Added description of Automatic Device Configuration (ADC)
- Added description of how to disable CIP Security
- Added description of how to add legacy devices to the security model
- Added description of how to Identify CIP Security-capable and CIP Security-enabled Devices
- Added description of Unsecure Device Management
- Added information to section Identify, Organize, and Create Zones
- Added information to section Back Up the Security Model
- Add information on how Set Mask Parameters on PowerFlex 755T Drives to Maintain Security
- Added information on how to Use Syslog with CIP Security
- Added Chapter 5, Add or Replace A Device In a CIP Security System with the following sections:
  - Automatic Policy Deployment
  - Add a New Device That Supports Automatic Policy Deployment
  - Replace a Device That Supports Automatic Policy Deployment
  - Devices That Do Not Support Automatic Policy Deployment
- Added a CIP Security Compatibility section
- Added a History of Changes section

SECURE-AT001B-EN-P, August 2021

This revision:

- Added information about the following products that you can use with CIP Security
  - 1783-CSP CIP Security Proxy
  - Kinetix 5300 drives
  - PowerFlex® 755T drives
- Description of how to migrate an application from using FactoryTalk Policy Manager, version 6.11, to FactoryTalk Policy Manager, version 6.20
- Updated the description of Studio 5000 Logix Designer application
- Updated the description of ControlLogix® 5580 controllers
- Added a description of an initial security model deployment failure if a ControlLogix 5580 controller is in Run Mode
- Added a description of conditions in which you cannot download to a ControlLogix 5580 controller from an unsecure workstation
- Added a PowerFlex 755T drive to the CIP Bridging graphic
- Updated the description of the Replace Device limitation
- Added a description of the different security model deployment types
- Updated the description of how to back up the security model
- Added a description of how to restore FactoryTalk System Services
- Added a description of how to replace a CIP Security-enabled device
- Updated graphics to show a 1783-CSP CIP Security Proxy

Numerics

A

B

C

D

E

F

G

I

K

L

M

N

P

R

S

T

V

Z

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

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

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

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication SECURE-AT001D-EN-P - December 2023
Supersedes Publication SECURE-AT001C-EN-P - August 2022