FactoryTalk Policy Manager Getting Results Guide

Getting Results Guide

Original Instructions

Contents

Important user information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Preface

About this publication

This *Getting Results Guide* provides information on installing and using FactoryTalk® System Services and FactoryTalk Policy Manager.

Review this section for information about:

- Intended audience
- Where to find additional information
- Legal notices

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Intended audience

This guide is intended for the system administrator and assumes familiarity with:

- Microsoft® Windows® operating systems
- FactoryTalk Linx
- FactoryTalk Services Platform
- Allen-Bradley® programmable logic controllers (PLCs) and programmable automation controllers (PACs)
- Rockwell Automation control system development software

Legal Notices

Rockwell Automation publishes legal notices, such as privacy policies, license agreements, trademark disclosures, and other terms and conditions on the Legal Notices page of the Rockwell Automation website.

End User License Agreement (EULA)

You can view the Rockwell Automation End User License Agreement (EULA) by opening the `license.rtf` file in your product installation folder on your hard drive.

The default location of this file is: `C:\Program Files (x86)\Common Files\Rockwell\license.rtf`.

Open Source Software Licenses

The software included in these products contains copyrighted software that is licensed under one or more open source licenses.

You can view a full list of all open source software used in these products and their corresponding licenses by opening the `oss_licenses.txt` files located in your products' `OPENSOURCE` folders on your hard drive. These files are divided into these sections:

- Components
  Includes the name of the open source component, its version number, and the type of license.
- Copyright Text
  Includes the name of the open source component, its version number, and the copyright declaration.
- Licenses
  Includes the name of the license, the list of open source components citing the license, and the terms of the license.

The default locations of these files are:

- `C:\Program Files (x86)\Common Files\Rockwell\Help\FactoryTalk Policy Manager\ReleaseNotes\OPENSOURCE\oss_licenses.txt`
- `C:\Program Files (x86)\Common Files\Rockwell\Help\FactoryTalk System Services\ReleaseNotes\OPENSOURCE\oss_licenses.txt`

You may obtain the Corresponding Source code for open source packages included in these products from their respective project web sites. Alternatively, you may obtain complete Corresponding Source code by contacting Rockwell Automation via the **Contact** form on the Rockwell Automation website: https://www.rockwellautomation.com/en-us/company/about-us/contact-us.html. Please include *"Open Source"* as part of the request text.

Commercial Software Licenses

This software also includes these commercially licensed software components:

Component	Copyright
DevExpress .NET 2005 (Version 6.3.9)	Copyright 2000-2006 Developer Express Inc.
FDT-JIG FDT Interface Assembly (Version1.2.1.0)	Copyright (c) 2005 FDT-JIG
Iocomp .Net WinForms (Version 4.0.0)	Copyright 1998-2008 Iocomp Software Inc.
Microsoft Libraries (Visual Studio)	Copyright (C) Microsoft Corp.
Sanford State Machine Toolkit (Version 1.0.1.1)	Copyright 2007 Leslie Sanford

Additional information

For additional information about security policy, consult the following resources:

Resource name	Description
System Security Design Guidelines	Provide guidance in these areas: • System security • Networks and communications security • Control system hardening • User access management • Control system monitoring • Device disposal Download from the Rockwell Automation Literature Library, System Security Design Guidelines (publication SECURE-RM001).
Online help	The Help includes overview, procedural, screen, and reference information for the product. The Help contains these basic components: • Concepts • Procedures • Properties referenced To view context-sensitive help in FactoryTalk Policy Manager, select the Help **[?]** icon.
Release Notes	The Release Notes contains this information: • System requirements • System features • Anomalies • Functional changes • Application notes Release notes can be downloaded from the Product Compatibility and Download Center or opened from FactoryTalk Policy Manager by selecting the **Release Notes** link under the Help **[?]** icon on the main menu.
Rockwell Automation Knowledgebase	The Rockwell Automation Customer Support Center offers an extensive online database that includes frequently asked questions and the latest patches. The Knowledgebase web page leads to a comprehensive, searchable database of support information for all Rockwell Automation products. To access the Knowledgebase web page, visit https://rockwellautomation.custhelp.com/.
Rockwell Automation Technical Support	Questions concerning installation and use of FactoryTalk Policy Manager software are handled by the Rockwell Automation Customer Support Center. The center is staffed Monday through

Resource name	Description
	Friday, except on U.S. holidays, from 8 a.m. to 5 p.m. Eastern time zone for calls originating within the U.S. and Canada. To reach the Customer Support Center, call 440-646-3434 and follow the prompts. For calls originating outside the U.S. or Canada, locate the number in your country by visiting https://www.rockwellautomation.com/en-us/company/about-us/contact-us.html. When you call, you should be at your computer and be prepared to provide the following information: • The product version number • The type of hardware you are using • The exact wording of any errors or messages that appeared on your screen • A description of what happened and what you were doing when the problem occurred • A description of how you tried to solve the problem
Training	Rockwell Automation offers a wide range of training programs, from regularly scheduled classes to custom-tailored classes conducted at your site. If you need more information about these training programs, visit the Rockwell Automation site or contact the Rockwell Automation Training Coordinator. The web site address and telephone numbers are available at the bottom of the back cover.
Consulting	Rockwell Automation provides expert consulting and turnkey implementations for making optimal use of Rockwell Automation software products. Please contact your local representative for more information.

Getting started

Install, log on to, and learn about FactoryTalk Policy Manager.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

FactoryTalk Policy Manager

Use FactoryTalk Policy Manager to view, edit, and deploy the FactoryTalk system security policy configuration.

Policy model components

FactoryTalk Policy Manager divides the system security policy into different component areas of control. Use these components areas to design policy models that control the permissions and usage of devices within the system.

Zones

Groups of devices.

Devices

Computers, controllers, modules, HMI panels, CIP Proxy devices, OPC UA clients, OPC UA servers, and drives.

Conduits

Communication routes between components.

FactoryTalk Policy Manager enables you to use ODVA™ CIP Security™ and OPC UA standards to design the security policy model for your system.

FactoryTalk Policy Manager depends on FactoryTalk System Services for certificate services, policy deployment, and authentication. See FactoryTalk System Services on page 9.

FactoryTalk System Services

FactoryTalk System Services provide the policy authority, certificate authority, identity services, and deployment services required to enforce security policies.

Databases

FactoryTalk System Services use CouchDB for the creation and maintenance of policy databases.

Tip: FactoryTalk System Services depends on database services. Database services can take up to 2 minutes to start after the computer is restarted. During that time, FactoryTalk Policy Manager will be unable to connect to FactoryTalk System Services.

During the FactoryTalk System Services installation, CouchDB:

- Installs automatically if not already installed.
- Adds and configures the required administrative users and controls.
- Creates policy databases.

Services

FactoryTalk Policy Manager uses these FactoryTalk System Services:

Authentication Service

Authenticates users and validates user resource requests. Validates user credentials against FactoryTalk Directory and FactoryTalk security policy settings to obtain privileges associated with the user.

Certificate Service

Issues and manages X.509v3 certificates for use within the FactoryTalk system.

Deployment Service

Translates the security policy model defined using FactoryTalk Policy Manager to CIP™ and OPC UA configurations that are delivered to endpoints. Protocols configurations are deployed independently.

Diagnostics Service

Makes FactoryTalk audit and diagnostic logs available as a web service.

Policy Service

Builds and manages network trust models and define security policy for CIP and OPC UA endpoints.

Differential deployment

Enables deployment of changes in the security policy model only to the affected devices, instead of deploying the model to all devices.

Support for CIP Security Proxy devices

Uses proxy devices to secure communications to and from devices that do not have CIP Security capabilities.

Backup and restore

Preserves and restores the security policy models in case of a system failure.

Security eventing

Sends eventing configuration to devices and stores events from FactoryTalk Policy Manager and FactoryTalk System Services as Syslog messages.

DTLS timeout

Configures the devices to close their DTLS sessions after a specified period of inactivity.

Install or update software

Install or update FactoryTalk Policy Manager and FactoryTalk System Services with a graphical user interface (GUI) installer.

IMPORTANT: The FactoryTalk Policy Manager installation agent opens these Windows Firewall ports: `UDP 5353` and `TCP 40014`. To operate correctly, the Automatic Policy Deployment functionality requires these ports to be open.

Automatic Policy Deployment uses the Enrollment over Secure Transport (EST) service. If your machine has multiple network interfaces, the EST service uses a random network interface by default. You can select a specific network interface by editing the `appConfiguration.json` file. You must be a Windows administrator and have a FactoryTalk Directory administrator account to specify the network interface for the EST service.

To install or update FactoryTalk Policy Manager and FactoryTalk System Services

1. Close all open programs.
2. Run the FactoryTalk Policy Manager installer and follow the installation wizard steps.
3. (optional) To add or remove the components that you want to install, select **Customize**.
4. Select **Install**.
5. Read and agree to the EULA.
6. Complete the installation.
7. Restart the machine.

IMPORTANT: FactoryTalk System Services start automatically after a few minutes when you restart your computer. During that time, you cannot use FactoryTalk Policy Manager.

- If you want to use the Automatic Policy Deployment functionality and the machine has multiple network interfaces, see Configure Automatic Policy Deployment for multiple network interfaces on page 47.
- If you do not want to use the Automatic Policy Deployment functionality. See Disable Automatic Policy Deployment on page 48.
- (recommended) Install the available updates.

Start FactoryTalk System Services

FactoryTalk System Services start automatically after a few minutes when you restart your computer. In some cases, you may need to start FactoryTalk System Services manually.

Prerequisites

Install FactoryTalk Policy Manager and FactoryTalk System Services. See Install or update software on page 10.

To start FactoryTalk System Services

1. Select Windows® **Start** and type `services.msc`
2. Select **Services**.
3. In the services list, right-click **FactoryTalk System Services** and select **Start**.

Log on to FactoryTalk Policy Manager

Logging on to FactoryTalk Policy Manager checks the credentials of your user account to determine the access to resources and the ability to edit the security policy.

Prerequisites

Confirm that FactoryTalk System Services are running. See Start FactoryTalk System Services on page 11.

To log on to FactoryTalk Policy Manager

1. Open FactoryTalk Policy Manager.
2. In **Username**, enter your FactoryTalk user name.
3. In **Password**, enter your FactoryTalk password.

   Tip: Select **Show password** to display the password you typed. Not recommended if others can easily view your workstation.

4. Select **LOG ON**.

You logged on to FactoryTalk Policy Manager.

Tip: If the communication with FactoryTalk System Services is interrupted while FactoryTalk Policy Manager is running, you may need to select **REFRESH** and log on to FactoryTalk Policy Manager again.

Learn about user groups, rights, and privileges. See User groups, rights, and permissions on page 12.

User groups, rights, and permissions

FactoryTalk Services Platform includes built-in security groups to define rights and permissions for users.

FactoryTalk Policy Manager user groups can have these rights and permissions:

Right	Group	Permissions
View	• Administrator • Engineers • Maintenance	• View security policy model; including the configuration of zones, devices, and conduits. • View global settings. • Display the Error pane. • Display the Results pane. • Deploy the security policy model. • Replace a device.
Edit	• Administrator	• Edit global settings. • Add, edit, and delete zones. • Add, edit, and delete conduits. • Discover, add, edit, and delete devices. • Add and configure Ethernet ports.

Right	Group	Permissions
		- Add, configure, and delete trusted IP ranges. - Deploy security policy models.
Deploy	- Administrator - Engineers - Maintenance	- Deploy security policy models. - Replace a device.
Validate	- Administrator - Engineers - Maintenance	- Validate security policy models.

Tip:

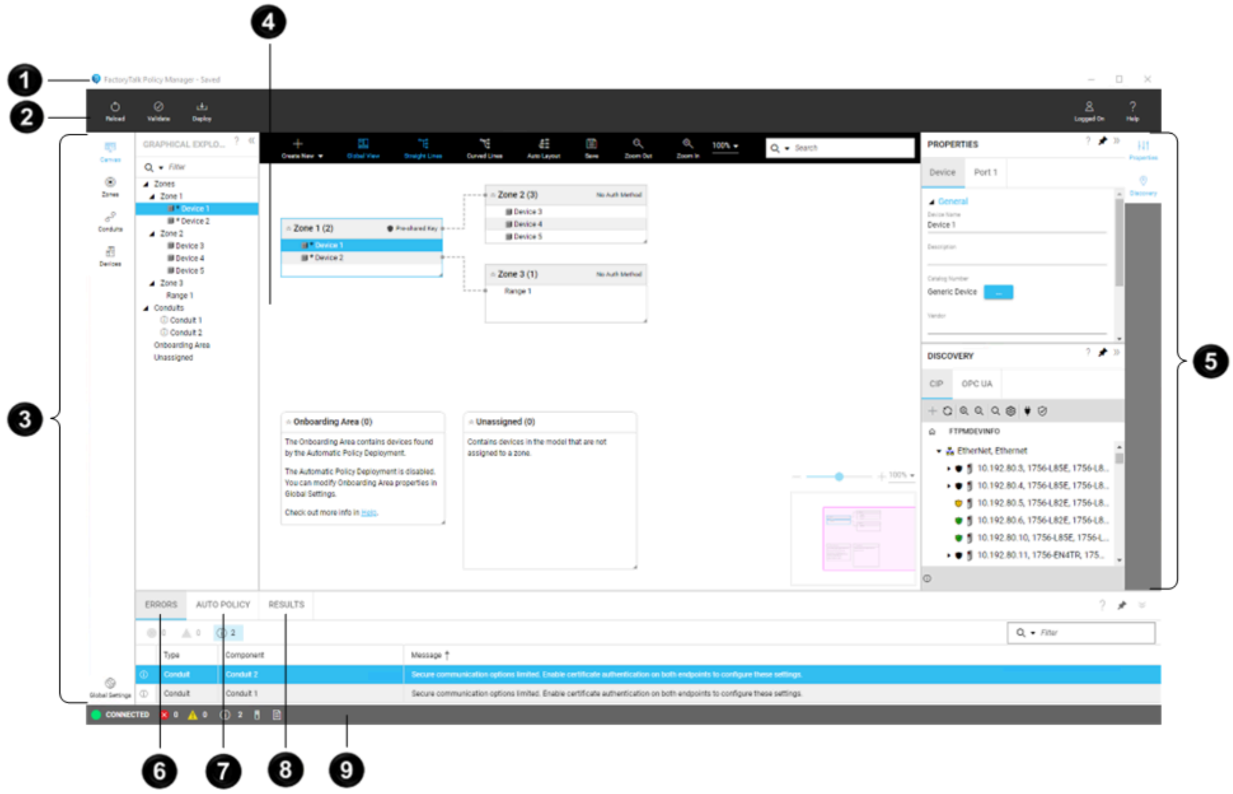
If you are logged on as an Administrator, but FactoryTalk Policy Manager is in the read-only mode, verify that:

- The FactoryTalk Directory services are running.
- The computer is connected to the FactoryTalk Directory.

FactoryTalk Policy Manager interface

Use FactoryTalk Policy Manager to configure the policy model.

Figure 1. FactoryTalk Policy Manager interface



The Onboarding Area contains devices found by the Automatic Policy Deployment.

The Automatic Policy Deployment is disabled. You can modify Onboarding Area properties in Global Settings.

Check out more info in Help.

Contains devices in the model that are not assigned to a zone.

Type	Component	Message
Conduit	Conduit 2	Secure communication options limited. Enable certificate authentication on both endpoints to configure these settings.
Conduit	Conduit 1	Secure communication options limited. Enable certificate authentication on both endpoints to configure these settings.

Table 1. Interface elements description

Item	Name	Description
❶	**Title** bar	Displays the status of the policy model. Saved models are local to the FactoryTalk Policy Manager database. Once you deploy a policy model, the **Title** bar does not display the status. If you change the deployed model, the **Saved** status displays again until you deploy the changes.
❷	**Main menu** bar	Allows you to: • Reload the policy model. • Validate the policy model. • Deploy the policy model. • Log on to and log off from FactoryTalk Policy Manager. • Open help.
❸	**Navigation** bar	Move between different views of the policy model and access **Global Settings**.
❹	**Canvas**, **Zones**, **Conduits**, or **Devices** view.	Displays policy model components in different views. Contains a toolbar with actions available for a selected policy model component.
❺	**Configuration** bar	Open the **Properties** pane to configure the selected policy model component. Open the **Discovery** pane to find devices in networks, add drivers, and bridge networks.
❻	**Errors** pane	Displays filterable errors, warnings, and info messages about the policy model when you validate or deploy the model.
❼	**Auto policy** pane	Displays filterable results of the last Automatic Policy Deployment. Select 💾 **Save** to export the results to a file for archival purposes. Select 🗑**Delete** to clear **Auto policy**. Select ⊗ 0 ⚠ 0 ⓘ 5 to filter the results based on the message type. Select a column header to sort the results.
❽	**Results** pane	Displays the results of the last policy model deployment.

Table 1. Interface elements description (continued)

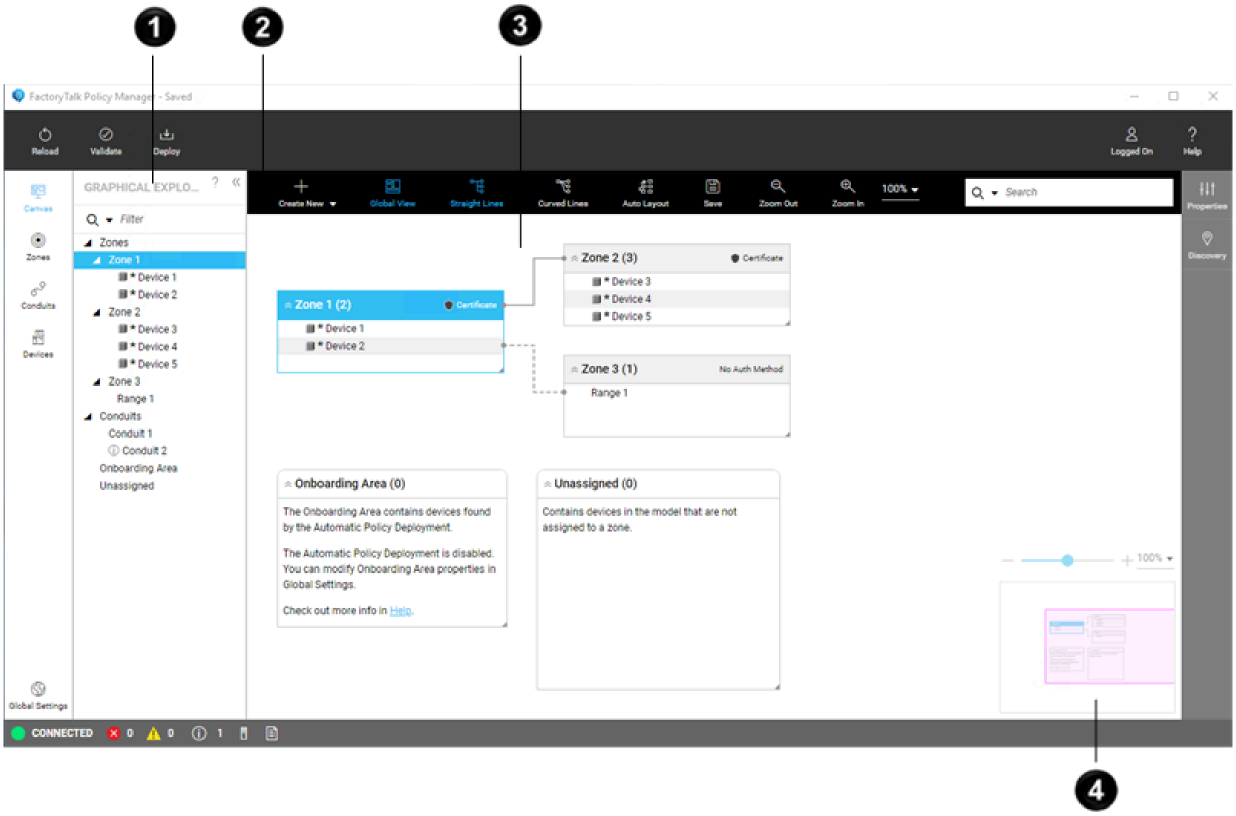
Item	Name	Description
		Select **Save** to export the results to a file for archival purposes.
9	**Status** bar	Displays the connection status to FactoryTalk System Services. Select ✕ 0 ⚠ 0 ⓘ 1 **Errors pane** to display **Errors**. Select **Automatic Policy Deployment result pane** to display **Auto policy**. Select **Results pane** to display **Deploy results**.

Canvas

Use canvas to manage zones, conduits, and devices with an interactive diagram and a tree visualization of the policy model.

Overview

Figure 2. Canvas interface



The Onboarding Area contains devices found by the Automatic Policy Deployment.

The Automatic Policy Deployment is disabled. You can modify Onboarding Area properties in Global Settings.

Check out more info in Help.

Contains devices in the model that are not assigned to a zone.

Item	Name	Description
1	**Graphical Explorer**	Browse the zones, devices, and conduits tree. See Graphical Explorer on page 18.

Item	Name	Description
❷	**Toolbar**	Interact with canvas. See Toolbar on page 16.
❸	**Components**	Visualizes zones, conduits, devices, and ranges. See Components on page 17.
❹	**Mini map**	Helps navigate complex policy models.

Toolbar

Use the toolbar to interact with canvas.

Tip: If the FactoryTalk Policy Manager window is not wide enough to fit all actions, you can view the hidden actions by selecting ⋮ **More Actions**.

Item	Description
Create New	Adds a zone, conduit, device, or range to the selected zone or **Unassigned**.
Global View	Shows or hides a mini map of the policy model visualization in the bottom-right corner of the model. Use to navigate complex policy models and adjust the zoom level of the policy model.
Straight Lines	Shows conduits as straight lines. Dotted conduits represent trusted unsecure connections. Solid conduits represent secure connections.
Curved Lines	Shows conduits as curved lines. Dotted conduits represent trusted unsecure connections. Solid conduits represent secure connections.
Auto Layout	Automatically lays out the policy model visualization.
Save	Saves the policy model visualization to a graphic file.
Zoom Out	Zooms out the policy model visualization.
Zoom In	Zooms in the policy model visualization.
Zoom	Displays the current zoom level of the policy model visualization. Enables you to select or enter a custom zoom level value. **Tip:** You can also zoom in and zoom out the policy model visualization by using the mouse wheel.
Search	Highlights policy model components based on the specified criteria. See Search Canvas on page 17.

Components

Canvas visualizes these policy model components.

Tip: You can move, resize, collapse, and expand containers in the policy model visualization. Use **Properties** to configure the policy model components.

Item	Description
Zone	Contains devices added to the policy model.
Conduit	Communication pathway, connecting pairs of policy model components. **Tip:** Dotted conduits represent trusted unsecure connections. Solid conduits represent secure connections.
Onboarding Area	Contains devices found by Automatic Policy Deployment that can be added to the policy model.
Unassigned	Contains devices added to the policy model but not added to any zone in the policy model.
Device	Represents a device added to a zone, discovered by Automatic Policy Deployment, or an unassigned device. **Tip:** You can drag devices and ranges between containers. If you move a device from the **Onboarding Area** to a **Zone** or to the **Unassigned** container, the device cannot be moved to the **Onboarding Area** container again.

Search Canvas

Use **Search** to find zones, conduits, devices, and other components on canvas. The search results are highlighted in yellow.

1. From the navigation bar, select **Canvas**.
2. On the toolbar, in **Search**, enter a query.

   Tip: You can press **Ctrl** + **F** to place the cursor in the **Search** field.

3. (optional) Restrict the search results by selecting ▼ **Filters to add to search field** and selecting **Zone**, **Conduit**, or **Device**.
4. (optional) Cycle through the search results by selecting ▶ **Go to next search result** or ◀ **Go to previous search result**.
5. (optional) Clear the search results by selecting ✕ **Clear search**.

Change Canvas layout

Change how the policy model representation is displayed.

1. From the navigation bar, select **Canvas**.
2. To change the layout:
   - Move a zone container. Select, hold and move the zone header.
   - Collapse or expand a zone container. In the zone header select ︽ or ︾.
   - Display conduits as curved lines. From the toolbar, select **Curved Lines**.
   - Display conduits as straight lines. From the toolbar, select **Straight Lines**.
   - Distribute containers automatically. From the toolbar, select **Auto Layout**.

Save Canvas to a graphic file

Save the policy model visualization to a graphic file.

1. From the navigation bar, select **Canvas**.
2. From the toolbar, select **Save**.
3. Select any of the following:
   - **Save entire canvas**. Saves the entire policy model visualization.
   - **Save only visible portion of canvas**. Saves the policy model visualization that is currently visible in the FactoryTalk Policy Manager window.
4. Select **Save**.
5. Navigate to the location to save the file and select **Save**.

Graphical Explorer

Use **Graphical Explorer** to browse the zones, devices, and conduits tree. You can filter, collapse, and expand the tree nodes.

Tip: Selecting a component in the **Graphical Explorer** tree focuses the policy model visualization on that component. Selecting a component in the policy model visualization, focuses the tree on that component.

You can expand or collapse the **Graphical Explorer** pane.

Table 2. Graphical Explorer pane elements

Item	Description
Filter	Filtered tree based on the specified criteria.
Zones	Zones added to the policy model and devices added to these zones.
Conduits	Conduits added to the policy model.
Onboarding Area	Devices found by Automatic Policy Deployment that can be added to the policy model.
Unassigned	Devices that are added to the policy model but are not added to any zone in the policy model.
« **Hide**	Collapses **Graphical Explorer**.
» **Show**	Expands **Graphical Explorer**.

Filter Graphical Explorer

Use **Filter** to find zones, conduits, and devices in the policy model tree.

1. From the navigation bar, select **Canvas**.
2. On the left, confirm that the **Graphical Explorer** pane is expanded.
3. Fill in the **Filter** field.
4. (optional) Restrict the filtering scope by selecting ▼ **Quick filter** and selecting: **Zones**, **Conduits**, or **Devices**.
5. (optional) Discard filters by selecting ✕ **Clear view**.

Tables

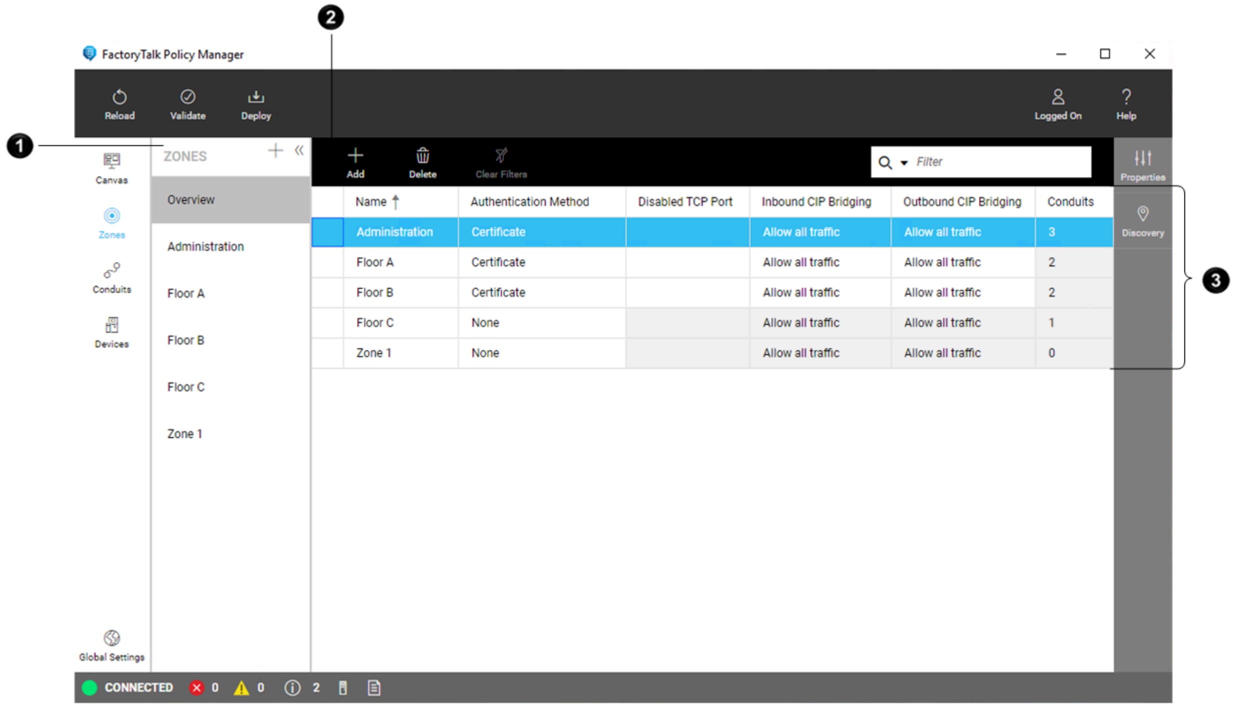
Manage zones, conduits, and devices in tables.

Zones table

Manage zones in a table. **We need the who/why/what/where info.**

Zones table - zones overview

Figure 3. Zones table, zones overview interface



Name	Authentication Method	Disabled TCP Port	Inbound CIP Bridging	Outbound CIP Bridging	Conduits
Administration	Certificate		Allow all traffic	Allow all traffic	3
Floor A	Certificate		Allow all traffic	Allow all traffic	2
Floor B	Certificate		Allow all traffic	Allow all traffic	2
Floor C	None		Allow all traffic	Allow all traffic	1
Zone 1	None		Allow all traffic	Allow all traffic	0

Table 3. Zones table, zones overview items

Item	Name	Description
❶	**Zones** pane	Displays the overview of all zones.
❷	**Toolbar**	Use the toolbar to interact with tables. See Table 4: Zones table, zones overview toolbar on page 20.

Table 3. Zones table, zones overview items (continued)

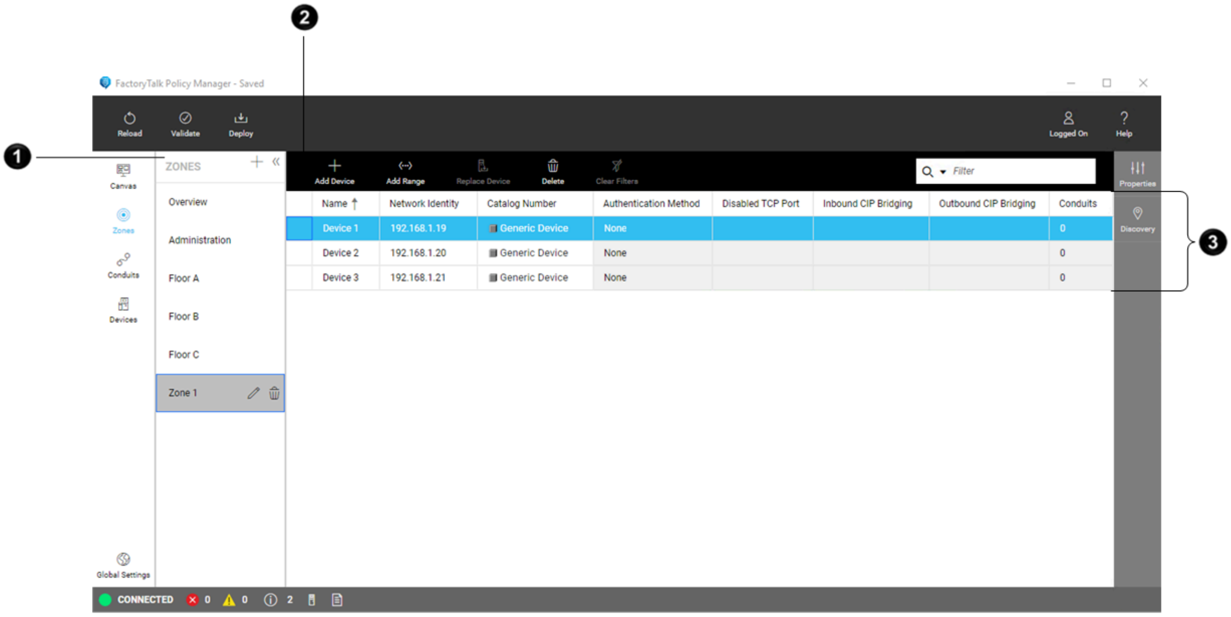
Item	Name	Description
3	**Table**	Lists all zones or devices and ranges in a single zone. Select not grayed-out table cells to edit values. Select a table header title to sort elements based on the column values. Drag a table header to change the order of columns in the table. Filter tables by hovering-over a table header, selecting ⛛ , and entering a query or selecting checkboxes.

Table 4. Zones table, zones overview toolbar

Item	Description
Add	Adds a zone.
Delete	Deletes the selected zone.
Clear Filters	Clears all filters.
Filter	Filters table rows based on the specific criteria. See Filter tables on page 24

Zones table - zone details

Figure 4. Zones table, zone details interface



Name	Network Identity	Catalog Number	Authentication Method	Disabled TCP Port	Inbound CIP Bridging	Outbound CIP Bridging	Conduits
Device 1	192.168.1.19	Generic Device	None				0
Device 2	192.168.1.20	Generic Device	None				0
Device 3	192.168.1.21	Generic Device	None				0

Table 5. Zones table, zone details items

Item	Name	Description
❶	**Zones** pane	Displays details about the selected zone.
❷	**Toolbar**	Use the toolbar to interact with tables. See Table 6: Zones table, zone details toolbar on page 21.
❸	**Table**	Lists devices and ranges in the selected zone. Select not grayed-out table cells to edit values. Select a table header title to sort elements based on the column values. Drag a table header to change the order of columns in the table. Filter tables by hovering-over a table header, selecting ▽ , and entering a query or selecting checkboxes.

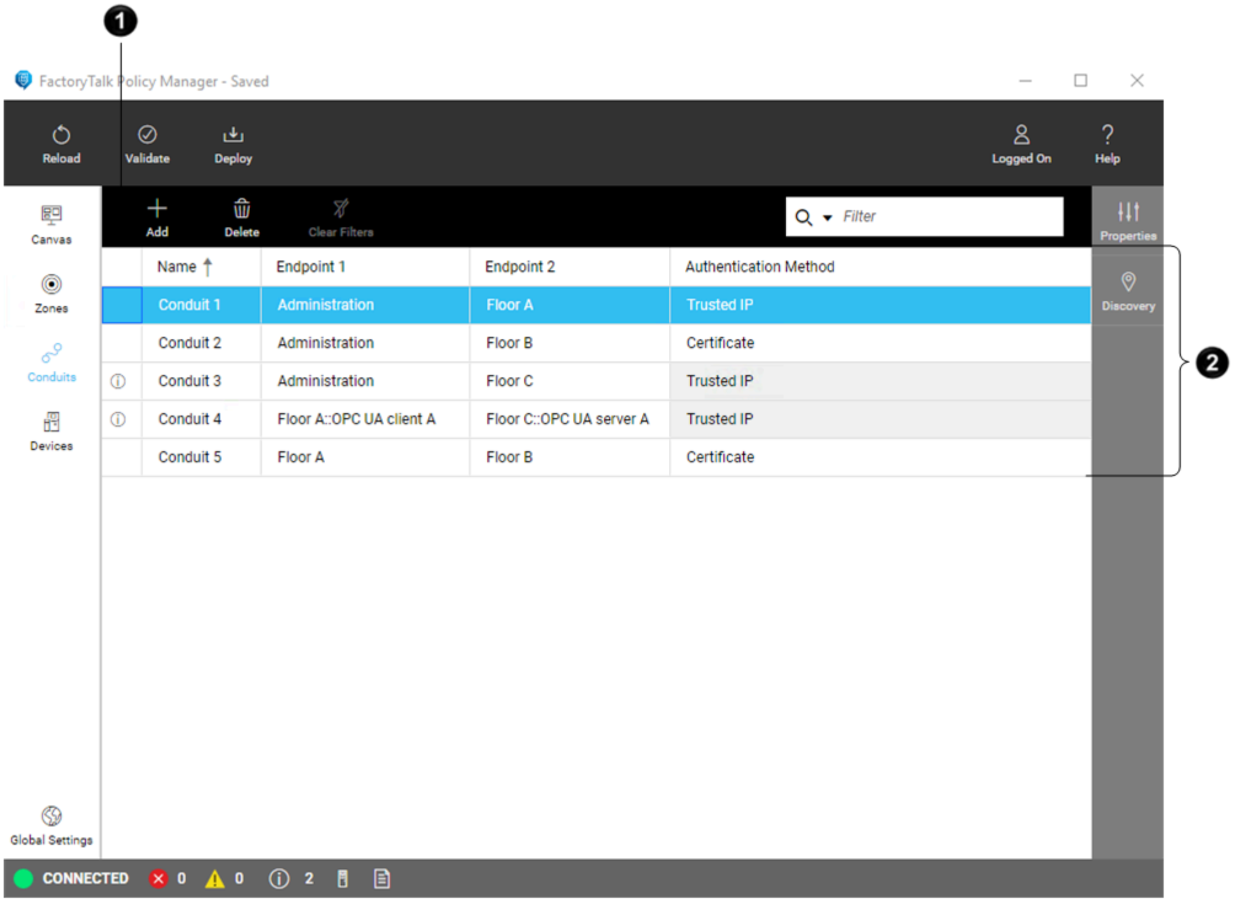
Table 6. Zones table, zone details toolbar

Item	Description
Add Device	Adds a device to the selected zone.
Add Range	Adds a range to the selected zone.
Replace Device	Replaces the selected device.
Delete	Deletes the selected device.
Clear Filters	Clears all filters.
Filter	Filters table rows based on the specific criteria. See Filter tables on page 24.

Conduits table

Manage conduits to add, edit, and delete connections between system components.

Figure 5. Conduits table interface



Name ↑	Endpoint 1	Endpoint 2	Authentication Method
Conduit 1	Administration	Floor A	Trusted IP
Conduit 2	Administration	Floor B	Certificate
Conduit 3	Administration	Floor C	Trusted IP
Conduit 4	Floor A::OPC UA client A	Floor C::OPC UA server A	Trusted IP
Conduit 5	Floor A	Floor B	Certificate

Table 7. Conduits table items

Item	Name	Description
❶	**Toolbar**	Use the toolbar to interact with tables. See Table 8: Conduits table toolbar on page 23.
❷	**Table**	Lists all conduits in the policy model. Select not grayed-out table cells to edit values. Select a table header title to sort elements based on the column values. Drag a table header to change the order of columns in the table. Filter tables by hovering-over a table header, selecting ▽, and entering a query or selecting checkboxes.

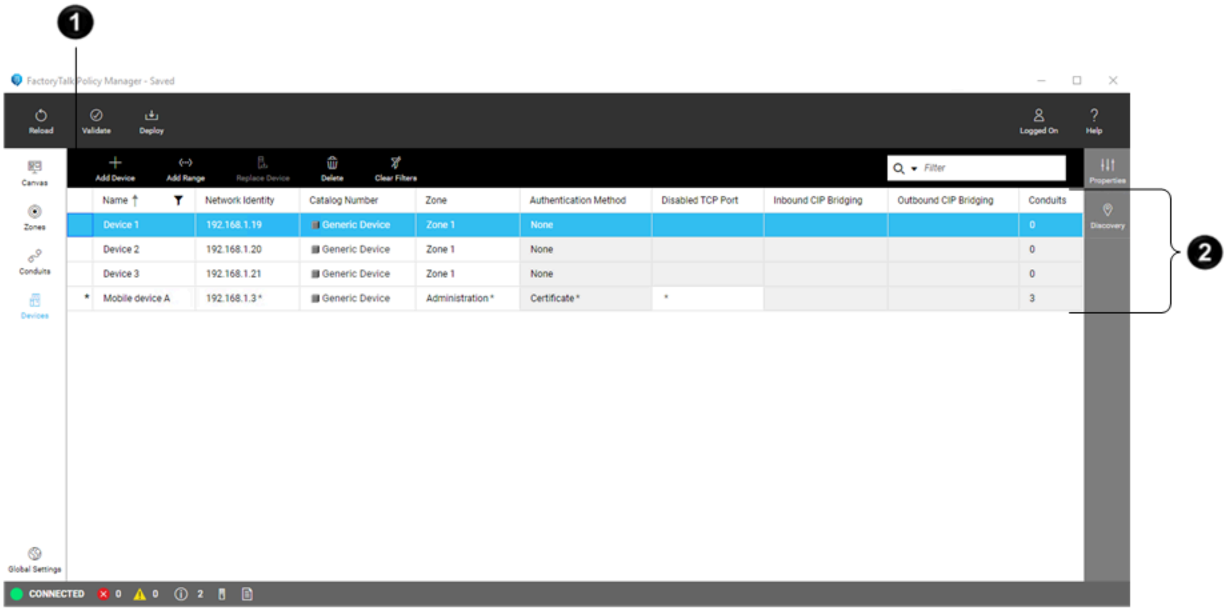
Table 8. Conduits table toolbar

Item	Description
Add	Adds a conduit.
Delete	Deletes the selected conduit.
Clear Filters	Clears all filters.
Filter	Filters table rows based on the specific criteria. See Filter tables on page 24

Devices table

Manage devices to add, edit, replace, and delete devices.

Figure 6. Devices table interface



	Name	Network Identity	Catalog Number	Zone	Authentication Method	Disabled TCP Port	Inbound CIP Bridging	Outbound CIP Bridging	Conduits
	Device 1	192.168.1.19	Generic Device	Zone 1	None				0
	Device 2	192.168.1.20	Generic Device	Zone 1	None				0
	Device 3	192.168.1.21	Generic Device	Zone 1	None				0
*	Mobile device A	192.168.1.3 *	Generic Device	Administration *	Certificate *	*			3

Table 9. Devices table items

Item	Name	Description
1	**Toolbar**	Use the toolbar to interact with tables. See Table 10: Devices table toolbar on page 24.
2	**Table**	Lists all devices in the policy model, unassigned devices, and devices to be deleted from the policy model. Select not grayed-out table cells to edit values. Select a table header title to sort elements based on the column values.

Table 9. Devices table items (continued)

Item	Name	Description
		Drag a table header to change the order of columns in the table. Filter tables by hovering-over a table header, selecting ▽ , and entering a query or selecting checkboxes.

Table 10. Devices table toolbar

Item	Description
Add Device	Adds a device to the selected zone.
Add Range	Adds a range to the selected zone.
Replace Device	Replaces the selected device.
Delete	Deletes the selected device.
Clear Filters	Clears all filters.
Filter	Filters table rows based on the specific criteria. See Filter tables on page 24.

Filter tables

Use the filter function in tables and lists to search for a particular object or to display only the objects that fit the chosen criteria.

1. From the navigation bar, select either **Zones**, **Conduits**, or **Devices**.
2. In **Filter**, enter a query.
   - Filter text can contain alphanumeric characters and can be full words, compound expressions, fragments of a word, or a single letter or number.
   - Clear the search text to return to the default view of the table or window.
   - To find an exact match to the keyword, enclose the keyword in quotation marks.
3. (optional) Select a filter category by selecting ▼ to narrow the search results to queries associated with the selected table column or item parameter.
4. (optional) Use operators in the search query to refine the search results using a logical statement:
   - AND to search for two or more keywords.
   - OR to search for several keywords.

Tip: An example of using operators between keywords to refine search results is

```
Device: 1756-L OR Device: 1768-L
```

This search locates both ControlLogix and CompactLogix controllers.

The table or window displays the results within a few seconds.

Select multiple table rows

Select multiple rows in a table to perform actions on multiple items.

1. From the navigation bar, select either **Zones**, **Conduits**, or **Devices**.
2. Select a row by selecting a cell in the first column of a row.
3. Either:
   - To add a row to the current selection, press **Ctrl** + **Mouse button**.
   - To continue the selection upward, press **Shift** + **Up Arrow**.

     Tip: If the selection moves over a previously selected row, it deselects that row.

   - To continue the selection downward, press **Shift** + **Down Arrow**.

     Tip: If the selection moves over a previously selected row, it deselects that row.

   - To select all rows between the previously selected row and the last selected row, press **Shift** + **Mouse button**.

SHARED PROPERTIES pane displays.

You can do the following on a multiple-row selection:

- View properties common to all selected items in **SHARED PROPERTIES**.
- Change the common properties of all selected items in **SHARED PROPERTIES**.

  Tip:
  - The values that are identical across all selected items are displayed.
  - The properties are editable even if no value is displayed.
  - Checkboxes display a hyphen **[-]** when only some items have a property selected.

- **Delete** selected items.
- **Edit** selected zones.

Discovery pane

Use the **Discovery** pane to browse discovered devices and OPC UA servers and their endpoints, configure networks, and manage drivers.

Tip: To open or close the **Discovery** pane, select **Discovery** from the right toolbar.

CIP

Table 11. Toolbar

Item	Description
+ **Add**	Adds selected CIP devices to the selected zone.
↻ **Auto browse**	Continuously discover CIP devices and networks.

Table 11. Toolbar (continued)

Item	Description
Zoom in	Increases the size of the network topology tree.
Zoom out	Decreases the size of the network topology tree.
Search	Toggles **Search** that provides a filtered list of devices based upon the specified search criteria.
Settings	Opens advanced network settings.
Configure Drivers	Adds a driver on the computer to provide communications to a network and configures existing drivers for edit or delete.
CIP Security Indicators	Show or hide the CIP Security configuration status of a device.

Table 12. CIP Security indicators

Indicator	Description
🛡	The device supports CIP Security and is not yet configured.
!	The device is in the CIP Security configuration process.
✓	The device is successfully configured with CIP Security.
?	The device is not recognized.
✖	The device configuration process encountered an error.
(no indicator icon)	The device does not support CIP Security.

OPC UA

Table 13. Toolbar

Item	Description
Add	Adds selected OPC UA devices to the selected zone.
Auto browse	Verify manually added OPC UA servers and their connection endpoints in the policy model.
Settings	Opens advanced network settings.
Discover OPC UA Server	Opens a dialog that enables you to add an OPC UA server and discover its connection endpoints.
Filter	Provides a filtered list of devices based on the filter query.

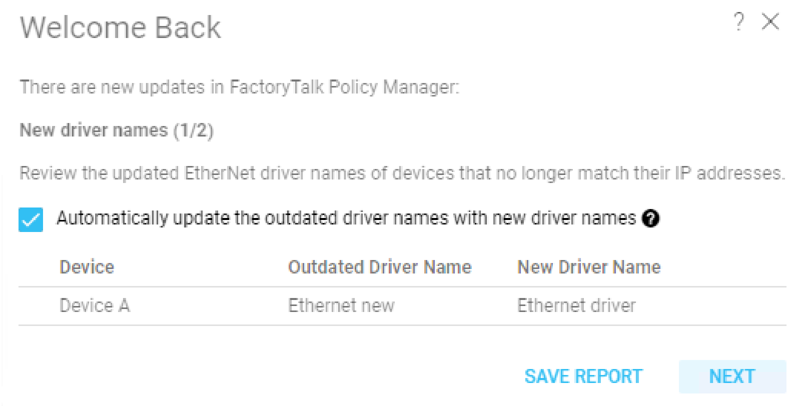
Welcome Back window

Review the updates to the policy model that have occurred since your last FactoryTalk Policy Manager session.

Tip: Select **Save report** to save the updates report to a file.

Updated EtherNet driver names

Figure 7. Welcome back window - updated EtherNet driver names



Welcome Back

There are new updates in FactoryTalk Policy Manager:

New driver names (1/2)

Review the updated EtherNet driver names of devices that no longer match their IP addresses.

☑ Automatically update the outdated driver names with new driver names ?

Device	Outdated Driver Name	New Driver Name
Device A	Ethernet new	Ethernet driver

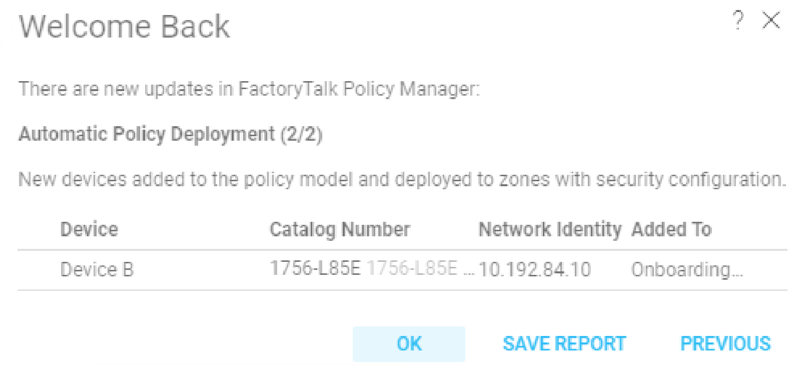
Review the updated EtherNet driver names of devices that no longer match their IP addresses.

You can either:

- Automatically update the outdated driver names with new driver names.
- Manually update the outdated driver names with new driver names later.

New devices

Figure 8. Welcome back window - new devices



Welcome Back

There are new updates in FactoryTalk Policy Manager:

Automatic Policy Deployment (2/2)

New devices added to the policy model and deployed to zones with security configuration.

Device	Catalog Number	Network Identity	Added To
Device B	1756-L85E 1756-L85E …	10.192.84.10	Onboarding…

Review the devices added to the policy model by Automatic Policy Deployment.

Keyboard shortcuts

You can use keyboard keys and their combinations in different user interface elements to perform various actions.

Panes

Key	Description
Tab	Moves focus to the next interface element.
Shift + **Tab**	Moves focus to the previous interface element.
Enter	Selects the focused interface element.
Ctrl + **F**	If available, focuses on **Search** or **Filter** in tables.

Pop-up windows

Key	Description
Esc	Closes the pop-up window.
F2	Submits changes.
Tab	Submits changes and moves to the next cell. Used on the last cell in the row moves to the first cell of the next row.
Shift + **Tab**	Submits changes and moves to the previous cell. Used on the first cell in the row moves to the last cell of the previous row.
Enter	Submits changes and moves to the next cell.
Shift + **Enter**	Submits changes and moves to the previous cell.
Ctrl + **Up arrow**	Moves cursor to the first character.
Ctrl + **Down arrow**	Moves cursor to the last character.
Ctrl + **Left arrow**	Moves cursor to the first character.
Ctrl + **Right arrow**	Moves cursor to the last character.
Page Up	Discards all changes, moves up 10 cells.
Page Down	Discards all changes, moves down 10 cells.

Tables

Table 14. Table rows

Key	Description
Ctrl + **Mouse button**	Adds the row to the current selection.
Shift + **Up arrow**	Continues selection upward. If the selection moves over a previously selected row, it deselects that row.
Shift + **Down arrow**	Continues selection downward. If the selection moves over a previously selected row, it deselects that row.
Shift + **Mouse button**	Selects all rows between the previously selected row and the last selected row.

Table 15. Table cells

Key	Description
Esc	Discards all changes, the cell remains selected.
F2	Submits changes.
Tab	Submits changes and moves to the next cell. Used on the last cell in the row moves to the first cell of the next row.
Shift + **Tab**	Submits changes and moves to the previous cell. Used on the first cell in the row moves to the last cell of the previous row.
Enter	Submits changes and moves to the next cell.
Shift + **Enter**	Submits changes and moves to the previous cell.

Table 15. Table cells (continued)

Key	Description
Shift + **Up arrow**	Selects all characters to the left of the cursor. If moved over previously selected characters, deselects the characters.
Shift + **Down arrow**	Selects all characters to the right of the cursor. If moved over previously selected characters, deselects the characters.
Shift + **Left arrow**	Selects a character to the left of the cursor. If moved over previously selected characters, deselects the characters.
Shift + **Right arrow**	Selects a character to the right of the cursor. If moved over previously selected characters, deselects the characters.
Ctrl + **Up arrow**	Moves cursor to the first character.
Ctrl + **Down arrow**	Moves cursor to the last character.
Ctrl + **Left arrow**	Moves cursor to the first character.
Ctrl + **Right arrow**	Moves cursor to the last character.
Page Up	Discards all changes, moves up 10 cells.
Page Down	Discards all changes, moves down 10 cells.

Trees

Key	Description
Home	Highlights the first item in the tree.
End	Highlights the last item in the tree.
Up arrow	Highlights previous item in the tree.
Down arrow	Highlights next item in the tree.
Left arrow	Collapses the selected item in the tree.
Right arrow	Expands the selected item in the tree.
Page up	Moves up 10 items.
Page down	Moves down 10 items.
Ctrl + **F**	Focuses on **Filter**.

Dropdown lists

Key	Description
Esc	Discards all changes, the cell remains selected.
F2	Submits changes, displays the list.
Tab	Submits changes and moves to the next cell. Used on the last cell in the row moves to the first cell of the next row.
Shift + **Tab**	Submits changes and moves to the previous cell. Used on the first cell in the row moves to the last cell of the previous row.
Space	Submits changes, the cell remains selected.
Enter	Submits changes and moves to the next cell.

Key	Description
Shift + **Enter**	Submits changes and moves to the previous cell.
Page Up	Discards all changes, moves up 10 cells.
Page Down	Discards all changes, moves down 10 cells.

Fields

Table 16. Description fields

Key	Description
Esc	Discards all changes, the cell remains selected.
F2	Submits changes.
Tab	Moves focus to the next field or interface element.
Shift + **Tab**	Moves focus to the previous field or interface element.
Enter	Submits changes and moves to the next field.
Shift +**Enter**	Breaks the line inside the field.

Table 17. Filter fields

Key	Description
Esc	Cancels filtering, deletes all characters from the field.
Tab	Moves focus to the next field or interface element.
Shift + **Tab**	Moves focus to the previous field or interface element.
Enter	Starts the search.
Ctrl + **Up arrow**	Moves cursor to the first character.
Ctrl + **Down arrow**	Moves cursor to the last character.
Ctrl + **Left arrow**	Moves cursor to the first character.
Ctrl + **Right arrow**	Moves cursor to the last character.

Context menus

Use context menus to perform operations on canvas, tables, or other interface elements.

Tip: The available context menu options depend on the selected item protocol.

Canvas

Table 18. Zone container

Command	Description
Go to Zone Table	Focuses on the zone in the Zone list.
View Properties	Opens zone properties.
Add Device	Opens a dialog to add a device.
Add Conduit	Opens a dialog to add a conduit.

Table 18. Zone container (continued)

Command	Description
Copy	Copies the zone.
Paste	Pastes the copied zone.
Delete	Deletes the zone.

Table 19. Device

Command	Description
Device Properties	Opens device properties.
Port Properties	Opens port properties of the device.
Add Conduit	Opens a dialog to add a conduit.
Cut	Cuts the device from the zone and enables you to paste the device into a different zone.
Copy	Copies the device.
Paste	Pastes the cut or copied device into the zone.
Go to Zone Table	Focuses on the device in the Zone table.
Replace Device	Opens a pop-up window to replace the device.
Delete	Deletes the device from the model.

Table 20. Blank canvas space

Command	Description
Paste	Pastes the copied zone.

Zones

You can open the context menu for each zone on the list.

Table 21. Zones list

Command	Description
View Properties	Opens the properties of the selected zone.
Copy	Copies the properties of the selected zone.
Paste	Creates a zone with the same properties as the last copied zone. The new zone has the same name as the original and adds a number in parentheses. The conduits and devices do not transfer from the original zone.
Delete	Deletes the selected zone.

Table 22. Overview table

Command	Description
Copy	Copies the properties of the selected zone.

Table 22. Overview table (continued)

Command	Description
Paste	Creates a zone with the same properties as the copied zone. The new zone has the same name as the original and adds a number in parentheses. The conduits and devices do not transfer from the original zone.
Go to Zone	Opens the device table of the selected zone.
Delete	Deletes the selected zone.

Table 23. Device table

Command	Description
Device Properties	Displays the properties pane of the device.
Port Properties	Displays the Port Properties of the selected device.
Cut	Removes the device from the selected zone. You can **Paste** this device to a different zone.
Copy	Copies the properties of the selected device.
Paste	• If you used **Cut**: Pastes the cut device to the selected zone. • If you used **Copy**: Creates a device with the same properties as the copied device. The new device has the same name as the original and adds a number in parentheses.
Replace Device	Opens the **Deploy Configuration to Replace Device** window. This command is active only if the device was already deployed.
Delete	Deletes the selected device.

Conduits

Table 24. Conduits table

Command	Description
View Properties	Opens the **Properties** pane of the selected conduit.
Delete	Deletes the selected conduit.

Devices

Table 25. Device table

Command	Description
Device Properties	Displays the properties pane of the device
Port Properties	Displays the port properties of the selected device.
Cut	Removes the device from the selected zone. You can **Paste** this device to a different zone.

Table 25. Device table (continued)

Command	Description
Copy	Copies the properties of the selected device.
Paste	• If you used **Cut**: Pastes the cut device to the selected zone. • If you used **Copy**: Creates a device with the same properties as the copied device. The new device has the same name as the original and adds a number in parentheses.
Go to Zone	Opens the device table of the zone that has the selected device is assigned.
Replace Device	Opens the **Deploy Configuration to Replace Device** window. This command is active only if the device was already deployed.
Delete	Deletes the selected device.

Discovery pane

The commands available in this menu depend on the selected item in the topology.

Table 26. Discovered CIP device

Command	Description
Add	Adds new devices to the selected zone.
Add Anchor	Anchors a topology node to the root so that it can be easily accessed without browsing the topology tree.
Driver Configuration	Opens **Configure Driver properties**.
View Property	Opens a list of all properties of the selected device.
Refresh	Refreshes the network topology.
Delete	Deletes the item from the topology.

Policy management capabilities

FactoryTalk Policy Manager enables you to configure and manage industrial control system policies from various domains, including: security, communication, and eventing.

CIP security policy

CIP Security helps protect an EtherNet/IP connected device from malicious communications.

Security within the system adheres to the ODVA™ CIP Security™ standard for usage of cryptographic keys and certificates.

Security

CIP Security helps protect an EtherNet/IP connected device from malicious communications by:

- Applying authentication rules and rejecting messages sent by untrusted people or untrusted devices
- Verifying that data has not been altered during transmission and reject data that fails the integrity check
- Helping to prevent accessing the EtherNet/IP data by unauthorized parties for additional confidentiality

CIP-secure policy models support these core security properties:

Property	Description
Device Identity	X.509v3 digital certificates provide cryptographically secure identities to devices.
Device Authentication	The Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) cryptographic protocols provide secure transport of EtherNet/IP traffic.
Data Integrity	Hashes or keyed-hash message authentication code (HMAC) provides data integrity and message authenticity to EtherNet/IP traffic.
Data Confidentiality	Data encryption helps prevent accessing the EtherNet/IP data by unauthorized parties.

Authentication methods

CIP-secure components may use these authentication methods:

Method	Description
Certificate	Established by the use of an X.509v3 certificate granted by a trusted certificate authority. You can use these options for I/O Data Security if a certificate is used as the authentication method additional security: **Integrity Only** Checks whether data was altered and whether the data was sent by a trusted entity. Altered and/or untrusted data is rejected. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **Tip:** Rockwell Automation recommends choosing this option.

Method	Description
Pre-shared key	Established by presentation of a shared secret key that is propagated to trusted devices in the system. A pre-shared key can be created manually or FactoryTalk Policy Manager can automatically generate pre-shared keys for distribution to the devices in your system.
Trusted IP	Established by identifying an IP address as trusted by the policy model. A set of IP addresses can be defined as a trusted range on your network. Appropriate for use with devices that are not CIP Security capable.

For more details about the CIP properties available for different policy model components, see:

- Zone properties on page 65
- Conduit properties on page 70
- Device properties on page 80

Conduits

With CIP endpoints, you can create these conduits:

Table 27. CIP conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	Device
Zone	Range
Device	Device
Device	Range

Conduits must follow these rules:

- Conduits cannot be duplicated, each combination of endpoints must be unique.
- One of the endpoints must be CIP Security or OPC UA security policy capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.
- Devices not assigned to any zone or onboarding devices cannot be used as endpoints.

Ingress/Egress rules

The Ingress/Egress Object is a set of rules that govern which network nodes can communicate to the device and through the device:

Ingress rules

Determine which other nodes can communicate with this device.

Egress rules

Determine how the device can communicate with other nodes.

For more information about the Ingress/Egress rules, refer to the ODVA™ documentation.

Compatibility

CIP Security features work with these Rockwell Automation products:

- FactoryTalk Linx version 6.11 or later
- ControlLogix® 5580 controllers firmware revision 32.00 or later
- 1756-EN4TR ControlLogix Module
- Kinetix® 5300 Drives
- Kinetix 5700 Drives
- PowerFlex® 755T
- 1783-CSP CIP Security Proxy
- CompactLogix™ 5380 controllers firmware revision 34.00 or later
- Compact GuardLogix® 5380 controllers firmware revision 34.00 or later
- GuardLogix® 5580 controllers firmware revision 34.00 or later

Enhanced device authentication

Enhanced device authentication ensures only trusted parties establish connections based on defined policies.

Operation

Enhanced device authentication adds the Subject Alternative Name (IP address) and may add DNS information unique for a device to its digital identity certificate. This method helps protect against identity spoofing.

You can customize the enhanced device authentication to:

- Receive notifications about devices that do not support enhanced device authentication.
- Prohibit the policy deployment to devices that fail enhanced device authentication.

IMPORTANT: It is recommended to prohibit the policy deployment to devices that fail enhanced device authentication.

To enable, disable, or configure enhanced device authentication, see Edit Global Settings on page 63.

Tip: Enabling enhanced device authentication involves the deployment of updates to all devices in the policy model. You can deploy the updates directly after enabling enhanced device authentication or do that later.

Supported devices

These devices support enhanced device authentication:

- ControlLogix® 5580 Controllers version 35.00 or later.
- ControlLogix® 5580 Process Controllers version 35.00 or later.
- GuardLogix® 5580 Controllers version 35.00 or later.
- CompactLogix™ 5380 Controllers version 35.00 or later.
- CompactLogix™ 5380 Process Controllers version 35.00 or later.
- Compact GuardLogix® 5380 Controllers version 35.00 or later.
- 1756-EN4TR ControlLogix® Module.
- FactoryTalk® Linx™ version 6.40 or later.

Automatic Policy Deployment

Automatic Policy Deployment leverages the ODVA CIP Security pull model that enables EtherNet/IP endpoints (for example, field devices) to initiate the deployment of policies defined on a system server.

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

Overview

By using Automatic Policy Deployment, you can improve the system:

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

Automatic Policy Deployment supports the following devices:

- ControlLogix 5580 controllers (version 34)
- GuardLogix 5580 controllers (version 34)
- CompactLogix 5380 controllers (version 34)
- Compact GuardLogix 5380 controllers (version 34)
- EtherNet/IP communication modules (1756-EN4TR, version 4.001)

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

Tip: 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.

Operation

Automatic Policy Deployment discovers the devices in the network that you can add to the policy model.

IMPORTANT: Automatic Policy Deployment can onboard and merge only a single EtherNet/IP interface of a device. This applies to CompactLogix 5380 controllers operating in the Dual IP mode.

IMPORTANT: Automatic Policy Deployment uses the Enrollment over Secure Transport (EST) service. If your machine has multiple network interfaces, the EST service uses a random network interface by default. To specify the network interface for the EST service, see Configure Automatic Policy Deployment for multiple network interfaces on page 47.

Depending on your requirements, you can set Automatic Policy Deployment to:

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

Tip: The Automatic Policy Deployment process is independent from the manual policy deployment process. The manual policy model deployment process can interrupt the Automatic Policy Deployment process. Once the policy model is deployed, Automatic Policy Deployment continues adding and merging the discovered devices.

For auditing and troubleshooting purposes, Automatic Policy Deployment indicates changes to the policy model with:

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

Table 28. Notification icons

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 are not a part of the policy model. You cannot 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.

IMPORTANT: Secure onboarding policy is effective only for embedded EtherNet/IP interfaces. Devices can still be accessed through backplanes.

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

IMPORTANT: When you move a device from the Onboarding Area to a zone or make the device unassigned, you cannot assign the device to the Onboarding Area again.

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

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

Merging

Depending on the policy 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 policy model.

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

Tip:

The following properties are never overwritten by the automatic merging process:

- IP address
- Device name
- Device description

The following tables illustrate the examples on how the automatic merging process operates in different scenarios.

Table 29. Scenario 1 - Device replacement (policy erased)

Onboarding device	Device in the policy model (Zone 1)	Merged device (Zone 1)	Description
IP Address: 192.168.1.68 Name: 1756-L81E Description: 1756-L81E Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN12345	IP Address: 192.168.1.68 Name: Line Controller Description: Main controller for assembly line Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN12345	IP Address: 192.168.1.68 Name: Line Controller Description: Main controller for assembly line Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN12345	All device parameters match: • Device name (retained) • Device description (retained) The device malfunctioned and was reset to factory defaults.

Table 30. Scenario 2 - Device replacement (serial number mismatch)

Onboarding device	Device in the policy model (Zone 1)	Merged device (Zone 1)	Description
IP Address: 192.168.1.68 Name: 1756-L81E Description: 1756-L81E Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN12345	IP Address: 192.168.1.68 Name: Line Controller Description: Main controller for assembly line Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN54321	IP Address: 192.168.1.68 Name: Line Controller Description: Main controller for assembly line Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN1234	All device parameters match except for: • Serial numbers (overwritten) • Device name (retained) • Device description (retained)

Table 30. Scenario 2 - Device replacement (serial number mismatch) (continued)

Onboarding device	Device in the policy model (Zone 1)	Merged device (Zone 1)	Description
			The device malfunctioned and was replaced with a new device.

Table 31. Scenario 3 - Device replacement (serial number and firmware revision mismatch)

Onboarding device	Device in the policy model (Zone 2)	Merged device (Zone 2)	Description
IP Address: 192.168.1.73 Name: 1756-L83E Description: 1756-L83E Product type: 14 Product code: 166 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN111213	IP Address: 192.168.1.73 Name: Machine Controller Description: Packaging machine controller Product type: 14 Product code: 166 Firmware major revision: 33 Firmware minor revision: 001 Serial number: SN313211	IP Address: 192.168.1.73 Name: Machine Controller Description: Packaging machine controller Product type: 14 Product code: 166 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN111213	All device parameters match except for: • Serial numbers (overwritten) • Firmware major revision (overwritten) • Device name (retained) • Device description (retained) The device malfunctioned and was replaced with a new device.

Table 32. Scenario 4 - Device replacement (several properties mismatch)

Onboarding device	Device in the policy model (Zone 3)	Merged device (Zone 3)	Description
IP Address: 192.168.1.82 Name: 1756-EN4TR Description: 1756-EN4TR Product type: 12 Product code: 258 Firmware major revision: 4 Firmware minor revision: 001 Serial number: SN223344	IP Address: 192.168.1.82 Name: Conveyor PF755T #12 Description: Conveyor drive #12 Product type: 45 Product code: 7 Firmware major revision: 10 Firmware minor revision: 00 Serial number: SN556677	IP Address: 192.168.1.82 Name: Conveyor PF755T #12 Description: Conveyor drive #12 Product type: 12 Product code: 258 Firmware major revision: 4 Firmware minor revision: 001 Serial number: SN223344	A non-typical scenario with device mismatch. The existing device is treated as obsolete and overwritten. The device parameters are merged: • Serial numbers (overwritten) • Device name (retained) • Device description (retained) • Product type (overwritten) • Product code (overwritten)

Table 32. Scenario 4 - Device replacement (several properties mismatch) (continued)

Onboarding device	Device in the policy model (Zone 3)	Merged device (Zone 3)	Description
			• Firmware major revision (overwritten) • Firmware minor revision (overwritten)

Manual merging

The merging process is manual if the onboarding device cannot be associated with any device in the policy model.

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

The following table illustrates an example of the manual merging process.

Onboarding device	Device in the policy model	Merged device	Description
IP address: 192.168.1.68 Name: 1756-L81E Description: 1756-L81E Product type: 14 Product code: 164 Firmware major revision: 34 Firmware minor revision: 001 Serial number: SN12345	No match	N/A	No matching device found in the policy model. Device added to the Onboarding Area.

Secured device replacement

The secured device replacement process identifies onboarded devices against existing entries in the policy model based on the specific criteria and deploys the policies automatically.

The onboarding device matches the device in the policy model if the following properties are the same:

- IP address
- Vendor
- Product type
- Product code
- Major firmware revision (the same or higher)

IMPORTANT: The vendor certificate of a device determines the vendor property. Currently, FactoryTalk Policy Manager supports only Rockwell Automation vendor certificates.

Automatic Policy Deployment notifications

FactoryTalk Policy Manager displays the results of the Automatic Policy Deployment process in the **Results** pane. If needed, you can use the following messages to troubleshoot issues with Automatic Policy Deployment.

Tip: For detailed information about the Automatic Policy Deployment process for specific devices, see the FactoryTalk® Diagnostics log.

New devices

Table 33. Discovered devices without references in the policy model that Automatic Policy Deployment adds to the Onboarding Area

Message	Description
The device *{name}* (*{IP address}*) is enrolled. The device is added to Onboarding Area.	The discovered device had no reference in the policy model and was added to the Onboarding Area.
The Secure Onboarding Policy for device *{name}* (*{IP address}*) was not applied. The device does not support this policy.	Automatic Policy Deployment failed to deploy the policy to the discovered device. Verify if the device supports the policy.
The Secure Onboarding Policy for device *{name}* (*{IP address}*) was not applied because a valid FactoryTalk Linx Driver was not found.	Automatic Policy Deployment failed to deploy the policy to the discovered device. Verify if the correct EtherNet/IP driver is assigned to the discovered device. If the driver does not exists, add the driver with FactoryTalk Linx.
The device *{name}* (*{IP address}*) is enrolled. The device is added to Onboarding Area. Initiating secure onboarding.	The Automatic Policy Deployment process starts. The discovered device is added to the Onboarding Area. Establishing a connection between the discovered device and FactoryTalk Policy Manager or other devices in the policy model. The deployment process completion time depends on the number of discovered devices.
The device *{name}* (*{IP address}*) is enrolled. The device is added to Onboarding Area. The Secure Onboarding Policy was applied.	Automatic Policy Deployment added the device to the Onboarding Area and the deployment process completed. Established a connection between the device added to the Onboarding Area and FactoryTalk Policy Manager or other devices in the policy model. You can move the device from the Onboarding Area to the policy model.
The Secure Onboarding Policy for *{name}* (*{IP address}*) was not applied. Check event log for more details.	Automatic Policy Deployment failed to deploy the discovered device. The discovered device was not added to the Onboarding Area. Failed to establish a connection between the device added to the Onboarding Area and FactoryTalk Policy Manager or other devices in the policy model. For more information, see the FactoryTalk Diagnostics logs. Once you resolve the issue with the device, Automatic Policy Deployment will discover and process the device again.
The device *{name}* (*{IP address}*) was removed from the security model.	The device that was deployed to the policy model was deleted from the policy model.

Table 33. Discovered devices without references in the policy model that Automatic Policy Deployment adds to the Onboarding Area (continued)

Message	Description
	Automatic Policy Deployment removed the device from the policy model.

Devices qualified to merge

Table 34. Discovered devices with deployed references in the policy model that Automatic Secured Device Replacement merges into the policy model

Message	Description
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). All entries are merged. Initiating automatic secured device replacement.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model. Establishing a connection between the discovered device and FactoryTalk Policy Manager or other devices in the policy model. The deployment process completion time depends on the number of discovered devices.
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). All entries are merged. Policy deployment was successful.	The automatic secured device replacement process completed. The discovered device is merged with the previously deployed device in the policy model. Established a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. If needed, you can edit the merged device properties.
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). All entries are merged.	The automatic secured device replacement process is in progress. The discovered device is merged with the previously deployed device in the policy model.
Policy deployment for *{name}* (*{IP address}*) failed. Start Replace Device action manually.	The automatic secured device replacement process failed. Trying to establish a connection between the discovered device and FactoryTalk Policy Manager or other devices in the policy model. For more information, see the FactoryTalk Diagnostics logs. If needed, replace the device manually. For more information, see Devices on page 72.
Policy deployment for *{name}* (*{IP address}*) failed. The secure onboarding policy was not applied. The device does not support this policy.	The automatic secured device replacement process failed to deploy the policy to the discovered device. Verify if the device supports the policy.
Policy deployment for *{name}* (*{IP address}*) failed. The secure onboarding policy was not applied because a valid FactoryTalk Linx Driver was not found. Assign a valid driver and initiate Replace Device action manually.	The automatic secured device replacement process failed to deploy the policy to the discovered device. Verify if the correct EtherNet/IP driver is assigned to the discovered device. If the driver does not exists, you must add the driver with FactoryTalk Linx. Replace the device manually. For more information, see Devices on page 72.

Table 34. Discovered devices with deployed references in the policy model that Automatic Secured Device Replacement merges into the policy model (continued)

Message	Description
Device *{name}* (*{IP address}*) enrolled and qualified as replacement for Device *{name}* (*{Zone name}*). Entries merged.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model. The deployment process completion time depends on the number of discovered devices.
Deployment for *{name}* (*{IP address}*) unsuccessful. Initiating secure onboarding.	The automatic secured device replacement process failed. Reapplying the secure policy to the device. Establishing a connection between the discovered device and FactoryTalk Policy Manager or other devices in the policy model.
Policy for *{name}* (*{IP address}*) deployment failed.	The automatic secured device replacement process failed. For more information, see the FactoryTalk Diagnostics logs.
The secure onboarding policy for *{name}* (*{IP address}*) was applied successfully. Start Replace Device action manually.	The automatic secured device replacement applied the secure policy to the device. Established a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. Replace the device manually. For more information, see Devices on page 72.
Deployment for *{name}* (*{IP address}*) failed. The secure onboarding policy was not applied. Check event log for more details.	The automatic secured device replacement failed to deploy the policy to the discovered device. Failed to establish a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. Replace the device manually. For more information, see Devices on page 72. For detailed information about the automatic secured device replacement process, see the FactoryTalk Diagnostics logs.

Table 35. Discovered devices with not deployed references in the policy model that Automatic Policy Deployment merges into the policy model

Message	Description
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model. The deployment process completion time depends on the number of discovered devices.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied. The device does not support this policy.	The automatic secured device replacement process failed deploy the policy to the discovered device. Verify if the device supports the policy.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied because a valid FactoryTalk Linx Driver was not found.	The automatic secured device replacement process failed to deploy the policy to the discovered device.

Table 35. Discovered devices with not deployed references in the policy model that Automatic Policy Deployment merges into the policy model (continued)

Message	Description
	Verify if the correct EtherNet/IP driver is assigned to the discovered device. If the driver does not exists, add the driver with FactoryTalk Linx.
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged. Initiating secure onboarding.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model. Established a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. The deployment process completion time depends on the number of discovered devices.
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged. The secure onboarding policy was applied.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model. Established a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. The deployment process completion time depends on the number of discovered devices.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied. Check event log for more details.	The automatic secured device replacement process failed. Failed to establish a connection between the merged device and FactoryTalk Policy Manager or other devices in the policy model. For more information, see the FactoryTalk Diagnostics logs.

Table 36. Discovered devices with deployed references in the policy model that Automatic Policy Deployment merges into the policy model

Message	Description
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). All entries are merged.	The automatic secured device replacement process starts. The discovered device is merged with the matching device in the policy model.
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). The secure onboarding policy was not applied. The device does not support this policy.	The automatic secured device replacement process was unable to deploy the policy to the discovered device. Verify if the device supports the policy. The discovered device is merged with the matching device in the policy model.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied because a valid FactoryTalk Linx Driver was not found. Assign a valid driver and Replace Device.	The automatic secured device replacement process failed to deploy the policy to the discovered device. Verify if the correct EtherNet/IP driver is assigned to the discovered device. If the driver does not exists, add the driver with FactoryTalk Linx. Replace the device manually. For more information, see Devices on page 72.

Table 36. Discovered devices with deployed references in the policy model that Automatic Policy Deployment merges into the policy model (continued)

Message	Description
The device *{name}* (*{IP address}*) is enrolled and qualified as a replacement for the device *{name}* (*{Zone name}*). All entries are merged. Initiating secure onboarding.	The discovered device is merged with the matching device in the policy model. Establishing a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model. The automatic secured device replacement process starts. The deployment process completion time depends on the number of discovered devices.
Device *{name}* (*{IP address}*) enrolled and qualified as replacement for Device *{name}* (*{Zone name}*). All entries are merged. The secure onboarding policy was applied successfully.	The automatic secured device replacement process completed. Established a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied. Check event log for more details.	The automatic secured device replacement process failed to deploy the discovered device. Failed to establish a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model. For more information, see the FactoryTalk Diagnostics logs. Once you resolve the issue with the device, Automatic Policy Deployment will discover and process the device again.

Table 37. Discovered devices with not deployed references in the policy model that Automatic Policy Deployment merged into the policy model

Message	Description
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged.	The Automatic Policy Deployment process starts. The discovered device is merged with the matching device in the policy model.
The secure onboarding policy for (*{name}* (*{IP address}*) was not applied. The device does not support this policy.	The Automatic Policy Deployment process failed to deploy the policy to the discovered device. Verify if the device supports the policy.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied because a valid FactoryTalk Linx Driver was not found. Perform manual merge in a destination zone.	The Automatic Policy Deployment process failed to deploy the policy to the discovered device. Verify if the correct EtherNet/IP driver is assigned to the discovered device. If the driver does not exists, add the driver with FactoryTalk Linx.
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged. Initiating secure onboarding.	The discovered device is merged with the matching device in the policy model. The secure onboarding process starts. Establishing a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model.

Table 37. Discovered devices with not deployed references in the policy model that Automatic Policy Deployment merged into the policy model (continued)

Message	Description
	The deployment process completion time depends on the number of discovered devices.
The device *{name}* (*{IP address}*) is enrolled and qualified to merge with existing *{name}* (*{Zone name}*) device in the model. All entries are merged. The secure onboarding policy was applied.	The Automatic Policy Deployment process added the device to the policy model and the deployment process completed. Established a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model.
The secure onboarding policy for *{name}* (*{IP address}*) was not applied. Check event log for more details.	The Automatic Policy Deployment process failed to deploy the discovered device. Failed to establish a connection between the device added to the policy model and FactoryTalk Policy Manager or other devices in the model. For more information, see the FactoryTalk Diagnostics logs.

Configure Automatic Policy Deployment for multiple network interfaces

Automatic Policy Deployment uses the Enrollment over Secure Transport (EST) service. If your machine has multiple network interfaces, the EST service uses a random network interface by default. You can select a specific network interface by editing the `appConfiguration.json` file.

Tip: You must be a Windows administrator and have a FactoryTalk Directory administrator account to specify the network interface for the EST service.

1. In a text editor, open the FactoryTalk System Services configuration file: `C:\ProgramData\Rockwell Automation\FactoryTalk System Services\config\admin\appConfiguration.json`
2. Add a configuration for the EST service.

   IMPORTANT: For the hostname property value, use the IP address.

   ```
   "est": {
       "port": 40014,
       "filePathCertificate": "",
       "filePathPrivateKey": "",
       "hostname": "192.168.1.100"
   }
   ```
3. Save the configuration file.
4. Restart FactoryTalk System Services.

Export Automatic Policy Deployment results

Export Automatic Policy Deployment results to a file for archival purposes.

Tip:

If you close FactoryTalk Policy Manager with unsaved Automatic Policy Deployment results, a dialog appears. In the dialog, you can select either:

- **Export**. Exports the Automatic Policy Deployment results and then closes FactoryTalk Policy Manager.
- **Close**. Closes FactoryTalk Policy Manager without exporting the Automatic Policy Deployment results.
- **Cancel**. Closes the dialog and does not close FactoryTalk Policy Manager.

To export Automatic Policy Deployment results

1. In the status bar, select **Automatic Policy Deployment result pane**.
2. In **Auto Policy**, select **Save** to export the Automatic Policy Deployment results to a file.

Disable Automatic Policy Deployment

Disable Automatic Policy Deployment by editing global settings and manually closing ports on the machine.

Tip: The FactoryTalk Policy Manager installation agent opens these Windows Firewall ports: `UDP 5353` and `TCP 40014`. To operate correctly, the Automatic Policy Deployment functionality requires these ports to be open.

1. Open FactoryTalk Policy Manager, select **Global Settings** and clear the **Enable automatic device discovery and onboarding** checkbox.
2. Manually close the `UDP 5353` and `TCP 40014` ports on the machine.

CIP Bridging Control

CIP Bridging Control enables you to control the traffic flow between physical communication interfaces and backplanes.

Overview

Devices within an Industrial Control System (ICS) may involve multiple network interfaces. The use of Common Industrial Protocol (CIP) on the backplanes and communication ports of Rockwell Automation devices can facilitate physical network segmentation. For EtherNet/IP interfaces, you can provide data bridging between two separate physical Ethernet networks by using CIP.

The CIP Security communication modules and embedded EtherNet/IP interfaces can analyze and then allow or deny network traffic according to device-specific policies. You can use CIP Bridging Control to help prevent unintended data flows from occurring, especially data flows originating from unsecured parts of the system to secure parts of the system.

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

Operation

You can configure endpoint-specific rules for bridging between:

- EtherNet/IP interface and backplane
- USB interface and backplane

Due to the architectural differences between devices, endpoint-specific settings can take various forms. For enhanced fidelity, policy definition capabilities often specify the traffic direction property.

Tip: By default, the bridged traffic flows without any restrictions like in a CIP-based device that does not support CIP Security.

CIP bridging settings hierarchy

The CIP Bridging Control settings can be global or specific to a port, device, or zone.

Settings levels

The following list outlines the CIP bridging settings levels (from the lowest level to the highest level):

1. Port-level settings
2. Device-level settings
3. Zone-level settings
4. Global settings

The CIP Bridging Control settings follow these conventions:

- The lower-level settings must be compliant with the higher-level settings.
- The lower-level settings can be stricter than the higher-level settings.
- If the lower-level settings are less strict than the higher-level settings, the higher-level settings overwrite the lower-level settings.

Port-level settings

These settings apply to EtherNet/IP interfaces and provide the distinction between secure and Trusted IP (permitted) traffic.

Tip: During the initial policy deployment, FactoryTalk Policy Manager attempts to identify the modules that occupy chassis slots.

Device-level settings

These settings enable or disable the communication bridging between the USB port of a device and a backplane or other physical ports.

Zone-level settings

These settings ensure compliance for all port-level and device-level settings. The port-level and device-level settings can be stricter than zone-level settings.

The following table shows examples of zone-level settings paired with port-level settings:

Table 38. Zone settings and port settings

Zone settings	Port settings	Description
Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Allow all traffic	Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Chassis size: 4 • Slots disabled: none	Allowed configuration. The port-level settings (lower-level settings) and zone-level settings (higher-level settings) match.
Inbound CIP bridging • Allow secure trafic Outbound CIP bridging • Allow all traffic	Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Chassis size: 4 • *Slots disabled: 1, 2, 3*	Allowed configuration. The port-level settings (lower-level settings) are stricter than the zone-level settings (higher-level settings).
Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Block all traffic	Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Chassis size: 4 • *Slots disabled: none*	Disallowed configuration. The port-level settings (lower-level settings) are less strict than the zone-level settings (higher-level settings).

Global settings

Global policy ensures compliance for all zones in the model. The zone-level settings can be stricter than global settings.

The following table shows examples of global settings paired with zone-level settings:

Table 39. Global settings and zone settings

Global settings	Zone settings	Description
Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Allow all traffic	Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • Allow all traffic	Allowed configuration. The port-level settings (lower-level settings) and zone-level settings (higher-level settings) match.
Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • *Allow all traffic*	Inbound CIP bridging • Allow secure traffic Outbound CIP bridging • *Block all traffic*	Allowed configuration. The zone-level settings (lower-level settings) are stricter than the global settings (higher-level settings).
Inbound CIP bridging • *Allow secure traffic* Outbound CIP bridging • Allow all traffic	Inbound CIP bridging • *Allow all traffic* Outbound CIP bridging • Allow all traffic	Disallowed configuration. The zone-level settings (lower-level settings) are less strict than the global settings (higher-level settings).

CIP Proxy devices

The CIP Proxy device is CIP-Security capable and can be communicated to securely. It is placed on the communication path to a non-CIP Security capable device and allows for secure communication to that device.

IMPORTANT: CIP Proxy devices cannot be used as proxies for controllers or HMI devices.

When first installed, the proxy device allows all communication to pass through. Once the proxy is configured to represent a device, then it only allows communication to that one device. The proxy can only represent a device that does not yet exist in the security policy model. To configure a device as a proxied device after it has been added to the security policy model, delete the device and add it again as a proxied device. After you deploy the security policy model, you cannot change which device is proxied until you delete the proxy and the proxy device, and add them again.

The CIP Proxy device has the same device properties as other devices when configured using FactoryTalk Policy Manager:

- Vendor
- Firmware Revision
- CIP Security capable
- Ports

CIP Proxy devices have only a single port. That port is used to proxy the port of another device. The device being proxied is identified using the **Port Proxied** setting.

The CIP Proxy device can be placed in a different zone than its proxied device. When you move a CIP Proxy device to a different zone in the model, the proxied device is not affected, it stays assigned to the same zone.

Tip: If you used the EDS file or **Discovery** to add the CIP Proxy device and associate a proxied device, the properties settings are automatically configured. If you are working with a Generic device, you must configure the proxy manually.

OPC UA security policy

Manage connections between OPC UA servers, OPC UA clients, and other components of your system policy model.

For more information about OPC UA, refer to Unified Architecture - OPC Foundation.

OPC UA servers

In FactoryTalk Policy Manager, OPC UA servers are device types, which you can add to the policy model and use as conduit endpoints. You can also import certificates of OPC UA servers. The certificates are exported to `C:\ProgramData\Rockwell Automation\FactoryTalk System Services\OPC UA Deployments`

OPC UA servers support these authentication methods:

Certificate

Authenticate with an X.509 certificate granted by a trusted certificate authority.

Username and password

Authenticate with a username and password or as an anonymous user.

Table 40. OPC UA Security levels

Message security mode	Security policy	Security level
None	None- None	Low security
Sign	Basic128Rsa15	
Sign & Encrypt	Basic128Rsa15	
Sign	Basic256	
Sign & Encrypt	Basic256	
Sign	Aes128Sha256RsaOaep	Medium security
Sign & Encrypt	Aes128Sha256RsaOaep	
Sign	Basic256Sha256	Hight security
Sign & Encrypt	Basic256Sha256	
Sign	Aes256Sha256RsaPss	
Sign & Encrypt	Aes256Sha256RsaPss	

Tip: Rockwell Automation recommends setting message security mode to Sign & Encrypt.

Each OPC UA server has its own trust list and admin list. If you add an OPC UA server to a zone for the first time and deploy the policy model configuration, the zone trust list and admin list overwrites the OPC UA server trust list and admin list. Consecutive deployments merge the OPC UA server and zone trust lists and admin lists.

For more information about OPC UA server properties, see Device properties on page 80.

OPC UA clients

In FactoryTalk Policy Manager, you can add OPC UA clients to the policy model and use as them conduit endpoints. You can also import and export certificates of OPC UA clients. The certificates are exported to `C:\ProgramData\Rockwell Automation\FactoryTalk System Services\OPC UA Deployments`

IMPORTANT: If you export OPC UA certificates or CSRs from an OPC UA device and the security policy model contains both a certificate and a CSR, only the certificate is exported.

OPC UA clients may support these authentication methods:

Certificate

Authenticate with an X.509 certificate granted by a trusted certificate authority.

Username and password

Authenticate with a username and password or as an anonymous user.

OPC UA security policy in zones and conduits

Zones and conduits follow these non-editable OPC UA security policy settings:

- OPC UA clients trust OPC UA servers
- OPC UA servers do not trust OPC UA servers
- OPC UA clients do not trust OPC UA clients

Conduits with OPC UA endpoints

With OPC UA endpoints, you can create these conduits:

Table 41. OPC UA conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	OPC UA server
Zone	OPC UA client
Zone	Range
OPC UA client	OPC UA server

Conduits must follow these rules:

- Conduits cannot be duplicated, each combination of endpoints must be unique.
- One of the endpoints must be CIP Security or OPC UA security policy capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.
- Devices not assigned to any zone or onboarding devices cannot be used as endpoints.

Compatibility

OPC UA security policy features work with these Rockwell Automation product families:

- ControlLogix® 5580 controllers firmware revision 36.00 or later

  Tip: 1756-L81E and 1756-L81EK controllers are not supported.

- GuardLogix® 5580 controllers firmware revision 36.00 or later

  Tip: 1756-L81ES and 1756-L81ESK controllers are not supported.

- CompactLogix™ 5380 controllers firmware revision 36.00 or later
- Compact GuardLogix® 5380 controllers firmware revision 36.00 or later
- ControlLogix® Process controllers firmware revision 36.00 or later

  Tip: 1756-L81E and 1756-L81EK controllers are not supported.

- CompactLogix™ Process controllers firmware revision 36.00 or later
- FactoryTalk® Logix Echo version 36.00 or later

Related information

Policy model configuration on page 58

Security Eventing

Use Security Eventing to configure the logging of messages that are sent between devices.

The Security Eventing service requires a Syslog server to operate. The Security Eventing policy is applied to every device in the policy model that supports Security Eventing.

To enable, disable, or configure Security Eventing, see Edit Global Settings on page 63.

Policy model

The security policy model of your system includes zones, conduits, and devices.

Zones

Zones form groups of logical or physical devices to which security settings are applied. Devices within a zone trust each other, except for OPC UA servers.

Zones can contain CIP and OPC UA devices.

To configure zones, see Zones on page 63.

Conduits

Conduits are communication pathways in the policy model, connecting pairs of policy model components.

You can create conduits between these components:

Table 42. CIP conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	Device
Zone	Range
Device	Device
Device	Range

Table 43. OPC UA conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	OPC UA server
Zone	OPC UA client
Zone	Range
OPC UA client	OPC UA server

Conduits must follow these rules:

- Conduits cannot be duplicated, each combination of endpoints must be unique.
- One of the endpoints must be CIP Security or OPC UA security policy capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.
- Devices not assigned to any zone or onboarding devices cannot be used as endpoints.

To configure conduits, see Conduits on page 69.

Devices

Devices include:

- Computers
- Controllers
- Modules
- HMI panels
- OPC UA clients
- OPC UA servers
- Drives

Some devices do not support CIP Security or OPC UA security policy and cannot authenticate themselves to the system. For such devices, consider using these approaches:

CIP Proxy device

A CIP Proxy device can be placed in front of the non-CIP securable device. The CIP Proxy device controls the communication to the device it proxies and can sign and encrypt data from the device. For more information, see CIP Proxy devices on page 50.

Trusted IP address

The device is assigned an IP address that is trusted by the system and permitted to communicate within the security zone. However, these devices are not able to sign or encrypt communications.

To configure devices, their ports, and device ranges, see Devices on page 72.

Policy model planning

To plan the policy model, establish the following:

- Zones and their security requirements
- Devices, their IP addresses, and zone assignments
- Conduits to define trust relationships between policy model components

For an example, see Policy model example on page 55.

Policy model example

The policy model example includes three zones connected with conduits that contain different device types.

Figure 9. Policy model example

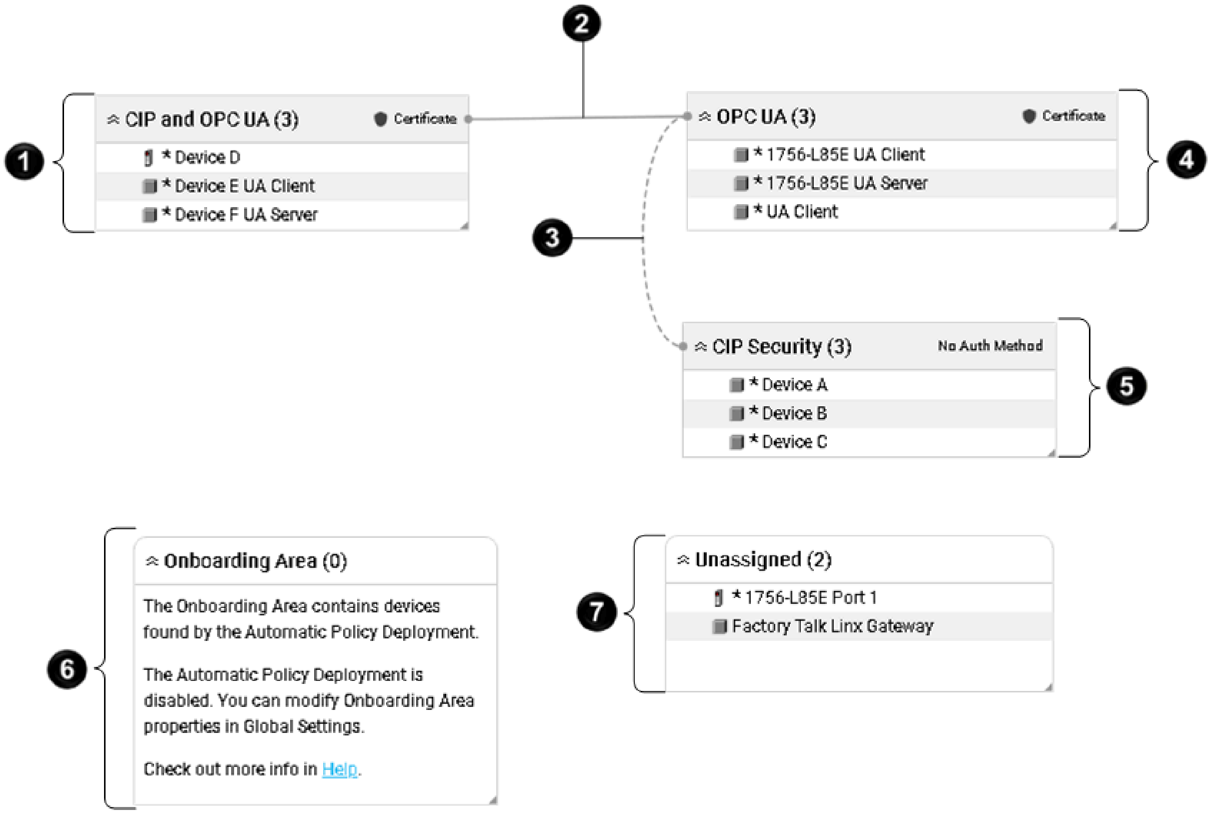


Table 44. Diagram description - policy model example

Item	Name	Description
1	**CIP and OPC UA** zone	Contains OPC UA devices and CIP devices.
2	Secure **conduit**	Connects **CIP and OPC UA** zone with **OPC UA** zone.
3	Trusted unsecure **conduit**	Connects **OPC UA** zone with **CIP Security** zone.
4	**OPC UA** zone	Contains OPC UA devices only, including two OPC UA clients and one OPC UA server.
5	**CIP Security** zone	Contains three CIP devices.
6	**Onboarding Area** container	Contains devices found by Automatic Policy Deployment that can be added to the policy model. There are no devices found by Automatic Policy Deployment in this example.
7	**Unassigned** container	Contains devices added to the policy model but not added to any zone in the policy model.

Table 44. Diagram description - policy model example (continued)

Item	Name	Description
		There are two unassigned devices in this example.

Policy model auditing

FactoryTalk System Services generate diagnostic messages upon specific actions and log them toFactoryTalk Diagnostics. These messages can be later reviewed as a part of an audit.

Message categories

The diagnostic messages are divided into these categories:

Model deployment

Sent when you deploy a security policy model or cancel deployment.

Model creation

Sent when you create a security policy model.

Model editing

Sent when you edit the security policy model.

Policy model configuration

Manage zones, conduits, devices, and ranges.

Global Settings

Use **Global Settings** to define the settings applied to all devices contained in the model. Only administrators can edit **Global Settings**.

IMPORTANT: Rockwell Automation recommends configuring **Global Settings** before using the certificate authentication method.

Tip: Changes are saved when you select another field.

General

Property	Description
Model Name	The name of the policy model managed by this instance of FactoryTalk Policy Manager.

Certificate Settings

Property	Description
Organization	The name of your organization.
City/Location	The legally registered location of your organization.
State/Province	If applicable, the state or province where an organization is using the certificate.
Country	The country where an organization operates.

Device Authentication

Property	Description
Enable enhanced device authentication	Enabling enhanced device authentication involves the deployment of updates to all devices in the policy model. You can deploy the updates directly after enabling enhanced device authentication or do that later.
Display deployment warnings for devices that do not support enhanced device authentication	For more information about the supported devices, see Enhanced device authentication on page 36.
Skip or Continue the device policy deployment if a device cannot be authenticated	**Skip** If a device fails the enhanced device authentication check, the device policy deployment process continues. **Continue**

Property	Description
	If a device fails the enhanced device authentication check, policy deployment to that device continues and a warning appears.
Include DNS Information	Includes DNS information to the digital identity certificate of the device.

Port Settings

Table 45. DTLS settings

Property	Description
DTLS timeout	Enter a value between 1 and 3600 seconds. The default value is 12 seconds. If the device does not support the timeout functionality, a warning appears in **Device Properties**.

Table 46. CIP Bridging settings

Allow or restrict communication to and from the backplane of eligible devices in all zones of the security policy model. The CIP bridging settings affect secured EtherNet/IP interfaces and USB ports (if present). The selected option becomes default for all zones and devices.

Property	Description
Inbound CIP Bridging to the Backplane	**Allow all traffic** Allows bridging secure and trusted IP traffic from the EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). Allows bridging unsecure traffic from the USB port. **Tip:** Physical port support depends on the hardware platform. **Allow secure traffic** Allows bridging only secure traffic from the secured EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). Blocks bridging unsecure traffic from the USB port.

Table 46. CIP Bridging settings

Allow or restrict communication to and from the backplane of eligible devices in all zones of the security policy model. The CIP bridging settings affect secured EtherNet/IP interfaces and USB ports (if present). The selected option becomes default for all zones and devices.

(continued)

Property	Description
	Tip: Physical port support depends on the hardware platform. **Block all traffic** Blocks bridging any traffic from the secured EtherNet/IP interface and the USB port.
Outbound CIP Bridging from the Backplane	**Allow all traffic** Allows bridging all traffic to the Ethernet port and the USB port. **Block all traffic** Blocks bridging traffic to the Ethernet port and the USB port.

Automatic Policy Deployment

Tip:

Changes to the Automatic Policy Deployment settings take immediate effect. To avoid onboarding devices with unintended settings, you can edit the Automatic Policy Deployment settings:

- With the FactoryTalk System Services server disconnected from the network.
- When you do not expect any devices to be onboarded.

Property	Description
Enable automatic device discovery and onboarding	Enables Automatic Policy Deployment that: • Starts the Domain Name Server-Service Discovery (DNS-SD) services to enable device discovery and certificate provisioning. • Starts the Enrollment over Secure Transport (EST) system service, which responds to endpoint queries. • Merges the discovered devices with the matching devices in the policy model. • Adds the discovered devices to the Onboarding Area if the discovered device does not match any device in the policy model.

Property	Description
Enable automatic secured device replacement	Deploys the configuration of onboarded devices that match the devices in the policy model based on the specific criteria automatically. This feature requires the **Enable automatic device discovery and onboarding** checkbox selected.
Enable secure onboarding	During onboarding, discovered devices can receive different sets of temporary policies that determine their networking behavior until they are provisioned with final policies. Prevents the onboarding devices from establishing connections with any other device in the network except for FactoryTalk Policy Manager. This feature requires the **Enable automatic device discovery and onboarding** checkbox selected.

Security Eventing Settings

Table 47. Security Eventing Settings

Property	Description
Enable security eventing using Syslog server	Enables devices that support security eventing to start sending Syslog messages as configured in the policy. These settings apply to all devices that support security eventing.

Table 48. Syslog Server Settings

Use these settings to identify the location of the Syslog server.

Property	Description
IP Address	Identifies the Syslog server by the IP address.
Hostname	Identifies the Syslog server by the DNS host name.
Port	Identifies the communications port on the server to receive the Syslog messages. Default port number is 514.
Protocol	Configures logging. • Select **UDP** for low-priority logging. UDP is not a guaranteed reliability protocol, log data that is transferred using UDP can be lost in transit due to various network problems. • Select **TCP** for log data that cannot tolerate loss and which must be retained.

Table 49. Filter Settings

Use these settings to filter the event messages that are logged to the Syslog server.

Property	Description
Event types that will generate messages	Used to determine which event types generate messages. **Failures only** Logs events upon failures related to model deployment, device discovery, component connections, and component authentications or authentications. **Failures and successes** Logs all success and failure events related to model deployment, device discovery, component connections, and component authentications or authorizations.
Lowest level of severity to log	Logs messages that are greater than or equal to the severity level selected. Defined severity levels from highest to lowest are: **Emergency** System is unusable. **Alert** Action must be taken immediately. **Critical** Critical operational conditions such as device hardware major faults. **Error** Error conditions in software applications and device hardware minor faults. **Warning** Warning conditions in software applications and hardware. **Notice** Significant conditions that may require special handling. **Information** Informational messages about software or hardware operations. **Audit** Messages from the auditing service.

Table 49. Filter Settings

Use these settings to filter the event messages that are logged to the Syslog server.

(continued)

Property	Description
	Debug Messages about the programmatic operations of the software.

Table 50. Message Settings

Property	Description
Details to include in message	Specifies details included in the message. **Sequence ID** Uniquely identify the type and purpose of the message. **Time quality (sync info, time zone accuracy)** Describes the system time mechanism used by the message originator.
Time resolutions	Defines the level of precision used in the time stamp of the log messages: • **Seconds** • **Milliseconds** • **Microseconds** • **Nanoseconds**

Edit Global Settings

Edit Global Settings to change the policy model name, configure certificate and ports settings, and enable or disable features.

Prerequisites

- Log on to FactoryTalk Policy Manager as an administrator.
- Learn about the available settings. See Global Settings on page 58.

To Edit Global Settings

1. From the navigation bar, select **Global Settings**.
2. Edit fields.

Tip: Changes are saved when you select another field or exit **Global Settings**.

Zones

Zones form groups of logical or physical devices to which security settings are applied. Devices within a zone trust each other, except for OPC UA servers.

Add a zone

Add zones to establish areas of security policy. Devices assigned to a zone trust each other.

1. From the navigation bar, select either:
   - **Canvas** and then select **Create New > Zone**.
   - **Zones** and then select + next to **ZONES**.

   Tip: You can also select **Overview** and then select **Add** from the toolbar.

2. Make edits to **ZONE PROPERTIES**.

   For more information, see Zone properties on page 65.

Add devices to the zone. See Devices on page 72.

Duplicate a zone

Copy and paste a zone to duplicate the zone with its properties.

1. From the navigation bar, select either **Canvas** or **Zones**.

   Tip: In **ZONES**, select **Overview** to see all zones in a table.

2. Right-click a zone and select **Copy**.

   Tip: Changing between different views does not discard the copied item.

3. Right-click blank area and select **Paste**.

Add devices to the zone. See Devices on page 72.

Edit a zone

Edit the properties of a zone to specify a name, description, and enable security settings.

1. From the navigation bar, select either:
   - **Canvas** and then select a zone.
   - **Zones** and then, next to the zone, select ✎.

   Tip: You can also select **Overview** and then select a zone from the list.

2. Make edits to **ZONE PROPERTIES**.

   For more information, see Zone properties on page 65.

Add devices to the zone. See Devices on page 72.

Delete a zone

Deleting a zone **removes all devices, conduits, and endpoints** assigned to the zone.

Prerequisites

To retain the devices from the zone to delete, assign devices to different zones or unassign the devices from zones. If needed, recreate the conduits.

To delete a zone

1. From the navigation bar, select either **Canvas** or **Zones**.

   Tip: In **ZONES**, select **Overview** to see all zones in a table.

2. Right-click the zone to delete and select **Delete**.

   NOTE: To delete multiple zones, either:

   - In **ZONES**, hold **Ctrl**, select multiple zones, and then select 🗑**Delete** next to any selected zone.
   - In **Overview**, hold **Ctrl**, select multiple zones, and then select 🗑**Delete** from the toolbar.

3. Select **DELETE**.

The zone is no longer a part of the policy model.

Zone properties

Use zone properties to define the policy settings to apply to devices that are assigned to this zone.

General

The settings in this area differentiate this zone from other zones.

Property	Description
Name	The name for the zone.
Description	A description for the zone.

CIP Security

The settings in this area relate to how the devices in the zone communicate with other devices.

Table 51. CIP security settings

Property	Description
Enable CIP Security	Enable CIP Security options for the zone. When selected, additional configuration options are available. Non-CIP Security capable devices can be added to a zone with CIP Security enabled. These devices will have an information icon displayed stating **Incompatible with zone configuration**. These devices will not receive CIP Security policy themselves, but devices in this zone that are CIP Security capable will add the IP address of the non-CIP Security capable

Table 51. CIP security settings (continued)

Property	Description
	device to their Trusted IP list so that communication between the devices can occur.
Authentication Method	Select which method the devices use to authenticate. **Certificate** A digital certificate is an electronic representation of an identity. A certificate binds the identities public key to its identifiable information, such as name, organization, email, username, and/or a device serial number. This certificate is used to authenticate the connection to other devices. Selected by default when CIP Security is enabled. **Pre-shared Key** A pre-shared key is a secret that is shared among trusted entities. FactoryTalk Policy Manager can create a key that can be shared. To generate a pre-shared key, select **Auto-generate key**. To view the key, select **Show Key**. **Tip:** Once the authentication method is saved, you cannot show a pre-shared key. Non-CIP Security capable devices do not use any authentication method. If non-CIP Security capable devices are present in a zone, an information message displays `stating incompatible devices in zone` when **Certificate** or **Pre-shared Key** is selected.
I/O Data Security	Select the type of security check to perform on the input and output data. **Integrity Only** Checks whether data was altered and whether the data was sent by a trusted entity. Altered and/or untrusted data is rejected. Selected by default when CIP Security is enabled. **Integrity & Confidentiality**

Table 51. CIP security settings (continued)

Property	Description
	Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **Tip:** Rockwell Automation recommends choosing this option. **None** No I/O Data Security setting is selected. Even when no I/O security is configured, only devices within the zone or from a conduit are capable of I/O data communications. Other devices will be blocked. Non-CIP Security capable devices do not use any I/O Data Security method. If non-CIP Security capable devices are present in a zone, an information message displays stating `incompatible devices in zone` when **I/O Data Security** is selected.
Messaging Security	Select the type of security check to perform on messages received by devices in the zone. **Integrity Only** Checks whether data was altered and whether the data was sent by a trusted entity. Rejects altered and/or untrusted data. Selected by default when CIP Security is enabled. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data . Non-CIP Security capable devices do not use any Messaging Security and cannot provide data integrity checking. If non-CIP Security capable devices are present in a zone, an information message displays stating `incompatible devices in zone` when **Messaging Security** is selected.
DIsable port HTTP (80)	Select to disable communication over port 80.

Table 52. CIP Bridging settings

This functionality applies only to zones with CIP Security enabled. The available options may be restricted by Global Settings.

Property	Description
Inbound CIP Bridging to the backplane	**Allow all traffic** Allows bridging of secure and trusted IP traffic from the EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). Allows bridging of unsecure traffic from the USB port. **Tip:** Physical ports support is dependent on the hardware platform. **Allow secure traffic** Allows bridging of only secure traffic from the secured EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). Blocks bridging of unsecure traffic from the USB port. **Tip:** Physical ports support is dependent on the hardware platform. **Block all traffic** Blocks bridging of any traffic from the secured EtherNet/IP interface.
Outbound CIP Bridging from the backplane	**Allow all traffic** Allows bridging of all traffic to the EtherNet/IP interface and the USB port. **Block all traffic** Blocks bridging of any traffic to the EtherNet/IP port and the USB port.

OPC UA

Zones and conduits follow these non-editable OPC UA security policy settings:

- OPC UA clients trust OPC UA servers
- OPC UA servers do not trust OPC UA servers
- OPC UA clients do not trust OPC UA clients

Conduits

Conduits are communication pathways in the policy model, connecting pairs of policy model components.

You can create conduits between these components:

Table 53. CIP conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	Device
Zone	Range
Device	Device
Device	Range

Table 54. OPC UA conduits

Endpoint 1	Endpoint 2
Zone	Zone
Zone	OPC UA server
Zone	OPC UA client
Zone	Range
OPC UA client	OPC UA server

Conduits must follow these rules:

- Conduits cannot be duplicated, each combination of endpoints must be unique.
- One of the endpoints must be CIP Security or OPC UA security policy capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.
- Devices not assigned to any zone or onboarding devices cannot be used as endpoints.

Add a conduit

Add a conduit to connect two endpoints. An endpoint can be either a device or a zone.

1. From the navigation bar, either:
   - Select **Canvas** and then select **Create New > Conduit** from the toolbar.

     > **Tip:** You can also right-click a zone, device, or range and then select **Add Conduit**.

   - Select **Conduits** and then select **Add** from the toolbar.
2. In **CONDUIT PROPERTIES**, under **Endpoint 1**, select ....

3. Select a zone or device to assign as the first endpoint of the conduit and select **OK**.

> **Tip:** Use **Filter** to find endpoints.

4. Under **Endpoint 2**, select ... .
5. Select a zone or device to assign as the second endpoint of the conduit and select **OK**.
6. Select **Next**.
7. Make changes in **CONDUIT PROPERTIES**.

   For more information, see Conduit properties on page 70.

Edit a conduit

Conduits allow trusted communication outside of zones. Conduits require two endpoints.

1. From the navigation bar, select either **Canvas** or **Conduits**.
2. Select the conduit to edit.
3. Make changes in **CONDUIT PROPERTIES**.

   For more information, see Conduit properties on page 70.

Delete a conduit

Delete a conduit to remove a connection between two endpoints.

1. From the navigation bar, select **Conduits**.
2. Right-click the conduit to delete and select **Delete**.

> **NOTE:** To delete multiple conduits, hold **Ctrl**, select multiple conduits, and then select 🗑**Delete** from the toolbar.

3. Select **DELETE**.

The conduit is no longer part of the policy model.

Conduit properties

Use conduit properties to define the endpoints and security settings to apply to communications over this conduit. Endpoints are either a zone, a device, or a port of a device.

Each conduit must be a unique combination of endpoints.

General

Property	Description
Name	Type a name for the conduit.
Description	Type a description for the conduit.

Connection

Property	Description
Endpoint 1	The first endpoint of the conduit. The list is composed of the zones and devices that are identified in FactoryTalk Policy Manager.
Endpoint 2	The second endpoint of the conduit.

CIP Security Communication

Property	Description
Authentication Method	Determines how the conduit verifies the identity of the assigned devices and/or zones. **Trusted IP** Devices and zones are trusted for communications based on their IP address. No additional security checks are performed. **Certificate** Devices and zones are trusted by presenting a certificate that establishes their identity. With this setting selected, configure the **I/O Data Security** and **Messaging Security** settings. **Tip:** If an endpoint is a zone and the conduit uses certificate authentication, devices in that zone that do not support CIP Security will not use the certificate for communication. The CIP Security capable devices will trust the non-CIP Security devices using Trusted IP.
I/O Data Security	Determines the type of security check performed on the input and output data. **Integrity Only** This option checks if the data was altered. If detected, rejects altered data. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **None**

Property	Description
	With this option, no security checks are performed on input and output data. This setting is available when you choose **Certificate** as the **Authentication Method**.
Messaging Security	Determines the type of security check performed on messages received by assets in the zone. **Integrity Only** This option checks if the data in the message was altered. If detected, rejects altered data **Integrity & Confidentiality** This option checks if the data in the message was altered and that the message was sent by a trusted entity. Rejects the data if it was altered or if it originated from an untrusted entity. This setting is available when you choose **Certificate** as the **Authentication Method**.

Devices

Devices are the modules, drives, controllers, HMI panels, computers, CIP Proxy devices, OPC UA servers, and OPC UA clients that work together to create a FactoryTalk system.

Tip: Add devices that share security requirements and that should trust each other to a zone. A device can have one or more ports that are added to the policy model. Connect devices to other devices or zones with conduits.

Discovery

Use **Discovery** to find devices in networks, add drivers, and bridge networks.

Show or hide the Discovery pane

Use **Discovery** to traverse the FactoryTalk Linx network tree and find devices.

In the right toolbar, select **Discovery**.

Add discovered devices

Add the discovered devices the device list and assign them to zones.

Tip: Discovery can show multiple child devices under one CIP Proxy device when a security policy is not yet deployed to the CIP Proxy device. After security policy deployment, **Discovery** shows only the proxied device as a child.

To add a device manually, see Add a device on page 76.

Prerequisites

Enable automatic device discovery. See Configure automatic device discovery on page 76.

To add discovered devices

1. From the navigation bar, either:
    - Select **Canvas** and then select a zone or **Unassigned** to contain the device.
    - Select **Zones** and then select a zone to contain the device.
    - Select **Devices** to contain the device in the devices list not assigned to any zones.
2. In **Discovery**, select either **CIP** or **OPC UA**.
3. (optional, CIP only) Enable or disable CIP Security indicators by selecting ✓ **Show CIP Security Indicators** from the toolbar.

    For more information, see Discovery pane on page 25.
4. (optional) Filter the list of discovered devices.

    For more information, see Search discovered devices on page 73.
5. Either:
    - In **Discovery**, select a device or multiple devices and then select +.
    - In **Discovery**, right-click a device and select **+ Add**.
    - Drag a device from **Discovery** to the table in **Zones** or **Devices**.
    - Drag a device from **Discovery** to a zone or **Unassigned** in **Canvas**.

The selected discovered devices are added to the zone or unassigned devices list.

Search discovered devices

Use **Discovery** to search for a device to determine its location. After the initial discovery of the network topology, you can use filters to limit the scope of the search.

When using search, take a note of these functional details:

- Search only examines devices detected or viewed by the browser. Initiating a search will not cause the browser to discover a new device.
- Search queries can contain alphanumeric characters, full words, compound expressions, fragments of a word, or a single letter or number.
- Search includes predefined search criteria to filter search results by device, name, path, and IP address.
- Enclose search queries in quotation marks to find exact matches.

- Use operators in the search query to refine the search results using a logical statement.
  - AND to search for two or more keywords.
  - OR to search for several keywords.

> **Tip:** An example of using operators between keywords to refine search results is: `Device: 1756-L OR Device: 1768-L`
>
> This search locates both ControlLogix and CompactLogix controllers.

- Clear the search query to return to the network topology tree view.

To search discovered devices

1. In **Discovery**, select either **CIP** or **OPC UA**.
2. (CIP only) From the **Discovery** toolbar, select 🔍 **Search**.
3. In **Search** or **Filter**, enter a query.
4. (optional, CIP only) Select a search filter by selecting ▼ to narrow the search results to:

   Device

   The name of the device. For example, `1756-L`

   Address

   The IP address or a portion of the IP address of the device: For example, `10.122.155`

   OnlineName

   The online name of the device. For example, `Packaging line`

   Location

   The communications path used for the device: For example, `AB-Eth`

Discovery displays results within a few seconds, regardless of pressing **Enter**.

Configure a driver

A driver is the software interface to the computer or workstation hardware that allows the computer to communicate with a network to detect and communicate with a control system device.

1. In **Discovery**, on the **CIP** tab, select 🔌 **Configure Drivers**.
2. In **Configure Drivers**:
   - To configure a new driver, under **Available Driver Types**, select a driver, and select **Add New**.
   - To edit a configured driver, next to the driver name, select ⚙ **Settings**.
3. (optional) On the **General** tab, assign a name for the device.
4. Under **Discovery Method**, select either:
   - **Device List/Range**. A discovery message is sent to each specified individual IP address. The list can identify target devices using the device name, IP address, or IP address range.
   - **Broadcast**. A broadcast UDP message is sent to all devices on the network at once.
5. In **Interface** select the physical port of the computer.
6. (optional) To listen on port 44818 and update **Discovery** in response to network browse requests, select **Listen on Ethernet/IP encapsulation ports**.

Tip: Selecting **Listen on Ethernet/IP encapsulation ports** shows your computer in the network tree.

7. Select **Tuning** and configure the tuning settings to change how fast items on the network are discovered.
   - **Device discovery poll rate (msec)**. Defines how often (in milliseconds) the Discovery pane requests data from a device. For example, a poll rate of 1000 ms results in data being requested every second. This setting is inactive when the driver uses broadcast discovery.

     Tip: When a driver makes a discovery request to a device, it waits for the amount of time specified by the Device discovery poll rate before making a request to a new device. Setting this rate to a higher value slows down the rate that devices appear in the browser tree, and reduces the number of messages sent on the network.

   - **Offline device discovery poll rate**. Defines how often (in milliseconds) the Discovery pane waits to try to establish communication with an offline device. For example, a poll rate of 10,000 results in a 10-second delay before additional requests are sent to a device that was offline. This setting is inactive when the driver uses broadcast discovery.

     Tip: Setting this rate to a higher value slows down the rate that a newly attached device appears in the browser tree, and reduces the number of messages sent on the network.

   - **Poll interval between discovery cycles (msec)**. The number of milliseconds that occur between each query of the network by the **Discovery** pane.

     Tip: After a driver polls the network branch, it waits the amount of time specified by the Poll Interval between discovery cycles before starting another discovery cycle. Setting the Poll interval between discovery cycles to a higher value reduces the number of network messages sent.

   - **Poll timeout (msec)**. Specifies the amount of time (in milliseconds) to wait for a device to respond to a request.
   - **Maximum concurrent packets to this network**. Used to configure the maximum number of requests that can be waiting for a response on this network at any given time as part of the discovery process.
8. (optional) Select **Auto remove offline devices** to hide offline devices from **Discovery**.
9. Select **OK**.
10. Select **Close**.

Delete a driver

Delete drivers that you no longer need.

1. In **Discovery**, on the **CIP** tab, select **Configure Drivers**.
2. Next to the configured driver to delete, select **Delete**.
3. Select **DELETE**.

4. Select **OK**.
5. Select **Close**.

Bridge networks

Bridge networks to create conduits between networks.

1. From **Discovery**, on the **CIP** tab, select ⚙ **Settings**.
2. On the **Bridged** tab, select **+ Add New**.
3. In **Name**, enter a name for the bridge.
4. Next to **Selected Target Bridge Network**, select **Browse**.
5. Either:
   - To create a bridge path, in **Bridge Path Selection**, select the network to connect the current network and then select **OK**.
   - To add an existing bridge path from another bridge, select **Copy Setting From** and select a configuration.
6. Select **OK**.

Configure automatic device discovery

Enable or disable the automatic discovery of CIP or OPC UA devices in the **Discovery** pane.

- To enable the automatic discovery of CIP devices:
  1. In **Discovery**, select **CIP**.
  2. Select ⟳ **Auto browse** to enable or disable the automatic discovery of CIP devices.
- To enable the automatic discovery of OPC UA devices:
  1. In **Discovery**, select **OPC UA**.
  2. Select ⟳ **Auto browse** to enable or disable the automatic discovery of OPC UA devices.

Add a device

Manually add a device to a zone or to the devices list.

Tip: To add a discovered device, see Add discovered devices on page 72.

1. From the navigation bar, either:
   - Select **Canvas** and then select a zone or **Unassigned** to contain the device.
   - Select **Zones** and then select a zone to contain the device.
   - Select **Devices** to contain the device in the devices list not assigned to any zones.
2. Either:
   - In **Canvas**, from the navigation bar, select **Create New > Device**.

     Tip: You can also right-click a zone or **Unassigned** and then select **Add Device**.

   - In **Zones** or **Devices**, from the navigation bar, select **Add Device**.
3. Select the device type and then select **OK**.
4. In **PROPERTIES**, edit the device properties and ports properties.

   For more information, see Device properties on page 80 and Ports on page 83.

Duplicate a device

Copy and paste a device to duplicate the device with its properties.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone.
   - Select **Devices**.
2. Right-click a device and select **Copy**.
3. Right-click blank space and select **Paste**.

Tip: You can paste the device to the same zone, a different zone, or to the list of unassigned devices. Switching between **Canvas**, **Zones**, and **Devices** does not discard the copied device.

Edit a device

Edit the device properties to change the device information, security options, or zone assignment.

Tip: You can edit the zone assignment of a device by dragging and dropping the device in **Canvas**. See Move a device on page 77.

1. From the navigation bar, either:
   - Select **Canvas** and then select a device.
   - Select **Zones** and then select a zone and a device.
   - Select **Devices** and then select a device.
2. In **PROPERTIES**, edit the device properties and ports properties.

   For more information, see Device properties on page 80 and Ports on page 83.

Deploy the policy model to apply the changes.

Move a device

You can move devices in the **Canvas** policy model visualization and in the **Graphical Explorer** tree.

Tip: You can also move a device by editing the device properties. See Edit a device on page 77.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone.
   - Select **Devices**.
2. Right-click a device and select **Cut**.
3. Right-click the blank space and select **Paste**.

Tip: You can paste the device to a different zone or to the list of unassigned devices. Switching between **Canvas**, **Zones**, and **Devices** does not discard the copied device. In **Canvas**, you can drag devices between containers. You can also drop devices from the **Graphical Explorer** tree to the **Canvas** policy model visualization or in the opposite way.

IMPORTANT: In **Canvas**, when you move a device from the **Onboarding Area** to a **Zone** or to the **Unassigned** container, the device cannot be moved to the **Onboarding Area** container again.

The device is moved to another zone. The OPC UA client and OPC UA server pair moves together.

Replace a device

Replace a device if a device that was configured has failed or must be rotated out for maintenance.

Tip: Device replacement enables the identity and the security configuration of the previous device to be assigned to the replacement device.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone.
   - Select **Devices**.
2. Right-click the device to replace and select **Replace Device**.

   Tip: In **Zones** or **Devices**, you can also select the device to replace and then select **Replace Device** from the toolbar.

3. In **Deploy Configuration to Replace Device** select when to reset the communication ports on the device:
   - To reset the ports automatically as part of the replacement process, select **During policy deployment**.
   - To reset the ports manually at a later time, select **After deployment**. The security policy is not being enforced on the device until the ports are reset.
4. Deploy the policy model to apply the security policies to the replaced device.

   For more information, see Policy model validation and deployment on page 91.

Remove the security policy from a device

If you deployed the policy model and the device communications were reset, the device is constrained by the security policy.

IMPORTANT: Even if you uninstall FactoryTalk Policy Manager and FactoryTalk System Services, the security policy configured for the device is still in effect.

1. From the navigation bar, either:
   - Select **Canvas** and then select a device.
   - Select **Zones** and then select a zone and a device.
   - Select **Devices** and then select a device.
2. Unassign the device from a secure zone or delete the device:
   - In **Properties**, on the **Port** tabs, in **Zone**, choose either **Unassigned** or a zone that is not CIP Security or OPC UA security policy enabled.
   - Right-click the device and select **Delete**. Select **DELETE** in the confirmation dialog.
3. Deploy the policy model and select to reset the communications channels during deployment.

   For more information, see Policy model validation and deployment on page 91.

The device security configuration is reset to none.

Remove the device from the model or reconfigure the device.

Tip: You can remove the security policy from the device by deleting the device from the security policy model. The changes take place during the next deployment.

Delete a device

Delete a not deployed device or a deployed device and its security configuration.

IMPORTANT: If a device has multiple ports, the additional ports must be deleted to delete the device. Such devices are shown in the device table with the port name appended after the device name; for example, `Device3:Port2`

If you delete a device from the proxy-proxied pair, both devices are deleted. The deleted device remains in the **Device** table until the next time the model is deployed. The properties of deleted devices are read-only.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone.
   - Select **Devices**.
2. Right-click the device to delete and select **Delete**.

   NOTE: To delete multiple devices, in **Zones** or **Devices**, hold **Ctrl**, select multiple devices, and then select 🗑**Delete** from the toolbar.
3. Select **DELETE**.
4. (deployed devices only) Deploy the policy model to clear the security policies from the deleted the device.

   For more information, see Policy model validation and deployment on page 91.

The device name and properties are struck-through. You cannot edit or assign deleted devices to the policy model.

To remove the device from the policy model and clear the device configuration, deploy the policy model. See Deploy a policy model on page 91.

Device properties

Use device properties to define the device information, security, and network settings for a device.

Device properties defined using the electronic data sheet (EDS) for the device cannot be modified. A device can have one or more ports that are added to the policy model.

Some of the following properties may be read-only for:

- The devices added to the Onboarding Area by Automatic Policy Deployment.
- The devices that are not added to a secure zone.

Device

Table 55. General

The settings that provide the identification parameters of the device.

Property	Description
Device Name	The name of the device. The name is required and must be unique. Generic devices are automatically named `Device <number>`. Devices selected by catalog number or discovered are already named.
Description	An optional description for the device. The description of generic devices is empty by default. Devices selected by catalog number or discovered may have an existing description.
Catalog number	If defined using device discovery, the catalog number cannot be changed. Otherwise, choose a catalog number from the list. Choosing a Rockwell Automation catalog number automatically completes the Vendor information. A device without a catalog number is listed as a **Generic Device**.
Vendor	The name of the device's vendor. If a Rockwell Automation/Allen-Bradley catalog number was provided, this setting is completed by default and cannot be modified.
Firmware Revision	The firmware revision number of a device. Required to enable CIP Security for a device. This setting is required to apply CIP Security settings to the device ports. FactoryTalk Policy Manager automatically assigns

Table 55. General

The settings that provide the identification parameters of the device.

(continued)

Property	Description
	the latest firmware revision to devices added using a catalog number or using **Discovery**.
CIP Security capable	Identifies whether a device can use the security settings of the zone. Select to configure additional CIP Security settings for a generic device. The Catalog Number and firmware revision determine the CIP Security capability of a device automatically.

Table 56. USB

Property	Description
Disable CIP Bridging through USB	When selected, it disables inbound and outbound CIP Bridging through the USB port. When cleared, it enables inbound traffic through the USB port. Outbound traffic is enabled if the device supports it. This setting is only available for the devices with the **Capable** property enabled. The available options may be restricted by Global Settings.

Table 57. Ports

These settings identify the ports available on the device.

Property	Description
Port name and number	The name and number of ports available on the device. Select ✎ next to the port number to configure port properties, such as the port name, description, EtherNet driver, IP address, and protocols used by the device. For more information, see Port properties on page 85.

Tip: For generic devices, you can manually add ports as needed by selecting **+** next to **Ports**.

For CompactLogix 5380 Controllers and Compact GuardLogix 5380 Controllers that operate in dual mode, you cannot add **Port 2**.

UA Client

Table 58. Client configuration

Item	Description
Name	OPC UA client name. **Tip:** The default **UA Client** tab title changes if you change the OPC UA client name.
IP Address	IP address of the OPC UA client.

Table 59. Policies

Item	Description
Zone	The zone that the OPC UA client is assigned to.

Table 60. Client certification

Item	Description
Export	Exports the OPC UA client certificate.
Import	Imports the OPC UA client certificate.

Item	Description
Sharing identity with the server	OPC UA client shares its identity with the OPC UA server identity. The identity includes the PKI certificate, username, and password.

UA Server

Table 61. Server configuration

Item	Description
Name	OPC UA server name. **Tip:** The default **UA Server** tab title changes if you change the OPC UA server name.
Server URI	Non-editable OPC UA server URI based on the OPC UA server certificate.
Server URL	The URL of the OPC UA server endpoint.
Endpoint	List of endpoints with the Sign & Encrypt security policy mode or stricter. For more information, see OPC UA security policy on page 51. Select **Refresh** to refresh the list.
Endpoint Encryption to use for Deployment	Encryption algorithm for the OPC UA server endpoint to use for deployment.

Table 61. Server configuration (continued)

Item	Description
	None Use no encryption for server endpoint deployment. **Aes256** Use the Aes256-Sha256-RsaPss encryption algorithm for server endpoint deployment. **Tip:** The encryption algorithm may change if you specify a different endpoint in **Server URL**.

Table 62. Policies

Item	Description
Zone	The zone that the OPC UA server is assigned to.

Table 63. Server Credentials

Item	Description
Anonymous	Log on as an anonymous user to the OPC UA server.
Username	The user name to log on to the OPC UA server.
Password	The password to log on to the OPC UA server.
Show Password	Shows the password.

Table 64. Server Certification

Item	Description
Import	Imports the OPC UA server certificate.
Verify	Verifies connection to the OPC UA server.
Sharing identity with the client	OPC UA server shares its identity with the OPC UA client identity. The identity includes the PKI certificate, username, and password.

Ports

A port represents a physical socket of a device that allows communication with another device.

Tip: FactoryTalk Linx Devices, CIP Proxy devices, and Rockwell Automation devices that are identified by catalog number have only a single port. CIP Proxy devices and proxied devices have an additional section in **PORT PROPERTIES** indicating the paired device.

Add ports to Generic Devices to add them to the security policy model.

Add a port

Add ports to generic devices to match the device configuration.

Tip: By default, each new generic device has a single unconfigured port. Use this procedure to add more ports.

1. From the navigation bar, either:
   - Select **Canvas** and then select a device.
   - Select **Zones** and then select a zone and a device.
   - Select **Devices** and then select a device.
2. In **PROPERTIES**, next to **Ports**, select **+**.
3. In **PROPERTIES**, select the tab associated with the port to configure and edit the port properties.

   For more information, see Port properties on page 85.

Edit a port

Devices have ports that are associated with IP addresses, ports, and protocols. Devices that have a specific catalog number have a predefined number of ports with assigned protocols.

Tip: If a device does not have a catalog number, FactoryTalk Policy Manager adds it as a **Generic Device**. When a security policy model includes generic devices, configure the number of ports on the device.

1. From the navigation bar, either:
   - Select **Canvas** and then select a device.
   - Select **Zones** and then select a zone and a device.
   - Select **Devices** and then select a device.
2. In **PROPERTIES**, select the tab associated with the port to configure and edit the port properties.

   For more information, see Port properties on page 85.

Delete a port

Delete not needed ports from devices.

Prerequisites

Confirm that the device has more than one port configured.

1. From the navigation bar, either:
   - Select **Canvas** and then select a device.
   - Select **Zones** and then select a zone and a device.
   - Select **Devices** and then select a device.
2. In **Properties**, under **Ports**, next to the port to delete, select 🗑**Delete**.
3. Select **DELETE**.

Port properties

Devices have logical ports that are associated with IP addresses, ports, and protocols.

Some of the following properties may be read-only for:

- The devices added to the Onboarding Area by Automatic Policy Deployment.
- The devices that are not added to a secure zone.

Device

This area displays information about the device on which the port is present.

Property	Description
Device name	The name of the device. Select ✎ next to the device name to open the device properties.
Device description	Read-only information that describes the device function.
Device catalog number	Read-only information that provides the catalog number of the device.

For more information, see Device properties on page 80.

General

Use this area to configure the port on the device.

Property	Description
Port Name	The name of the port.
Description	The optional description for the port.
EtherNet Driver name	A dropdown list of the available EtherNet drivers used for communication. This property is only available for the devices that support CIP Security. The default name is `Ethernet`. If the list does not contain a driver, add the driver with FactoryTalk® Linx™.
IP Address	The IP address of the Ethernet port, for example: `10.88.11.11`

Property	Description
	You cannot edit the IP address if you: • Deployed the security policy to the device. • Moved a device from the Onboarding Area to the policy model. If the **Clear configuration for previous IP Address** dialog appears, either: • Select **CLEAR CONFIGURATION** if the previous IP address is assigned to a different device. The IP address and the device name are shown grayed-out and struck through in the **Devices** table These devices are removed from the policy model at the next deployment. • Select **DON'T CLEAR CONFIGURATION** if the previous IP address is not in use. **IMPORTANT:** Changing the IP Address of a CIP Security Capable device in a CIP Security enabled zone after deployment requires that the security configuration be cleared for the previous address if that IP address is in use.
Port Proxied	Appears only for proxy devices. Shows the name and the IP address of the device secured by this proxy device. Select the pencil icon ✏ next to the device name to open the port properties.
Proxy Device	Appears only for proxied devices. Shows the name and the IP address of the device securing this proxy device. Select the pencil icon ✏ next to the device name to open the device properties.

Policies

Use this area to select the security zone and communication settings for the port.

Table 65. Properties

Property	Description
Zone	The name of the zone to which the port is assigned. If Automatic Policy Deployment is enabled, the Onboarding Area displays in the list of zones.
Disable port HTTP (80)	For CIP Security capable devices only. When a device is CIP Security capable and placed in a zone using the certificate authentication method, the HTTP Port usage can be disabled.

Table 65. Properties (continued)

Property	Description
	When viewing the device list, the Disabled TCP Port column reflects whether HTTP port 80 has been disabled.

Table 66. CIP Bridging properties

This functionality applies only to CIP Security capable devices.

Property	Description
Model Name	The name of the policy model managed by this instance of FactoryTalk Policy Manager.
Inbound CIP Bridging	**Allow all traffic** Allows bridging of secure and trusted IP traffic from the EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). **Tip:** Physical ports support is dependent on the hardware platform. **Allow secure traffic** Allows bridging of only secure traffic from the secured EtherNet/IP interface to backplane and other physical ports (for example: Ethernet, USB). **Tip:** Physical ports support is dependent on the hardware platform. **Block all traffic** Blocks bridging of any traffic from the secured EtherNet/IP interface.
Outbound CIP Bridging	**Chassis size** Displays the number of slots in a chassis. The default number of slots for manually added devices is 10. Change this value to reflect the chassis capacity. Slot **1 - 10**

Table 66. CIP Bridging properties

This functionality applies only to CIP Security capable devices.

(continued)

Property	Description
	Select chassis slots for which to disable CIP Bridging.

Ranges

Configure trusted IP ranges to incorporate groups of devices not capable of CIP Security or OPC UA security policy into the policy model.

Tip: A trusted IP range is a contiguous set of IP addresses that are known to contain good devices, but that cannot use certificates or pre-shared keys to authenticate identities or authorize access. If a device has an IP address within a defined trusted IP range, the authentication method for the device is set to **None**.

Add a range

Configure a trusted range of IP addresses that are known to contain good devices.

1. From the navigation bar, select either:
   - **Canvas** and then select **Unassigned** or a zone to contain the range.
   - **Zones** and then select a zone to contain the range.
   - **Devices** to add a range unassigned to any zone.
2. Select either:
   - In **Canvas**, from the toolbar, select **Create New > Range**.
   - In **Zones** or **Devices**, from the toolbar, select **Add Range**.
3. Make changes in **RANGE PROPERTIES**.

   For more information, see Range properties on page 89.

Edit a range

Edit the properties of a trusted IP addresses range.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone that contains the range.
   - Select **Devices**.
2. Select the range to edit.
3. Make changes in **RANGE PROPERTIES**.

   For more information, see Range properties on page 89.

Move a range

Move a range to a different zone.

Tip: You can also move a device by editing the device properties. See Edit a range on page 88.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone that contains the range.
   - Select **Devices**.
2. Right-click a range and select **Cut**.
3. Right-click blank space and select **Paste**.

Tip: You can paste the range to a different zone or to the list of unassigned devices. Switching between **Canvas**, **Zones**, and **Devices** does not discard the copied device.

In **Canvas**, you can drag devices between containers. You can also drop ranges from the **Graphical Explorer** tree to the **Canvas** policy model visualization or in the opposite way.

IMPORTANT: In **Canvas**, when you move a range from the **Onboarding Area** to a **Zone** or to the **Unassigned** container, the device cannot be moved to the **Onboarding Area** container again.

Delete a range

Delete a range of trusted IP addresses that you no longer need.

1. From the navigation bar, either:
   - Select **Canvas**.
   - Select **Zones** and then select a zone that contains the range.
   - Select **Devices**.
2. Right-click the range to delete and select **Delete**.

NOTE: To delete multiple ranges, hold **Ctrl**, select multiple ranges, and then select 🗑**Delete** from the toolbar.

3. Select **DELETE**.

The range is deleted and is no longer a part of the policy model.

Range properties

Use range properties to define pools of IP addresses that can be used to permit unsecure communication within the policy model.

IMPORTANT: Add IP addresses only for devices that are intended to originate connections. Limit the usage of this method as it deteriorates the level of security of the system.

Table 67. Properties

Property	Description
Name	The name of the range. The name is required and must be unique.
Description	An optional description for the range.
Start IP Address	The first IP address of the range.
End IP Address	The last IP address of the range
Zone	The security zone to which the range is assigned. **Tip:** If you add a range from within the **Zone** list, the range is automatically assigned to the currently selected zone.

Policy model validation and deployment

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

Changing the security policy of an item requires resetting the communications channel which results in a short loss of connectivity. During deployment, there is an option of resetting the communication as part of deployment, or deploying the changes without resetting the communication channel so that the reset can occur at a different time than the deployment process.

If changes are made to the policy after it is deployed, an asterisk `(*)` will appear next to the device, indicating that the configured policy has not been deployed to that device.

After the initial deployment, a differential deployment can be done to deploy just items changed since the last deployment. Differential deployment includes any changes made in the model or made to the physical device in the field such as in the event of device replacement.

Reload a policy model

Reloading the model synchronizes FactoryTalk Policy Manager and FactoryTalk System Services and refreshes the display of possible conflicts so that you can address them before deployment.

From the FactoryTalk Policy Manager toolbar, select **Reload**.

FactoryTalk Policy Manager refreshes the display with the most recent information from FactoryTalk System Services.

Validate a policy model

Validate a policy model to confirm that all devices are operational and have network access.

1. From the toolbar, select **Validate** and then select either:
   - **CIP protocol** to validate connections between CIP Security system components.
   - **OPC UA protocol** to validate connections between OPC UA system components.

   Tip: You can stop the validation process at any time by pressing **STOP VALIDATION** in the status bar.

   Results displays any potential warnings or errors.
2. (optional) Save the validation results by selecting 💾 **Save**.

Deploy a policy model

Deploy the security policy model to apply zones, conduits, and devices configurations.

Prerequisites

Confirm that all devices are operational and have network access. See Validate a policy model on page 91.

To deploy a policy model

1. From the FactoryTalk Policy Manager toolbar, select **Deploy** and then select either:
   - **CIP Security** to deploy policy model configuration to CIP Security system components.
   - **OPC UA Security** to deploy policy model configuration to OPC UA system components.

2. In **Scope of Deployment**, select either:
   - **Changed device communication ports only**. Differential deployment. Use to deploy the security configuration to devices that have been changed since the last deployment. This type of deployment includes any changes made in the model configuration or changes made to the physical device, such as when a device is replaced for maintenance.
   - **All device communication ports in the model**. Full deployment.

   The list of devices identifies the devices that will be configured when this model is deployed.

   Tip: Scroll down or select **More details** to review the list. The list may contain devices that you have not modified directly. This can happen modification of one device impacted a related device. If the list contains unexpected devices, select **CANCEL** and then change the model as needed.

3. (optional) To retain the devices marked to be deleted from the model in case of a communication failure, select **Retain deleted devices and ports in policy model after failed deployments**.

   Tip: If the **Retain deleted devices and ports in policy model after failed deployments** checkbox is cleared and a device cannot be removed from the security model, the device will not be visible in FactoryTalk Policy Manager and the device configuration will not be reset.

4. Choose when to reset the communication channels for the items includes in the security policy model. Select either:
   - **Reset existing connections**. The communication port closes and reopens on the device during the deployment process. Similar to resetting the network card on a computer, the device stays functional but is disconnected from the network for a few moments. Using this option applies the new policy to the device at the same time that the policy is deployed.
   - (CIP only) **Do not reset existing connections**. The security policy settings will be deployed to the device but are not in effect. The communications ports must be reset before the security policy is used. This option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function. Connections with 1783 CIP Security® Proxy always reset during the policy model deployment.

     Tip: If you choose to reset the communication after deployment, the security policy may be applied to the devices at different times, depending on the device type, function and state of the control system.

5. Select either:
   - **Validate and deploy**. To validate the connections between system components and then deploy the policy model.
   - **Skip validation and deploy**. To deploy the policy model.

   Results updates with the results of the deployment as it occurs.

You can stop the deployment process at any point. If you stop the deployment process, the configured assets remain configured. Stopping the deployment process does not roll back the changes that have occurred.

IMPORTANT: If you stop the deployment process during deploy, this can leave the system in an unexpected state. Communications between devices could be permanently interrupted requiring module reset.

- Once the deployment is complete, a summary report lists the successes, failures, and errors encountered during the process.

Tip: Select **Save** to export the results to a file for archival purposes.

The possible deployment results are:

Configuration complete

No issues identified.

Configuration complete

Warnings identified. See Deployment results on page 93.

Configuration not complete

Error identified. See Deployment results on page 93.

- If changes are made the policy after it is deployed, an asterisk `(*)` appears next to the device, indicating that the configured policy has not been deployed to that device.
- Once the model is deployed and communications reset on the device, the device will only accept communications from other devices in the same zone or using conduits configured to enable communications with other security zones or devices. The device can still send communication to other devices.

Deployment results

The tables provide a reference of the possible errors encountered during deployment. Items in brackets are placeholders for specific items that are identified as appropriate for the environment.

Tip: Third-party devices may not support all security capabilities and features of FactoryTalk Policy Manager. Depending on the device specifications, you may have to adjust your security policy model.

Deployment errors

Error	Description
Cannot read the state of the CIP Security Object for *<device name> <endpoint name>*.	The system cannot obtain information if the device is CIP Security capable.
Unable to retrieve the list of administered ports for *<device name> <endpoint name>*.	The system cannot obtain information on device ports. The device may not support ports or CIP Security.

Error	Description
<*device name*> does not support configuration for the port.	The device is in a zone that has disabled communication over the specified port. The device does not support individual port configuration. Make sure that the device is CIP Security capable.
Cannot obtain the list of available encryption methods for <*device name*> <*endpoint name*>.	The system cannot determine if the device supports any encryption methods. Check the device specifications.
Unable to retrieve the list of supported encryption methods for <*endpoint name*>.	The system cannot retrieve information on which encryption methods supported by the device. Check the device specifications.
Unable to set encryption method for <*endpoint name*>.	The system cannot set which encryption method is used by the device. Update the device firmware.
Unable to retrieve the pre-shared key from <*endpoint name*>.	The device does not support pre-shared key authentication, the device lost data, or the device replacement procedure was not followed. Go to the specified zone, generate a new pre-shared key and redeploy the security policy model.
Unable to set the pre-shared key from <*endpoint name*>.	The device does not support pre-shared key authentication, the device lost data, or the device replacement procedure was not followed. Go to the specified zone, generate a new pre-shared key and redeploy the security policy model.
Unable to clear the pre-shared key from <*endpoint name*>.	The previously assigned pre-shared key could not be removed from the device.
Unable to retrieve the active certificate from <*endpoint name*>.	The system cannot connect to the Certificate Management Objects on the device.
Unable to assign a certificate to <*endpoint name*>.	The system could not switch from the default certificate to a new certificate on the device.
Unable to create Certificate Management Objects for <*endpoint name*>.	The system could not create a certificate for the device. The device may have insufficient space. Review the security policy model and check if the number of conduits to the device does not exceed the capacity of the device. Contact the device's manufacturer.
Unable to retrieve the certificate attributes for <*endpoint name*>.	The system could not retrieve the certificate from the device.
Device certificate is invalid or unverified for <*endpoint name*>.	The device is unable to verify its certificate.
CA certificate is invalid or unverified for <*endpoint name*>.	The device is unable to verify the Certificate Authority certificate.

Error	Description
Unable to delete certificate from <*endpoint name*>.	The firmware of the device may be preventing the system from deleting the certificate from the device.
Unable to read certificates from <*endpoint name*>.	The system could not read the certificate from the device.
No new identity certificates assigned for <*endpoint name*>.	The system could not locate expected certificates on the device.
Unable to obtain the list of trusted authorities for <*endpoint name*>.	The device cannot access the list of zone certificates.
Unable to assign a trusted authority certificate for <*device name*> <*endpoint name*>.	The device could not access one of its parameters.
Cannot get Trusted Devices.	The system could not retrieve the list of Trusted Devices form the device.
Cannot set Trusted Devices.	The system could not set the list of Trusted Devices for the device.
Cannot obtain a list of Certificate Management Objects for <*device name*> <*endpoint name*>.	The system could not retrieve a list of certificates from the device.
Unable to obtain required file object list on <*device name*> <*endpoint name*>.	The system encountered a problem communicating with the device.
Unable to obtain required file object on <*device name*> <*endpoint name*>.	The system encountered a problem communicating with the device.
Endpoint <*path*> does not support configuring state of: <*protocol*> <*port number*>.	The device does not support the mentioned communication protocol or port. Check if the device supports the protocol or port.
Cannot read device IE setting from <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Cannot verify IE rules on <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Unable to obtain the max instance for <*endpoint name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Cannot read device IE rules from <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Cannot read device IE rules size from <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Cannot get number of instances from <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Cannot get configuration sequence count from <*device name*>.	The system encountered a problem with the Ingress/Egress rules on the device. The device may not support this feature.
Unable to obtain the list of port instances for <*endpoint name*>, not supported by the device.	The device may not support this feature. Check the list of ports supported by the device and make the required changes in the security policy model.

Error	Description
Unable to read the proxy instance attributes for *<endpoint name>*.	The system was unable to retrieve data from the device set as a proxy device in the security policy model. Check if the device has proxy capabilities, check if the firmware is proxy-capable.
Unable to read the number of proxied endpoints supported by *<endpoint name>*.	The system was unable to retrieve data from the device set as a proxy device in the security policy model. Check if the device has proxy capabilities, check if the firmware is proxy-capable, check if the device is connected to a proxied device in the security policy model.
Unable to set the list of proxied endpoints for the proxy: *<endpoint name>*.	The system was unable to retrieve data from the device set as a proxy device in the security policy model. Check if the device has proxy capabilities, check if the firmware is proxy-capable, check if the device is connected to a proxied device in the security policy model.
Unable to connect to the endpoint (*<device name>*) using the *<device path>*.	Specific to 1756-EN4TR devices in redundant adapter mode. Turn off the redundant adapter mode on the device and redeploy the CIP Security policy.

Deployment warnings

Table 68. Deployment warnings

Warning	Description
Cannot read the Device Identity for the *<device name>* *<endpoint name>*	The system is unable to read a CIP Security object containing device identifiers. Make sure that the device is CIP Security capable, cycle power to the device, check physical connection to the device, update the device firmware.
<device name> does not support configuration for port.	The device has been placed in a zone that has disabled communication over the specified port, but the device does not support the individual port configuration. Make sure that the device is CIP Security capable, update device firmware.
Device does not support configuration of the DTLS Timeout setting.	Check if the device supports the DTLS Timeout setting, update device firmware, or disable the DTLS Timeout setting.
Device *<device name>* cannot configure Trusted IP lists.	Trusted IP Lists are a feature specific to Rockwell Automation/Allen-Bradley devices. Check the device specifications.
Device *<device name>* does not support Trusted IP lists.	Trusted IP Lists are a feature specific to Rockwell Automation/Allen-Bradley devices. Check the device specifications.
Cannot set IE rules on *<device name>*.	The system encountered a problem with the Ingress/Egress rules on the device.

Table 68. Deployment warnings (continued)

Warning	Description
	Cycle power to the device, retry deployment, or replace the device.
Unable to obtain the device IE support settings for *<endpoint name>*.	The system encountered a problem with the Ingress/Egress rules on the device. Cycle power to the device, retry deployment, or replace the device.
Unable to obtain the IE rules for *<endpoint name>*.	The system encountered a problem with the Ingress/Egress rules on the device. Cycle power to the device, retry deployment, or replace the device.
Unable to obtain converted IE rules for *<endpoint name>*.	The system encountered a problem with the Ingress/Egress rules on the device. Cycle power to the device, retry deployment, or replace the device.

Deployment troubleshooting

Troubleshoot issues with policy model deployment to resolve deployment errors and warnings.

General troubleshooting

- Update software, and check software compatibility. For more information, see Install or update software on page 10 and the release notes.
- Check error and warning messages for possible solutions
- Check the network
- Check the physical connection of the device
- Cycle power to the device
- Retry policy model deployment
- Reset the device to factory settings
- Update device firmware

1756-EN4TR troubleshooting

1756-EN4TR devices do not support CIP Security in redundant adapter mode.

If a 1756-EN4TR device is installed, uses CIP Security, and is reconfigured to be part of a redundant adapter pair, the module loses its CIP Security configuration, and the I/O chassis loses communication with the controller. To resolve the issue, deploy the CIP Security policy again.

OPC UA troubleshooting

If CompactLogix or ControlLogix controllers are in the RUN mode, you must power cycle the controllers to complete their configuration even if OPC UA policy deployments succeed.

For more information about the supported CompactLogix and ControlLogix, see OPC UA security policy on page 51.

Policy model backup and restoration

Create backup files to preserve and restore the policy models for your system in case of a failure.

Tip: Create a backup after a policy deployment to keep the backup files synchronized with the current security policy. FactoryTalk System Services store the FactoryTalk Policy Manager policy model in a policy database.

Back up a policy model

Back up FactoryTalk System Services to save a copy of the policy model and its associated certificates.

1. Open the command prompt as an Administrator.
2. In the command prompt, enter `cd "C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services"`
3. Run the backup utility by entering one of these commands:
   - To create a plaintext backup of the data, enter `FtssBackupRestore -B`
   - To create an encrypted backup of the data, enter `FtssBackupRestore -B -P` *`password`* or `FtssBackupRestore -B -P "`*`password`*`"`

     This creates an encrypted backup of the data using the password supplied after the `-P` parameter. Quotation marks are optional. This password must be supplied to restore the data.

   The `backup.zip` file is created. Once performed, the FactoryTalk Services Platform Backup includes this file.
4. Verify that the backup file is present in this location `C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTSS_Backup`

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

Restore a policy model

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

1. Verify the `backup.zip` file is present in this location `C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTSS_Backup`
2. Open the command prompt as an Administrator.
3. In the command prompt, enter `cd "C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services"`
4. Run the FactoryTalk System Services Backup & Restore Utility by entering either:
   - Policy model from a plaintext backup. Enter `FTSSBackupRestore -R`
   - Encrypted backup. Enter `FTSSBackupRestore -R -P "password"` or `FTSSBackupRestore -R -P password`

     This restores an encrypted backup that is decrypted using the password supplied after the `-P` parameter. Quotation marks are optional.

Rockwell Automation Support

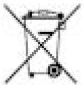
Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

Rockwell Automation maintains current product environmental information on its website at https://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) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846