CIP Security Proxy

Catalog Number 1783-CSP
CIP Security Proxy User Manual

Important User Information

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

## Preface
- Summary of Changes ........................................ 5
- Terminology .................................................. 6

## Chapter 1
### 1783-CSP Proxy Overview
- 1783-CSP Proxy Components .............................. 8
  - Rotary Switches ........................................... 9
  - Ethernet Ports ............................................ 9
  - DIP Switches ............................................. 10

## Chapter 2
### 1783-CSP Proxy in a CIP Security Architecture
- Facilitate Secure Communication ........................ 11
- Network Traffic Supported ................................. 13
  - Network and Device Side Connections ................. 13
  - Before the 1783-CSP Proxy is Configured for CIP Security ................................. 14
  - After the 1783-CSP Proxy is Configured for CIP Security ......................... 15
- Connect to EtherNet/IP Topologies ...................... 17
  - Network Port Connections ............................... 17
  - Network Communication Rates ........................... 19
- Secure the Programming Connection to the CompactLogix 5370 and CompactLogix 5380 Controllers ........................................ 19
- Secure the Programming Connection to the ControlLogix 5570 and ControlLogix 5580 Controllers ........................................ 30
- Secure the Programming Connection to Redundant ControlLogix 5570 or ControlLogix 5580 Controllers ......................... 36
- Use of Produce-Consume Tags and Message Instructions .......... 45
  - Produce-Consume Tags .................................. 45
  - Message Instructions .................................... 46
- Additional Considerations ................................ 46
  - Simple Network Management Protocol (SNMP) Not Supported ................................. 46
  - Use of Multicast Connections ............................ 46
  - Precision Time Protocol ................................ 46
  - Automatic Device Replacement ......................... 46
- Proxied Device Support ................................ 47
  - Devices That Cannot Be Used As a Proxied Device .... 47
  - Devices That Can Be Used As A Proxied Device in a Limited Manner ......................... 47
  - Devices That Have Been Tested ........................ 47
  - Devices That Have Not Been Tested .................... 48
  - Connect to a Network That Does Not Use CIP Security ......................... 48
  - Unsupported Topologies ................................ 49
# Table of Contents

## Chapter 3
Configure and Operate the 1783-CSP Proxy

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the IP Address</td>
<td>53</td>
</tr>
<tr>
<td>Set the IP Address with the Rotary Switches</td>
<td>54</td>
</tr>
<tr>
<td>Use Other Methods to Set the IP Address</td>
<td>55</td>
</tr>
<tr>
<td>Install the Proxy</td>
<td>55</td>
</tr>
<tr>
<td>Configure the 1783-CSP Proxy</td>
<td>56</td>
</tr>
<tr>
<td>Add a 1783-CSP Proxy to the System</td>
<td>57</td>
</tr>
<tr>
<td>Deploy the Security Model</td>
<td>65</td>
</tr>
<tr>
<td>Change Proxied Device That Is Connected to Proxy</td>
<td>67</td>
</tr>
<tr>
<td>New Proxied Device Is Same Device Type and Same IP Address</td>
<td>67</td>
</tr>
<tr>
<td>New Proxied Device is Different Device Type</td>
<td>68</td>
</tr>
<tr>
<td>Use the 1783-CSP Proxy As a DLR Supervisor</td>
<td>74</td>
</tr>
<tr>
<td>Use Protected Mode</td>
<td>75</td>
</tr>
<tr>
<td>CIP Security Configuration Changes</td>
<td>75</td>
</tr>
<tr>
<td>Enable Protected Mode</td>
<td>76</td>
</tr>
<tr>
<td>Disable Protected Mode</td>
<td>76</td>
</tr>
<tr>
<td>Reset the Proxy</td>
<td>77</td>
</tr>
<tr>
<td>Tasks After You Reset the Proxy</td>
<td>77</td>
</tr>
<tr>
<td>Update 1783-CSP Proxy Firmware</td>
<td>78</td>
</tr>
<tr>
<td>Determine If Firmware Needs to Be Updated</td>
<td>78</td>
</tr>
<tr>
<td>Obtain 1783-CSP Proxy Firmware</td>
<td>78</td>
</tr>
<tr>
<td>Use ControlFLASH Plus or ControlFLASH Software to Update Firmware</td>
<td>78</td>
</tr>
</tbody>
</table>

## Chapter 4
Troubleshoot the 1783-CSP Proxy

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Add-on Profile</td>
<td>79</td>
</tr>
<tr>
<td>Add the 1783-CSP Proxy to the Project</td>
<td>80</td>
</tr>
<tr>
<td>Monitor the Diagnostics</td>
<td>82</td>
</tr>
<tr>
<td>Port Diagnostics Dialog Box</td>
<td>82</td>
</tr>
<tr>
<td>Use the Web Server</td>
<td>82</td>
</tr>
<tr>
<td>Home Webpage</td>
<td>83</td>
</tr>
<tr>
<td>Diagnostics Overview Webpage</td>
<td>83</td>
</tr>
<tr>
<td>Network Settings Webpage</td>
<td>84</td>
</tr>
<tr>
<td>Ethernet Statistics Webpage</td>
<td>85</td>
</tr>
<tr>
<td>Ring Statistics Webpage</td>
<td>86</td>
</tr>
<tr>
<td>1588 PTP (Time Sync) Webpage</td>
<td>87</td>
</tr>
<tr>
<td>Disable the Web Server</td>
<td>88</td>
</tr>
<tr>
<td>Use Syslog with the 1783-CSP Proxy</td>
<td>89</td>
</tr>
</tbody>
</table>

## Appendix A
Status Indicators

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Indicators</td>
<td>91</td>
</tr>
</tbody>
</table>

## Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>93</td>
</tr>
</tbody>
</table>
Preface

This manual describes how to use a 1783-CSP CIP Security™ Proxy, catalog number 1783-CSP, to connect devices that are not CIP™ Security-capable to an industrial automation control system (IACS) that uses CIP Security.

Make sure that you are familiar with the following before you use this manual:
- Understanding of EtherNet/IP™ networking fundamentals
- Understanding of network security technologies and concepts
- Understanding of implementing CIP Security with Rockwell Automation™ products

IMPORTANT We strongly recommend that you have a thorough understanding of CIP Security and how to implement it in an IACS before you use the 1783-CSP Proxy. For more information, see the following before you proceed:
  - Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD022
  - CIP Security with Rockwell Automation products, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001
  - FactoryTalk® Policy Manager Getting Results Guide, publication FTALK-GR001

Summary of Changes

This publication has been revised as noted in the following chapter.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated components list to remove the MAC ID label from list. The MAC IDs are on the Product ID sticker on the shipping carton.</td>
<td>8</td>
</tr>
<tr>
<td>Updated section Secure the Programming Connection to the CompactLogix 5370 and CompactLogix 5380 Controllers</td>
<td>19</td>
</tr>
<tr>
<td>Updated section Secure the Programming Connection to the ControlLogix 5570 and ControlLogix 5580 Controllers</td>
<td>30</td>
</tr>
<tr>
<td>Added a section on how to secure the programming connection to a redundant pair of ControlLogix 5570 or ControlLogix 5580 controller</td>
<td>36</td>
</tr>
<tr>
<td>Added how you can use produce-consume tags and message instructions with the 1783-CSP CIP Security Proxy</td>
<td>45</td>
</tr>
<tr>
<td>Clarified that you cannot use Simple Network Management Protocol with the 1783-CSP CIP Security Proxy</td>
<td>46</td>
</tr>
<tr>
<td>Added devices that have been tested, and can be used, with the 1783-CSP CIP Security Proxy</td>
<td>47</td>
</tr>
<tr>
<td>Added content to section New Proxied Device Is Same Device Type and Same IP Address</td>
<td>67</td>
</tr>
<tr>
<td>Updated section Use Syslog with the 1783-CSP Proxy</td>
<td>89</td>
</tr>
</tbody>
</table>
The following terms are used in this manual.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOP</td>
<td>Add-on Profile</td>
</tr>
<tr>
<td>CIP</td>
<td>Common Industrial Protocol (CIP)</td>
</tr>
<tr>
<td>CIP Security</td>
<td>An open-standard secure communication mechanism that addresses the need for CIP-connected devices to be protected from potential EtherNet/IP network security exploitation.</td>
</tr>
<tr>
<td>CIP Security-capable device</td>
<td>An IACS device that natively supports the CIP Security standard.</td>
</tr>
<tr>
<td>Device side</td>
<td>The side of the 1783-CSP Proxy that contains a device that is not CIP Security-capable.</td>
</tr>
<tr>
<td>FactoryTalk Linx</td>
<td>The data server used for EtherNet/IP communication to deliver information from Allen-Bradley® control products to the IACS.</td>
</tr>
<tr>
<td>FactoryTalk Policy Manager</td>
<td>Software that you use as the graphical user-interface (GUI) commissioning tool for CIP Security IACS devices. You use this tool to configure, deploy, and view the system communication security policies.</td>
</tr>
<tr>
<td>FactoryTalk System Services</td>
<td>Software that runs as a service in the background to help enable the deployment of CIP Security policies that are configured in the FactoryTalk Policy Manager commissioning tool.</td>
</tr>
<tr>
<td>IACS</td>
<td>Industrial automation control system</td>
</tr>
<tr>
<td>Network side</td>
<td>The side of the proxy that connects to the CIP Security zone.</td>
</tr>
<tr>
<td>Proxied device</td>
<td>A non-CIP Security-capable device that is connected to the 1783-CSP Proxy device port.</td>
</tr>
<tr>
<td>Security Model</td>
<td>A fully-configured instance of zones, devices, and conduits, along with their respective CIP Security properties, in FactoryTalk Policy Manager software. The zones and conduits structure the security model. The security model is deployed to the devices in the IACS via security profiles for individual devices.</td>
</tr>
<tr>
<td>Security Policy</td>
<td>A comprehensive set of security requirements that are defined by an organization that outline security rules and required controls in order to achieve a desired security posture. Understanding the security threats, risks, and vulnerabilities of a system is the starting point for any security policy. FactoryTalk Policy Manager applies the policy to the devices via the security model, and the devices then enforces the security policy.</td>
</tr>
<tr>
<td>Security Profile</td>
<td>A set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability. A security profile describes what security features a given device supports. The device enforces the security policy based on its security profile.</td>
</tr>
</tbody>
</table>
1783-CSP Proxy Overview

The 1783-CSP Proxy is a DIN rail-mounted, standalone device that lets you connect a device that is not CIP™ Security-capable, also known as the proxied device, to an IACS that has CIP Security™ enabled with Rockwell Automation™ products.

The 1783-CSP Proxy connects a proxied device to the CIP Security architecture. The 1783-CSP Proxy performs security functionality on behalf of the device.

**IMPORTANT** We strongly recommend that you install the 1783-CSP Proxy and the proxied device in the same secure cabinet. By doing so, you increase the level of security for communication between the devices. A physically-secure cabinet reduces accessibility to the devices by unauthorized personnel and reduces the risk of compromise.
1783-CSP Proxy Components

Figure 1 shows the 1783-CSP Proxy components.

Figure 1 - 1783-CSP Proxy Components

Table 1 describes the 1783-CSP Proxy components.

Table 1 - 1783-CSP Component Descriptions

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 DIP switches</td>
<td>Configure the 1783-CSP Proxy to operate in DLR Supervisor mode, that is, as the Ring Supervisor, when the 1783-CSP Proxy is on a DLR network.</td>
</tr>
<tr>
<td>2 Panel mount tab</td>
<td>Used to mount the 1783-CSP Proxy onto a panel.</td>
</tr>
<tr>
<td>3 Status Indicators</td>
<td>Provide information about the operating status of the 1783-CSP Proxy.</td>
</tr>
<tr>
<td>4 Device port</td>
<td>Port that connects a device that is not CIP Security-capable to the 1783-CSP Proxy.</td>
</tr>
<tr>
<td>5 DIN rail latch</td>
<td>Used to lock the 1783-CSP Proxy onto the DIN rail.</td>
</tr>
<tr>
<td>6 DIP switch setting label</td>
<td>Describes how to use the DIP switch settings.</td>
</tr>
<tr>
<td>7 Rotary switches</td>
<td>Set an IP address for the 1783-CSP Proxy.</td>
</tr>
<tr>
<td>8 Switch settings label</td>
<td>Describes how to use the rotary switches.</td>
</tr>
</tbody>
</table>
| 9 Network ports   | • Port 1 - rear  
                     • Port 2 - front  
                     Ports that connect the 1783-CSP Proxy to the network side of the IACS, that is, the side of the 1783-CSP Proxy with CIP Security enabled. |
| 10 DC connector   | Connects power to the 1783-CSP Proxy.                                     |
Rotary Switches

The 1783-CSP Proxy has three rotary switches on the side.

Figure 2 - Rotary Switches

The positions to which you set the switches before turning on power determine how the 1783-CSP Proxy operates after powering up.

Table 2 - Rotary Switch Positions

<table>
<thead>
<tr>
<th>Switch Position</th>
<th>Description</th>
<th>For more information, see page</th>
</tr>
</thead>
<tbody>
<tr>
<td>999</td>
<td>Switch position out of the box. The 1783-CSP Proxy ships without an IP address and is DHCP-enabled.</td>
<td>53</td>
</tr>
<tr>
<td>xxx</td>
<td>If set to a valid number, the switches set the 1783-CSP Proxy IP address to 192.168.1.xxx. Valid numbers range from 002…254.</td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>Disables Explicit Protected mode</td>
<td>76</td>
</tr>
<tr>
<td>900</td>
<td>Enables Explicit Protected mode</td>
<td></td>
</tr>
<tr>
<td>988</td>
<td>Resets the 1783-CSP Proxy to its out-of-box state.</td>
<td>77</td>
</tr>
</tbody>
</table>

Ethernet Ports

The 1783-CSP Proxy has three Ethernet ports. The front port is a Device port that connects a non-CIP Security-capable device to the 1783-CSP Proxy.

You can connect the other two ports, that is, the Network ports, to EtherNet/IP™ networks that use a DLR, star, or linear topology.

Figure 3 - Ethernet Ports
DIP Switches

The 1783-CSP Proxy has DIP switches on the top of it.

You use switch 1 to configure the 1783-CSP Proxy as a ring supervisor on a DLR network. The Ethernet ports, that is, the Network ports, on the bottom of the 1783-CSP Proxy connect it to the DLR network.

For example, the Device port can connect to a proxied device that was previously directly connected to a DLR network or connected to a DLR network via a 1783-ETAP tap. The Network ports on the proxy can connect to the DLR where the proxied device had been connected.

For more information on the sides of the proxy, see Network and Device Side Connections on page 13.

Out of the box, the switches are in the Off position.

Figure 4 - DIP Switches

The positions at power-up determine the DLR network configuration.

Table 3 - DIP Switch Positions

<table>
<thead>
<tr>
<th>Position</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Power-up Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td></td>
<td></td>
<td>You use FactoryTalk® Linx software or the AOP in Logix Designer application to configure the 1783-CSP Proxy to be the Ring Supervisor on the DLR network.</td>
</tr>
<tr>
<td>On</td>
<td></td>
<td></td>
<td>The 1783-CSP Proxy functions as the Ring Supervisor on the DLR network with factory default settings.</td>
</tr>
</tbody>
</table>

For more information on how to use a 1783-CSP Proxy on a DLR network, see page 74.
Chapter 2

1783-CSP Proxy in a CIP Security Architecture

This section describes how the 1783-CSP Proxy fits into a CIP Security™ architecture that is implemented with Rockwell Automation™ products.

Facilitate Secure Communication

The 1783-CSP Proxy connects a non-CIP Security-capable device to an IACS with CIP Security implemented so that the device can participate in secure communication with CIP™ Security-capable devices on the EtherNet/IP™ network.

Figure 5 on page 12 shows two IACS.

- IACS 1 (before inserting the 1783-CSP Proxy) - Communication between the 1734-AENTR EtherNet/IP communication module and the CIP Security-enabled devices is permitted communication, based on IP address, but not secure communication.

  Communication is permitted because it was added to the secure zone in FactoryTalk® Policy Manager.

  This IACS does not include a 1783-CSP Proxy.

- IACS 2 (after inserting the 1783-CSP Proxy) - A 1783-CSP Proxy provides CIP Security for the 1734-AENTR communication module. As such, communication between the 1783-CSP Proxy and the CIP Security-enabled devices is secure communication.

  This IACS does include a 1783-CSP Proxy.

IMPORTANT Communication between the 1783-CSP Proxy and the other secured devices in the security zone is secure regarding CIP Security and the security policy for the IACS.

  The communication between the 1783-CSP Proxy and the proxied device is not secured regarding CIP Security.

  Therefore, we strongly recommend that you install the 1783-CSP Proxy and the proxied device in the same cabinet. By installing them in a secure enclosure, you establish a degree of physical security.
Figure 5 - IACS With and Without 1783-CSP Proxy Connected

IACS 1
System does not include a 1783-CSP Proxy.

IACS 2
System includes 1783-CSP Proxy.

Secure Communication
The 1734-ENTR communication module is directly connected to the IACS. Communication with the module is permitted but not secure.

Permitted Communication
The 1734-ENTR communication module is connected to the IACS via the 1783-CSP Proxy. Communication with the module is secure.
Network Traffic Supported

The 1783-CSP Proxy modifies CIP secured traffic on the network side to be non-CIP Secured so that a non-CIP Security-capable device can consume it. Likewise the 1783-CSP CIP Proxy modifies traffic from the non-CIP Security-capable device to be CIP Secured.

Network and Device Side Connections

You use the Network ports to connect to the following sides of an application:

- **Network side** - The network side connects the 1783-CSP Proxy to the side of the IACS that has CIP Security enabled.
- **Device side** - The device side connects the 1783-CSP Proxy to one device for which the 1783-CSP Proxy is providing CIP Security.

Figure 6 shows a 1783-CSP Proxy that is connected to the Network side and the Device side of an IACS.

Figure 6 - 1783-CSP Proxy Connected to Network and Device Sides

![Diagram of 1783-CSP Proxy Connected to Network and Device Sides]
Before the 1783-CSP Proxy is Configured for CIP Security

After the 1783-CSP Proxy has been installed, but before you configure it, network traffic occurs back and forth between all devices in the IACS. This includes between the proxied device and other devices.

That is, the 1783-CSP Proxy forwards all traffic in both directions, network side to device side and device side to network side.

As noted on page 11, we strongly recommend that you install the 1783-CSP Proxy and the proxied device in the same secure enclosure to establish a degree of physical security.

Figure 7 shows the devices in the IACS. In this case, all network traffic can occur because the security model has not been deployed.

Figure 7 - Network Communication Before Security Model is Deployed
After the 1783-CSP Proxy is Configured for CIP Security

After you configure the security model and deploy it to all CIP Security-capable devices, communication occurs between devices that reside in the same security zone or different zones that are connected via conduits.

If not permitted by the security model that has been deployed, communication requests are rejected. Some of the examples in this section show rejected communication.

Table 4 describes the different types of communication that can occur after a security model is deployed.

<table>
<thead>
<tr>
<th>Communication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>Network traffic between CIP Security-enabled devices</td>
</tr>
<tr>
<td>Permitted</td>
<td>Network traffic between devices, where at least one of them is not CIP Security-enabled.</td>
</tr>
</tbody>
</table>
| Rejected           | Network traffic between the devices that are part of the security zone and the following:  
  • Devices that are outside the IACS.  
  • Devices that are connected to the 1783-CSP Proxy other than the device that was selected in the security zone. |

Communication Between 1783-CSP and Proxied Device

Communication between the 1783-CSP Proxy and the proxied device is not secure. However, the network traffic between CIP Security-enabled devices and the 1783-CSP Proxy is secure.

Figure 8 shows an IACS in which a security model was deployed.

**IMPORTANT** The traffic between the 1783-CSP Proxy and the PowerFlex® 527 drive is not secure. That is, it is not secured regarding CIP Security. If you install the 1783-CSP Proxy and the PowerFlex 527 drive in the same cabinet, you establish a degree of physical security.
Figure 8 - Network Communication After Security Model is Deployed - Example 1

This traffic is not secured regarding CIP Security.
Connect to EtherNet/IP Topologies

You can connect the 1783-CSP Proxy to different types of EtherNet/IP network topologies.

Network Port Connections

The 1783-CSP Proxy can connect to the following EtherNet/IP network topologies on the network side of the IACS:

- Device Level Ring Topology
- Linear Topology
- Star Topology

Device Level Ring Topology

You can connect both network ports on the 1783-CSP Proxy to a DLR ring. The traffic between the 1783-CSP Proxy and the proxied devices is not CIP secured.

Figure 9 - Two 1783-CSP Proxies in a DLR Topology
Linear Topology

You can connect both network ports on the 1783-CSP Proxy into a linear topology. The traffic between the 1783-CSP Proxy and the proxied devices is not CIP secured.

Figure 10 - 1783-CSP Proxy on a Linear Topology

Star Topology

You can connect the 1783-CSP Proxy to a star topology via a switch. The traffic between the 1783-CSP Proxy and the proxied device is not CIP secured.

Figure 11 - 1783-CSP Proxy on a Star Topology
Network Communication Rates

You can configure the 1783-CSP Proxy network and device ports to communicate at the following rates:

- 10 Mbps
- 100 Mbps
- 1 Gbps

By default, the 1783-CSP Proxy is configured for Auto Negotiate. You can force the communication rate to a specific speed if necessary, however.

Secure the Programming Connection to the CompactLogix 5370 and CompactLogix 5380 Controllers

You can secure connections between a workstation that is running a Logix Designer application and a CompactLogix™ 5370 or CompactLogix 5380 controller through a 1783-CSP Proxy. Connections from the controllers to devices on the network are not secure.

Alternatively, you can use CompactLogix 5380 controllers, firmware revision 34.011 or later, to connect directly to the controller Ethernet port and secure connections between a workstation and the CompactLogix 5380 controller without using a 1783-CSP Proxy.

For more information, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

This section describes the following scenarios with CompactLogix 5370 or 5380 controllers:

- CIP Security with CompactLogix 5370 Controllers Connected to the I/O Network Via a 1783-ETAP Tap
- CIP Security with CompactLogix 5370 or CompactLogix 5380 Controllers - Connected Directly to the I/O Network

IMPORTANT

If you are using Dual-IP EtherNet/IP mode with a CompactLogix 5380 controller, firmware revision 31.011...33.xxx, we recommend that you design and deploy your CIP Security model before you download your Logix Designer application project.

For more information on using Dual-IP EtherNet/IP mode with CIP Security, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

If you are using Linear/DLR (not using Dual-IP) EtherNet/IP mode, with either of the following controllers:

- CompactLogix 5380 controllers, firmware revisions 31.011...33.xxx
- CompactLogix 5370 controllers, firmware revision 31.011 or later

make sure that the devices that are used in the IACS are installed, configured and operating as expected before you use a 1783-CSP Proxy.

For example, upgrade firmware revisions as necessary and configure the I/O devices. Then take the necessary steps to use a 1783-CSP Proxy to implement CIP Security as shown in this section.

Your application must include the following for this to apply:

- Logix Designer application, version 31.00.00 or later, and a compatible controller firmware revision
- FactoryTalk Linx software, version 6.20 or greater
Figure 12 shows an application in which the workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a CompactLogix 5370 controller via a 1783-CSP Proxy. The controller is operating in Linear/DLR EtherNet/IP mode.

The steps beginning on page 21 describe how to set up the scenario shown in Figure 12.

**IMPORTANT** This example uses a CompactLogix 5370 controller. The same steps apply if you are using a CompactLogix 5380 controller, firmware revisions 31.011...33.xxx, instead.

Figure 12 - CIP Security with CompactLogix 5370 Controllers Connected to the I/O Network Via a 1783-ETAP Tap

Connection between the workstation and the controller, via the 1783-CSP Proxy, is secure.

**IMPORTANT**: This example shows the controller that is connected to a DLR ring. The controller can be connected to any valid I/O architecture, for example, a Linear topology that does not include a 1783-ETAP tap, and the concepts that are described in this section still apply.
Complete the following steps.

1. Confirm that all I/O devices are configured and operating as expected. For more information, see page 19.

2. Disconnect the I/O devices from the controller.
   The 1783-CSP Proxy must see only the controller because that will be the proxied device.
3. Disconnect the workstation from the controller, and install the 1783-CSP Proxy.

4. Connect the workstation to a Network port on the 1783-CSP Proxy. Do not connect to the 1783-CSP Proxy Device port.
5. Connect the 1783-CSP Proxy Device port to the controller. Do not connect to a 1783-CSP Proxy Network port.

6. Add the 1783-CSP Proxy and controller to the security model in FactoryTalk Policy Manager software while there is no other device connected to the controller.

7. Deploy the updated security model in FactoryTalk Policy Manager software.
8. Re-connect the I/O devices to the controller.

After the security model is deployed and the I/O devices are re-connected, only the controller is added to the security model. As a result, the following apply:

- CompactLogix 5370 and CompactLogix 5380 controllers in DLR/Linear mode - FactoryTalk Linx software can discover the controller but not the devices connected to the other port on the controller. For example, controller project upload/download and monitoring are available.
- CompactLogix 5380 controllers in Dual-IP mode - FactoryTalk Linx software can discover the controller and the devices connected to the other port on the controller. For example, in addition to controller access, drive parameter upload/download and monitoring are available.

We strongly recommend that you install all devices, including the 1783-CSP Proxy in the same secure enclosure.

By installing them in a secure enclosure, you establish a degree of physical security.
Figure 13 shows an application in which the workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a CompactLogix 5370 controller via a 1783-ETAP tap.

In this scenario, the controller is directly connected to the network via its Network ports.

The steps beginning on page 26 describe how to set up the scenario shown in Figure 13.

**IMPORTANT** This example uses a CompactLogix 5370 controller. The same steps apply if you are using a CompactLogix 5380 controller, firmware revisions 31.011…33.xxx, in DLR/Linear mode instead.

**Figure 13 - CIP Security with CompactLogix 5370 or CompactLogix 5380 Controllers - Connected Directly to the I/O Network**

**IMPORTANT:** This example shows the controller that is connected to a DLR ring. The controller can be connected to any valid I/O architecture, for example, a Linear topology that does not include a 1783-ETAP tap, and the concepts that are described in this section still apply.
Complete the following steps.

1. Confirm that all I/O devices are configured and operating as expected. For more information, see page 19.

2. Disconnect the I/O devices from the CompactLogix 5370 controller.
3. Disconnect the workstation from the 1783-ETAP tap, and install the 1783-CSP Proxy.

4. Connect the workstation to a Network port on the 1783-CSP Proxy. Do not connect to the 1783-CSP Proxy Device port.
5. Connect the 1783-CSP Proxy Device port to the controller. Do not connect to a 1783-CSP Network port.

6. Add the 1783-CSP Proxy and controller to the security model in FactoryTalk Policy Manager software while there is no other device connected to the controller.

7. Deploy the updated security model.

8. Disconnect the 1783-CSP Proxy Device port from the controller.
9. Connect the 1783-CSP Proxy Device port to the 1783-ETAP tap Device port. Do not connect to a 1783-CSP Proxy Network port.

10. Re-connect the I/O devices to the controller.
After the security model is deployed and the I/O devices are re-connected, only the controller is added to the security model.

As a result, FactoryTalk Linx software can discover the controller but not the devices connected to the other port on the controller. For example, controller project upload/download and monitoring are available.

We strongly recommend that you install all devices, including the 1783-CSP Proxy in the same secure enclosure, as shown. By installing them in a secure enclosure, you establish a degree of physical security.

Secure the Programming Connection to the ControlLogix 5570 and ControlLogix 5580 Controllers

You can secure connections between a workstation that is running a Logix Designer application and a ControlLogix 5570 controller or a ControlLogix 5580 controller, through a 1783-CSP Proxy.

Alternatively, you can use ControlLogix 5580 controllers, firmware revision 32.011 or later, to secure the connections between the workstation and controller without using a 1783-CSP Proxy.

**IMPORTANT** Before you use a 1783-CSP Proxy in the following configurations, make sure that the devices that are used in the IACS are installed, configured and operating as expected. For example, upgrade firmware revisions as necessary and configure the I/O devices. Then take the necessary steps to use a 1783-CSP Proxy to implement CIP Security with the controller. Your application must include the following for this to apply:

- One of the following controllers:
  - ControlLogix 5570 controllers, firmware revision 31.011 or later
  - ControlLogix 5580 controllers, firmware revision 31.xxx
- Logix Designer application, version 31.00.00 or later, and a compatible controller firmware revision
- FactoryTalk Linx software, version 6.20 or greater

**Figure 14 on page 31** shows an application in which a workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a ControlLogix 5570 controller via a 1783-CSP Proxy and a 1756-EN2T EtherNet/IP communication module in slot 1.

The controller is connected to a DLR network via a 1756-EN2TR EtherNet/IP communication module in slot 2 of the same chassis.

**IMPORTANT** This example uses a ControlLogix 5570 controller. The same steps apply if you are using a ControlLogix 5580 controller, firmware revision 31.xxx, instead.
Figure 14 - ControlLogix 5570 Controllers - Single Chassis Connected to I/O Network Devices

Connection between the workstation and the controller, via the 1783-CSP Proxy, is secure.

*IMPORTANT:* This example shows the controller that is connected to a DLR ring. The controller can be connected to any valid I/O architecture, for example, a Linear topology, and the concepts that are described in this section still apply.

Remember, the 1756-EN2T EtherNet/IP adapter in slot 1 is used for the Logix Designer application programming software, and the 1756-EN2TR EtherNet/IP adapter is used for I/O devices.
Complete the following steps.
1. Confirm that all I/O devices are configured and operating as expected.
   For more information, see page 30.
2. Disconnect the workstation from the 1756-EN2T EtherNet/IP communication module, and install the 1783-CSP Proxy.
3. Connect a 1783-CSP Proxy Network port to the workstation. Do not connect to the 1783-CSP Device port.
4. Connect the 1783-CSP Proxy Device port to the 1756-EN2T EtherNet/IP adapter in slot 1. Do not connect the communication module to a 1783-CSP Proxy Network port.
5. Add the 1783-CSP Proxy and 1756-EN2T EtherNet/IP adapter in slot 1 to the security model in FactoryTalk Policy Manager software.

6. Deploy the updated security model.
   Only the 1756-EN2T in slot 1 is added to the security model.
   The application can perform the following functions on the ControlLogix 5570 controller and the I/O devices that are connected to the 1756-EN2TR EtherNet/IP communication module in slot 2.
   - Download to or upload from the devices
   - Update firmware revisions
   - Monitor diagnostics

Secure the Programming Connection to Redundant ControlLogix 5570 or ControlLogix 5580 Controllers

You can secure connections between a workstation that is running a Logix Designer application and a ControlLogix 5570 or ControlLogix 5580 controller redundant pair through a 1783-CSP Proxy, firmware revision 1.002 or later. The secure connection supports class 3 communications, for example, program upload or download and to monitor diagnostics.

Alternatively, you can use ControlLogix 5580 controllers, firmware revision 34.011 or later, and 1756-EN4TR communication modules, firmware revision 4.001 or later, to secure the connections between the workstation and controller without using a 1783-CSP Proxy.

For more information, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

**IMPORTANT** Before you use a 1783-CSP Proxy in the following configurations, make sure that the devices that are used in the IACS are installed, configured and operating as expected. For example, upgrade firmware revisions as necessary and configure the I/O devices. Then take the necessary steps to use a 1783-CSP Proxy to implement CIP Security with the controller. Your application must include the following for this to apply:

- One of the following controllers:
  - ControlLogix 5570 controllers, firmware revision 31.011 or later
  - ControlLogix 5580 controllers, firmware revision 31.011...33.xxx
- Logix Designer application, version 31.00.00 or later, and a compatible controller firmware revision
- FactoryTalk Linx software, version 6.20 or greater

**Figure 15 on page 37** shows an application in which a workstation that is running the Logix Designer application and FactoryTalk Linx software is connected to a ControlLogix 5570 controller redundant pair via a 1783-CSP Proxy and 1756-EN2TR EtherNet/IP communication modules in slot 1 of each chassis. The communication modules must be configured for IP swapping.

The controllers are connected to I/O devices on a DLR network via 1756-EN2TR EtherNet/IP communication modules in slot 2 of the chassis.

**IMPORTANT** This example uses a ControlLogix 5570 controller. The same steps apply if you are using a ControlLogix 5580 controller, firmware revisions 31.011...33.xxx.

The example includes 1756-EN2TR EtherNet/IP adapter in the redundant chassis pair for the uplink. You can also use 1756-EN2T EtherNet/IP adapters.
Connection between the workstation and the controller redundant pair, via the 1783-CSP Proxy, is secure. Thus, the workstation and 1783-CSP Proxy are in the Security Zone.

**TIP:** You can use redundancy workstations in the Security Zone. In that case, though, you need to connect the redundant stations to a switch that is connected to the 1783-CSP Proxy.

### IMPORTANT:
- Be aware that the proxy and the switch are each a single point of failure.
- The 1756-EN2TR EtherNet/IP communication modules in slot 1 of the redundant chassis pair must be configured for IP address swapping.
- This example shows the controller redundant pair connected to a DLR ring. You can also use a PRP architecture.

Remember, the 1756-EN2TR EtherNet/IP adapters in slot 1 of each chassis are used for the Logix Designer application programming software. The 1756-EN2TR EtherNet/IP adapter in slot 2 of each chassis is used for I/O devices. You can also use 1756-EN2T EtherNet/IP adapters in slots 1 and 2.
Complete the following steps.

1. Confirm that all I/O devices are configured and operating as expected.
   For more information, see page 36.
2. Disconnect the workstation from the 1756-EN2TR EtherNet/IP communication module, and install the 1783-CSP Proxy.
3. Connect a 1783-CSP Proxy Network port to the workstation. Do not connect to the 1783-CSP Device port.
4. Disconnect the primary chassis from the switch.
5. Connect the 1783-CSP Proxy Device port, not the other network port, directly to the primary 1756-EN2 module. The 1783-CSP Proxy must only be able to discover the primary 1756-EN module and no other devices. The connection from the workstation to the 1783-CSP Proxy is secure.
6. Add the 1783-CSP Proxy and 1756-EN2TR adapter in slot 1 of the primary chassis to the security model in FactoryTalk Policy Manager software.

7. Deploy the updated security model. Only the 1756-EN2TR EtherNet/IP adapter in slot 1 is added to the security model.

8. Disconnect the 1783-CSP Proxy Device port from the primary chassis.
9. Connect the primary chassis to the switch and the 1783-CSP Proxy Device port to the switch. Do not connect the other 1783-CSP Network port to the switch.

The connection from the workstation to the 1783-CSP Proxy is secure.
The application can perform the following functions on the redundant ControlLogix 5570 controller and the I/O devices that are connected to the 1756-EN2TR EtherNet/IP communication modules in slot 2 of the redundant chassis pair.

- Download to or upload from the devices
- Update firmware revisions
- Monitor diagnostics

**Use of Produce-Consumne Tags and Message Instructions**

You can use Produce-Consumne tags and Message instructions with a 1783-CSP Proxy as described in this section.

**Produce-Consumne Tags**

The producer can have CIP Security Proxy securing it because it does not open the connection.

The consumer **cannot** have CIP Security Proxy securing it because it must open a connection. Secure the consumer with a CIP Security-capable device, for example, a 1756-EN4TR module.
Message Instructions

If connected messaging is used, the controller that contains that message instruction cannot be secured through the 1783-CSP Proxy because that is the controller initiating the connection. The 1783-CSP Proxy cannot initiate a secured connection. This is true for either CIP data table read or CIP data table write messages.

Additional Considerations

The following considerations apply when you use the 1783-CSP Proxy.

Simple Network Management Protocol (SNMP) Not Supported

The 1783-CSP Proxy does not support SNMP.

Use of Multicast Connections

You cannot use Multicast connections with CIP Security.

Before you implement CIP Security in an application that uses Multicast connections, you must complete the following steps:

1. Change the connections from Multicast to Unicast.
2. Validate that the application is working as expected.
3. Apply/deploy the CIP Security policies.

If you deploy the security model before you change the connections to Unicast, the application loses communication. As a result, it can be more complex to troubleshoot the application so that it works as expected.

Precision Time Protocol

The 1783-CSP Proxy can be used in a system that includes CIP Sync™ and uses Precision Time Protocol (PTP) per IEEE-1588. All Ethernet ports on the 1783-CSP Proxy support the distribution of PTP packets in real-time IACS, including systems with Integrated Motion on EtherNet/IP.

For more information on PTP, see the Integrated Architecture® and CIP Sync Configuration Application Technique, publication IA-AT003.

Automatic Device Replacement

You can use Automatic Device Replacement (ADR) with the 1783-CSP Proxy.

As a function of the security model that is deployed, the following identity attributes must match the device:

- Device Type
- Product Code
- Vendor Id

As a function of the controller connection, if exact keying is required, the major firmware revision and minor firmware revision must match also.
Proxied Device Support

This section describes the level of support for devices to be used as proxied devices with a 1783-CSP Proxy.

Devices That Cannot Be Used As a Proxied Device

You cannot use the following devices as proxied devices with a 1783-CSP Proxy:

- Computers
  Computers can use CIP Security via FactoryTalk Linx software. Applications on your workstation that do not use FactoryTalk Linx software cannot be CIP Secured.
- Operator interfaces and HMI devices
  These devices open CIP connections. The 1783-CSP Proxy cannot open secure CIP connections.

Devices That Can Be Used As A Proxied Device in a Limited Manner

You can use the following devices as proxied devices with a 1783-CSP Proxy in a limited manner:

- CompactLogix 5370 and 5380 controllers
  For more information, see Secure the Programming Connection to the CompactLogix 5370 and CompactLogix 5380 Controllers on page 19
- ControlLogix 1756-ENx modules with ControlLogix 5570 and 5580 controllers
  For more information, see Secure the Programming Connection to the ControlLogix 5570 and ControlLogix 5580 Controllers on page 30

Devices That Have Been Tested

Rockwell Automation has tested the following devices that you can use with the 1783-CSP Proxy:

- 1769 EtherNet/IP adapters
- CIP Safety Encoder (843ES-SIP14BA1)
- Compact 5000™ EtherNet/IP adapters
- Compact 5000 Safety I/O modules
- E300™ Electronic Overload Relay
- FLEX™ I/O EtherNet/IP adapters
- FLEX 5000™ EtherNet/IP adapters
- FLEX 5000 Safety I/O modules
- Kinetix® 5500 drives\(^{(a)}\)
- Multi Function Access Box (442G-MAB)
- POINT I/O™ EtherNet/IP adapters
- POINT I/O Safety modules
- PowerFlex 525 drives
- PowerFlex 527 drives - Tested Motion only, safety only, and both motion and safety together.
- PowerFlex 7 series drives
- PowerMonitor™ 5000 units
- SLC™ 500 EtherNet/IP adapters

\(^{(a)}\) When you use the 1783-CSP Proxy, with CIP Security enabled on a Kinetix 5500 drive as the proxied device, the cyclic update period cannot be faster than 4.0 ms.
**Devices That Have Not Been Tested**

Other CIP-compliant devices are expected to work but Rockwell Automation has not tested all of them.

We recommend that before you use a CIP-compliant device with the 1783-CSP Proxy in normal operating conditions that you test it.

**Connect to a Network That Does Not Use CIP Security**

You can use the 1783-CSP Proxy in a manner similar to a 1783-ETAP tap. In this case, however, CIP Security cannot used. The 1783-CSP Proxy Device port is connected to the workstation, and, in this example, the Network ports are connected to the linear network.

The 1783-CSP Proxy might be used to replace a 1783-ETAP to take advantage of the 1 Gbps network communication rate and/or rotary switches to assign an IP address. However, even if it is not configured, the 1783-CSP Proxy can only communicate with one device, that is, the device that is connected to the device port.

The workstation can then, for example, upload/download a controller project and monitor a controller on the network.
Chapter 2          1783-CSP Proxy in a CIP Security Architecture

Unsupported Topologies

This section shows topologies that the 1783-CSP Proxy does not support.

IMPORTANT All of the examples in this section assume that the system shown has CIP Security implemented.

Figure 16 - 1783-CSP Proxy Device Port Connected to a Controller

A connection between the 1783-CSP Proxy device port and controller is not supported except in the scenarios that are described in Secure the Programming Connection to the CompactLogix 5370 and CompactLogix 5380 Controllers on page 19. The CompactLogix 5370 controller cannot be on the Device side of the 1783-CSP Proxy and control CIP Secured I/O devices because the Proxy cannot open a secure connection to the I/O devices.
A connection between the 1783-CSP Proxy Device port and the HMI device is not supported because the Proxy cannot open a secure connection back to the controller.

A connection between the 1783-CSP Proxy Device port and the 1783-ETAP tap is not supported, except as shown in page 29, because the Proxy can only support a single device.
Figure 19 - 1783-CSP Proxy Device Port Connected to a Linear Topology

A connection between the 1783-CSP Proxy Device port and the 1783-ETAP tap is not supported, except as shown in page 29, because the Proxy can only support a single device.

Figure 20 - 1783-CSP Proxy Device Port Connected to a Star Topology

A connection between the 1783-CSP Proxy Device port and the star topology is not supported because the Proxy can only support a single device.
A connection between the workstation and the 1783-CSP Proxy device port is not supported in a CIP Security implementation.

Figure 21 - Workstation Connected to the 1783-CSP Proxy Device Port and Network Ports Connected to a Linear or DLR Network When CIP Security is Being Implemented

A connection between the Device ports on the 1783-CSP Proxies is not supported because the Proxies do not support a secure tunnel.

Figure 22 - Two 1783-CSP Proxies Connecting Different Networks
Configure and Operate the 1783-CSP Proxy

This chapter describes how to prepare the 1783-CSP Proxy and configure it.

Set the IP Address

When the 1783-CSP Proxy is in the out-of-the-box state, the following apply regarding IP addresses:

- The 1783-CSP Proxy does not have an IP address.
- The rotary switches on the 1783-CSP Proxy are set to 999.
- The 1783-CSP Proxy is DHCP-enabled. That is, the 1783-CSP Proxy is configured to obtain an IP address via a DHCP server.

**IMPORTANT** A dynamic IP address means that every time power is cycled to the 1783-CSP Proxy, the address is cleared and the proxy requests an IP address via DHCP.

We recommend that you set the IP address to a static configuration so that you are not required to set an IP address each time that power is cycled.

- If there is no DHCP server or the DHCP server is not configured to set the IP address, you must set the IP address manually.
- The 1783-CSP Proxy issues requests for an IP address via DHCP until you use one of the tools that are described in this chapter to set an IP address.
- The 1783-CSP Proxy is configured so that the IP address is dynamic.
- Make sure that you assign a unique IP address to the 1783-CSP Proxy, that is, use an IP address that differs from all other devices on the EtherNet/IP™ network.

If the 1783-CSP Proxy uses the same IP address as another device on the network, the result is a Duplicate IP address condition.
Set the IP Address with the Rotary Switches

If the network uses the 192.168.1.x range of addresses, use the rotary switches to set the last octet of network IP address. Valid numbers range from 002...254.

**IMPORTANT** When you use the rotary switches to set the IP address:
- The rotary switches only set the IP address when power is cycled.
- The address is static and remains the same on future power cycles.

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

To set the IP address, turn the switches to the desired numbers before you install the 1783-CSP Proxy. The leftmost switch represents the most significant digit in the octet, the middle switch represents the second digit, and the rightmost switch represents the least significant digit.

At power-up, the 1783-CSP Proxy reads the rotary switches to determine if they are set to a valid number for the last octet of the IP address. If the settings are a valid number, the following conditions result:
- IP address = 192.168.1.xxx (where xxx represents the switch settings)
- Subnet mask = 255.255.255.0
- Gateway address = 192.168.1.1
- The 1783-CSP Proxy does not have an assigned host name, nor does it use any Domain Name System.

**Set the IP Address with Switches in Position 999**

You can set a static IP address on the 1783-CSP Proxy when the rotary switches are set to 999 by using one of the software methods described on page 55 to set the IP address and then disable DHCP on the proxy.

As a result, the IP address will not change with future power cycles.
Use Other Methods to Set the IP Address

If the network does not use 192.168.1.x, do not change the switch positions before you install the 1783-CSP Proxy. After you install and power up the 1783-CSP Proxy, you can use the following to set the network IP address:

- DHCP server
- BOOTP DHCP EtherNet/IP Commissioning Tool - We recommend that you use version 3.02.00 or later.
  For more information on how to use these methods, see the EtherNet/IP Network Devices User Manual, publication ENET-UM006.
- FactoryTalk® Linx software - You must use version 6.20 or later with the 1783-CSP Proxy.
  For more information on how to set the IP address with FactoryTalk Linx software, see the FactoryTalk Linx Getting Results Guide, publication LNXENT-GR001.

Install the Proxy

Before you can configure or operate the 1783-CSP Proxy, you must install it. For detailed information on how to install it, see the CIP Security™ Proxy Installation Instructions, publication 1783-IN019.

If you did not set the IP address before you installed the 1783-CSP Proxy, that is, you did not use the rotary switches, you must set the IP address after installation.

To set the IP address after you install the 1783-CSP Proxy, see Use Other Methods to Set the IP Address.

The installation process, as described in publication 1783-IN019, includes connecting the 1783-CSP Proxy to the IACS network. If you do not complete all installation steps and connect the 1783-CSP Proxy to the IACS, you cannot proceed with the configuration process.
Configure the 1783-CSP Proxy

**Table 5** describes the software that is required to use a 1783-CSP Proxy in an IACS with CIP™ Security.

<table>
<thead>
<tr>
<th>Software Application</th>
<th>Description</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Policy Manager</td>
<td>Secure software application to configure, deploy, and view system communication security policies.</td>
<td>Version 6.20(1), (2), (3)</td>
</tr>
<tr>
<td>FactoryTalk System Services</td>
<td>Deploys the security policies that are configured in FactoryTalk Policy Manager.</td>
<td>Version 6.20(1), (3)</td>
</tr>
<tr>
<td>Studio 5000 Logix Designer</td>
<td>Logix Designer application is a comprehensive programming software that you use with Logix 5000™ controllers. In an IACS with CIP Security implemented, the software is only used with ControlLogix® 5580 controllers.</td>
<td>Version 31.00.00(1), (4)</td>
</tr>
</tbody>
</table>

(1) You download software at the Rockwell Automation Product Compatibility and Download Center (PCDC). To visit the PCDC, go to: http://compatibility.rockwellautomation.com/Pages/home.aspx

(2) FactoryTalk Policy Manager, version 6.20 or later, is an independent installation package. FactoryTalk System Services, version 6.20 or later, is part of the FactoryTalk Policy Manager installation.

(3) **IMPORTANT**: The minimum required software version at the initial release of CIP Security from Rockwell Automation was version 6.11. In that case, the software was a component that you were required to install when you installed FactoryTalk Services Platform. If you are using version 6.11, you must upgrade to version 6.20 or later to use a 1783-CSP Proxy. Before you migrate from version 6.11 to version 6.20 or later, we recommend that you see the Rockwell Automation Knowledgebase article ‘FactoryTalk Policy Manager download and install’. The article is available at https://rockwellautomation.custhelp.com/app/home:

(4) CIP Security is not supported to Studio 5000 Logix Designer software versions prior to 31. If you use software version 31.00.00, you must use a controller with firmware revision 31.xxx. In this case, you must also use a 1756-EN4TR ControlLogix EtherNet/IP communication module in the same chassis as the controller to secure communication in the IACS. **IMPORTANT**: Logix Designer application, version 31.00.00, requires that you use ControlLogix 5580 controller, firmware revision 31.xxx, but ControlLogix 5580 controllers do not support CIP Security previous to firmware revision 32.011. If you use software version 31.00.00 and firmware revision 31.xxx, you must use a 1756-EN4TR EtherNet/IP adapter in the controller chassis. We recommend that you upgrade your Logix Designer application to version 32.00.00 or later and ControlLogix 5580 controller to compatible firmware revision 32.011 or later.
Add a 1783-CSP Proxy to the System

You configure the 1783-CSP Proxy in the following scenarios:
- After adding the proxy between the IACS and a non-CIP Security-capable device that is already connected to the system.
  In this scenario, you must disconnect the non-CIP Security-capable device from the system before you add the proxy to the system.
- After adding both the proxy and a non-CIP Security-capable device as a pair initially.

**IMPORTANT** This section assumes that CIP Security has previously been deployed before you add the 1783-CSP Proxy and proxied device.

Complete the following steps:
1. If the device to be proxied for already exists in the IACS, disconnect it from the network.
   If the proxied device does not exist in the IACS, skip to step 2.
2. Install the 1783-CSP Proxy.
   For more information on how to install the Proxy, see the CIP Security Proxy Installation Instructions, publication 1783-IN013.
3. Connect the IACS to the 1783-CSP Proxy network port(s).
4. Connect the proxied device to the 1783-CSP Proxy device port
5. Open FactoryTalk Policy Manager software.
6. Select the zone name from the Zones list, and add the 1783-CSP Proxy to the zone.
   You can add the 1783-CSP Proxy in the following ways:
   - Discover devices via FactoryTalk Linx. (Discovery)
   - Add the device manually. (Add Device)
7. To use the **Discovery method** to add the proxy to the zone, complete the following steps.
   a. Click Discovery.
   b. In the DISCOVERY area, select the proxy and click the + symbol.

When you use the Discovery method, you can also add a device by clicking it in the list and dragging it to the center of the screen.
A dialog box confirms that you want to add the 1783-CSP Proxy and the proxied device.

c. Click what you want to add to the security model. Typically, you add both the 1783-CSP Proxy and the proxied device.
- The 1783-CSP Proxy and the proxied device that is connected to it.
- The 1783-CSP Proxy only.

d. Click Add.

**IMPORTANT**

If the proxied device already existed in the security model, you must delete it from the security model first.

If you fail to delete the proxied device that already existed in the security model, when you click Add, the software alerts you to the fact that you cannot add the device to the security model.

The 1783-CSP Proxy and the proxied device that is connected to it are added to the security model.
8. To use the **Add Device method** to add the proxy to the zone, complete the following steps.

a. Click Add Device.

b. In the catalog number list, choose the 1783-CSP Proxy, and click OK.
c. In the catalog number list, choose the proxied device that is connected to the 1783-CSP Proxy, and click OK.

**IMPORTANT** Make sure that you choose a proxied device that is supported by a 1783-CSP Proxy. Do not choose a device that is not supported by a 1783-CSP Proxy. For more information on device support, see Proxied Device Support on page 47.
d. Select the 1783-CSP Proxy and set the IP address.
e. Change the EtherNet Driver Name field to match the driver name in the DISCOVERY section below it. In this example, the EtherNet Driver Name is changed to AB_ETHIP-1.
f. Select the proxied device and set the IP address.

9. Confirm that the proxied device is in the correct zone. In this case, the correct zone is Zone 1.

10. Deploy the updated security model as described beginning on page 65.
Deploy the Security Model

**IMPORTANT** Make sure that all devices are operational and have network access.

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

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

To deploy the policy, complete the following steps in FactoryTalk Policy Manager.

1. Click Deploy.

![Deploy button](image)

Depending on the size of your application, the following dialog box can appear on the screen after you click Deploy.

![Validation dialog box](image)

2. When the Deploy dialog box appears, complete the following steps.
   a. Choose the Deployment scope based on your application. We recommend that you use the default option. That is, Changed device communication ports only.

![Deploy dialog box](image)

Changing security policies requires resetting device communication ports, resulting in a short loss of connectivity.
b. Choose one of the following options for when to reset the communication channels for the items included in the security model:

- **During policy deployment** - The CIP connection is closed and reopened on the device during the deployment process.
  Similar to when the network card on a computer is reset, the device stays functional but is disconnected from the network for a few moments. This option applies the new profile to the device at the same time that the security model is deployed.

- **After deployment** - Security policy settings are deployed to the device but are not applied to existing connections. That is, connections that are already established continue to use the security policy that was in effect when the connection was initially established.
  The new security profiles are applied to new connections or when the existing connections are closed and re-opened. For example, the existing connections can be closed and re-opened by cycling power to the 1783-CSP Proxy, or inhibiting and uninhibiting the 1783-CSP Proxy and proxied device.

**IMPORTANT**
If the 1783-CSP Proxy is in the out-of-box state, whether you choose During deployment or After deployment, all I/O connections are reset during deployment.

If the proxy already has a security profile and the security policy is being changed, the I/O connections are reset based on your choice, that is, During deployment or After deployment.

The During policy deployment option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.
3. Click DEPLOY.

After the policy is deployed, a green shield appears in FactoryTalk Linx software for the 1783-CSP Proxy and the proxied device. The shield indicates that the corresponding device is secured.

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

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

Change Proxied Device That Is Connected to Proxy

This section describes the following situations in which the proxied device that is connected to a 1783-CSP Proxy is changed.

- New Proxied Device Is Same Device Type and Same IP Address
- New Proxied Device is Different Device Type

New Proxied Device Is Same Device Type and Same IP Address

In this case, you are replacing a proxied device with a device of the same device type and the same IP address.

In this case, the same device type is not restricted to the exact catalog number. It can be a device from the same product family. For example, you can remove a 1756-EN2TR communication module with a 1756-EN4TR communication module and the steps below still apply.

Complete the following steps.

1. Disconnect the original proxied device from the device port on the 1783-CSP Proxy.
2. Connect the new proxied device to the device port on the 1783-CSP Proxy.

The security model still applies and does not need to be redeployed.
New Proxied Device is Different Device Type

In this case, you are replacing a proxied device with another proxied device that is another device type.

**IMPORTANT** The steps apply if the new device uses the same or a different IP address.

In [Figure 23](#) a PowerFlex® 525 drive that uses IP address 192.168.1.233, that is, the original proxied device, is replaced by a PowerMonitor™ 5000 unit that also uses IP address 192.168.1.233.

**Figure 23 - Replace Proxied Device - Different Device Type and Same IP Address**
Complete the following steps.

1. Select the 1783-CSP Proxy from the list of devices, and click Delete.

When you delete the 1783-CSP Proxy, the proxied device is also deleted. A warning dialog box appears.

2. Click Delete.

3. Disconnect the original proxied device from the 1783-CSP Proxy.

4. Click Deploy to deploy the updated security model.
5. When the Deploy dialog box appears, choose the Deployment scope and reset device communication ports option.

6. Click DEPLOY.
   For more information on the reset device communication ports option, see page 66.

---

The During policy deployment option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.

The 1783-CSP Proxy and the proxied device are deleted from the security model.

7. Connect the new proxied device to the 1783-CSP Proxy.
8. Use one of the methods described beginning on page 57 to add the 1783-CSP Proxy to the security model.

This example uses the Discovery method.

9. Click Discovery.

10. In the DISCOVERY area, select the proxy and click the + symbol.

When you use the Discovery method, you can also add a device by clicking it in the list and dragging it to the center of the screen.

A dialog box confirms that you want to add the 1783-CSP Proxy and the proxied device.
11. Click what you want to add to the security model. Typically, you add both the 1783-CSP Proxy and the proxied device.
   - The 1783-CSP Proxy and the proxied device that is connected to it.
   - The 1783-CSP Proxy only.
12. Click Add.

**IMPORTANT** If you fail to delete the proxied device that already existed in the security model, when you click Add, the software alerts you to the fact that you cannot add the device to the security model.

13. Click Deploy to deploy the security model.

14. When the Deploy dialog box appears, choose the Deployment scope and when to reset device communication ports.
15. Click DEPLOY.
For more information on the reset device communication ports option, see page 66.

The During policy deployment option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.

After the policy is deployed, a green shield appears in FactoryTalk Linx software for the 1783-CSP Proxy and the proxied device. The shield indicates that the corresponding device is secured.

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

The 1783-CSP Proxy and the new proxied device are added to the security model.
Use the 1783-CSP Proxy As a DLR Supervisor

You can use the 1783-CSP Proxy as a DLR supervisor, that is, Ring Supervisor. The 1783-CSP Proxy has DIP switches on the top of it. Out of the box, the switches are in the Off position.

You use switch 1 to configure the 1783-CSP Proxy to be the Ring Supervisor on a DLR network. The position of switch 2 does not affect DLR Supervisor configuration.

We recommend that you confirm that the switches are in the correct settings before you turn on power to the 1783-CSP Proxy.

<table>
<thead>
<tr>
<th>Position</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Power-up Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td></td>
<td></td>
<td>The proxy is not enabled to be a DLR Supervisor unless you use software to enable it as a DLR Supervisor and configure DLR Supervisor-related parameters. That is, the proxy is not a DLR Supervisor until you configure it to be one via software. (1)</td>
</tr>
<tr>
<td>On</td>
<td></td>
<td>-</td>
<td>The proxy is enabled to be a DLR Supervisor. If necessary, you can configure remaining DLR Supervisor parameters, for example, supervisor precedence, via software. (1)</td>
</tr>
</tbody>
</table>

(1) You use FactoryTalk Linx software or an Add-on Profile in Logix Designer application to configure the parameters. For information about supervisor-related parameters, see the EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

To change the DLR Supervisor mode, complete the following steps.

1. Turn power off from the 1783-CSP Proxy.
2. Move the switches to the desired positions.
3. Cycle power to the 1783-CSP Proxy.

The state of the switches is read-only at power-up. Changes to the switch positions while power is on do not take effect until power is cycled.
Use Protected Mode

The 1783-CSP Proxy supports protected mode. When the Proxy is in this mode, you cannot perform any of these actions:

- Change Ethernet configuration settings, such as port speed.
- Change IP settings, such as IP address, mask, and DHCP mode.
- Update the device firmware.
- Disable or re-enable Ethernet ports via the Module Properties dialog box in the Logix Designer application project.
- Reset the Proxy via the Module Properties dialog box in the Logix Designer application project.

CIP Security Configuration Changes

CIP Security configuration includes parameters that are configured in FactoryTalk Policy Manager software and deployed to the 1783-CSP Proxy via FactoryTalk System Services.

Restrictions on CIP Security Configuration Imposed by Protected Mode

Whether the security model has been deployed to the 1783-CSP Proxy or not determines what putting the 1783-CSP Proxy in protected mode means.

- If the 1783-CSP Proxy has not been configured for CIP Security when you transition the 1783-CSP Proxy to explicit protected mode, any attempt to configure the 1783-CSP Proxy for CIP Security are rejected. The rejection is indicated in FactoryTalk Policy Manager software as a deployment failure.
- If the 1783-CSP Proxy has been configured for CIP Security when you transition the 1783-CSP Proxy to explicit protected mode, attempts to configure the 1783-CSP Proxy for CIP Security are accepted. The CIP Security configuration changes are successful in this case because the changes are coming from the trusted policy authority.
Enable Protected Mode

To transition the 1783-CSP Proxy to the protected mode, complete the following steps.

1. Power down the 1783-CSP Proxy.
2. Set the rotary switches to position ‘900’.
3. Power up the 1783-CSP Proxy.
4. Wait for the 1783-CSP Proxy power-up sequence to complete.
   The power-up sequence is complete when the status indicator states are as follows:
   - OK status indicator - Flashes red
   - LINK 1, LINK 2, and DEVICE PORT status indicators - Off
5. Power down the 1783-CSP Proxy.
6. Set the rotary switches to the position used before you started this sequence of steps.
7. Power up the 1783-CSP Proxy.

The device is in Protected Mode.

Disable Protected Mode

To disable protected mode, complete the following steps.

1. Power down the 1783-CSP Proxy.
2. Set the rotary switches to 000.
3. Power up the 1783-CSP Proxy.
4. Wait for the 1783-CSP Proxy power-up sequence to complete.
   The power-up sequence is complete when the status indicator states are as follows:
   - OK status indicator - Flashes red
   - LINK 1, LINK 2, and DEVICE PORT status indicators - Off
5. Power down the 1783-CSP Proxy.
6. Set the rotary switches to the position used before you started this sequence of steps.
7. Power up the 1783-CSP Proxy.

The 1783-CSP Proxy is in Unprotected Mode.
**Reset the Proxy**

You can use the rotary switches to reset the 1783-CSP Proxy to the out-of-box state.

**IMPORTANT**  When you use the rotary switches to reset the proxy, you reset it to its out-of-box state. That is, you erase all 1783-CSP Proxy configuration. This includes configuration settings for the 1783-CSP Proxy. The configuration of the 1783-CSP Proxy includes information related to the proxied device. We recommend that you exercise caution when you use the rotary switches to reset the 1783-CSP Proxy to its out-of-box state because you are changing the proxied device’s security policy.

To reset the 1783-CSP Proxy to its out-of-box state, complete the following steps.
1. Power down the 1783-CSP Proxy.
2. Set the rotary switches to 888.
3. Power up the 1783-CSP Proxy.
4. Wait for the 1783-CSP Proxy power-up sequence to complete.
   - The power-up sequence is complete when the status indicator states are as follows:
     - OK status indicator - Flashes red
     - LINK 1, LINK 2, and DEVICE PORT status indicators - Off
5. Power down the 1783-CSP Proxy.
6. Set the rotary switches to the desired position.
7. Power up the 1783-CSP Proxy.

**Tasks After You Reset the Proxy**

Complete the tasks for each scenario that is described in the following table.

The tasks described here are similar to the tasks described in the section beginning on page 67.

<table>
<thead>
<tr>
<th>If You Plan to Use the 1783-CSP Proxy This Way After It Is Reset</th>
<th>Then Complete These Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>The 1783-CSP Proxy continues to use the same IP address and connects to the same proxied device.</td>
<td>Redeploy the security model to update the configuration on the 1783-CSP proxy and proxied device.</td>
</tr>
</tbody>
</table>
| The 1783-CSP Proxy uses a different IP address and connect to the same proxied device. | 1. Change IP address in the port properties section of FactoryTalk Policy Manager software.  
2. Deploy the updated security model. |
| Either of the following:  
  - The 1783-CSP Proxy continues to use the same IP address but connect to a different proxied device that uses the same IP address as the previous proxied device.  
  - The 1783-CSP Proxy uses a different IP address and connect to a different proxied device that uses a different IP address. | 1. Delete the 1783-CSP Proxy and proxied device from the security model.  
2. Deploy the updated security model.  
3. Add the 1783-CSP Proxy and proxied device to the security model.  
4. Deploy the updated security model. |
| The 1783-CSP Proxy is removed from the IACS. | 1. Delete the 1783-CSP Proxy and proxied device from the security model.  
2. Deploy the updated security model. |
Update 1783-CSP Proxy Firmware

To update the 1783-CSP Proxy firmware, if necessary, complete the following tasks:

- Determine If Firmware Needs to Be Updated
- Obtain 1783-CSP Proxy Firmware
- Use ControlFLASH Plus or ControlFLASH Software to Update Firmware

Determine If Firmware Needs to Be Updated

To determine if the 1783-CSP Proxy needs a firmware update, check catalog number 1783-CSP at the Rockwell Automation Product Compatibility and Download Center (PCDC).

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

Obtain 1783-CSP Proxy Firmware

You can obtain the latest firmware revision from the PCDC. To visit the PCDC, go to: http://compatibility.rockwellautomation.com/Pages/home.aspx

Use ControlFLASH Plus or ControlFLASH Software to Update Firmware

For information on how to use ControlFLASH Plus™ or ControlFLASH™ software, see the following:

- ControlFLASH Plus Quick Start Guide, publication CFP-QS001
- ControlFLASH User Manual, publication 1756-UM105

---

**IMPORTANT**

Security settings are expected to be retained when firmware is updated. However, the settings can be lost and the security model must be redeployed.
Troubleshoot the 1783-CSP Proxy

This section describes the AOP and web server diagnostics that are available with the 1783-CSP Proxy.

---

**IMPORTANT** You do not use the AOP to configure CIP™ Security parameters. You configure CIP Security™ parameters in FactoryTalk® Policy Manager software.

You use the AOP to configure, and monitor, non-CIP Security-related parameters in a Logix Designer application project.

---

You access the diagnostics via the module properties dialog box in Studio 5000 Logix Designer® application, version 32.00.00 or later. You can use the available diagnostic information to monitor and troubleshoot the 1783-CSP Proxy behavior.

Diagnostic information is available for the 1783-CSP Proxy and the proxied device.

Install Add-on Profile

You are not required to add the 1783-CSP Proxy to a Logix Designer application project to use the proxy.

Because you are not required to add the 1783-CSP Proxy to the Logix Designer application project, the application excludes a module properties dialog box for the 1783-CSP Proxy. You must install an Add-on Profile (AOP) in the software first.

To download the AOP, check catalog number 1783-CSP at the PCDC at:  
http://compatibility.rockwellautomation.com/Pages/home.aspx

Use the Module Profiles Setup tool to install the profile in the Logix Designer application.
Add the 1783-CSP Proxy to the Project

Complete the following steps to add the 1783-CSP Proxy to your Logix Designer application project.
1. Create a project.
2. Right-click Ethernet, and choose New Module.
3. On the Select Module Type dialog box, choose the 1783-CSP Proxy catalog number, and click Create.
4. On the New Module dialog box, complete the following tasks on the General category tab:
   a. Type a name.
   b. Enter the IP address.
   c. If necessary, click Change to configure the module definition. The Module Definition dialog box appears.
   d. Change the parameters as necessary.

5. Click OK to close the Module Definition dialog box.
6. Click OK to create the module in the project.
Monitor the Diagnostics

To monitor diagnostic information for the 1783-CSP Proxy, complete the following steps.

1. Confirm that the Logix Designer application is online.
2. Click the Port Configuration category, and click the ellipsis in the Port Diagnostics column for the port or device diagnostics that you must monitor.

Port Diagnostics Dialog Box

Use the Web Server

The 1783-CSP Proxy provides diagnostic webpages that track diagnostics that are related to the proxy performance.

To access the diagnostic webpages, follow the following steps.

1. Open your web browser.
2. In the Address field, type the IP address of the 1783-CSP Proxy and press Enter.

**IMPORTANT** The web server is not secure, that is, http.

3. To access the information that you need, use the links in the left-side navigation bar.
Chapter 4  Troubleshoot the 1783-CSP Proxy

Network Settings Webpage

![Network Settings Webpage Screenshot](image-url)
### Ethernet Statistics Webpage

#### Interface Counters Device Port
- In Octets: 23397651
- In Ucast Packets: 101080
- In Nucast Packets: 2111
- In Discards: 1
- In Errors: 0
- In Unknown Proto: 0
- Out Octets: 9943170
- Out Ucast Packets: 125446
- Out Nucast Packets: 30764
- Out Discards: 0
- Out Errors: 0

#### Interface Counters Network Ports
- In Octets: 12444450
- In Ucast Packets: 102271
- In Nucast Packets: 18852
- In Discards: 0
- In Errors: 0
- In Unknown Proto: 0
- Out Octets: 30310631
- Out Ucast Packets: 144681
- Out Nucast Packets: 37561
- Out Discards: 0
- Out Errors: 0

#### Media Counters Device Port
- Alignment Errors: 0
- FCS Errors: 0
- Single Collisions: 0
- Multiple Collisions: 0
- SQE Test Errors: 0
- Deferred Transmissions: 0
- Late Collisions: 0
- Excessive Collisions: 0
- MAC Transmit Errors: 0
- Carrier Sense Errors: 0
- Frame Too Long: 0
- MAC Receive Errors: 0

#### Media Counters Link 1 (rear)
- Alignment Errors: 0
- FCS Errors: 0
- Single Collisions: 0
- Multiple Collisions: 0
- SQE Test Errors: 0
- Deferred Transmissions: 0
- Late Collisions: 0
- Excessive Collisions: 0
- MAC Transmit Errors: 0
- Carrier Sense Errors: 0
- Frame Too Long: 0
- MAC Receive Errors: 0

#### Media Counters Link 2 (front)
- Alignment Errors: 0
- FCS Errors: 0
- Single Collisions: 0
- Multiple Collisions: 0
- SQE Test Errors: 0
- Deferred Transmissions: 0
- Late Collisions: 0
- Excessive Collisions: 0
- MAC Transmit Errors: 0
- Carrier Sense Errors: 0
- Frame Too Long: 0
- MAC Receive Errors: 0

Seconds Between Refresh: 15  Disable Refresh with 0.
Chapter 4  Troubleshoot the 1783-CSP Proxy

Ring Statistics Webpage
### 1588 PTP (Time Sync) Webpage

#### General Information
- **PTP enabled**: True
- **Is the grandmaster**: False
- **Is synchronized to a master**: False
- **Sync status**: 0x0
- **UTC time**: Thu Jan 1 02:27:43 1970
- **System time**: 0x00000080c97ab1b7
- **Steps removed**: 0
- **Domain number**: 0
- **Offset from master**: 0
- **Max Offset from master**: 0
- **Mean path delay to master**: 0
- **System to local clock offset**: 0x0000000000000000
- **Grandmaster Name**: CIP Secure Proxy
- **Grandmaster Description**: Rockwell Automation:1783-CSPx006d38
- **Grandmaster Protocol Address**: 192.168.1.101

#### Clock Info

<table>
<thead>
<tr>
<th>Clock</th>
<th>Priority 1</th>
<th>Class</th>
<th>Accuracy</th>
<th>Variance</th>
<th>Priority 2</th>
<th>Identifier</th>
<th>Time Source</th>
<th>UTC Offset</th>
<th>Time Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>128</td>
<td>248</td>
<td>254</td>
<td>65535</td>
<td>128</td>
<td>0x34009efff30be</td>
<td>Internal Oscillator</td>
<td>37</td>
<td>0x8</td>
</tr>
<tr>
<td>Parent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x34009efff30be</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grandmaster</td>
<td>128</td>
<td>248</td>
<td>254</td>
<td>65535</td>
<td>128</td>
<td>0x34009efff30be</td>
<td>Internal Oscillator</td>
<td>37</td>
<td>0x8</td>
</tr>
</tbody>
</table>

#### Port Info

<table>
<thead>
<tr>
<th>Port</th>
<th>Port State</th>
<th>Log Announce Interval</th>
<th>Log Sync Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxied Ethernet Port</td>
<td>Master</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Network Ethernet Port</td>
<td>Master</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Seconds Between Refresh: **15**  Enable Refresh with 0.
Disable the Web Server

You can disable the web server on a 1783-CSP Proxy when there is a proxied device connected to it, and an I/O connection to the proxied device is open.

Complete the following steps.

1. In the Logix Designer application project, check the Inhibit Module checkbox for the proxied device.
   The Inhibit Module field is available on the Connection tab in the Module Properties dialog box.

2. In FactoryTalk Policy Manager software, check the Disable port HTTP (80) checkbox on Port Properties.
3. Deploy the updated Security Model.
4. In the Logix Designer application project, uncheck the Inhibit Module checkbox for the proxied device.

To re-enable the webserver on a 1783-CSP Proxy after it has been disabled, repeat the steps described previously in this section. At step 2, however, you uncheck the Disable port HTTP (80) checkbox.

Use Syslog with the 1783-CSP Proxy

The 1783-CSP Proxy is syslog-enabled. For more information on Syslog than is provided in this section, see the CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.

Syslog is a standardized and widely used event message logging technology. CIP Security-capable devices are syslog-enabled. Syslog is a standard for event logging. You use Syslog to generate, store, report and analyze security-related events.

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

Table 6 lists the events that are specific to the 1783-CSP Proxy.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Associated Message</th>
<th>Description of Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>discovery_device_up</td>
<td>A new device was discovered at address.</td>
<td>The event occurs when the discovery agent detects a new device on the network.</td>
</tr>
<tr>
<td>discovery_device_down</td>
<td>The device at address was disconnected.</td>
<td>The event occurs when the discovery agent detects a device has left the network.</td>
</tr>
</tbody>
</table>

For a complete list of syslog messages, see the Logix 5000 Controller and I/O Fault Codes and Syslog Messages Reference Data, publication 1756-RD001.
Notes:
This section describes the status indicators that are used with the 1783-CSP Proxy.

The 1783-CSP Proxy uses the following status indicators:
- OK status indicator - Indicates module status
- LINK 1 status indicator - Indicates network port 1 link status
- LINK 2 status indicator - Indicates network ports 2 link status
- DEVICE PORT status indicator - Indicates device port link status

For information on each indicator, see Table 7 on page 92.
### Table 7 - 1783-CSP Status Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>State</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OK</strong></td>
<td>Off</td>
<td>There is no power supplied to the device.</td>
<td>Turn on power to the device.</td>
</tr>
<tr>
<td></td>
<td>Flashing green</td>
<td>The device has not been configured. In this state, the device transmits all traffic.</td>
<td>Configure the device.</td>
</tr>
<tr>
<td></td>
<td>Steady green</td>
<td>The device is operating as expected.</td>
<td>None</td>
</tr>
</tbody>
</table>
|           | Flashing red        | Minor Fault - One or more recoverable minor faults are detected on the device. The following are possible minor faults: | One of the following:  
  - The device is performing a firmware flash update. Wait for the firmware update to finish and use the device as desired.  
  - IP Address switches do not match configuration in use.  
  - The device has completed a reset to factory default request due to the switches being set to 888 at power-up, and a power cycle is required. Cycle power to the device.  
  - The device is acknowledging a change of protected mode operation:  
    - 900 - enter protected mode  
    - 000 - exit protected mode  
  - None |
|           | Steady red          | Major fault - One or more nonrecoverable major faults are detected on the device. | Cycle power to the device. If the indicator remains steady red, return the device to Rockwell Automation. |
|           | Flashing red/green  | The device is in Self-Test.                                                 | 1. Let the self-test process complete.  
  2. If necessary, take action that is based on the state of the OK status indicator. |
| **LINK 1, LINK 2, DEVICE PORT** | Off | No physical link is detected.                                                | Troubleshoot the network to address any issues that are preventing expected operation. |
|           | Steady green        | A link is established on the port at a network communication rate of 100 Mbps or 1 Gbps. There is no activity on the link, though. IMPORTANT: This state is expected on one of the ports if the proxy is serving as an active DLR supervisor. | If activity is expected on the link, troubleshoot the application to address any issues that are preventing expected operation. |
|           | Flashing green      | A link is established on the port at a network communication rate of 100 Mbps or 1 Gbps. There is activity on the link. | None                                                                                 |
|           | Steady yellow       | A link is established on the port at a network communication rate of 10 Mbps. There is no activity on the link, though. | If activity is expected on the link, troubleshoot the application to address any issues that are preventing expected operation. |
|           | Flashing yellow     | A link is established on the port at a network communication rate of 10 Mbps. There is activity on the link. | None                                                                                 |
A
AOP
  install 79
  automatic device replacement 46

B
BOOTP-DHCP server
  set IP address 55

C
CIP Security-capable
  software
    FactoryTalk Linx 56
    FactoryTalk Policy Manager 56
    FactoryTalk System Services 56
  configuration
    protected mode 75
  connections
    device side 13
    multicast 46
    network side 13
    secure programming connection
      CompactLogix 5370 controllers 19 - 30
      CompactLogix 5380 controllers 19 - 30
      ControlLogix 5570 controllers 30 - 36
      ControlLogix 5570 or 5580 redundant controllers 36 - 45
  ControlLogix redundancy 36 - 45

D
DC connector 8
  deploy
    security profile 65
  device port 8
  device-level ring topology 17
  devices
    proxy is not supported 47
  DHCP server
    set IP address 55
  diagnostics
    monitor in Studio 5000 Logix Designer 82
  DIN rail latch 8
  DIP switches 10
    DLR supervisor 74
    label 8
    position description 10
    DLR supervisor 74
    configure DIP switches 10

E
ethernet ports 9
EtherNet/IP topologies 17
  device-level ring 17
  linear 18
  star 18
  explicit protected mode
    disable 9
    enable 9

F
FactoryTalk Linx 6, 36, 56
  set IP address 55
FactoryTalk Policy Manager 6, 56
FactoryTalk System Services 6, 56
  firmware
    update on the proxy 78

I
install the AOP 79
install the proxy 55
IP address
  BOOTP-DHCP 55
  DHCP server 55
  FactoryTalk Linx 55
  rotary switches 9, 54
  set 53 - 55

L
limitations
  automatic device replacement 46
  multicast connections 46
  linear topology 18

M
monitor diagnostics 82
multicast connections 46

N
network
  communication rates 19
  network communication
    permitted 15
    rejected 15
    secure 15
  network ports 8, 9
  network topologies 17
    device-level ring 17
    linear 18
    star 18
Index

O
out-of-box state
reset the proxy 77

P
power the proxy
DC connector 8
product compatibility and download center
(PCDC) 78
protected mode 75
disable 76
enable 76
proxied device
replace 67
proxy components 8 - 10
DIP switches 10
ethernet ports 9
rotary switches 9
proxy firmware
update 78

R
reset the proxy 77
rotary switches 9
label 8
position descriptions 9
set IP address 54

S
security profile
deploy 65
set IP address 53 - 55
BOOTP-DHCP 55
DHCP server 55
FactoryTalk Linx 55
rotary switches 54
software
ControlFLASH 78
ControlFLASH Plus 78
FactoryTalk Linx 6, 18, 30, 36, 56
FactoryTalk Policy Manager 6, 56
FactoryTalk System Services 6, 56
set the IP address 55
Studio 5000 Logix Designer 19, 30, 36
install the AOP 79
monitor diagnostics 82
star topology 18
status indicators 8, 91
Studio 5000 Logix Designer 36
install the AOP 79
monitor diagnostics 82
syslog 89

U
update proxy firmware 78

W
web server
use to troubleshoot issues 82
Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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