



CIP Security 在罗克韦尔自动化产品中的应用



Allen-Bradley

by ROCKWELL AUTOMATION

重要用户须知

在安装、配置、操作或维护本产品之前，请阅读本文档以及“其他资源”章节所列的文档，了解关于安装、配置和操作该设备的信息。除了所有适用的条例、法律和标准的要求之外，用户还必须熟悉安装和接线说明。

包括安装、调整、投入运行、使用、装配、拆卸和维护等在内操作必须由经过适当培训的人员根据适用的操作守则来执行。

如果未遵照制造商所指定的方式使用该设备，将可能导致该设备提供的保护失效。

在任何情况下，对于因使用或操作该设备造成的任何间接或连带损失，罗克韦尔自动化公司概不负责。

本手册中包含的示例和图表仅用于说明。由于任何具体安装都涉及众多变数和要求，罗克韦尔自动化公司对于依据这些示例和图表所进行的实际应用不承担任何责任和义务。

对于因使用本手册中所述信息、电路、设备或软件而引起的专利问题，罗克韦尔自动化公司不承担任何责任。

未经罗克韦尔自动化公司的书面许可，不得复制本手册的全部或部分内容。

在整本手册中，我们在必要的地方使用了以下注释，来提醒您留意安全注意事项。



警告：标识在危险环境下可能导致爆炸，进而导致人员伤亡、物品损坏或经济损失的操作或情况。



注意：标识可能导致人员伤亡、物品损坏或经济损失的操作或情况。注意符号可帮助您确定危险情况，避免发生危险，并了解可能的后果。

重要信息 标识对成功应用和了解本产品有重要作用的信息。

标签也可能位于设备表面或内部，提供具体的预防措施。



电击危险：位于设备（例如，变频器或电机）表面或内部的标签，提醒相关人员可能存在危险电压。



灼伤危险：位于设备（例如，变频器或电机）表面或内部的标签，提醒相关人员表面可能存在高温危险。



弧闪危险：位于设备（例如，电机控制中心）表面或内部的标签，提醒相关人员可能出现弧闪。弧闪可导致重伤或死亡。佩戴适当的个人防护设备 (PPE)。遵循所有安全工作规范和个人防护设备 (PPE) 的规章要求。

	前言	5
	变更摘要	5
	第 1 章	
工业安全概述	工业自动化控制系统环境	7
	安全威胁	7
	漏洞和漏洞利用	8
	安全评估	9
	深度防御架构	10
	CIP Security 为 ODVA 标准	11
	设备标识 / 身份验证	12
	安全数据传输	13
	第 2 章	
支持 CIP Security 的 罗克韦尔自动化产品	软件和硬件	15
	CIP Security 软件应用程序	15
	支持 CIP Security 的硬件设备	17
	使用罗克韦尔自动化产品的优势	18
	CIP Security 属性	18
	安全配置文件和属性	18
	CIP Security 组件	19
	安全模型	22
	区域属性	22
	导管属性	23
	限制和注意事项	24
	双端口设备	24
	如果 ControlLogix 5580 控制器处于工作模式， 则初始安全模型部署失败	24
	无法从非安全工作站下载到 ControlLogix 5580 控制器	25
	如果安全配置文件不匹配，则工作站无法连接到安全的 ControlLogix 5580 控制器	26
	CIP 桥接	27
	网络地址转换	27
	使用多播连接	29
	自动设备更换	29
	RSLinx Classic 软件	29

CIP Security 实现流程	第 3 章	
	设计和安装系统.....	31
	识别、组织和创建区域.....	32
	创建区域.....	33
	配置区域.....	35
	识别、组织和创建导管.....	36
	创建导管.....	37
	配置导管.....	41
	识别和创建安全功能 / 策略.....	43
	部署安全模型.....	44
	备份安全模型.....	47
	将安全模型备份保存到另一安全位置.....	47
	不同于 FactoryTalk Directory 备份文件.....	47
	恢复 FactoryTalk System Services.....	48
	删除安全策略.....	49
	从软件应用程序中删除安全策略.....	49
	从设备中删除安全策略.....	53
	更换系统中支持 CIP Security 的设备.....	56
CIP Security 实现示例架构	第 4 章	
	实现的第一阶段.....	57
	创建区域.....	57
	创建区域至区域导管.....	59
	配置导管安全策略.....	60
	部署安全策略.....	61
	实现的第二阶段.....	62
	创建设备至设备导管.....	62
	创建区域至设备的导管.....	63
	创建导管安全策略.....	64
	部署安全策略.....	65
	索引	67
	其他资源	71

本手册介绍了如何在工业自动化控制系统 (IACS) 中实施通用工业协议 (CIP™) Security 标准。本手册的其余部分均使用术语 CIP Security™。

在使用本手册之前，请确保您熟悉以下内容：

- 基本了解 EtherNet/IP™ 网络基础知识
- 基本了解网络安全术语和概念
- 使用 Rockwell Automation® 软件，例如：
 - FactoryTalk® Policy Manager
 - FactoryTalk Linx
 - Studio 5000 Logix Designer®

变更摘要

下表列出了本版出版物中所作的变更。全篇采用变更条指示所作的变更。

主题	页码
新增了有关可与 CIP Security 配合使用的以下产品的信息 · 1783-CSP CIP Security Proxy · Kinetix 5300 驱动器 · PowerFlex® 755T 变频器	整本手册
有关如何将应用程序 FactoryTalk Policy Manager 从版本 6.11 升级到版本 6.20 的说明	15
更新了有关应用程序 Studio 5000 Logix Designer 的说明	16
更新了有关 ControlLogix® 5580 控制器的说明	17
新增了当 ControlLogix 5580 控制器处于工作模式时，初始安全模型部署失败的说明	24
新增了有关无法从不安全的工作站下载到 ControlLogix 5580 控制器的状态说明	25
在 CIP 桥接图中添加了 PowerFlex 755T 变频器	27
更新了有关设备自动替换功能限制的说明	29
新增了有关不同安全模型部署类型的说明	45
更新了有关如何备份安全模型的说明	47
新增了有关如何恢复 FactoryTalk System Services 的说明	48
新增了有关如何更换 CIP Security 使能设备的说明	56
更新了显示 1783-CSP CIP Security Proxy 的图形	第 4 章

注：

工业安全概述

本部分将概述 CIP Security™。

工业自动化控制系统环境

过去，工业自动化控制系统 (IACS) 一直为物理隔离环境，是运行专有控制协议的孤立系统。但 IACS 网络正在朝着智能制造方向发展。

智能制造是数字化转型的门户，它连接工厂级和企业网络，并安全地连接人员、流程和技术。

总体上，这为联网的智能设备打开了新窗口，实现流程、数据和分析可视化。可视化促进更快作出更恰当决策，并且实现远程无缝连接。

随着 EtherNet/IP™ 标准日益发展，必须将这些孤立的 IACS 网络转变为智能制造、网络融合和工业安全网络。

安全威胁

为了满足实体端到端连接需求，IACS 网络向开放式以太网介质和互联网协议 (IP) 标准过渡，使得威胁范围扩大。

随着智能设备和端到端连接的增加，需要保护的资产越来越多，安全威胁的风险也越来越大。

安全风险有多种形式，例如：

- 威胁源起方试图未经授权地隐秘访问 IACS 网络，意欲实施恶意行为。
- 人员本着善意操作，但却无意中犯错，导致非预期后果。

重要信息 本出版物着重介绍恶意威胁源起方，也称为攻击者。本出版物其余部分均采用“攻击者”一词。
在本出版物中，攻击者是指个人或高级持续性威胁 (APT)，或一组协同操作的攻击者。

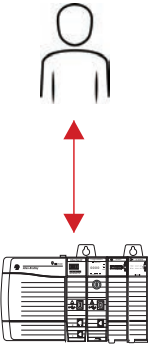
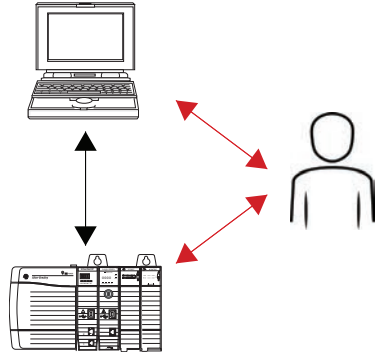
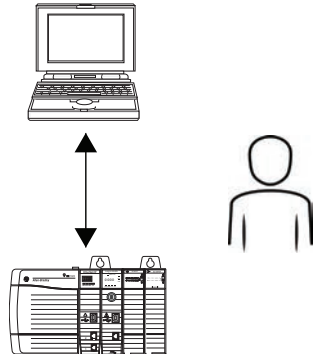
漏洞和漏洞利用

默认情况下，IACS 通信协议是专有且不安全的。其缺乏身份验证、完整性和保密性等安全属性。因此，数据和端点处于危险之中。这些安全属性是 IACS 设备保护自身免受网络攻击所必要的。

不安全的通信协议可被利用，从而使任何人都可访问并收集数据，而易受攻击的端点可能成为拒绝服务 (DoS) 和其它类型攻击的开放目标。

当攻击者访问系统时，他们通过多种方法来利用 IACS 通信协议漏洞。

表 1 - 攻击类型

攻击类型	描述	
DoS (未经授权开放访问)	攻击者执行 DoS 攻击，导致 CIP™ 设备无法运行。	
中间人攻击	攻击者窃听传输中的数据以改变 CIP 设备之间的通信。	
监视数据	攻击者监视或查看在 CIP 设备之间交换的敏感或机密数据。	

安全评估

获取安全评估是任何安全实现的起点。评估可为您提供当前安全状态，以及为实现优选可接受风险状态所需的缓解措施。

评估由操作技术 (OT) 和信息技术 (IT) 人员协作开展，旨在最大程度地保护机密性、完整性和可用性，同时不影响功能性与使用性。

执行安全评估分为三步。

1. 执行威胁评估。

威胁评估考察对给定设施 / 场所的一系列威胁，包括自然威胁、犯罪威胁、恐怖主义威胁和意外威胁。根据业务要求，公司应评估每种威胁的可能性。

2. 执行漏洞评估。

漏洞评估旨在确定可利用这些威胁的方法，并就如何解决这些漏洞提出建议。

对于每种漏洞，应该根据被利用的概率或难易程度以及在利用成功时所产生的成本或伤害影响进行评级。这为每种漏洞设定一个风险分数。

3. 执行风险评估。

风险评估对风险分数进行评价，并对每种风险做出反应。应对每种风险采取以下措施之一：

- **缓解** - 缓解风险需要说明采取了哪些措施来防止漏洞被利用。
- **终止** - 终止风险需要说明为防止漏洞被利用而移除或禁用的内容。
- **转移** - 转移风险需要说明为防止或应对漏洞被利用而正在该系统外执行哪些操作。
- **接受** - 接受风险时，需要注明风险接受方。

精确评估威胁和识别漏洞对于了解 IACS 资产风险至关重要。

深度防御架构

工业安全最好作为一个完整的系统在运营中实施。深度防御 (DiD) 方法是安全标准的通用方法。

DiD 安全方法建立了基于各种技术的多层保护机制，包括物理、电子和程序性安全防护措施。

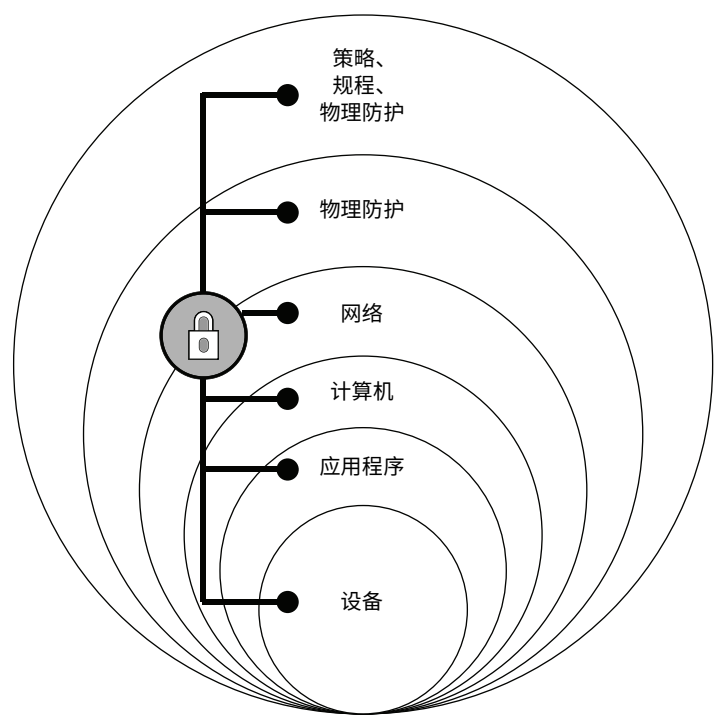
例如，可通过端口锁定限制对托管交换机的物理访问。然后放置边缘工业防火墙，以限制访问和阻止未批准流量。最后，在工业区和企业区之间使用工业非军用区 (IDMZ) 作为周界缓冲区。IDMZ 允许安全数据共享，并且无需直接连接即可执行服务。

以下是 DiD 安全方法的关键原则：

- 多层安全性更具有抗攻击能力
- 每一层都是对上面一层的补充
- 它不能替代系统中对防火墙或其他安全基础架构的需求。

DiD 方法的预期目标是，即使攻击者突破了一层防御，始终会有另一层来阻挡其突破。

图 1 - 深度防御架构



CIP Security 为 ODVA 标准

随着攻击者日趋复杂，网络融合打开了更多通往工业区的潜在门户，连接 CIP 的设备必须具有自我防御能力。

ODVA 意识到需要 CIP 连接设备保护，从而开发了 CIP Security。它是用于 EtherNet/IP 网络的开放式标准安全通信机制。

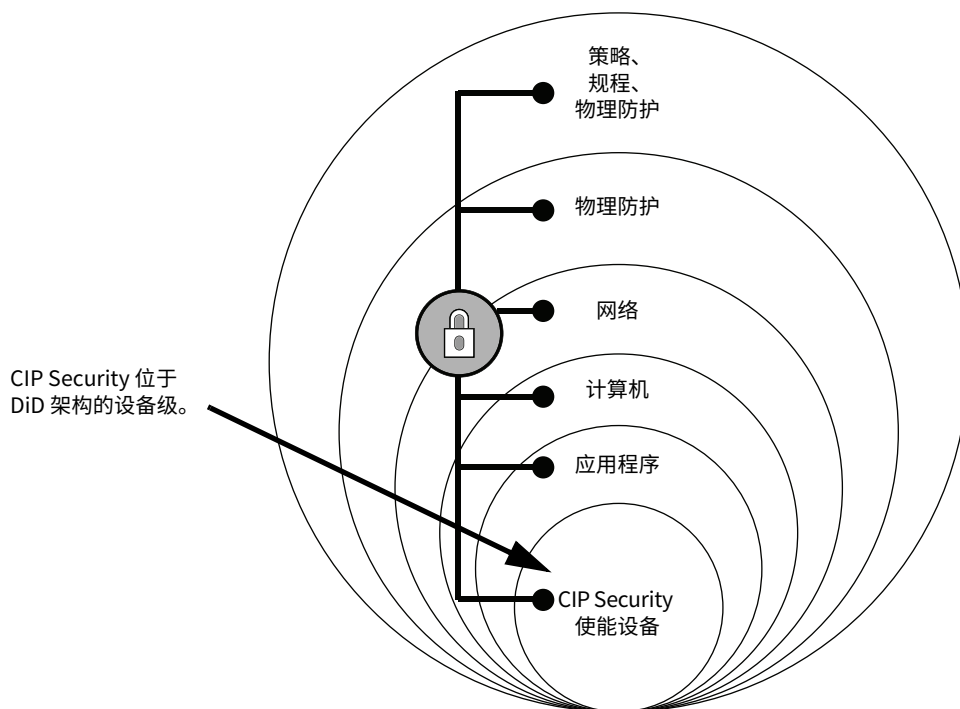
下列 CIP Security 属性是针对安全风险的对策：

- 设备标识和身份验证
- 数据完整性和身份验证
- 数据保密性（加密）

CIP Security 位于 DiD 架构中的设备级，使 CIP 连接设备在收发数据之前相互进行身份验证。设备连接仅限于可信设备。

或者，为了提高设备总体安全状态，可将它与数据完整性相结合，以防止数据包篡改和消息加密，从而避免出现意外数据读取和披露。

图 2 - CIP Security 作为深度防御架构的一部分



设备标识 / 身份验证

在设备开始通信之前，每台设备都必须能够验证其想要与之通信的设备是否真实。这样可以保护合法设备，防止非法设备伪装成系统组件来获取系统访问权限。

要构建此端点信任，可使用证书或预共享（密文）密钥为设备提供标识：

- **证书**用于基于 X.509v3 标准提供标识。

证书是通信各方与所谓证书颁发机构 (CA) 的公共实体之间达成的协议。可信的 CA 向申请人签发证书，以证明其身份。当通信各方交换由公共 CA 签名的证书时，可建立互信。

FactoryTalk® System Services 是证书颁发机构。该服务签发证书以保证通信方的真实性。

使用证书的好处之一是，证书提供更高级安全，而非预共享密钥。

- **预共享密钥**用于验证基于通信各方之间预先共享的密钥的标识。

预共享密钥是两个实体之间就确定标识和身份验证的参数达成的协议。这些实体是相互通信的设备。

使用预共享密钥的优点之一是，在建立连接时对性能的影响较小。

重要信息 设备只能使用一个预共享密钥，因此，在配置有预共享密钥的任何区域之间所需的任何导管都必须使用可信 IP 创建。

安全数据传输

CIP Security 基于传输层安全 (TLS) (RFC 5246) 和数据包传输层安全 (DTLS) (RFC 6347) 协议，用于在传输过程中保护 EtherNet/IP 数据。

TLS 和 DTLS 是网络协议，用于促进发起方和目标设备之间私下安全地进行数据传送。

TLS 提供以下安全属性：

- **身份验证** - 允许每台设备通过证书交换或预共享密钥确认其身份
- **完整性** - 确保数据在传输期间没有被篡改或伪造，且数据使用基于 TLS 散列的消息验证代码 (HMAC)
- **保密性** - 在发起方和目标设备之间传输数据时加密数据。加密数据可防止未经授权方读取数据。

DTLS 基于 TLS，但用于用户数据包协议 (UDP) 连接，而非传输控制协议 (TCP) 连接。

有关安全属性的完整描述，请参见 ODVA 主页：<https://www.odva.org/>。

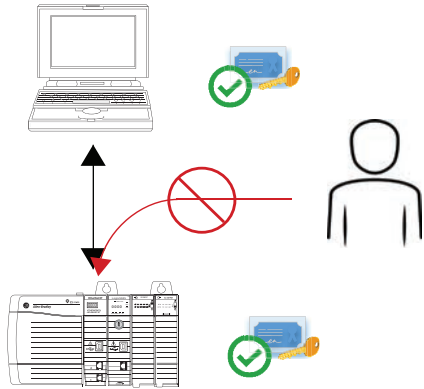
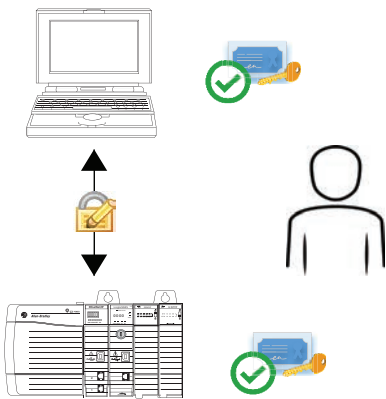
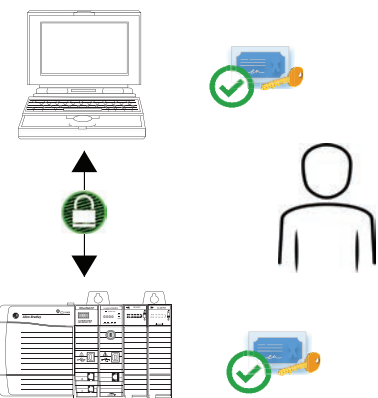
表 2 定义了第 14 页上表 3 的图标。

表 2 - CIP Security 图标

名称	符号	定义
证书		标识的电子表示。证书将身份公钥与其可识别信息绑定在一起，例如，名称、组织、电子邮件、用户名和 / 或设备序列号。 该证书用于验证与区域或设备的连接。当启用 CIP Security 时，默认选中。
预共享密钥		可信实体之间共享的密文，用于表示身份。FactoryTalk Policy Manager 可以创建一个可共享的密钥。
完整性		检查数据是否被更改以及数据是否由可信实体发送。修改和 / 或不可信的数据将被拒绝。
校验标记		该符号用于指示设备之间的通信端点已经过身份验证且可信任。
加密		对消息或信息进行编码，以防止未经授权方读取或查看 EtherNet/IP 数据。

表 3 介绍了安全数据传输如何使 CIP 连接设备帮助保护自身免于恶意通信。

表 3 - CIP Security 属性

CIP Security 属性	描述	
设备标识和身份验证	为设备提供安全标识的方法。可使用下列方法： · 证书（推荐） · 预共享密钥 这些属性共同帮助设备执行以下操作： · 拒绝由不可信设备发送的消息。 · 防止未经授权的设备建立连接。	FactoryTalk® Linx  1756-EN4TR 威胁源起方无法连接到 CIP 连接设备。
数据完整性和身份验证	为 EtherNet/IP 网络通信提供数据完整性和消息身份验证的方法。 让设备可执行以下操作： · 拒绝被篡改的数据。 · 防止篡改或修改通信。	FactoryTalk Linx  1756-EN4TR 攻击者可以查看数据，但无法更改数据。
数据保密性	使用加密对 EtherNet/IP 网络之间交换的消息或信息进行编码的方式。 让设备可执行以下操作： · 防止未经授权方查看 EtherNet/IP 数据。 · 防止监听或数据披露。 重要信息：此安全属性是可选的。一些 IACS 网络通信无需是安全的；通常目标是确保数据完整性和身份验证。 加密通常会影响网络适配器的容量。	FactoryTalk Linx  1756-EN4TR 攻击者无法查看数据。

支持 CIP Security 的罗克韦尔自动化产品

本节介绍在 IACS 中实现 CIP Security™ 的罗克韦尔自动化方法的组成部分和概念。

有关在 IACS 中使用支持 CIP™ Security 的产品所需任务的信息，请参见下表：

- 第 3 章 “[第 31 页的 “CIP Security 实现流程”](#)”
- 第 4 章 “[第 57 页的 “CIP Security 实现示例架构”](#)”
- 出版物 “[第 71 页的 “其他资源”](#)”

软件和硬件

支持 CIP Security 的 Rockwell Automation® 产品列表包括用于定义安全策略的软件和硬件产品，例如，FactoryTalk® Policy Manager 软件和 ControlLogix® 5580 控制器。

CIP Security 软件应用程序

重要信息 从罗克韦尔自动化产品兼容性与下载中心 (PCDC) 下载软件。

要访问 PCDC，请转到 <http://compatibility.rockwellautomation.com/Pages/home.aspx>。

- FactoryTalk® Policy Manager（版本 6.11）和 FactoryTalk System Services（版本 6.11）是 FactoryTalk Services Platform（版本 6.11）的组件。

当安装 FactoryTalk Services Platform（版本 6.11）时，必须从安装向导中选择 Customize，并选中 FactoryTalk Policy Manager 和 FactoryTalk System Services 组件的安装复选框。

有关详细信息，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

- FactoryTalk Policy Manager（版本 6.20 或更高版本）是一个独立安装包。FactoryTalk System Services（版本 6.20 或更高版本）是 FactoryTalk Policy Manager 安装包的一部分。FactoryTalk Services Platform（版本 6.20 或更高版本）不包括 FactoryTalk Policy Manager 或 FactoryTalk System Services。
- 在从版本 6.11 升级到版本 6.20 或更高版本之前，建议您访问罗克韦尔自动化知识库（网址：<https://rockwellautomation.custhelp.com/app/home>），阅读以下文章：
 - 备份和恢复 FactoryTalk Policy Manager 和 FactoryTalk System Services 的 CIP Security 模型，请单击[此处](#)
 - 未能通过 CIP Security 策略模型升级现有 FactoryTalk System Service 数据，请单击[此处](#)
 - 下载和安装 FactoryTalk Policy Manager，请单击[此处](#)

建议您使用最新版 FactoryTalk Policy Manager。

软件应用程序	描述	所需最低版本
FactoryTalk Policy Manager	FactoryTalk Policy Manager 是一种安全软件应用程序，用于配置、部署和查看系统通信安全策略。 安全策略分为不同的组件，即设备、区域和导管。可以使用这些组件设计安全模型，从而控制系统内设备的权限和使用情况。有关安全模型以及如何使用组件设计这些模型的更多信息，请参见第 18 页。 安全策略将一次性分配给设备。无需在设备级进行更改，否则如果出现人为失误，可能导致设备之间配置不一致的风险。	版本 6.11
FactoryTalk System Services	FactoryTalk System Services 是安全的 EtherNet/IP™ 客户端，在后台运行，用于部署在 FactoryTalk Policy Manager 中配置的安全策略。不得在客户端执行操作。 FactoryTalk System Services 在 FactoryTalk Directory 中提供以下内容，以强制实施基于 ODVA CIP Security 标准的安全策略： · 标识 / 身份认证服务 - 对用户进行身份验证并验证用户资源请求。根据 FactoryTalk Directory 和 FactoryTalk Security 策略设置验证用户凭证，以获取与用户相关联的特权。 · 证书服务 - 为 FactoryTalk Policy Manager 模型中的设备签发和管理证书。 · 部署服务 - 将安全策略转换为发送至端点的 CIP™ 配置。 · 策略服务 - 构建和管理 CIP 网络信任模型并定义 CIP 端点的安全策略。 · 诊断服务 - 提供 FactoryTalk 审计和诊断日志作为 Web 服务。	版本 6.11
FactoryTalk Linx	FactoryTalk Linx 是安全的 EtherNet/IP 客户端，通过 CIP Security 使设备在安全的 EtherNet/IP 网络上发起连接。 该服务器和通信服务允许设备与 FactoryTalk 软件系列产品和 Studio5000 Logix Designer 应用程序通信。 重要信息：不能使用 RSLinx® Classic 软件在 IACS 中实现 CIP Security。	版本 6.11
Studio 5000 Logix Designer®	Logix Designer 应用程序是一种与 Logix 5000™ 控制器配合使用的综合编程软件。在实现 CIP Security 的系统中，该软件与 ControlLogix 5580 控制器以及在同一机架中使用 1756 - EN4TR 通信模块的 ControlLogix 5570 或 5580 控制器配合使用。 重要信息：CIP Security 的实现无需 Logix Designer 应用程序。 但是，Logix Designer 应用程序用作支持 CIP Security 的软件，因为它支持 CIP 协议，并且使用 FactoryTalk Linx 软件通过 CIP 协议与其他设备通信。	版本 31.00.00 使用 ControlLogix 5570 或 5580 控制器和版本 31 实现 CIP Security 时，必须在机架中使用 1756 - EN4TR 通信模块。 要通过 ControlLogix 5580 控制器实现 CIP Security 并避免使用 1756-EN4TR 通信模块，必须使用版本 32.00.00 或更高版本。

支持 CIP Security 的硬件设备

以下硬件设备支持 CIP Security。

重要信息 下表列出了本出版物发布时支持 CIP Security 的产品。随着时间推移，将发布支持 CIP Security 的新产品。未来将发布现有不支持 CIP Security 的产品的新版本，使其能够支持 CIP Security。要查看产品是否支持 CIP Security，请参见产品文档。

硬件产品	描述	所需的最低固件版本
ControlLogix 5580 控制器	ControlLogix 5580 控制器使用公共 Logix 控制引擎和公共开发环境来控制大型控制系统。 控制器可与本地和远程设备进行通信，并可控制这些设备。例如，设备可以是 I/O 模块、网络通信模块、驱动器和操作员界面。 可使用 Logix Designer 应用程序配置 ControlLogix 5580 控制器。Logix Designer 应用程序版本必须与控制器上的固件版本兼容。 重要信息：不得使用 Logix Designer 应用程序来定义安全策略。应使用 FactoryTalk Policy Manager 来定义安全策略。	固件版本 31.011 如果使用版本 31.xxx，则控制器机架中还必须包含 1756-EN4TR 通信模块。 要通过 ControlLogix 5580 控制器实现 CIP Security 并避免使用 1756-EN4TR 通信模块，必须使用固件版本 32.011 或更高版本。
1756-EN4TR ControlLogix EtherNet/IP 通信模块	1756-EN4TR 通信模块执行以下功能： · 促进 ControlLogix 5580 控制器与 EtherNet/IP 网络上的设备之间的高速数据传输。 · 将 Logix 5000 控制系统连接到多个 EtherNet/IP 网络拓扑。	任意
Kinetix® 5300 驱动器	Kinetix 5300 驱动器是基于 EtherNet/IP 伺服驱动器的入门级集成运动驱动器，专为各种运动控制应用的中小型机器而设计。	固件版本 13.003
Kinetix 5700 驱动器	Kinetix 5700 驱动器是单轴和双轴逆变器，可用于将基于 EtherNet/IP 的集成运动控制扩展到轴计数和功率要求较高的大型定制机器。 驱动器具有内置双以太网端口，可将驱动器直接连接到 EtherNet/IP 网络。	固件版本 11.001
PowerFlex 755T 变频器	PowerFlex 755T 变频器、母线电源和公共母线逆变器提供公共母线、再生和高性能变频电机控制 10...6000 Hp。 PowerFlex 755T 变频器具有内置双以太网端口，可将变频器直接连接到 EtherNet/IP 网络。CIP Security 需要使用 PowerFlex 755T 主控制板上提供的内置双 EtherNet/IP 端口。该功能与网络选项卡不兼容。	固件版本 10.001
1783-CSP CIP Security Proxy	1783-CSP Proxy 是一种独立设备，可将不支持 CIP™ Security 的设备，也称为代理设备，连接到已启用 CIP Security 的 IACS。	任意

使用罗克韦尔自动化产品的优势

使用罗克韦尔自动化产品来实现 CIP Security 具有以下优势：

- **集中系统管理** - 使用 FactoryTalk Policy Manager 软件可一次性轻松创建和部署多个设备的安全策略。
- **微分段** - 将自动化应用程序分割成更小的单元 / 区域，从而降低攻击面。
- **HTTP 端口** - 在配置了 CIP Security 的系统中，可启用或禁用设备的非安全 (HTTP) 端口 / 协议。
- **既有系统支持** - 以下选项可用于在部署 CIP Security 功能的特定非安全通信网络中不支持 CIP Security 的产品：
 - **使用 1783-CSP CIP Security Proxy** 将不支持 CIP Security 的设备连接到已启用 CIP Security™ 的 IACS。
 - 使用新的 1756-EN4TR 通信模块**改装基于 ControlLogix 5570 的系统**。
 - **允许** - 根据 IP 地址授权特定通信。



在 FactoryTalk Policy Manager 中，导管的 **Authentication Method** 属性使用 Trusted IP 表示允许。

重要信息 确保在使用之前已了解允许安全措施的限制。

CIP Security 属性

CIP Security 由安全配置文件、属性和组件组成。这些关键机制有助于实现您尝试保护的资源的安全要求。

安全配置文件和属性

CIP Security 定义了安全配置文件的概念。安全配置文件是一组定义清晰的功能，用于促进设备互操作性和最终用户选择具有适当安全功能的设备。安全配置文件描述了给定设备支持的安全功能。设备根据其安全配置文件执行安全策略。

鉴于安全是一种平衡状态，而且并非所有 CIP 连接设备都需要相同的安全级别，因此 FactoryTalk Policy Manager 允许管理员在创建安全配置文件时仅启用所需的属性。

在启用 Data Integrity 和 Data Confidentiality 选项之前，必须先启用 Device Identity/Authentication 属性。

支持 CIP Security 的罗克韦尔自动化产品支持以下安全属性：

属性	描述
设备标识和身份验证	证书基于 X.509 v3 标准，用于提供标识。 预共享密钥是在提供标识的可信实体之间共享的密钥。 TLS 协议便于相互身份验证，从而创建可信的端点。
数据完整性	密钥散列消息认证码 (HMAC) 用作加密方法，为 EtherNet/IP 通信提供数据完整性和消息真实性。
数据保密性	数据加密用于对消息或信息进行编码，以防止未授权方读取或查看 EtherNet/IP 数据。

重要信息 本节的其余部分介绍了每个组件，对于区域和导管，还介绍了创建和配置组件的步骤。但是，相关描述并非详尽无遗。
有关安全模型的更多详细信息，包括配置它们时必须完成的任务，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

CIP Security 组件

FactoryTalk Policy Manager 将系统安全策略划分为不同的组件。以下组件用于设计安全模型：

- [设备](#)
- [区域](#)
- [导管](#)

设备

设备是共同创建 IACS 网络的模块、驱动器、控制器、HMI 面板、计算机和服务器。将共享特定功能安全要求的设备添加到同一区域。

在 IACS 网络中使用设备时，考虑安全模型中的设备：

- 当前支持 CIP Security 的罗克韦尔自动化产品列表请参见[第 15 页](#)和[第 17 页](#)。

更多支持 CIP Security 的罗克韦尔自动化产品正在开发中。

- 因为设备支持 CIP Security，所以无需在位于 IACS 网络中的该设备上启用 CIP Security。
- 可以在包含 CIP Security 使能设备的 IACS 中使用不支持 CIP Security 的设备。

区域

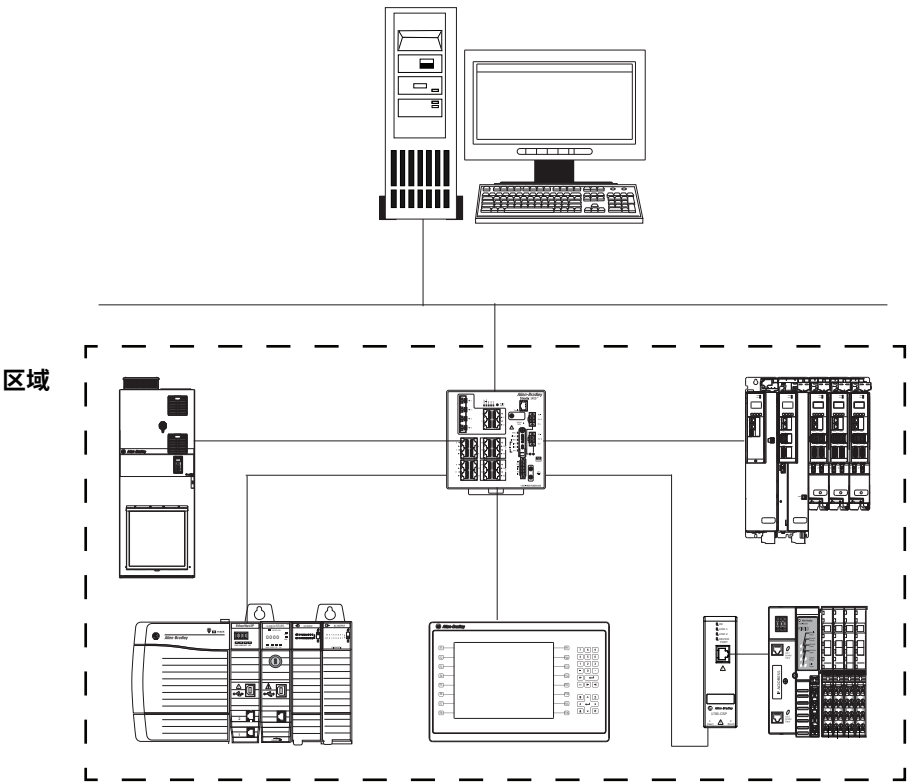
区域是向其添加设备的组。区域将建立有关数据完整性、数据隐私以及验证可信设备的身份验证方法的规则。

- 一个系统中可有多个区域，并且逐个区域设置安全策略。通过使用区域，可简化系统中大型设备组的管理。
- 区域可包括支持 CIP Security 的设备和不支持 CIP Security 的设备。一个 IACS 网络中可能有多个区域，但一个设备只能属于一个区域。
- 将支持 CIP Security 的设备添加到某个区域后，设备将使用该区域的策略设置。

同一区域内设备之间的通信是隐式的，而且是相互信任的。因此，无需在同一区域中的设备之间创建导管。

图 3 示出了包括支持 CIP Security 的设备的区域，例如 ControlLogix 5580 控制器，以及不支持 CIP Security 的设备，例如 PanelView™ Plus 终端。

图 3 - 安全模型 - 区域



导管

导管在区域外创建可信的通信路径。必须至少有两个端点，即区域或设备，才能创建导管。

导管通过以下方式促进安全通信：

- 区域至区域
- 设备至设备
- 设备至区域

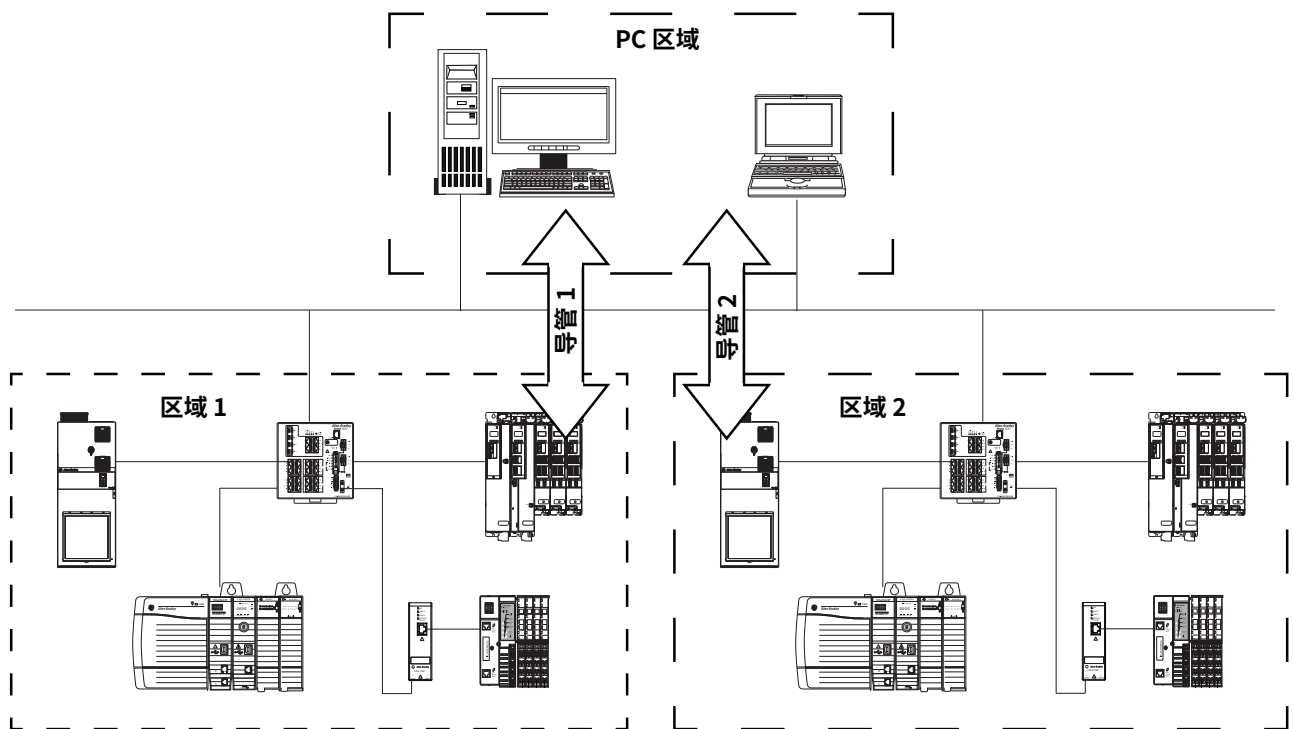
导管允许您使用以下方法配置各个区域以外的信任：

- 可信 IP 身份验证方法 - 根据资产 IP 地址为其分配信任关系。这也称为 Allowing。
- 证书身份验证方法 - 使用来自可信机构的证书建立设备标识。

重要信息 当前，设备无法使用多个预共享密钥。
如果需要在配置了预共享密钥的区域和其他区域之间进行通信，则必须将使用可信 IP 身份验证方法的导管配置为其他区域。

图 4 示出了多区域系统中的导管。

图 4 - 安全模型 - 导管



安全模型

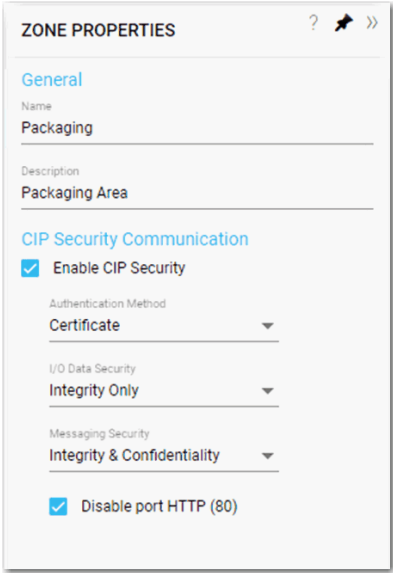
安全模型是 FactoryTalk Policy Manager 软件中完整配置的区域、设备和导管实例，以及其各自的 CIP Security 属性。区域和导管构成安全模型。安全模型通过各个设备的安全配置文件部署至 IACS 中的设备。

 如果多个设备使用相同的安全策略且位于同一区域，我们建议您在区域级配置安全策略。在区域级配置安全策略的优点在于，可一次性配置策略并将其应用于多个设备。此方法避免了本应使用相同策略的设备之间使用不同安全策略的可能性。

区域属性

表 4 列出了配置区域属性时可用的可配置字段。

表 4 - 区域安全属性

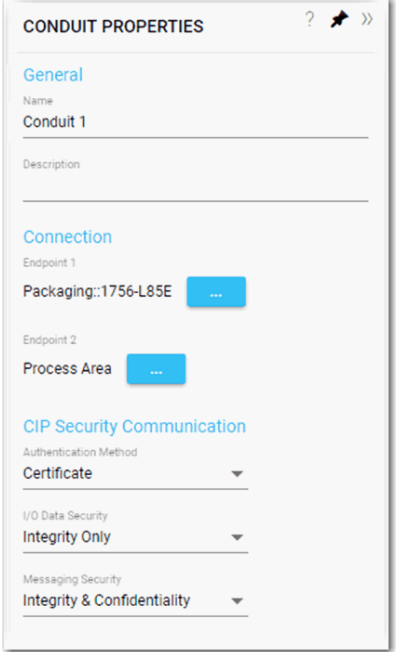
属性	可用选项	FactoryTalk Policy Manager 画面示例
Name	用户自定义	
Description	用户自定义	
Enable/Disable CIP Security	· Enable · Disable	
Authentication Method	· Certificate · Pre-Shared Key	
I/O Data Security	· None · Integrity Only · Integrity + Confidentiality	
Messaging Security	· Integrity Only · Integrity + Confidentiality	
Disable Ports - HTTP (80)	· Enable · Disable	

重要信息 有关区域属性的更多信息，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

导管属性

表 5 列出了配置导管安全策略时可用的可配置字段。

表 5 - 导管安全属性

属性	可用选项	FactoryTalk Policy Manager 画面示例
Name	用户自定义	
Description	用户自定义	
Connection 根据每个端点的分配方式，可以是以下任意一种： · 设备至设备 · 设备至区域 · 区域至区域	- Endpoint 1 (设备或区域) - Endpoint 2 (设备或区域)	
Authentication Method	- Trusted IP - Certificate	
I/O Data Security	- None - Integrity Only - Integrity + Confidentiality	
Messaging Security	- Integrity Only - Integrity + Confidentiality	

重要信息 有关 Conduit Properties 的更多信息，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

限制和注意事项

以下是罗克韦尔自动化在 IACS 中实现 CIP Security 的解决方案的限制和注意事项：

- [双端口设备](#)
- [如果 ControlLogix 5580 控制器处于工作模式，则初始安全模型部署失败](#)
- [无法从非安全工作站下载到 ControlLogix 5580 控制器](#)
- [如果安全配置文件不匹配，则工作站无法连接到安全的 ControlLogix 5580 控制器](#)
- [CIP 桥接](#)
- [网络地址转换](#)
- [使用多播连接](#)
- [自动设备更换](#)
- [RSLinx Classic 软件](#)

双端口设备

一些支持 CIP Security 的产品具有双内置以太网端口。在这些设备上，两个物理以太网端口共用一个 IP 地址。

可根据 IP 地址而非物理端口配置 CIP Security。在具有双内置以太网端口且支持 CIP Security 的设备上，将哪个物理端口连接到网络并不重要。部署安全模型时，安全策略适用于任一端口，具体取决于连接到网络的端口。

例如，1756-EN4TR 通信模块具有双内置以太网端口，共用一个 IP 地址。为模块配置 CIP Security 后，端口 1 或端口 2 可以物理连接到网络，安全策略仍然适用。

在具有支持 CIP Security 的双内置以太网端口的设备上，**不能**为该设备上的不同以太网端口配置**单独**的安全策略。

重要信息	某些具有双内置以太网端口的罗克韦尔自动化产品允许为每个端口配置单独的 IP 地址，例如，CompactLogix™ 5380 控制器。但是，这些产品目前并非支持 CIP Security 的设备。
-------------	--

如果 ControlLogix 5580 控制器处于工作模式，则初始安全模型部署失败

如果 ControlLogix 5580 控制器处于运行模式，即钥匙开关处于 RUN 位置，当第一次尝试在 FactoryTalk Policy Manager 软件中部署安全模型时，部署将会失败。如果控制器处于远程运行、远程编程或编程模式，则初始安全模型部署成功。

重要信息	该设计限制可保护控制器免受攻击者的 DoS 攻击。 资产所有者是唯一可对控制器进行物理访问的一方。确认控制器模式为远程运行、远程编程或编程，以便成功进行初始安全部署。如有需要，可在初始部署和未来安全模型部署成功后将控制器更改为运行模式。
-------------	---

在 ControlLogix 5580 控制器具有安全配置文件后，控制器模式不会影响将来的安全模型部署。

无法从非安全工作站下载到 ControlLogix 5580 控制器

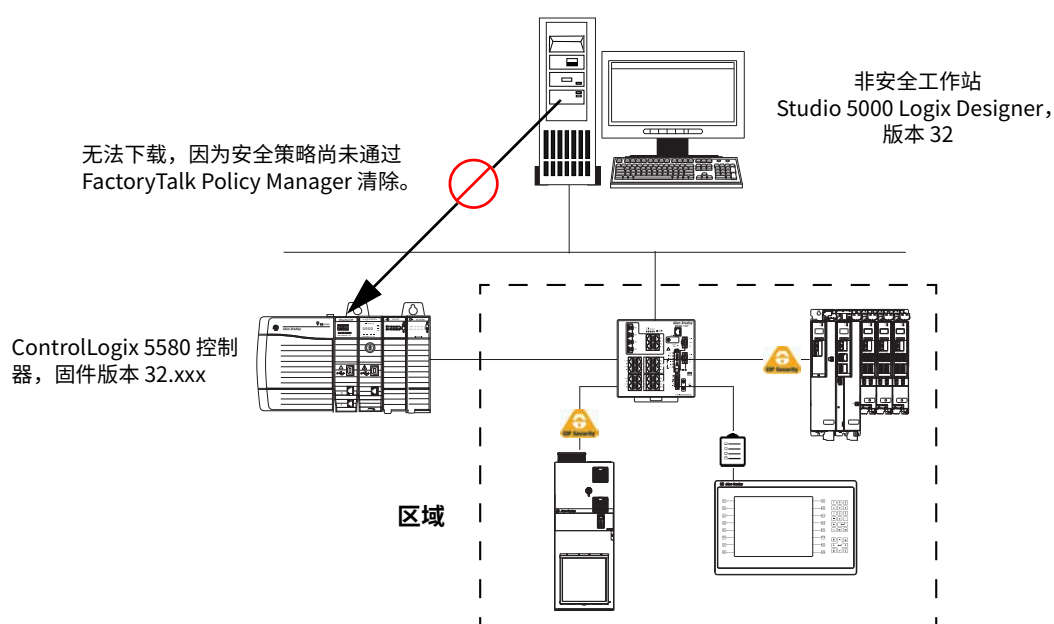
该限制仅在下列情况下存在：

- FactoryTalk Policy Manager, 版本 6.11
- FactoryTalk System Services, 版本 6.11
- Logix Designer 应用程序, 版本 32
- ControlLogix 5580 控制器, 固件版本 32.xxx



为避免此限制，请将上面列出的软件和控制器固件分别升级到下一主要版本和修订版。

在 ControlLogix 5580 控制器中启用 CIP Security 后，如果将 Logix Designer 应用程序项目从该区域删除，则无法将项目下载到控制器，除非先将控制器复位为出厂默认设置。

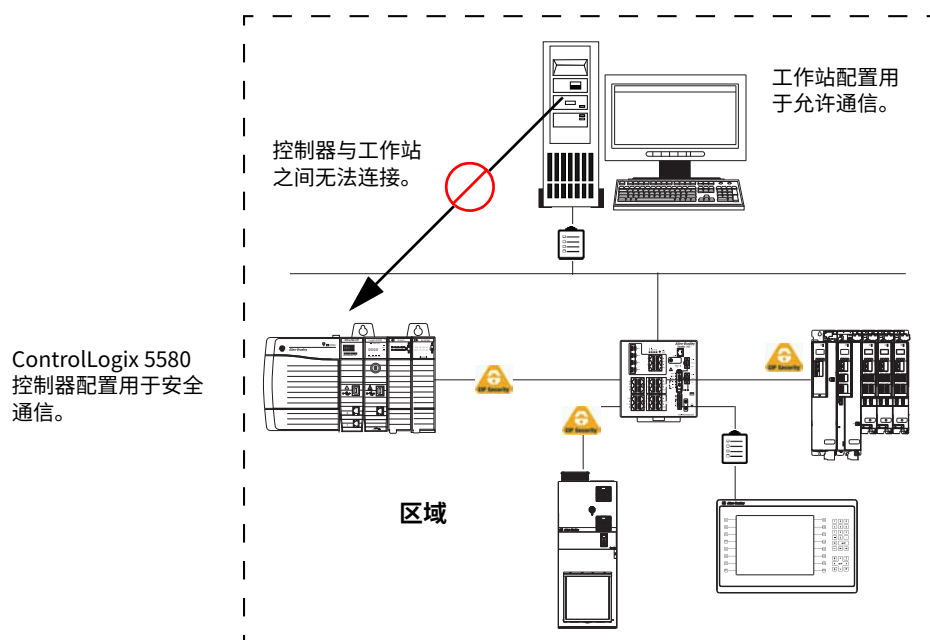


如果安全配置文件不匹配，则工作站无法连接到安全的 ControlLogix 5580 控制器

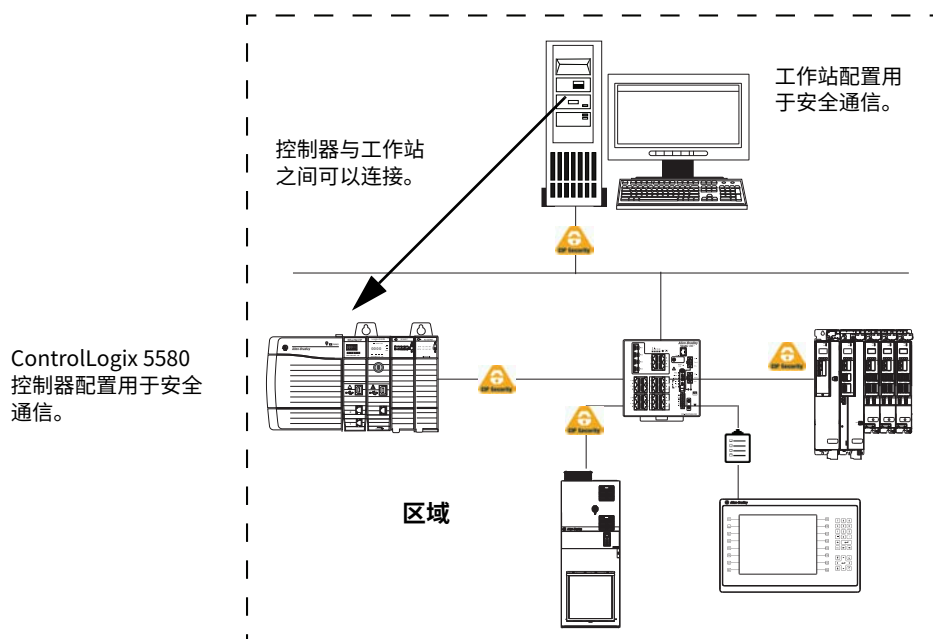
运行 Logix Designer 应用程序且配置用于允许通信的工作站，即 Authentication Method = Trusted IP，无法连接到配置用于安全通信的 ControlLogix 5580 控制器，即使用 Authentication Method = Certificate 或 Authentication Method = Pre-shared Key (PSK)。

重要信息 请注意以下几点：

- 该设计限制强制实施高安全标准来保护控制器，因为控制器是 IACS 中最宝贵的资产。
- 以下示例显示了位于同一区域的 ControlLogix 5580 控制器和工作站。无论控制器和工作站位于同一区域还是通过导管连接的单独区域，该限制都适用。



为避免此限制，请更新工作站安全配置文件以使用安全通信。

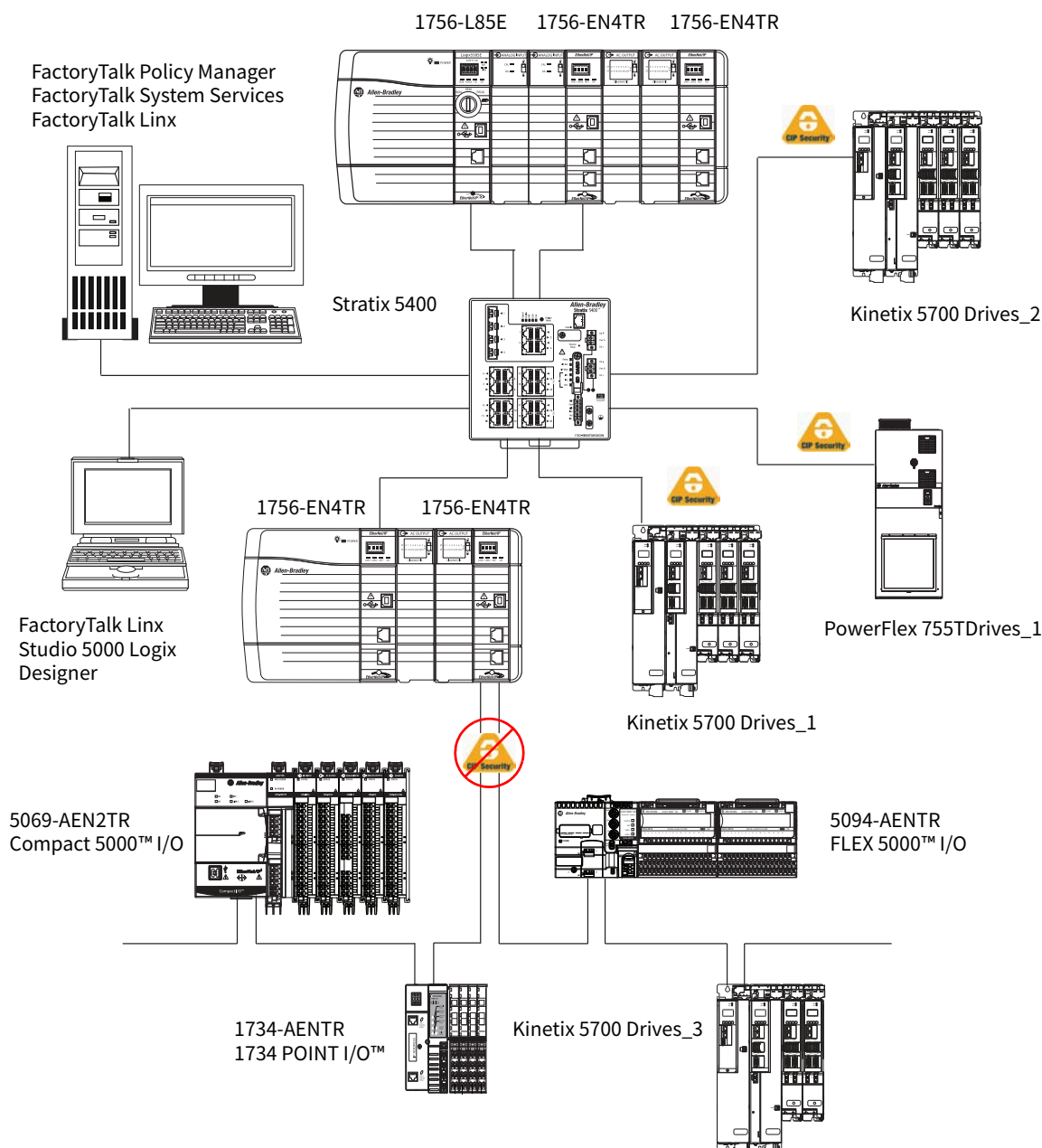


CIP 桥接

无法通过 CIP 网桥配置 CIP Security。例如，在下图中，可将 Kinetix 5700 Drives_1 和 Kinetix 5700 Drives_2 配置为 CIP Security，因为 Stratix® 5400 交换机是透明的。

无法为 CIP Security 配置 Kinetix 5700 Drive_3，因为它可通过 1756-EN4TR 通信模块、ControlLogix 背板以及其它 1756-EN4TR 通信模块访问。背板是通信模块之间的一个网桥。

也无法在线性网络上配置连接到 ControlLogix 下部机架插槽 3 中的 1756-EN4TR 通信模块的任何设备。

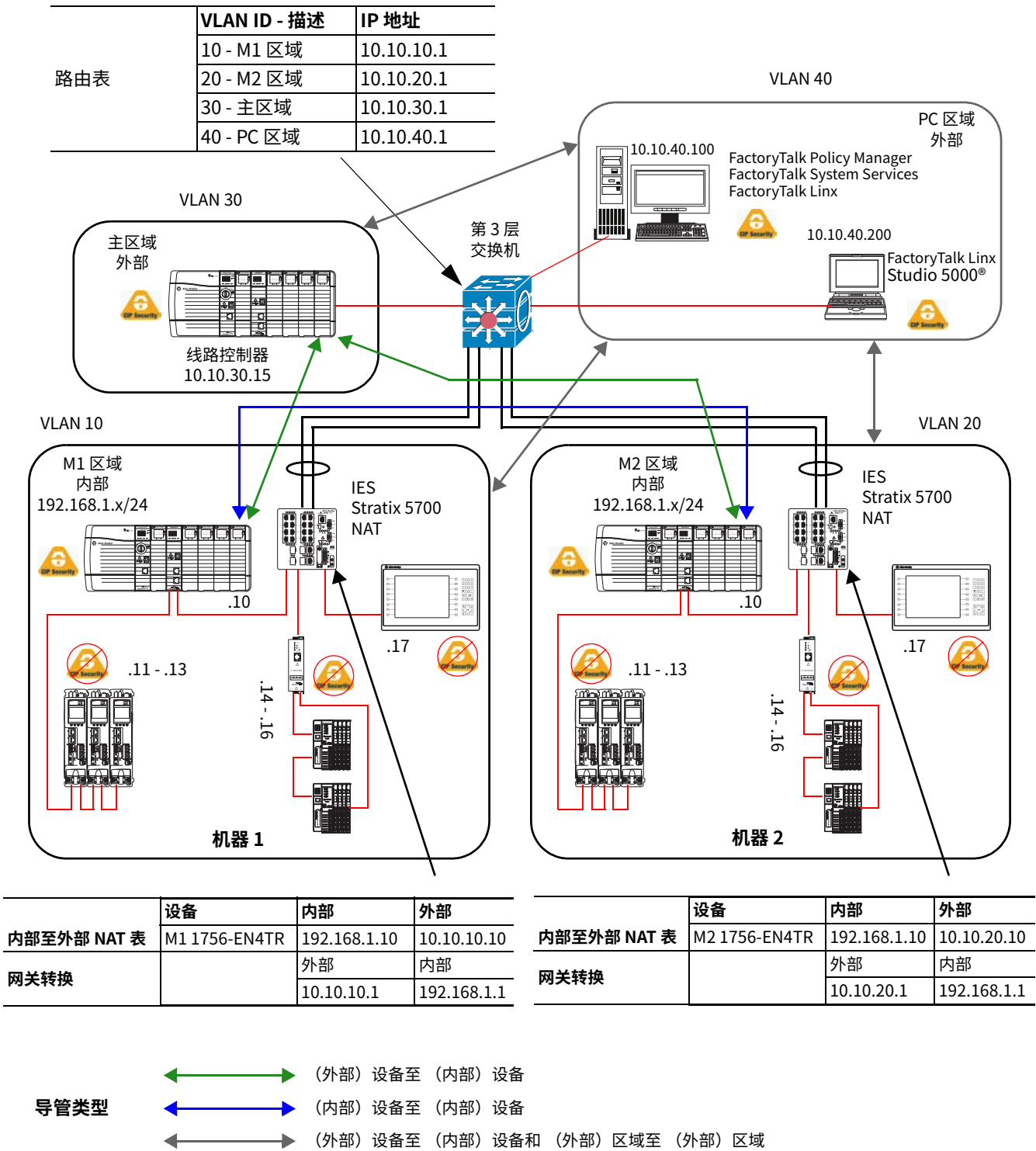


网络地址转换

只有当具有 FactoryTalk Policy Manager 的计算机 / 服务器能够通过 IP 地址访问 CIP Security 端点时，CIP Security 才支持网络地址转换 (NAT)。即，NAT 后方的设备具有可从外部设备访问的 IP 地址。

在本例中，M1 区（机器 1）中的 1756-EN4TR 可使用 CIP Security，因为执行 NAT 的 Stratix 5700 交换机包含 1756-EN4TR 的 NAT 转换和网关转换。当在网络中正确配置了带路由的 NAT 时，带有 FactoryTalk Policy Manager 的外部计算机 / 服务器可通过 Stratix 5700 交换机中配置的外部转换 IP 地址访问 CIP Security 端点。

在应用任何 CIP Security 实现之前，必须正确配置 NAT。有关详细信息，请参见 Deploying Network Address Translation within a CPwE Architecture Design and Implementation Guide，出版号：[ENET-TD007](#)。



使用多播连接

当前，**无法**将多播连接用于 CIP Security。因此，无法在 ControlLogix 冗余系统中使用 CIP Security。

自动设备更换

当前，**无法**使用自动设备更换 (ADR) 来更换使用 CIP Security 的 IACS 中的设备。如果更换设备，则必须手动重新部署安全模型。

重要信息	当使用 1783-CSP Proxy 将代理设备连接到使用 CIP Security 的 IACS 时，此限制不适用。如果将连接到 1783-CSP Proxy 的代理设备更换为相同设备，即相同的设备类型、产品目录号、固件版本和 IP 地址，则无需重新部署安全模型。有关如何在已实现 CIP Security 的 IACS 中使用 1783-CSP Proxy 的更多信息，请参见 CIP Security Proxy User Manual，出版号： 1783-UM013 。
-------------	---

RSLinux Classic 软件

无法使用 RSLinx® Classic 软件在 IACS 中实现 CIP Security。必须使用 FactoryTalk Linx 版本 6.11 或更高版本。

注：

CIP Security 实现流程

本节介绍在简单 IACS 中 Rockwell Automation® 产品实现 CIP Security™ 的整体流程。

有关更复杂的 IACS 的信息，请参见第 57 页的“CIP Security 实现示例架构”。

可使用安全评估流程为区域和导管分配安全级别。建议您根据在该区域中实现攻击目标时可能产生的后果来分配区域和导管安全级别。

有关详细信息，请参见第 9 页的“安全评估”。

设计和安装系统

必须在特定计算机上安装软件，并将硬件设备连接到 EtherNet/IP™ 网络。

重要信息 从罗克韦尔自动化产品兼容性与下载中心 (PCDC) 下载软件。

要访问 PCDC，请转到 <http://compatibility.rockwellautomation.com/Pages/home.aspx>。

- FactoryTalk® Policy Manager（版本 6.11）和 FactoryTalk System Services（版本 6.11）是 FactoryTalk Services Platform（版本 6.11）的组件。

当安装 FactoryTalk Services Platform（版本 6.11）时，必须从安装向导中选择 Customize，并选中 FactoryTalk Policy Manager 和 FactoryTalk System Services 组件的安装复选框。

有关详细信息，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

- FactoryTalk Policy Manager（版本 6.20 或更高版本）是一个独立安装包。FactoryTalk System Services（版本 6.20 或更高版本）是 FactoryTalk Policy Manager 安装包的一部分。FactoryTalk Services Platform（版本 6.20 或更高版本）不包括 FactoryTalk Policy Manager 或 FactoryTalk System Services。

- 在从版本 6.11 升级到版本 6.20 或更高版本之前，建议您访问罗克韦尔自动化知识库（网址：<https://rockwellautomation.custhelp.com/app/home>），阅读以下文章：

- 备份和恢复 FactoryTalk Policy Manager 和 FactoryTalk System Services 的 CIP Security 模型，请单击[此处](#)
- 未能通过 CIP Security 策略模型升级现有 FactoryTalk System Service 数据，请单击[此处](#)
- 下载和安装 FactoryTalk Policy Manager，请单击[此处](#)

建议您使用最新版 FactoryTalk Policy Manager。

IACS 设计至少应包含以下信息：

- 验证在 IACS 网络中实现 CIP Security 所需的系统组件。
- 现有设备和软件清单，包括固件版本。
- 详细观察并记录预期系统功能和操作。
- 详细观察并记录设备之间所需的数据流。

请记住，系统可包括支持或不支持 CIP™ Security 的产品。罗克韦尔自动化当前提供的支持 CIP Security 的产品列表如下所示：

- [第 15 页的“CIP Security 软件应用程序”](#)
- [第 17 页的“支持 CIP Security 的硬件设备”](#)

重要信息

在实现 CIP Security 之前，确认系统中所有设备的安装、配置和操作均按预期进行。例如，根据需要更新固件版本，使用设备配置 Logix Designer 应用程序项目，并将项目下载到设备。

识别、组织和创建区域

区域是向其添加设备的组。可将共享特定功能安全要求并相互信任的设备添加到同一区域。

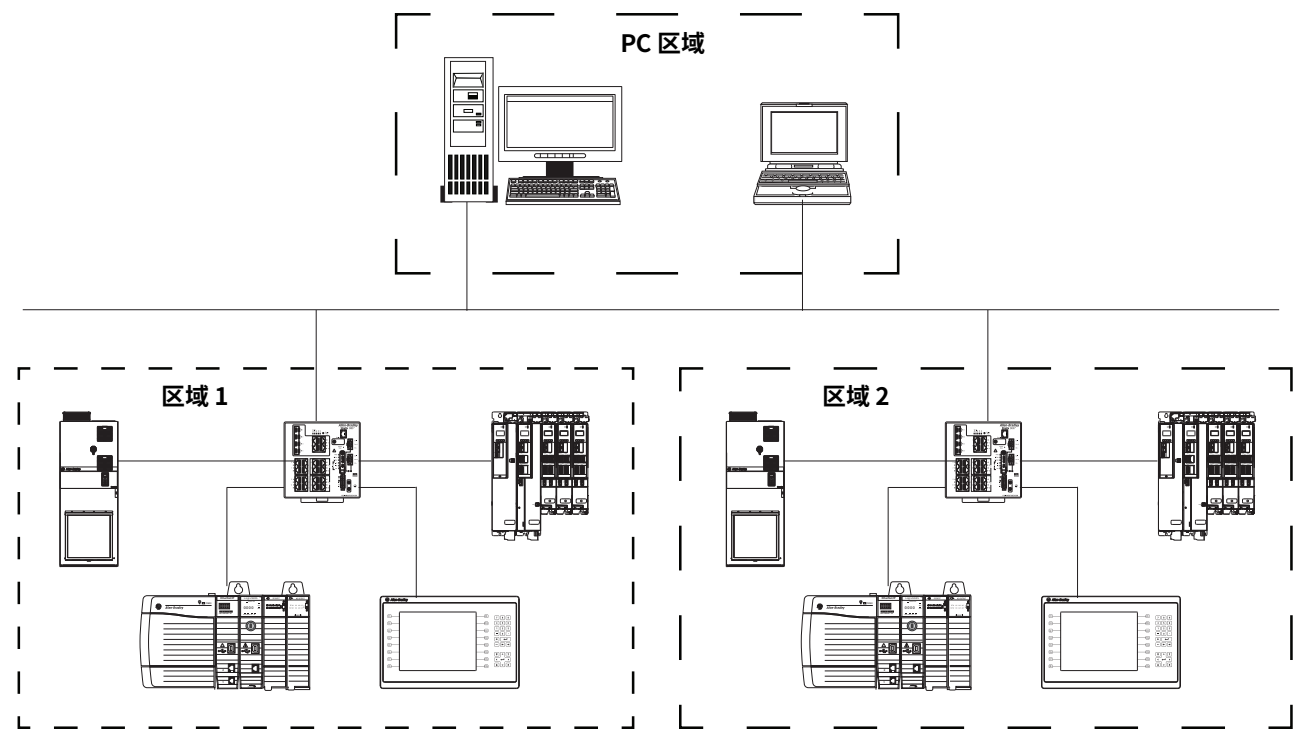
将设备添加到区域后，设备之间进行隐式通信，同时通过交换证书或预共享密钥建立互信。值得注意的是，在被视为“可信”的区域中，任何设备均只能被同一区域中的其他设备信任，而非被 IACS 中的所有设备信任。

例如，如果将 ControlLogix® 5580 控制器和 Kinetix® 5700 驱动器添加到区域 1 并且完整使用证书，则设备通过相互交换证书进行验证。

对于与支持 CIP Security 的设备处于同一区域但不支持 CIP Security 的设备，可以通过标准 44818 TCP 连接和 2222 UDP 连接进行通信。因此，无需在不支持 CIP Security 的设备之间创建允许列表。

可创建区域并添加不使用 FactoryTalk Linx 软件但仍需与 IACS 设备通信的其他计算机 / 服务器。不使用 FactoryTalk Linx 的设备被添加为通用设备。这样便可轻松在计算机 / 服务器与 IACS 设备之间创建 Trusted IP 导管。

图 5 - 系统实现 - 区域



识别并组织区域后，创建一个详细的安全矩阵，其中列出占据各区域的设备。

表 6 是包含区域和设备的安全矩阵。

表 6 - 安全矩阵 - 区域和设备

PC 区域	区域 1	区域 2
FactoryTalk Linx ⁽¹⁾ FactoryTalk Policy Manager FactoryTalk System Services	ControlLogix® 5580 控制器	ControlLogix 5580 控制器
Studio 5000 Logix Designer ⁽²⁾ FactoryTalk View	1756-EN4TR EtherNet/IP 通信模块	1756-EN4TR EtherNet/IP 通信模块
	Kinetix 5700 伺服驱动器	Kinetix 5700 伺服驱动器
	PowerFlex® 755T 变频器	PowerFlex 755T 变频器
	PanelView™ Plus 终端 ⁽³⁾	PanelView Plus 终端 ⁽³⁾

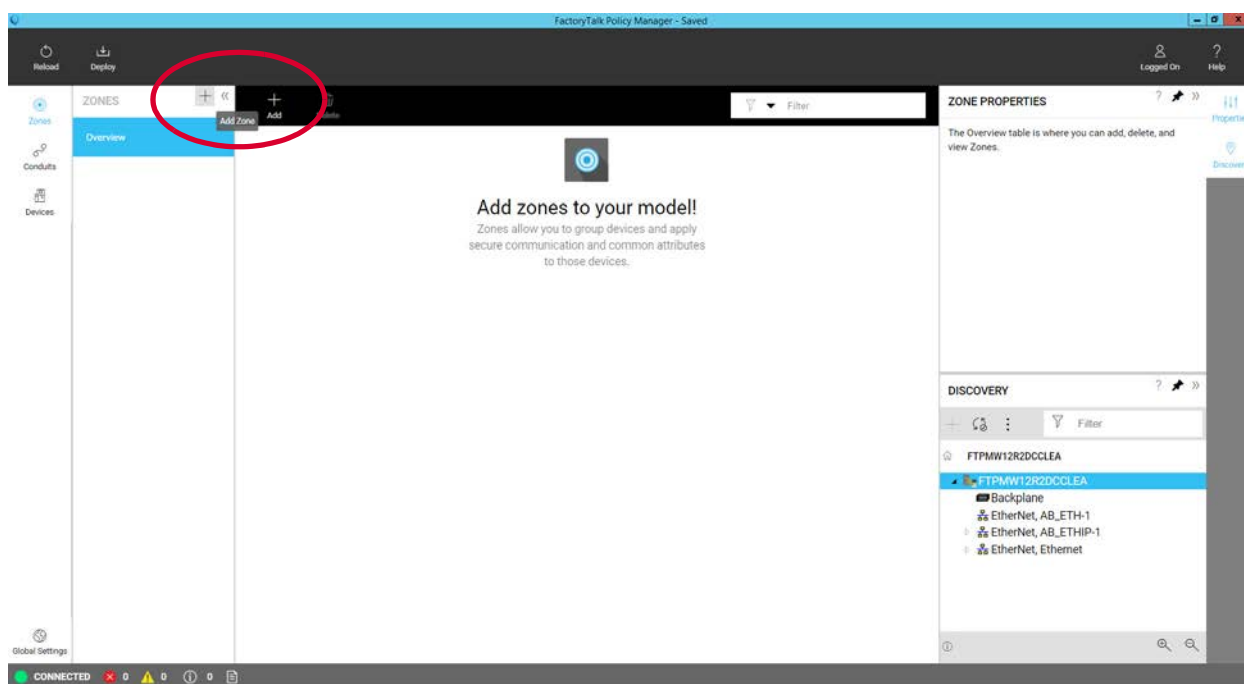
(1) 该组软件安装在同一台服务器 / 计算机上。

(2) 该软件安装在 FactoryTalk Linx、FactoryTalk Policy Manager 和 FactoryTalk System Services 之外的单独计算机上。

(3) 该设备不支持 CIP Security。

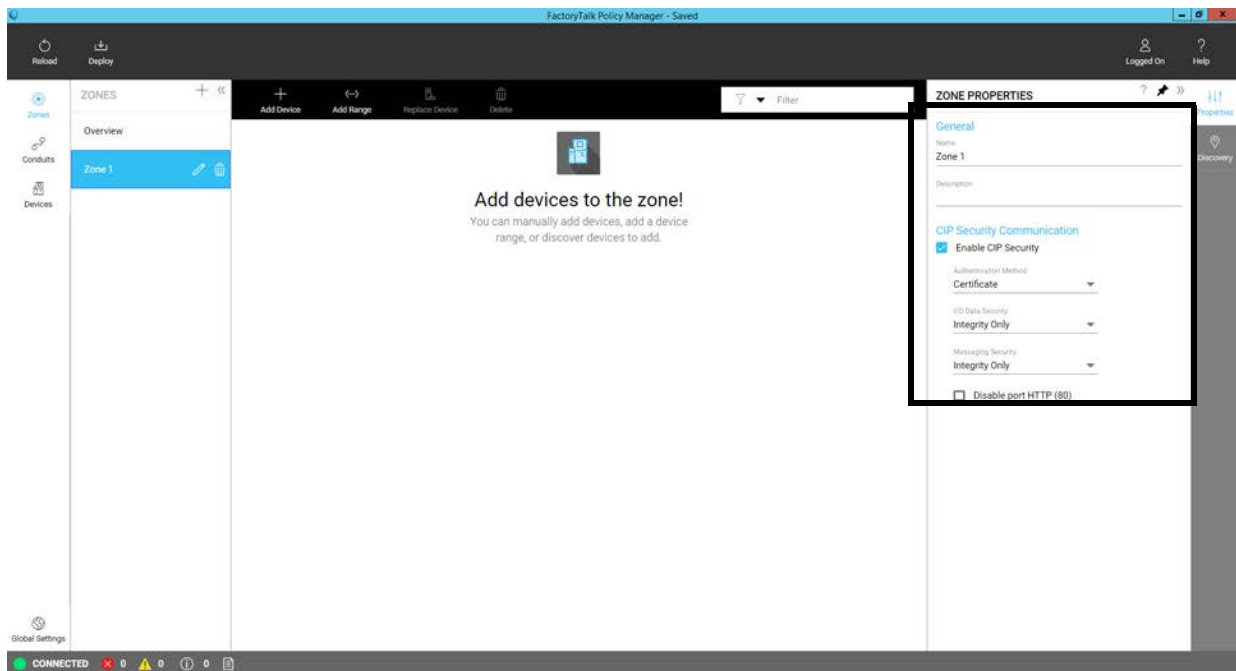
创建区域

1. 在 FactoryTalk Policy Manager 导航栏中，选择 **Zones**。
2. 在 **ZONES** 旁的工具栏上，单击 **+**。



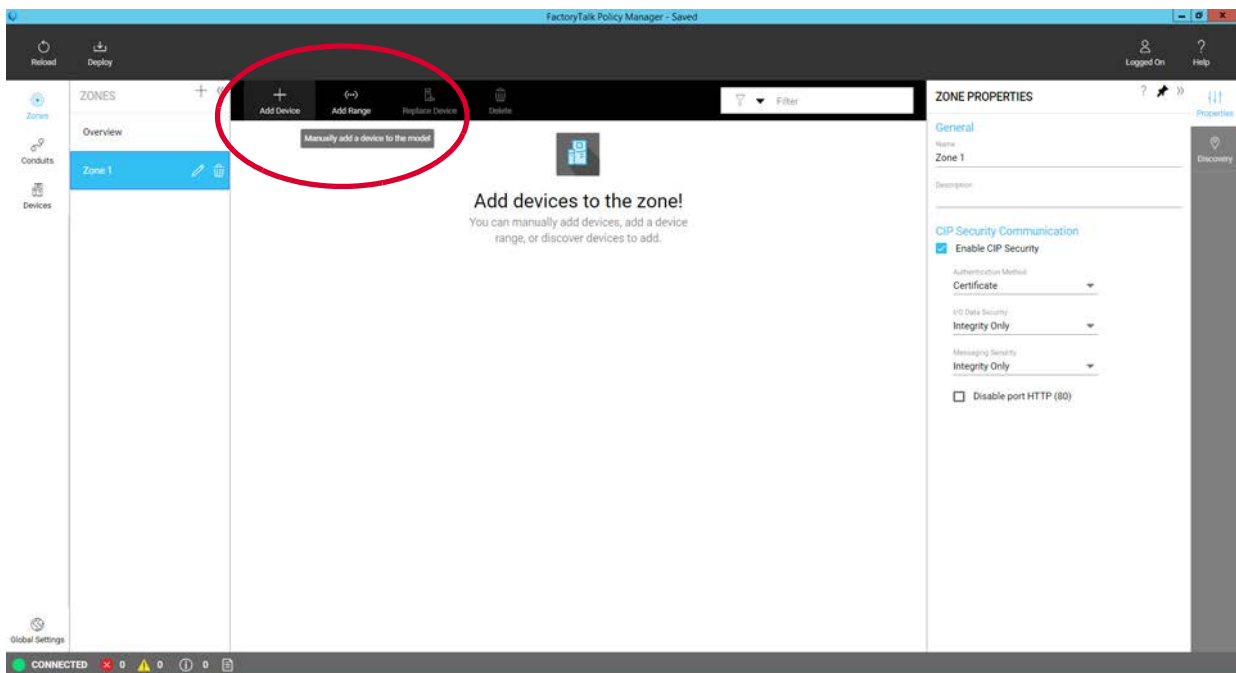
区域被添加至列表中，默认值如下所示：

- **Name** - Zone #
- **Description** - None
- **Enable CIP Security** - 默认情况下未选中。选中 Enable CIP Security 以配置 CIP Security 相关设置。



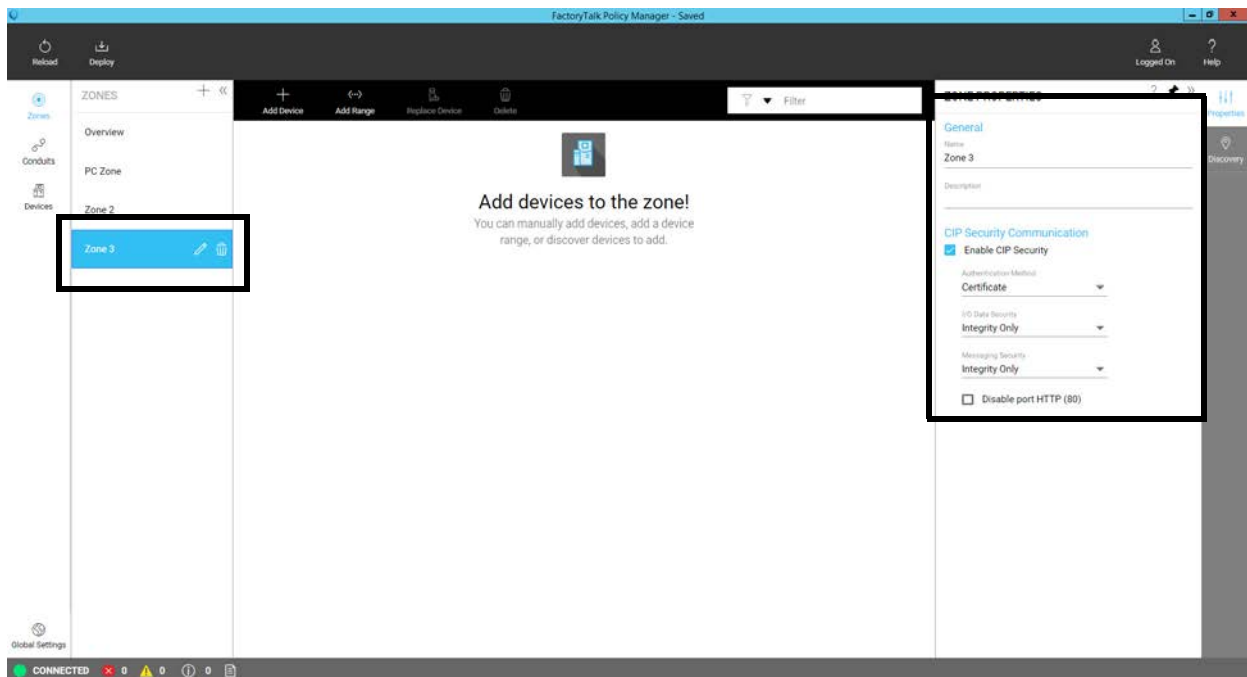
3. 将设备添加到区域。可通过三种方式添加设备：

- 通过 FactoryTalk Linx 发现设备。
- 手动添加设备。
- 添加 IP 地址范围内的所有设备。

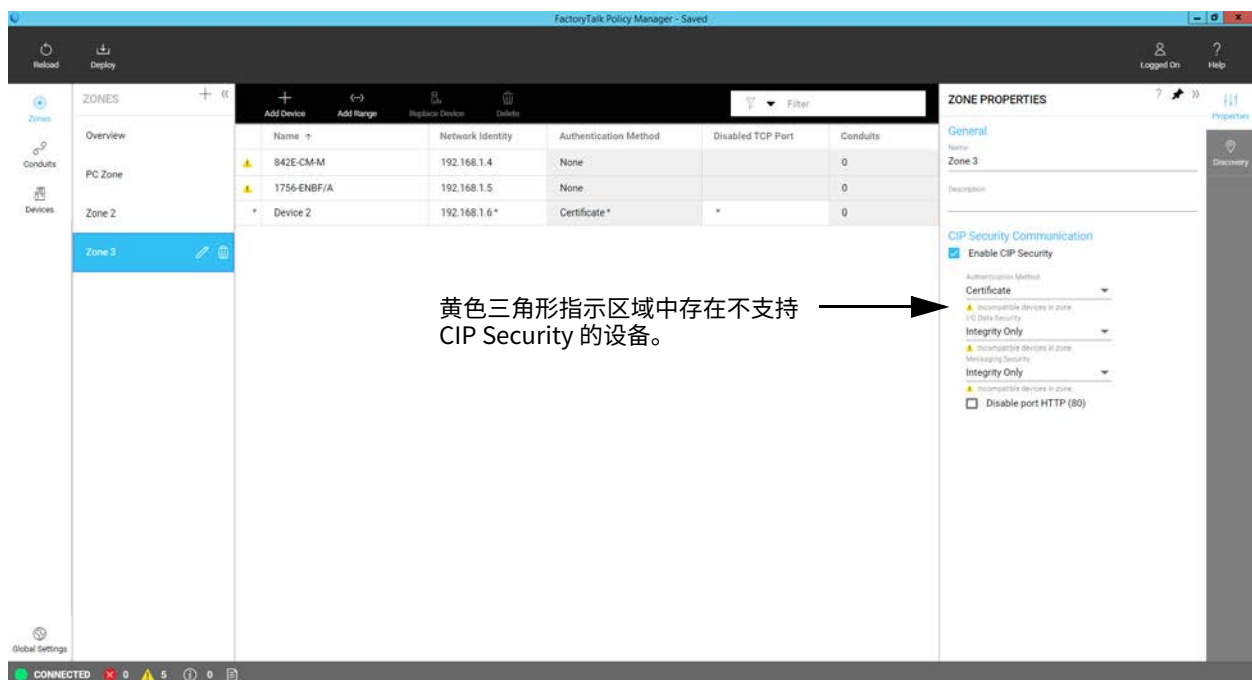


配置区域

1. 在 FactoryTalk Policy Manager 导航栏中，选择 **ZONES**。
ZONES 列显示已配置区域列表。
2. 在 **ZONES** 列中，选择一个区域。
3. 根据需要更改区域属性。



如果某个区域包含不支持 CIP Security 的设备，则区域属性中将显示警告通知。但无需允许列表。区域中所有支持 CIP Security 的设备自动允许该设备。



有关区域的详细信息，请参见：

- FactoryTalk Policy Manager 软件联机帮助
- FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)

识别、组织和创建导管

导管在区域之间、区域与设备之间以及独立区域中的设备之间创建显式可信通信路径。在创建、识别和组织导管后，更新安全矩阵以细化导管。

图 6 - 系统实现 - 导管

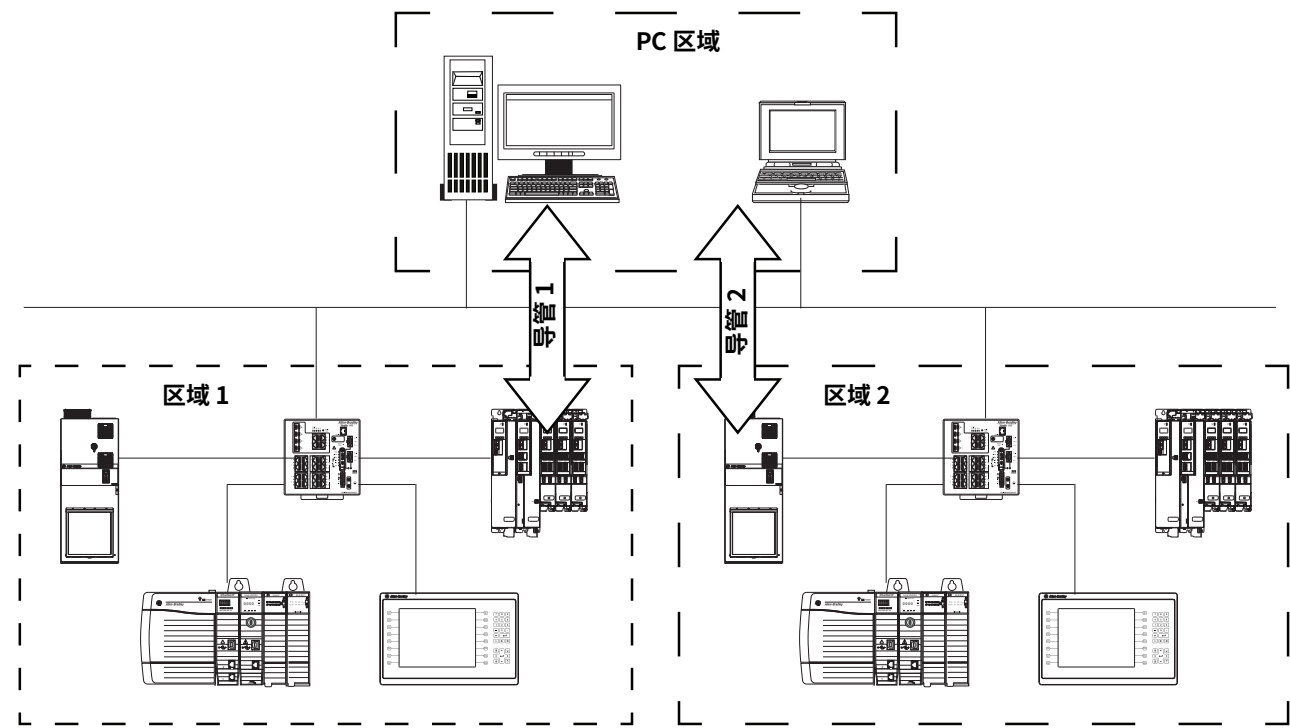


表 7 是标识和组织导管后更新的安全矩阵示例。

在该表中，“源”行与“目标”列的单元格交点表示区域之间导管的端点。例如，第 1 列 / 第 3 行的单元格交点表示导管 2 在 PC 区域和 区域 2 之间使用区域至区域路径。

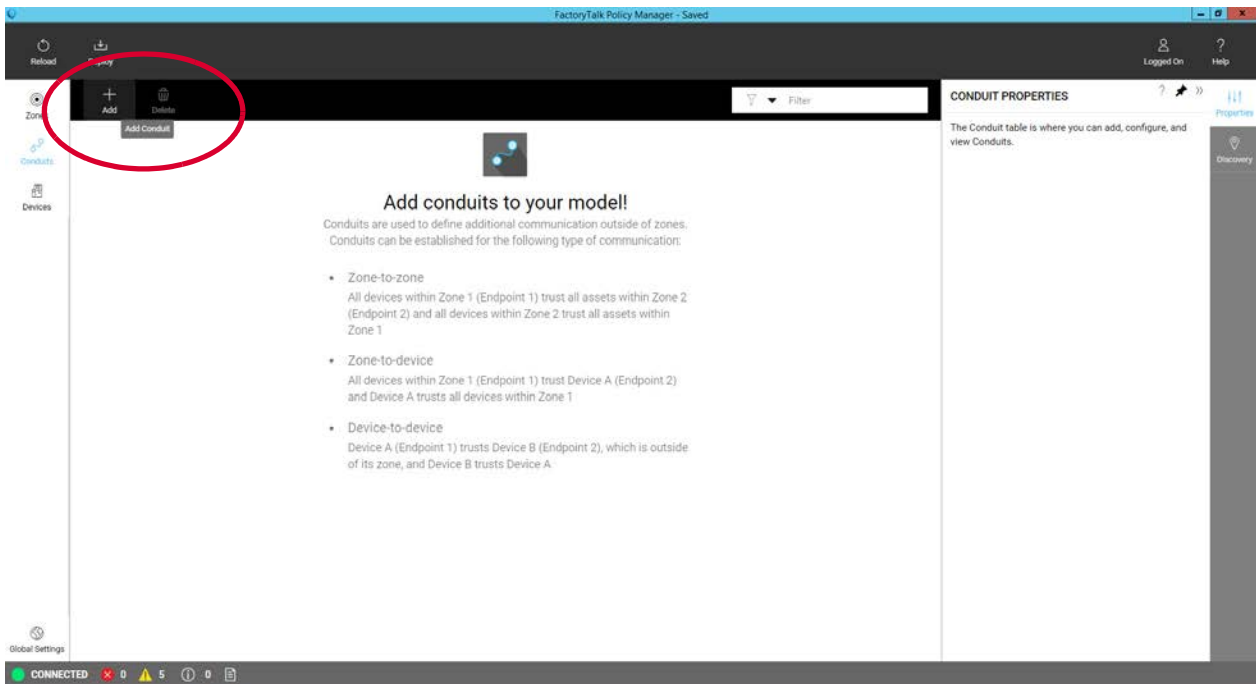
表 7 - 安全矩阵 - 导管

源	目标		
	PC 区域	区域 1	区域 2
PC 区域	允许 ⁽¹⁾	导管 1：区域至区域	导管 2：区域至区域
区域 1	导管 1：区域至区域	允许	拒绝
区域 2	导管 1：区域至区域	拒绝	允许

(1) 默认允许路径。

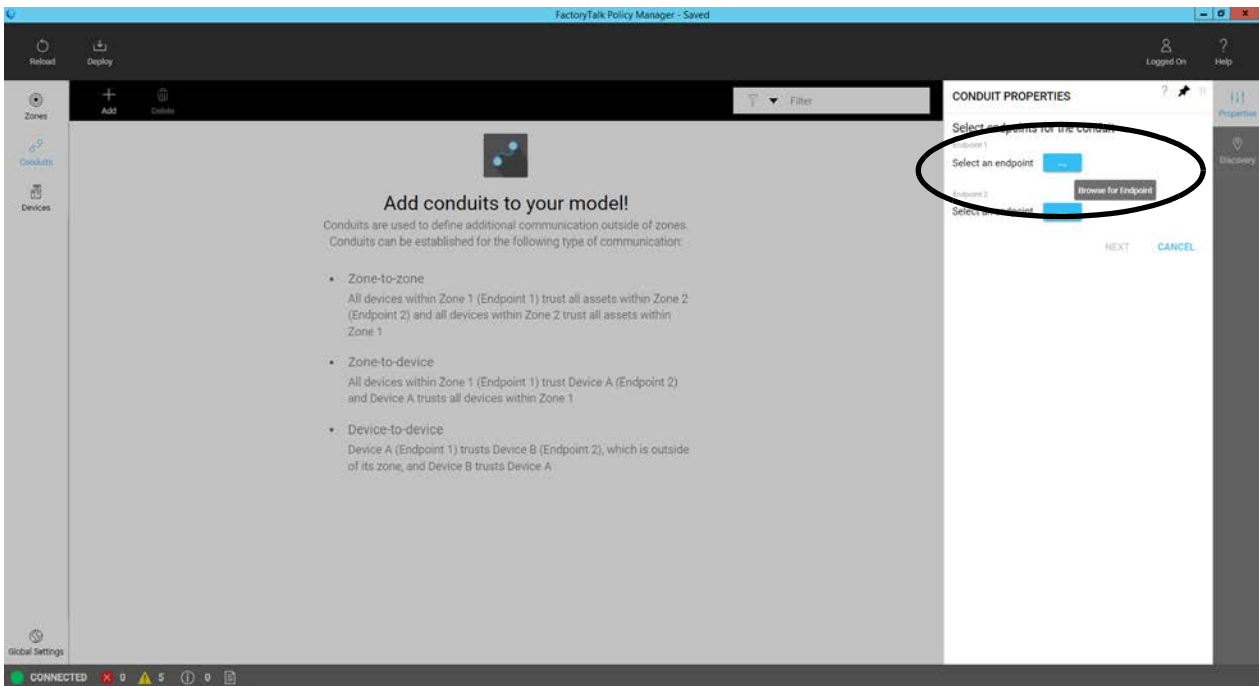
创建导管

1. 在 FactoryTalk Policy Manager 导航栏中，选择 Conduits。
2. 在工具栏上，单击 [+]。



CONDUIT PROPERTIES 窗格打开。

3. 在 Endpoint 1 中，在 Select an endpoint 旁，选择 Browse for Endpoint [...]

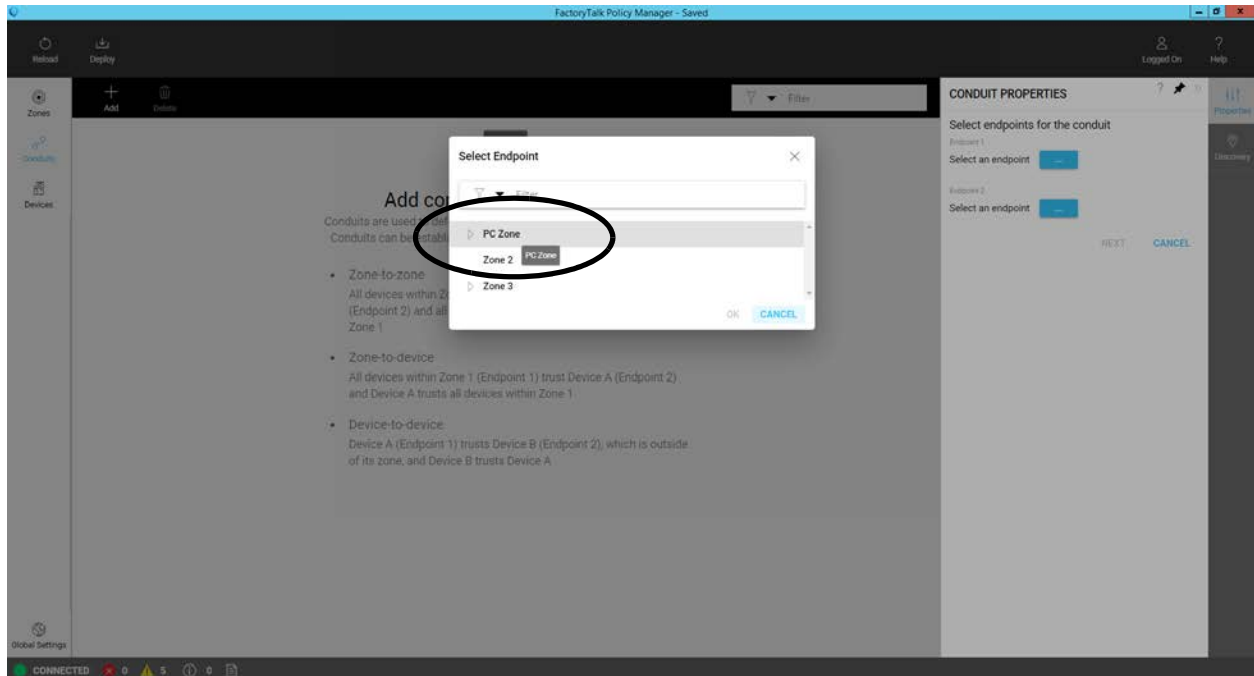


4. 选择 endpoint。

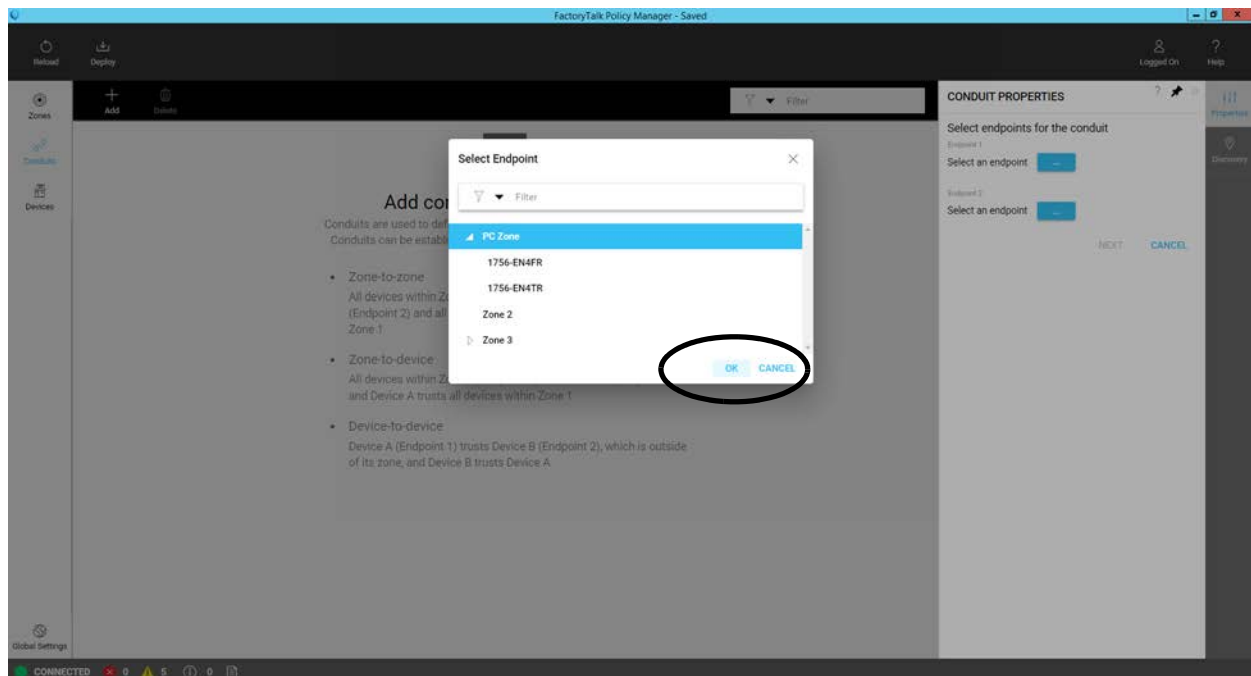
可选择一个区域或设备，将其指定为导管的第一端点。



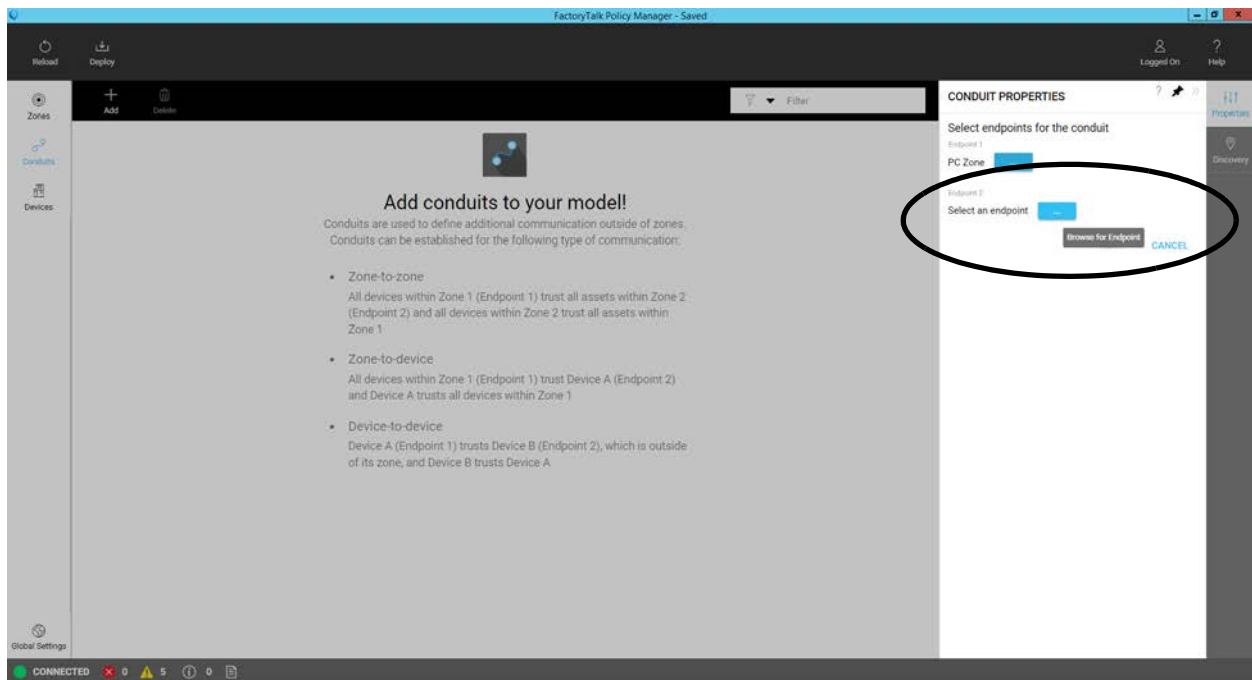
在 Filter 中，可键入名称的一部分，只列出符合该标准的端点。



5. 单击 OK。



6. 在 **Endpoint 2** 中，在 **Select an endpoint** 旁，选择 **Browse for Endpoint [...]**。

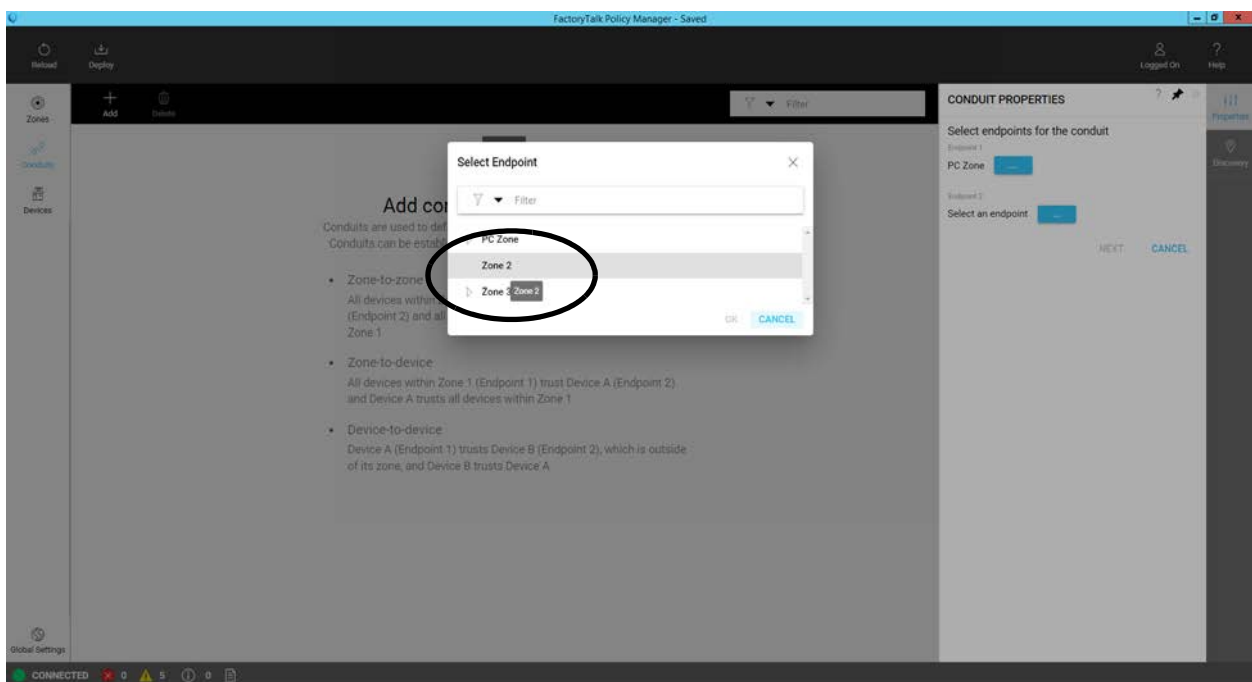


7. 要指定导管的第二端点，请选择一个区域或设备。

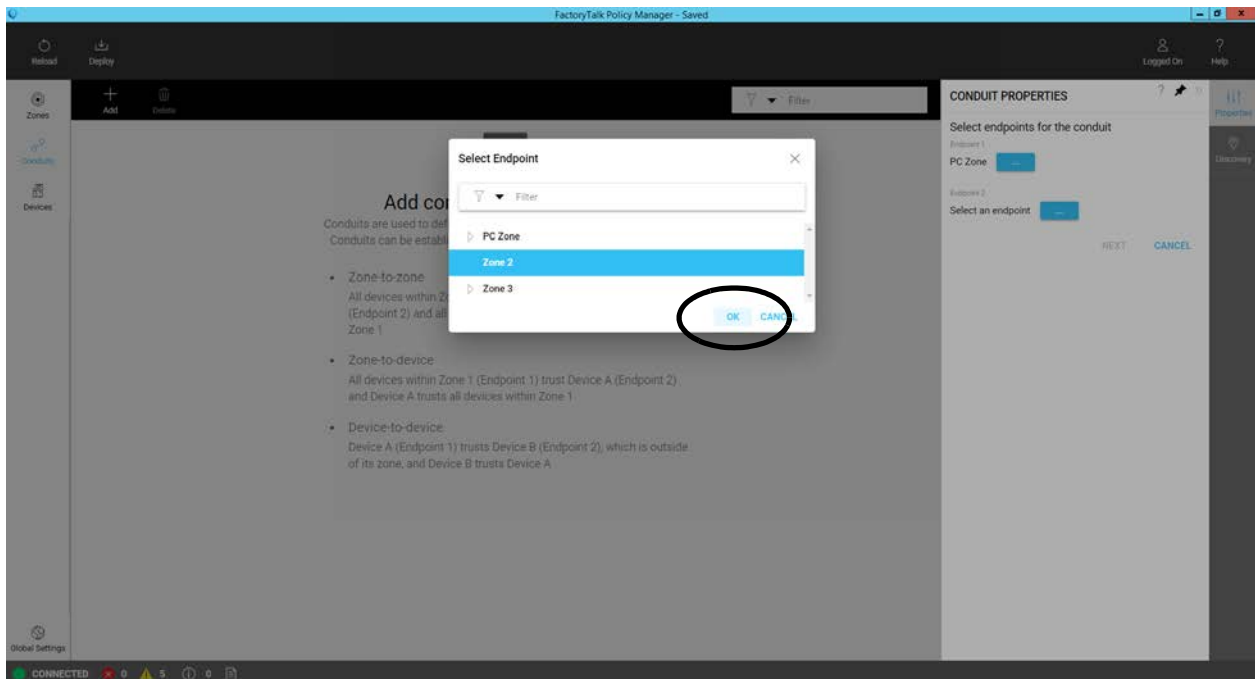
可选择 一个区域或设备，将其指定为导管的第二端点。



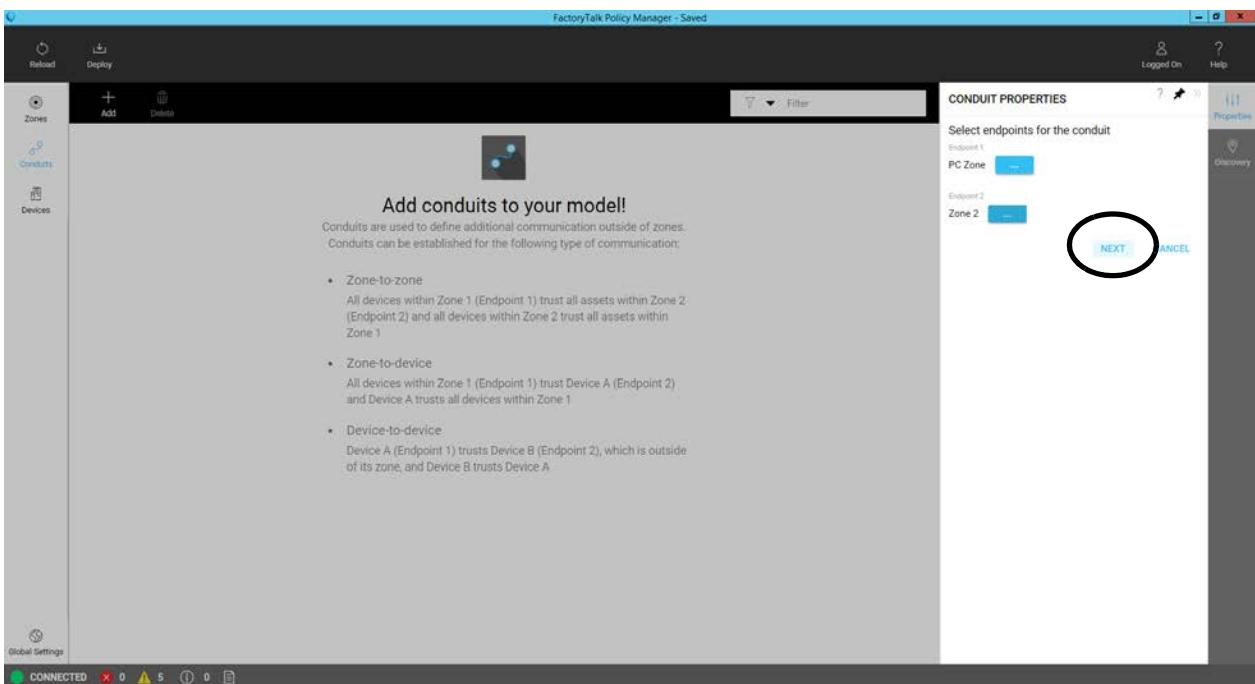
在 Filter 中，可键入名称的一部分，只列出符合该标准的端点。



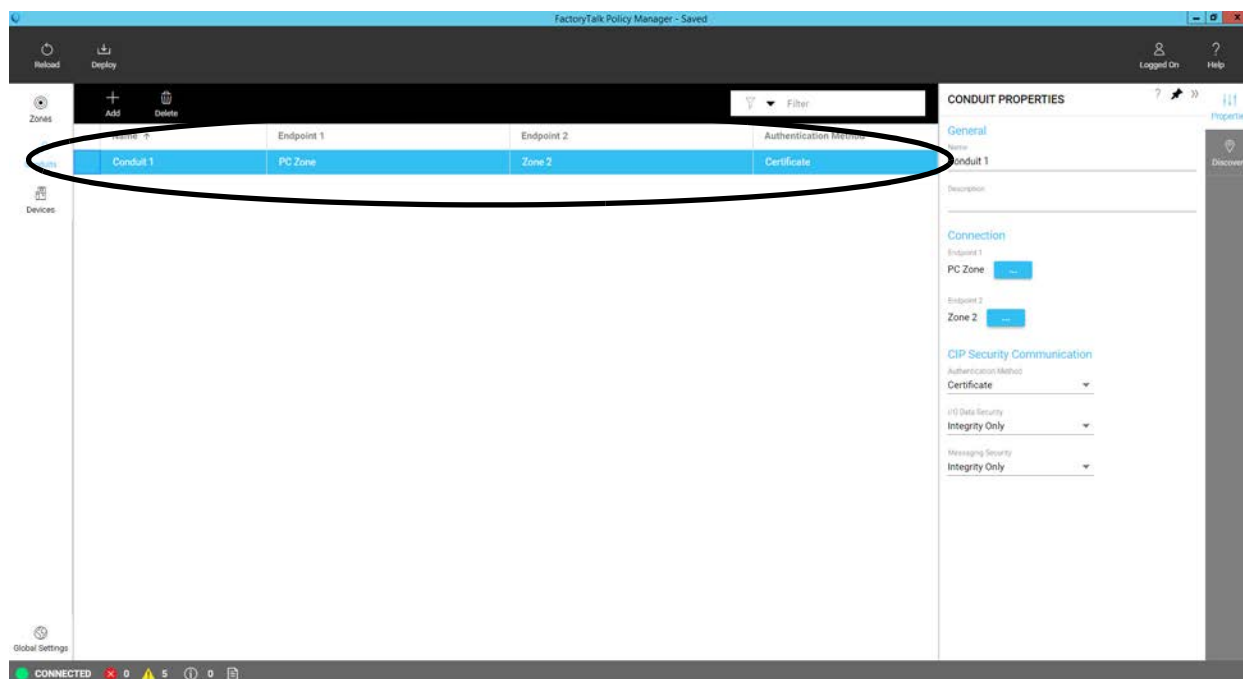
8. 单击 OK。



9. 单击 Next。



第一个导管显示在 Conduits 列表中。



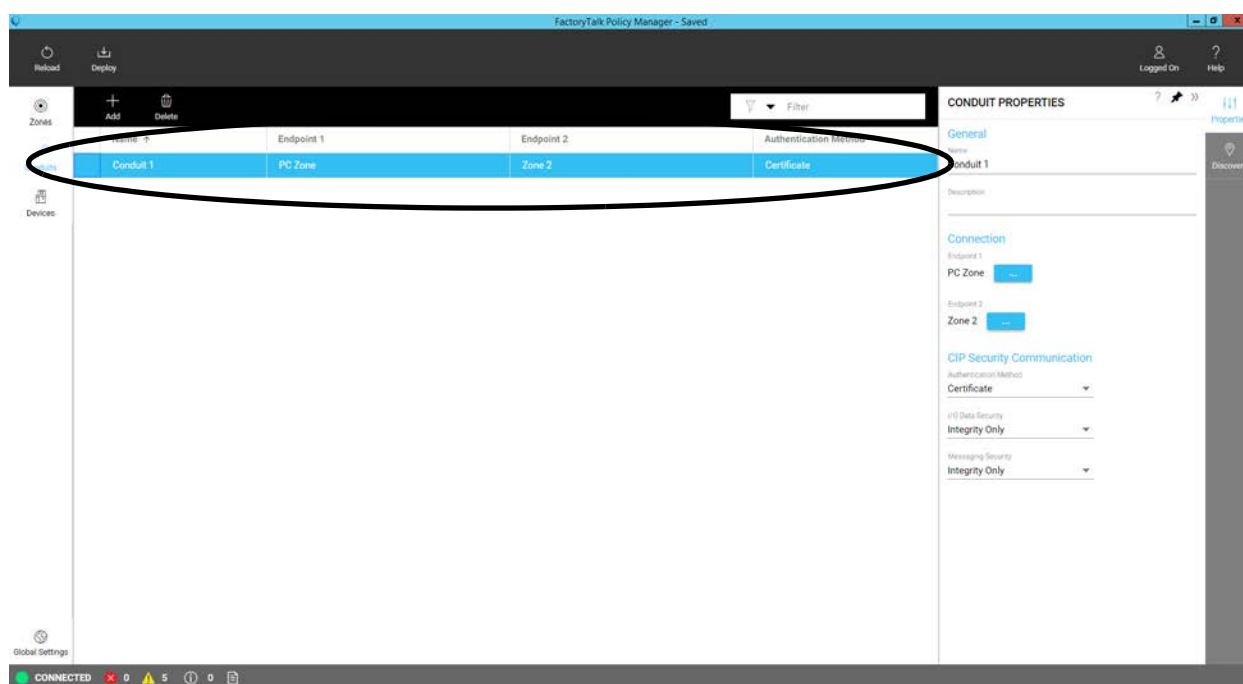
如果必须创建另一个导管，请重复该过程，从[第 37 页](#)的[步骤 2](#) 开始。

配置导管

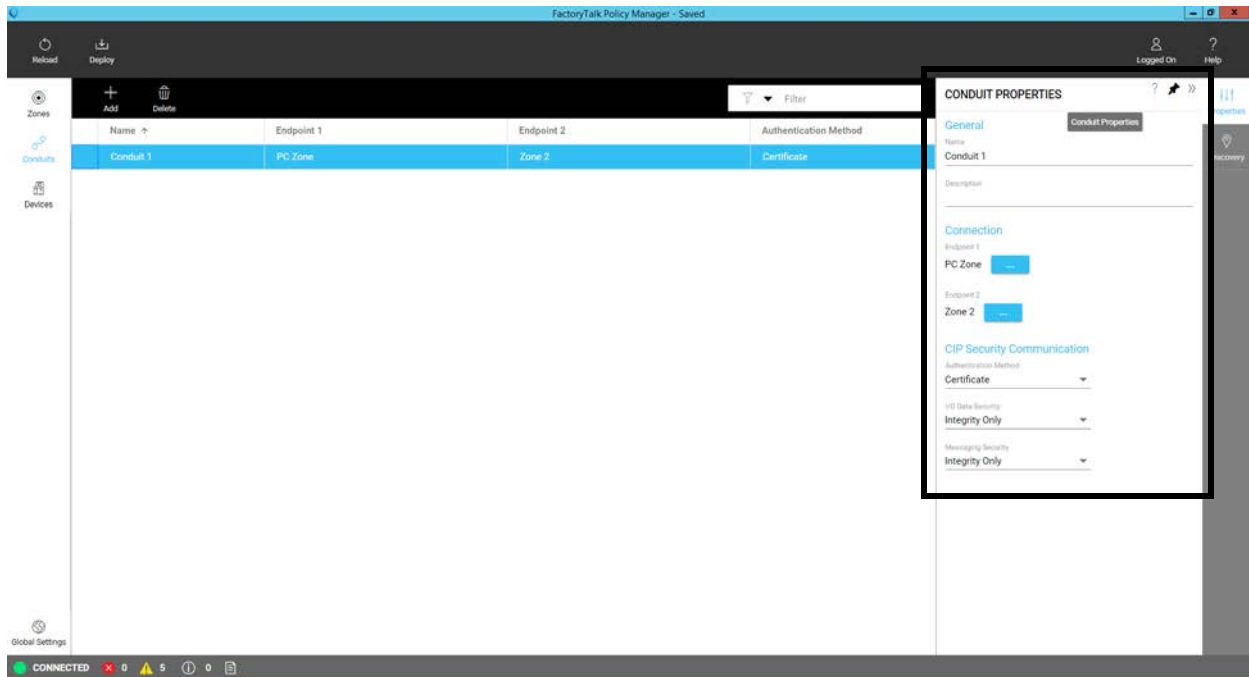
1. 在 FactoryTalk Policy Manager 导航栏中，选择 **Conduits**，然后选择要配置的导管。



CONDUIT PROPERTIES 自动打开，显示最近配置的导管。
要编辑另一导管，请从列表选择一个导管以显示其属性。



2. 根据需要更改导管属性。



如果两个端点都支持 **CIP Security**，则配置 **CIP Security Communication**。

- 在 **I/O Data Security and Messaging Security** 中，选择以下选项之一：
 - Integrity only - 用于检查数据或消息是否已更改，并拒绝更改的信息。
 - Integrity & Confidentiality - 用于检查完整性以及加密数据或消息，因此需要相应解密密钥来读取信息。拒绝更改的和 / 或不可信的信息，同时保护信息的保密性。
- 在 **I/O Data Security** 中，单击 None 停止对 I/O 数据进行附加安全检查。

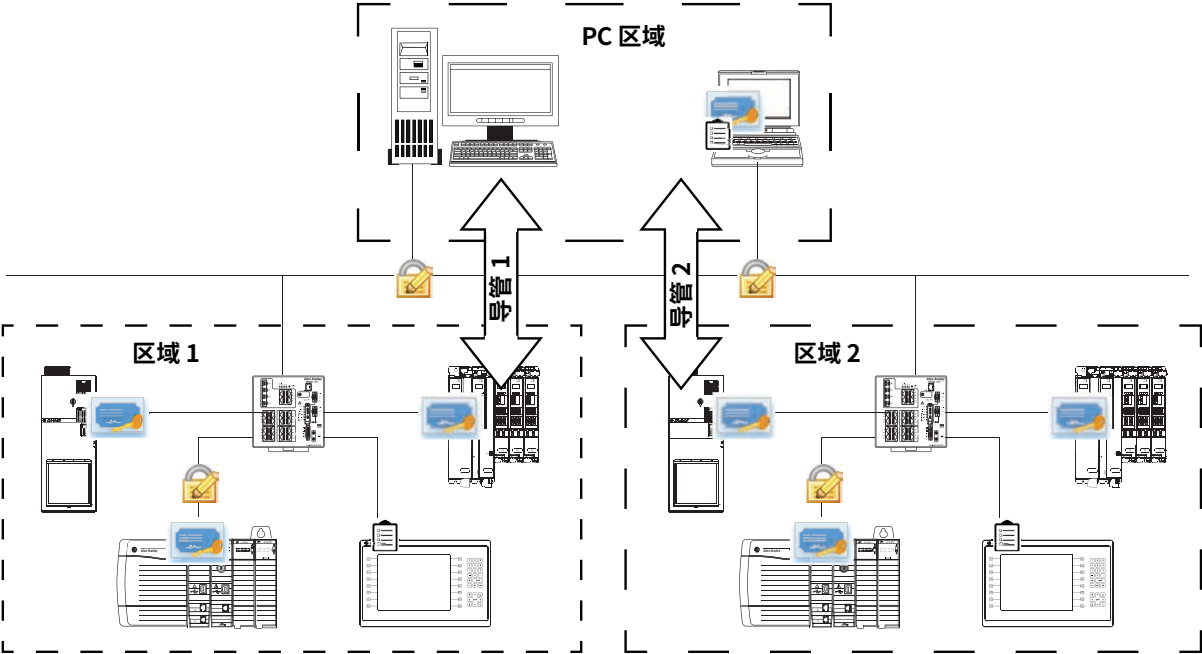
有关导管详细信息，请参见：

- FactoryTalk Policy Manager 软件联机帮助
- FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)

识别和创建安全功能 / 策略

安全策略根据设备功能和自动化应用程序的运行功能而创建。

图 7 - 系统实现 - 安全策略



确定并创建安全功能 / 策略后，更新安全矩阵，以细化导管之间的适用安全策略。例如，启用证书或预共享密钥、启用 / 禁用保密性和允许。

表 8 为更新后的安全矩阵，其中定义了安全功能和策略。

表 8 - 安全矩阵 - 安全功能和策略

导管 1 安全的 FactoryTalk Linx 通信 区域至区域 (确保与 FactoryTalk Linx 的通信安全。)	区域至区域		安全策略
	PC 区域	区域 1	· 证书 · 完整性 · 保密性
导管 2 安全的 FactoryTalk Linx 通信 区域至区域 (确保与 FactoryTalk Linx 的通信安全。)	区域至区域		安全策略
	PC 区域	区域 2	· 证书 · 完整性 · 保密性
可信 IP (允许)	区域 / 设备至区域 / 设备		
(不支持 CIP Security 的设备)	PC 区域 设备 - FactoryTalk Network Manager (IP 地址: xxx.xxx.xxx.xxx)	区域 1 - 设备	· Kinetix 5700 驱动器 (IP 地址: xxx.xxx.xxx.xxx) · ControlLogix 5580 控制器 (IP 地址: xxx.xxx.xxx.xxx) · 1756-EN4TR 模块 (IP 地址: xxx.xxx.xxx.xxx) · PanelView Plus 终端 (IP 地址: xxx.xxx.xxx.xxx) · PowerFlex 755T 变频器 (IP 地址: xxx.xxx.xxx.xxx)
		区域 2 - 设备	· Kinetix 5700 驱动器 (IP 地址: xxx.xxx.xxx.xxx) · ControlLogix 5580 控制器 (IP 地址: xxx.xxx.xxx.xxx) · 1756-EN4TR 模块 (IP 地址: xxx.xxx.xxx.xxx) · PanelView Plus 终端 (IP 地址: xxx.xxx.xxx.xxx) · PowerFlex 755T 变频器 (IP 地址: xxx.xxx.xxx.xxx)

部署安全模型

在配置了区域、导管和设备安全策略后，可以部署生成的安全模型。

在 FactoryTalk Policy Manager 软件中，单击 Deploy 按钮，以触发 FactoryTalk System Services 来部署安全模型。FactoryTalk System Services 在后台运行。不得在客户端执行操作。

重要信息 在部署的安全模型激活之前，必须复位所有已配置设备的通信，从而导致连接短暂丢失。

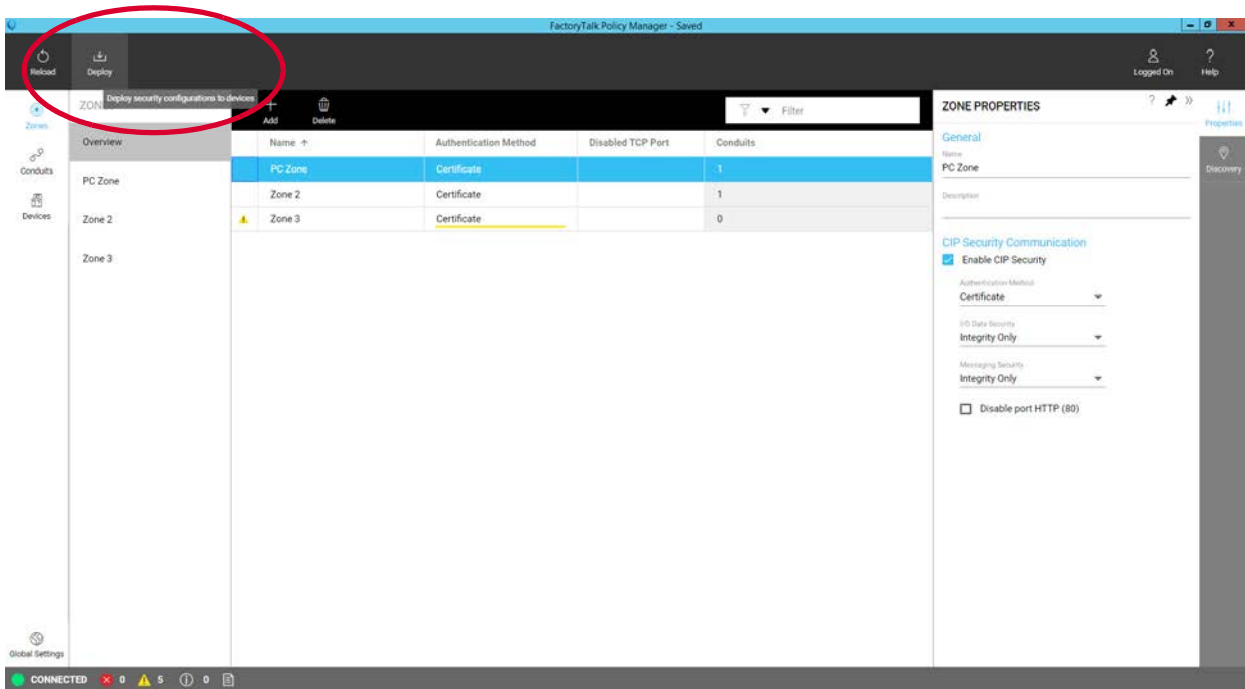
一旦部署并激活了安全模型，即在设备上复位通信，则设备仅接受来自同一区域中的其他设备的通信，或使用配置为启用与其他安全区域或设备通信的导管。

在部署安全模型之前，确保所有设备都处于运行状态，并具有网络访问权限。

在所有受影响的设备上部署并激活安全模型后，实时操作不再需要 FactoryTalk Policy Manager 和 FactoryTalk System Services。如果必须部署对安全模型的更改，则再次需要它们。

要部署模型，请完成以下步骤。

- 1. 在 FactoryTalk Policy Manager 工具栏上，选择 Deploy。



- 2. 查看 Deploy 对话框。

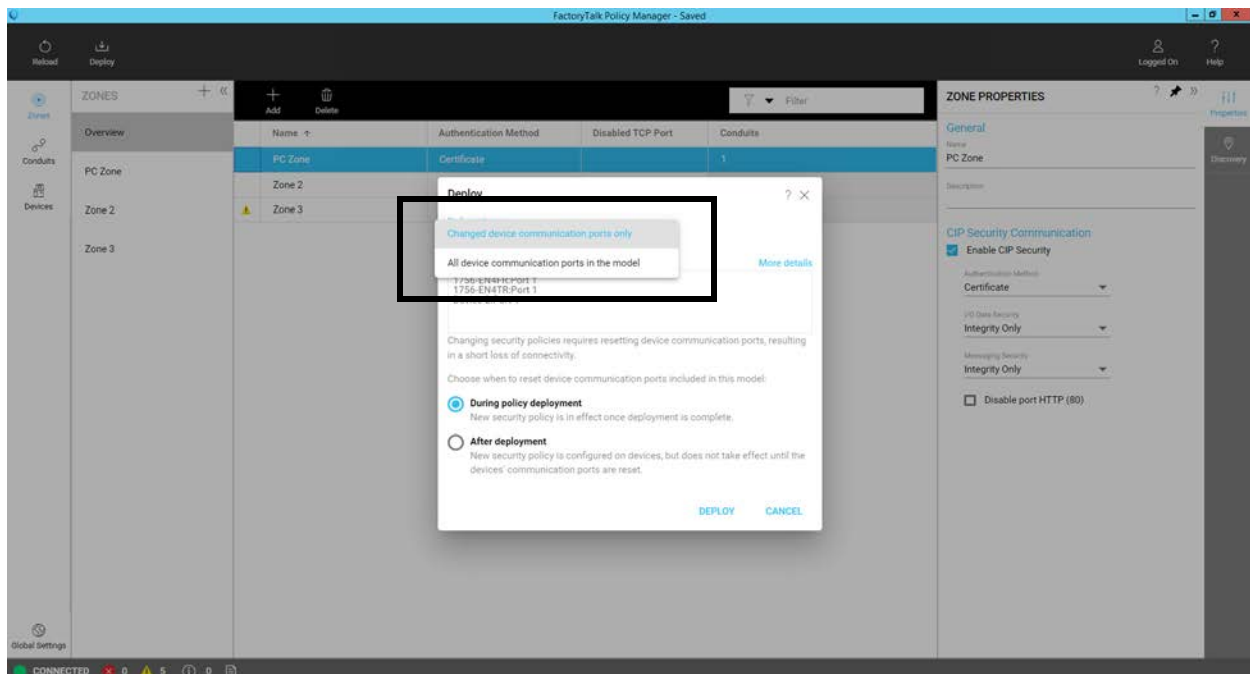
设备列表标识了部署此模型时要配置的设备。

重要信息 如果列表中包含非预期设备，请单击 CANCEL，然后根据需要更改模型。

3. 请完成以下步骤：

- a. 根据应用程序选择 Deployment 范围。
 - 为差分部署选择 Changed device communication ports only。
 - 选择模型中的所有设备通信端口进行全面部署。

建议您使用默认选项，即 Changed device communication ports only。



- b. 对于何时重置安全模型中所含项目的通信通道，请选择以下选项之一。

提供以下类型的部署：

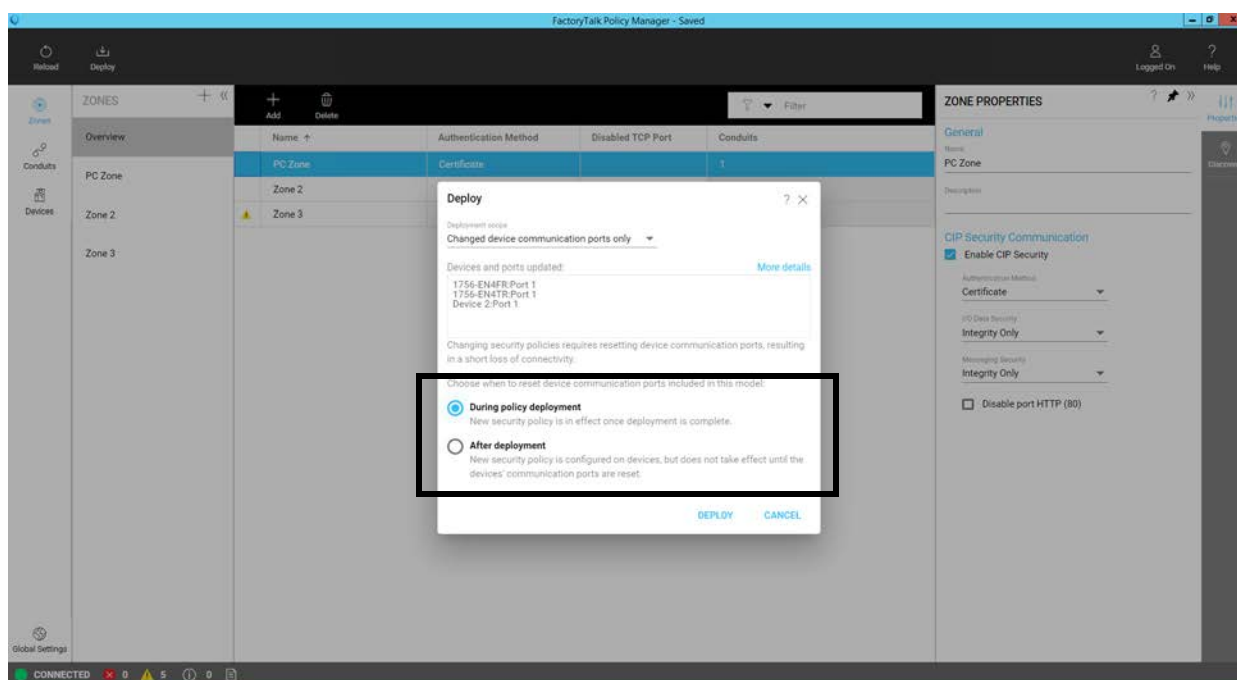
- During deployment - 在部署过程中，CIP 连接关闭并在设备上重新打开。

与重置计算机上的网卡类似，设备会保持运行但暂时与网络断开连接。当部署策略时，该选项将新策略应用于设备。

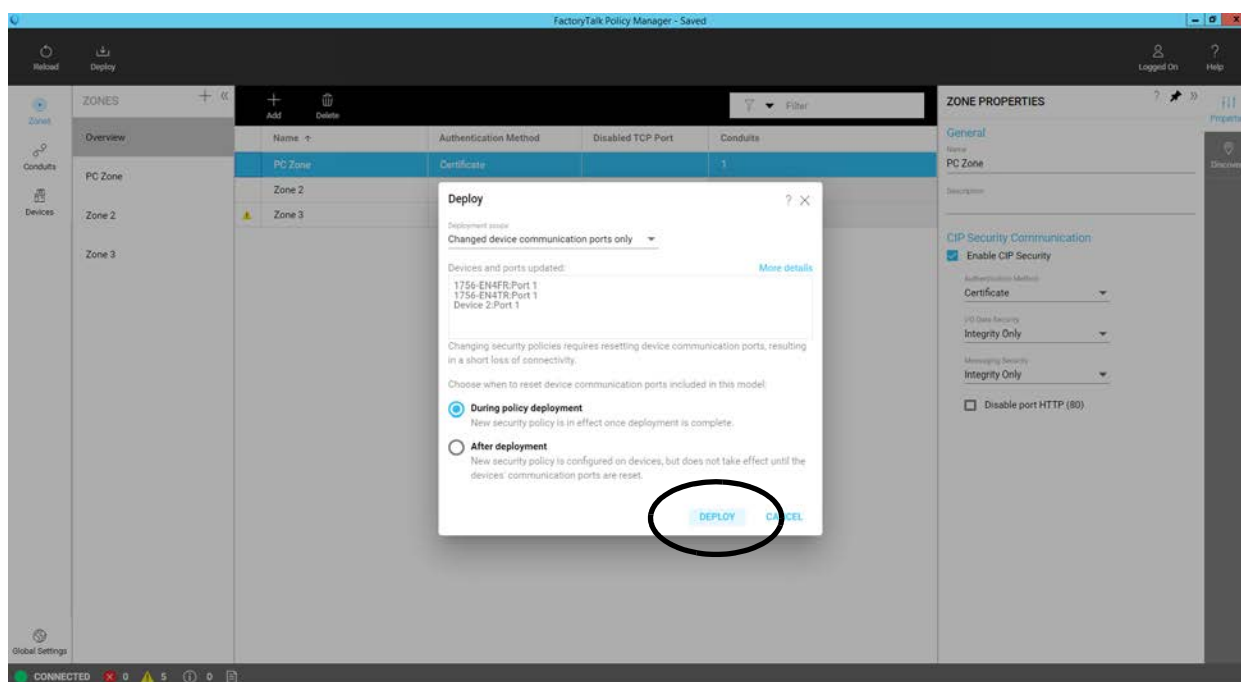
- After deployment - 安全策略更改仅在现有连接关闭并重新打开后才会应用于具有这些连接的设备。例如，可通过对设备循环上电或抑制和取消抑制连接来关闭和重新打开现有连接。

重要信息 使用 After deployment 选项，安全策略将单独应用于每个连接。如果连接复位延迟且发生意外连接中断，则系统可进入如下状态：安全策略仅在系统的某些部分中运行。在这种情况下，可能会发生意外连接中断。连接中断很难追踪。建议谨慎使用 After deployment 选项。

如果环境中存在定期维护重置程序，并且可以依靠它来执行该功能，则该选项非常有用。



4. 单击 DEPLOY。



Results 窗格随部署结果更新。完成部署后，将提供汇总报告，其中列出了在此过程中遇到的成功、失败和错误。

有关如何部署安全模型的信息，请参见 FactoryTalk Policy Manager Getting Results Guide，出版号：[FTALK-GR001](#)。

备份安全模型

无需备份安全模型。但是，**强烈建议**在每次策略部署后进行备份，以使备份文件与当前安全策略保持同步。

备份 FactoryTalk System Services，以保存安全模型及其关联证书的副本。创建模型后，FactoryTalk System Services 备份文件在执行后随 FactoryTalk Services Platform 备份一起提供。

重要信息 必须具有管理员权限才能备份 FactoryTalk System Services。

要备份安全模型，请完成以下步骤：

1. 以管理员身份打开命令提示窗口。
2. 在命令提示窗口中键入：

```
cd C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services
```

3. 键入以下命令之一，运行备份实用工具：

- FTSSBackupRestore -B -PW “password” （FactoryTalk System Services，版本 6.11）
 - FtssBackupRestore -B -P “password” （FactoryTalk System Service，版本 6.20 或更高版本）
- 使用引号中提供的密码创建加密数据备份。要恢复数据，必须提供该密码。

4. 文件 backup.zip 已创建。该文件包含在 FactoryTalk Services Platform 备份中。

确认文件位于以下位置：

```
C:\ProgramData\Rockwell\RNA Server\Global\RnaStore\FTSS_Backup
```



默认情况下，ProgramData 文件夹隐藏在 Windows 文件资源管理器中。

将安全模型备份保存到另一安全位置

建议您将 Backup.zip 文件保存到另一安全位置以及之前所述的 *FTSS_Backup* 文件夹中。

不同于 FactoryTalk Directory 备份文件

FactoryTalk Directory 为参与应用程序的所有产品提供集中查找服务，包括 FactoryTalk System Services 应用程序。建议您创建 FactoryTalk 备份文件，以便在发生系统故障时保存和恢复 FactoryTalk 系统。

需要明确的是，FactoryTalk Directory 备份不包括产品备份文件。必须将各个应用程序与 FactoryTalk Directory 备份分开备份。但是，一旦创建了安全模型（FTSS_Backup 文件夹）的备份，该文件夹在执行后将包含在 FactoryTalk Directory 备份中。

有关如何备份 FactoryTalk Directory 的详细信息，请参见 FactoryTalk Security System Configuration Guide，出版号：[FTSEC-QS001](#)。

恢复 FactoryTalk System Services

恢复 FactoryTalk System Services，使 FactoryTalk System Services 数据库返回已知良好状态。

重要信息 请注意以下几点：

- 如果恢复 FactoryTalk System Services，则将自动删除安全模型备份文件夹。因此，建议您将安全模型备份文件保存在单独位置，如第 47 页所述。
 - 恢复 FactoryTalk System Services 需要管理员权限。
-

要恢复 FactoryTalk System Services 数据库，请完成以下步骤：

1. 确认 backup.zip 文件位于以下位置：

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

2. 以管理员身份打开命令提示窗口。
3. 在命令提示窗口中键入：

cd C:\Program Files (x86)\RockwellSoftware\FactoryTalk System Services。

4. 键入以下命令之一，运行 FactoryTalk System Services 备份和恢复实用工具：
 - *FTSSBackupRestore -R -PW "password" (FactoryTalk System Services, 版本 6.11)*

或

· *FTSSBackupRestore -R -P "password" (FactoryTalk System Services, 版本 6.20 或更高版本)*

恢复数据库的加密备份，该备份使用 -P 参数后提供的密码进行解密。引号是可选的。

可在软件的更高版本中恢复 FactoryTalk System Services 数据库备份。例如，您可打开版本 6.11 和版本 6.20 或更高版本的 FactoryTalk System Services 数据库的备份。

-
- 重要信息**
- 在从版本 6.11 升级到版本 6.20 或更高版本之前，建议您访问罗克韦尔自动化知识库（网址：
- <https://rockwellautomation.custhelp.com/app/home>
- ），阅读以下文章：
- 备份和恢复 FactoryTalk Policy Manager 和 FactoryTalk System Services 的 CIP Security 模型，请单击[此处](#)
 - 未能通过 CIP Security 策略模型升级现有 FactoryTalk System Service 数据，请单击[此处](#)
 - 下载和安装 FactoryTalk Policy Manager，请单击[此处](#)
- 建议您使用最新版 FactoryTalk Policy Manager。
-

删除安全策略

如有必要，可以从软件应用程序和硬件设备中删除安全策略。

从软件应用程序中删除安全策略

可使用以下方法从 FactoryTalk Linx 中删除安全策略：

- FactoryTalk Policy Manager

使用 FactoryTalk Policy Manager 方法时，不仅从 FactoryTalk Linx 中删除安全策略。装有 FactoryTalk Linx 的计算机也不再出现在 FactoryTalk Policy Manager 中。

FactoryTalk Policy Manager **方法仅在**装有 FactoryTalk Linx 的计算机可以访问装有 FactoryTalk Policy Manager 的计算机时才有效。

- FactoryTalk Administration Console

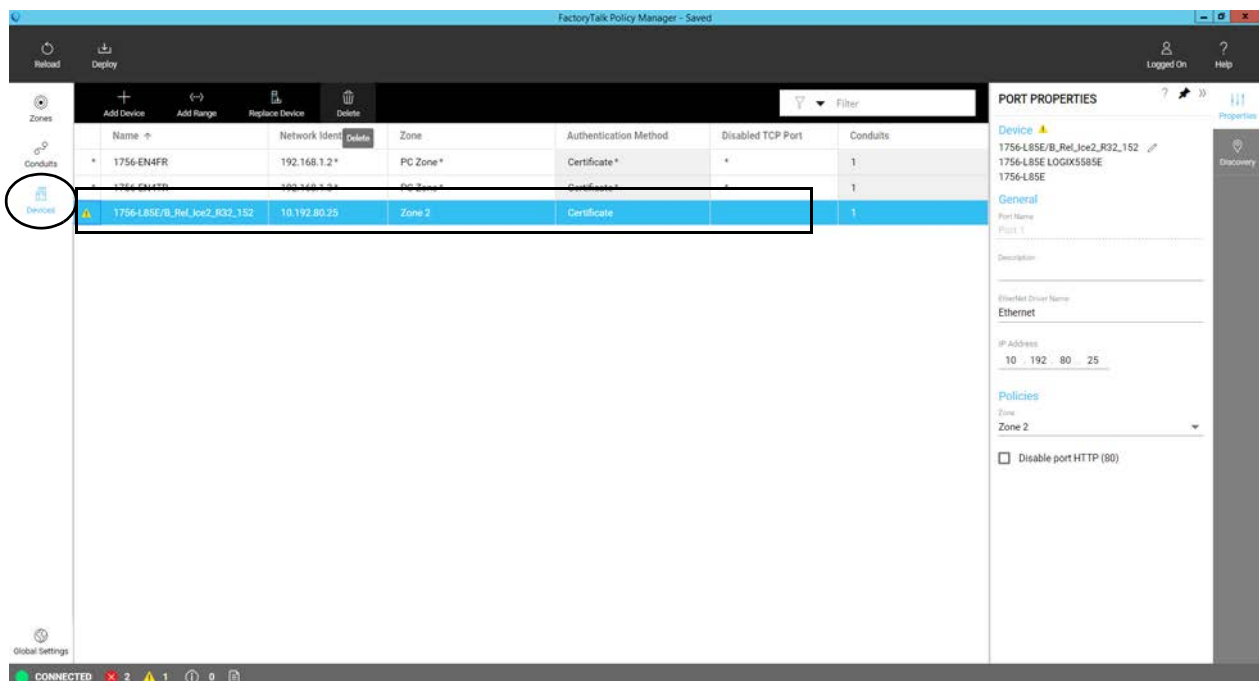
如果装有 FactoryTalk Linx 的计算机无法访问装有 FactoryTalk Policy Manager 的计算机，则必须使用 FactoryTalk Administration Console 方法。

使用 FactoryTalk Administration Console 方法时，从 FactoryTalk Linx 中删除安全策略。

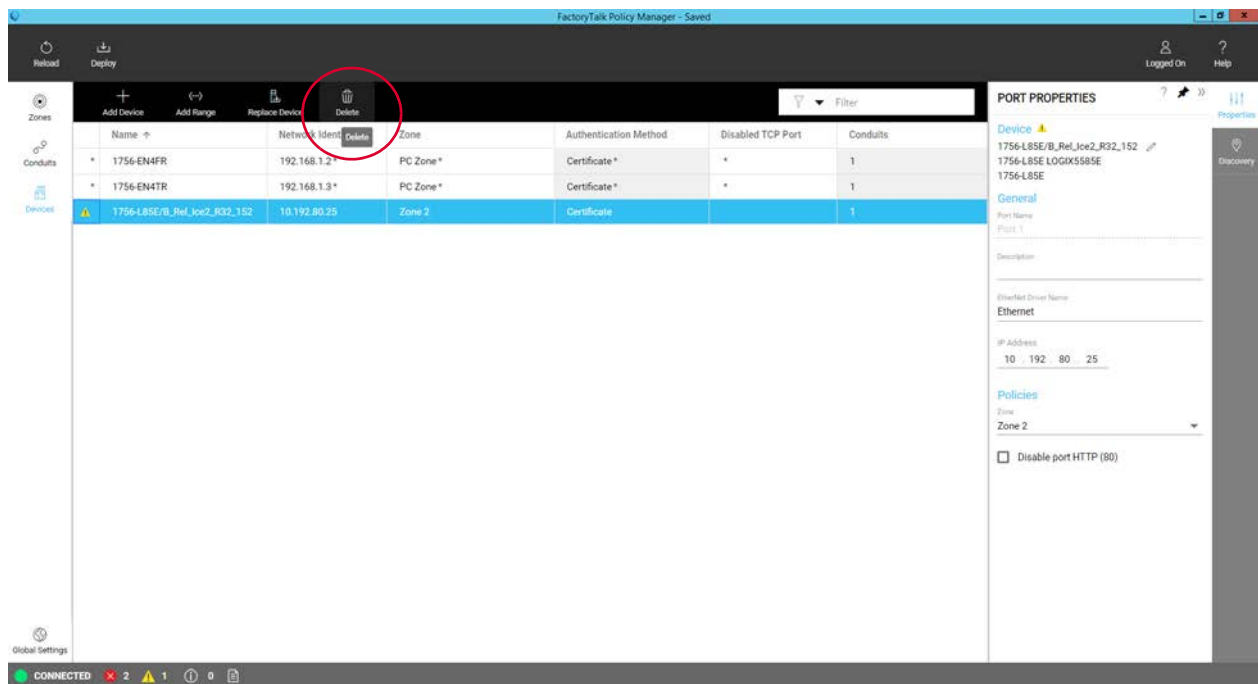
然后，必须返回 FactoryTalk Policy Manager 以删除装有 FactoryTalk Linx 计算机，然后重新部署模型，以便其他设备可以更新其信任模型。

通过 FactoryTalk Policy Manager 从 FactoryTalk Linx 中删除安全策略

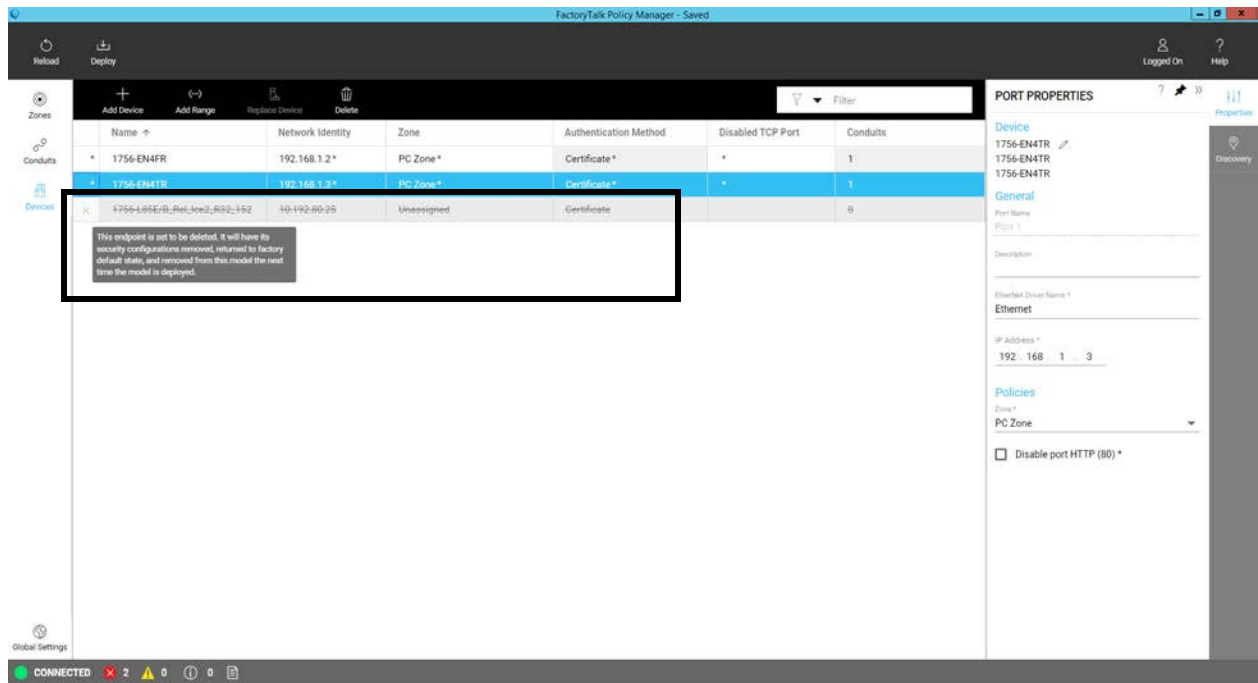
1. 在 FactoryTalk Policy Manager 导航栏中，选择 **Devices**，然后选择设备。



2. 在设备列表上方，单击 **Delete**。



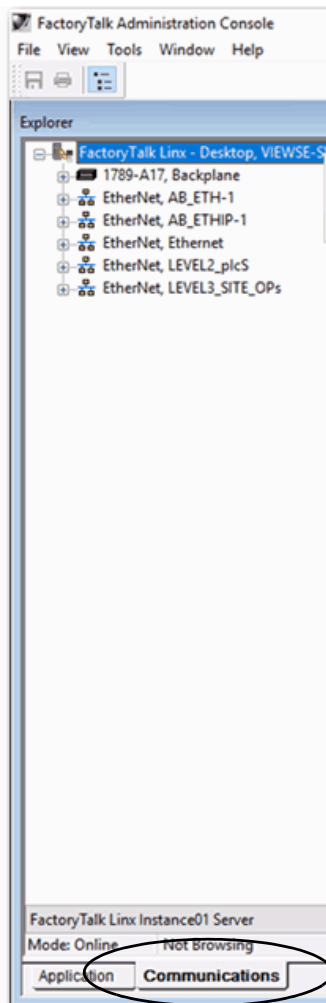
单击 Delete 后，设备会保留在表格中，但会被划掉。在下一步中部署更新后的安全模型和状态后，设备不再显示在列表中。



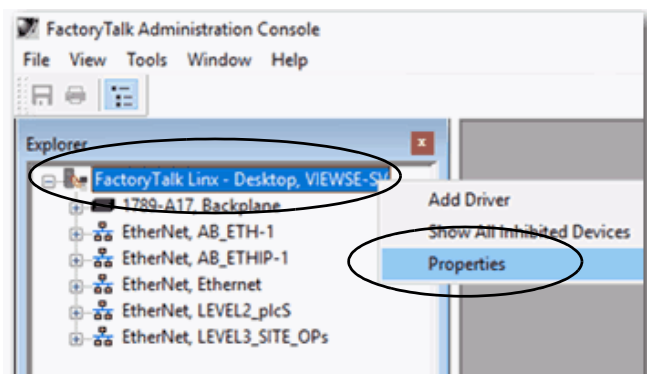
3. 按从第 44 页开始所述的方式部署安全模型，然后选择在部署期间重置通信通道。

通过 FactoryTalk Administration 从 FactoryTalk Linx 中删除安全策略

1. 为处于联机状态且具有适当安全策略的 IACS 启动 FactoryTalk Administration Console。
2. 在 Explorer 窗格底部，单击 Communications 选项卡。

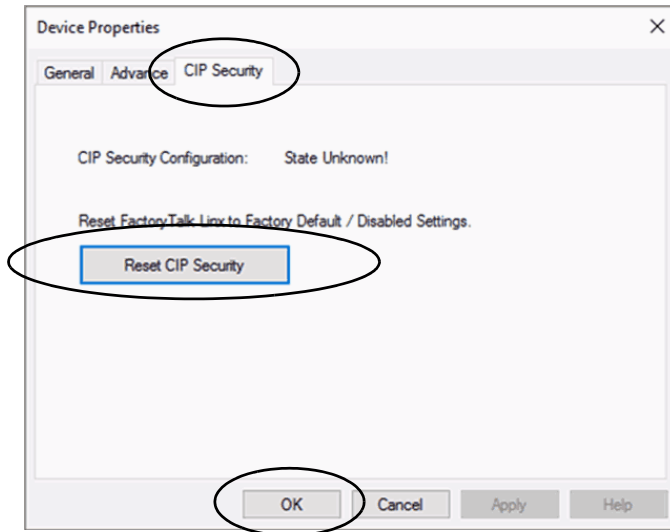


3. 右键单击 FactoryTalk Linx 并选择 Properties。



将显示 Device Properties 对话框。

4. 请完成以下步骤：
 - a. 单击 CIP Security 选项卡。
 - b. 单击 Reset CIP Security。
 - c. 单击 OK。



有关如何使用 FactoryTalk Administration Console 的更多信息，请参见软件联机帮助。

从设备中删除安全策略

可以使用以下方法从设备中删除安全策略：

- 通过 FactoryTalk Policy Manager - 此方法有两个选项。
 - 选项 1 - 更改设备安全策略。
 - 选项 2 - 从安全模型中删除设备。

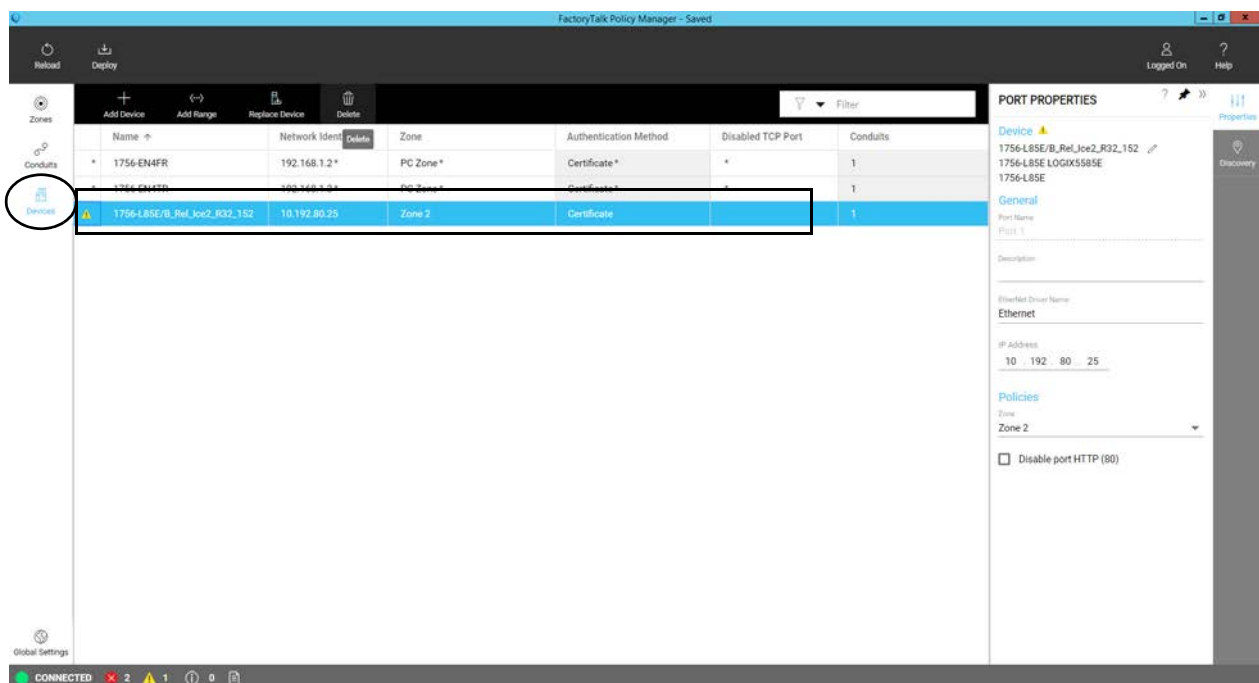
FactoryTalk Policy Manager 方法仅在设备可以访问装有 FactoryTalk Policy Manager 的计算机时才有效。

- 将设备重置为默认出厂设置。

如果设备无法访问装有 FactoryTalk Policy Manager 的计算机，则可以使用此方法。

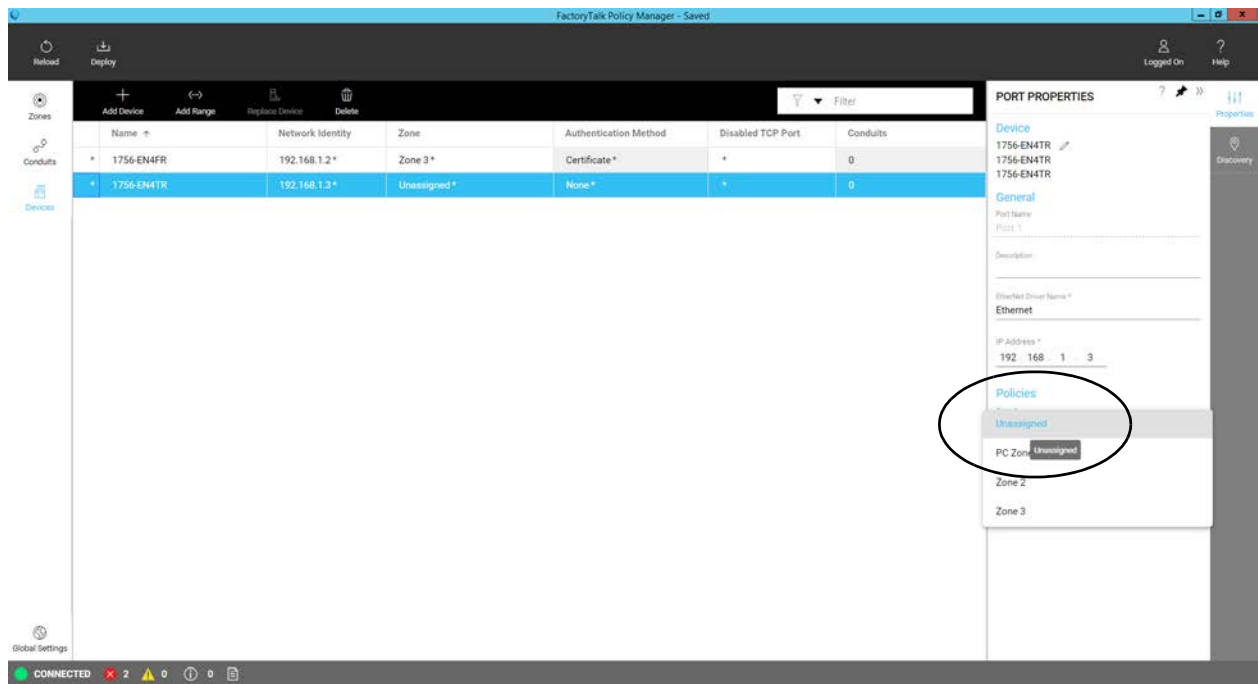
通过 FactoryTalk Policy Manager 从设备中删除安全策略 - 选项 1

1. 在 FactoryTalk Policy Manager 导航栏中，选择 **Devices**，然后选择设备。



显示 **PORT PROPERTIES**。

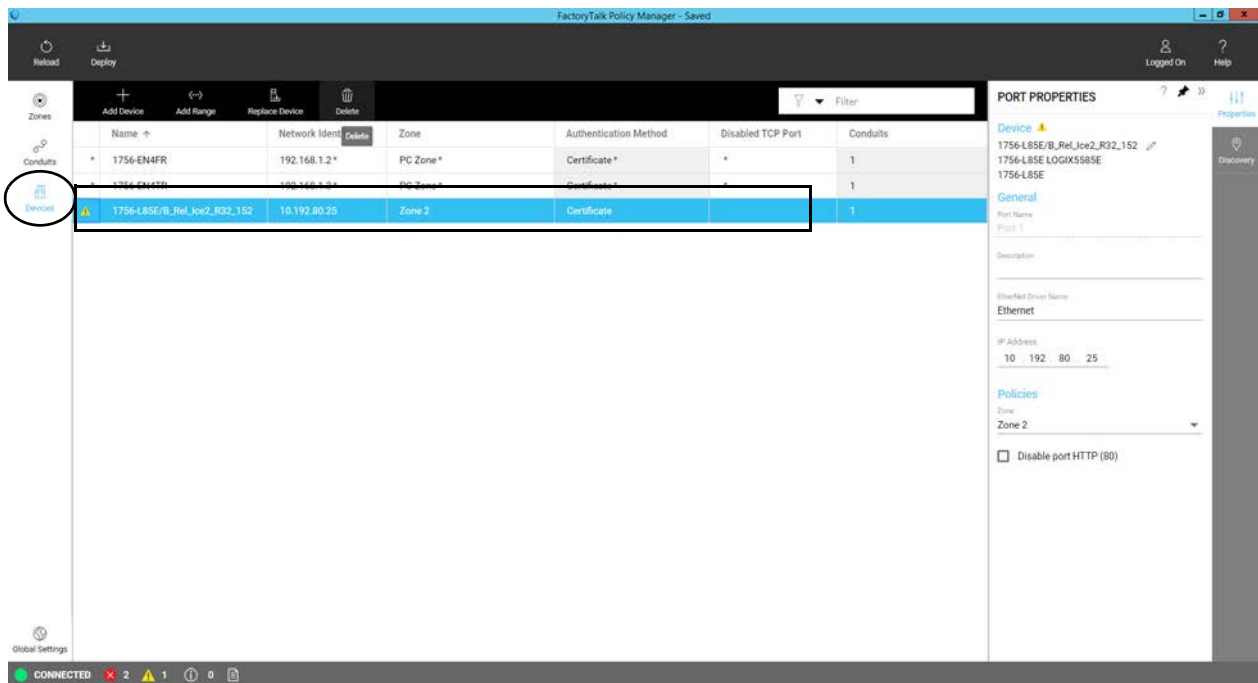
2. 在 **Policies** 区域中，更改设备的安全策略。
- 在 **Zone** 中，选择 **Unassigned** 或未启用 CIP Security 的区域。

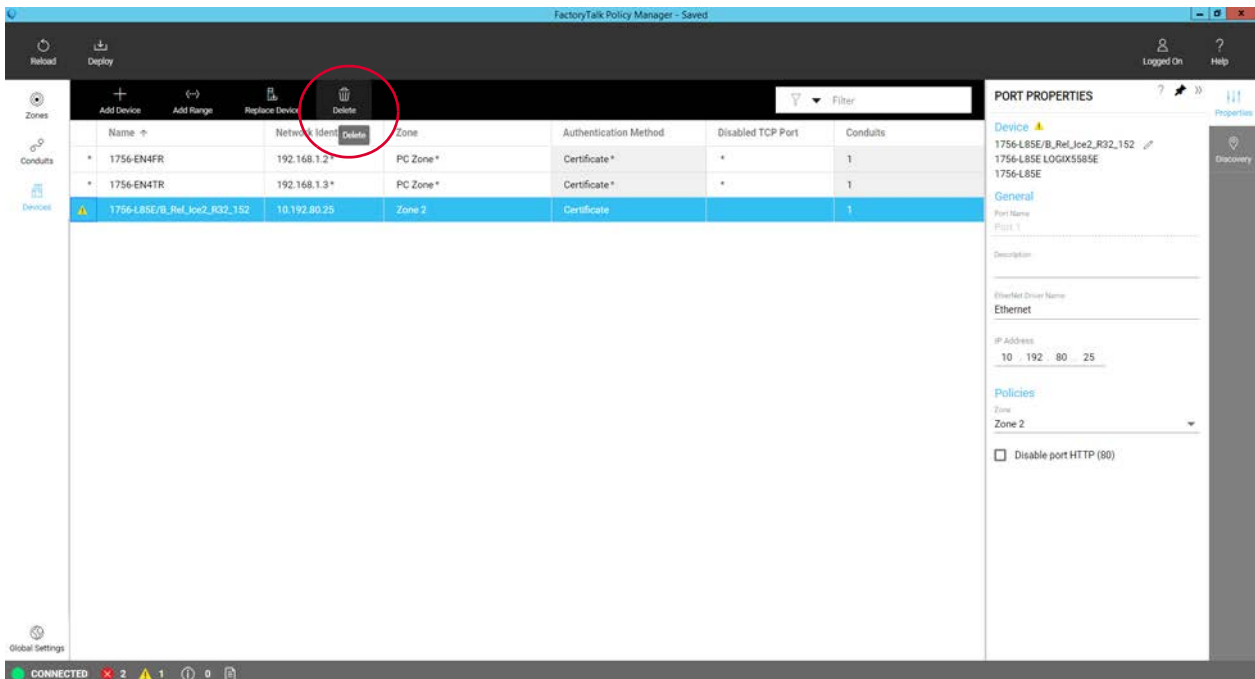


3. 按从第 44 页开始所述的方式部署安全模型，然后选择在部署期间重置通信通道。
- 设备安全策略重置为无。

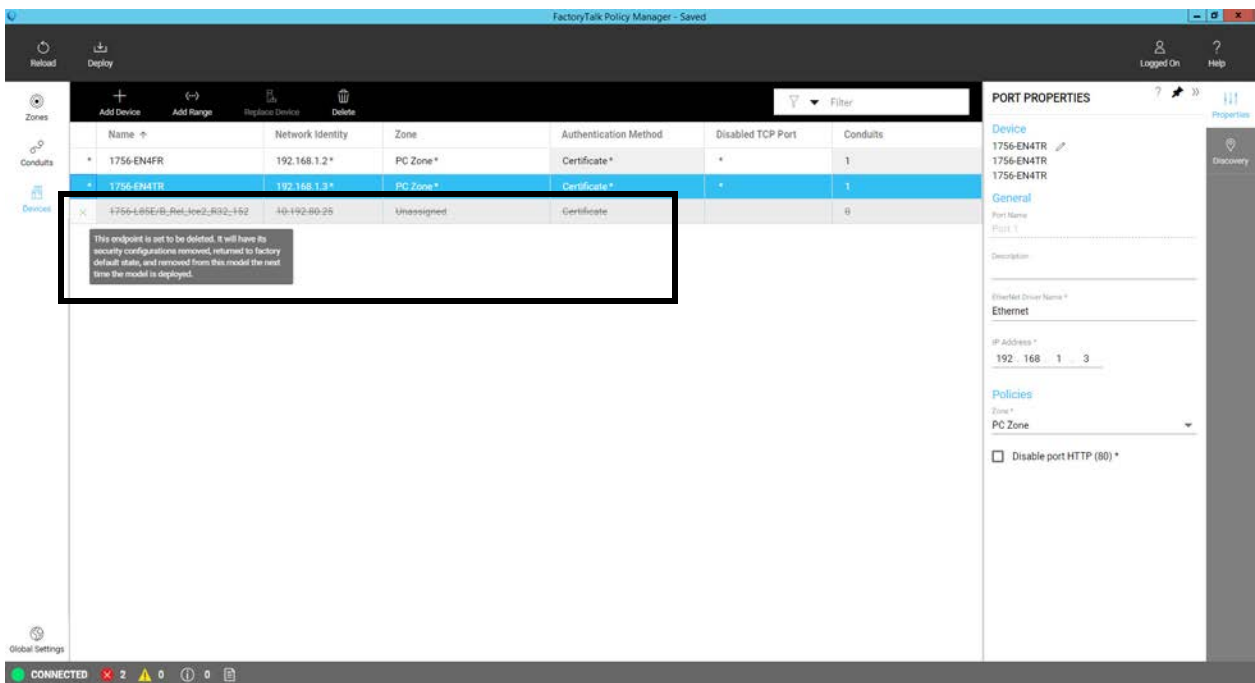
通过 FactoryTalk Policy Manager 从设备中删除安全策略 - 选项 2

1. 在 FactoryTalk Policy Manager 导航栏中，选择 **Devices**，然后选择设备。



2. 在设备列表上方，单击 **Delete**。

单击 Delete 后，设备会保留在表格中，但会被划掉。部署更新的安全模型和状态后，设备将不再显示在列表中。



3. 按从第 44 页开始所述的方式部署安全模型，然后选择在部署期间重置通信通道。

重要信息 如果 Deploy 尝试从设备中清除安全策略时无法访问该设备，则尝试失败并且安全策略保留在设备中。

通过将设备复位到出厂默认状态，从设备中删除安全策略

可将设备复位为出厂默认状态，从而从设备中删除安全策略。

重要信息 将设备复位为出厂默认设置的方法以及每个设备处于出厂默认状态时的条件各不相同。在将设备复位为出厂默认状态以删除安全策略之前，请注意复位可能对 IACS 造成的影响。将设备复位为出厂默认状态可能会以与 CIP Security 无关的方式影响整个系统。

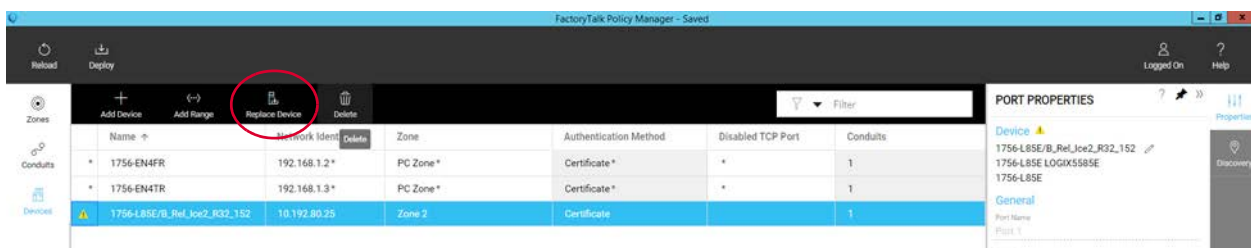
有关如何将设备复位为出厂默认状态的信息，请参见该设备的技术文档。

更换系统中支持 CIP Security 的设备

在实现了 CIP Security 的 IACS 中，按以下步骤更换 CIP Security 使能设备。在这种情况下，替换设备的类型和配置与原始设备相同，例如，相同 IP 地址。

请完成以下步骤：

1. 断开原始设备与网络的连接。
2. 将新设备连接到网络。
3. 在 FactoryTalk Policy Manager 导航栏中，选择 Replace Device。



4. 出现下列对话框时，选择何时复位模型中各端口上的设备通信，然后单击 Deploy。

Deploy Configuration to Replaced Device
? X

Deploy last deployed security configuration to following device and its port.

Device Name: 1756-L85E/B_Rel_Ice2_R32_152 3

Port Name: Port 1

EtherNet Driver Name: Ethernet

IP Address: 10.192.80.25

[View full details of deployed security configuration](#)

Any modifications to the model since last deployment will not be included in this deployment.

This device in the model will be updated with the last deployed configuration. Changing security policies requires resetting all 1756-L85E/B_Rel_Ice2_R32_152 3 communication ports, resulting in a short loss of connectivity.

Choose when to reset device communication ports included in this model:

☐ During policy deployment
New security policy is in effect once deployment is complete.

☐ After deployment
New security policy is configured on device, but does not take effect until the device's communication ports are reset.

DEPLOY
CANCEL

CIP Security 实现示例架构

本节介绍已实现 CIP Security™ 的 IACS 示例。

实现的第一阶段

在 CIP Security 实现的第一阶段，确保计算机 (PC) 区域和每个 IACS 区域之间的通信安全。通信的安全程度取决于系统需求。

有关可用于确保通信安全的 CIP™ Security 属性的更多信息，请参见第 13 页的“安全数据传输”。

建议您确保计算机区域与各 IACS 区域之间的通信安全，因为来自 Windows 操作系统的大多数漏洞存在于此。

在该阶段，完成以下任务：

- [创建区域](#)
- [创建区域至区域导管](#)
- [部署安全策略](#)

创建区域

创建区域和所有适用设备，包括支持 CIP Security 的设备和不支持 CIP Security 的设备。

- PC 区域（FactoryTalk® 站点服务器和工程师站 [EWS]）
- 单元区域 A（控制器区域）
- 单元区域 B（I/O 区域）
- 单元区域 C（控制器区域）

重要信息 本节中的示例区域都位于同一子网 /VLAN 中。

图 8 - CIP Security 架构 - 区域

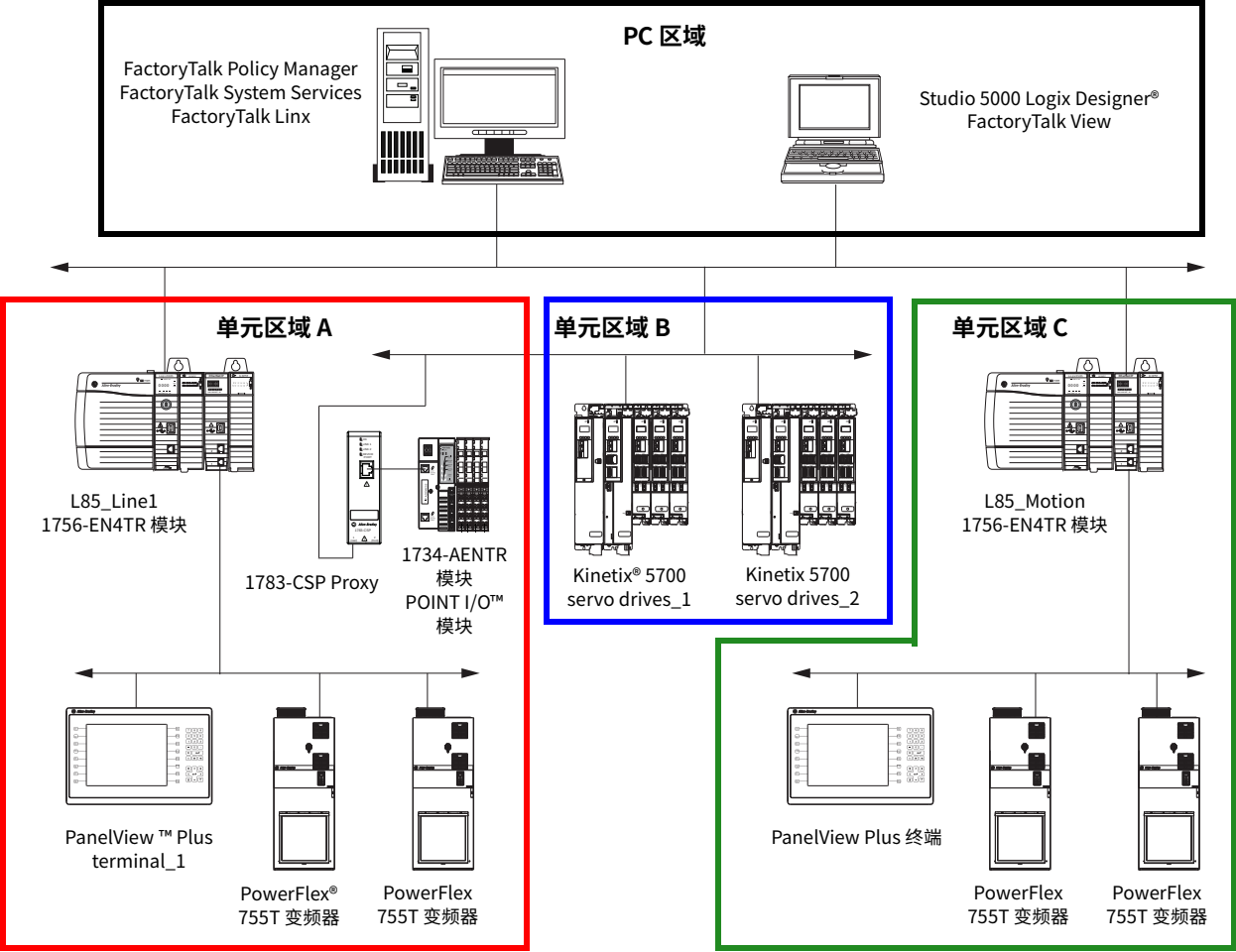


表 9 是包含区域和设备的安全矩阵。

表 9 - 安全矩阵 - 区域

PC 区域软件	单元区域 A	单元区域 B	单元区域 C
FactoryTalk Linx ⁽¹⁾ FactoryTalk Policy Manager FactoryTalk System Services	L85_Line1	Kinetix 5700 servo drives_1	L85_Motion
Studio 5000 Logix Designer ⁽¹⁾ FactoryTalk View	1756-EN4TR 模块	Kinetix 5700 servo drives_2	1756-EN4TR 模块
	1783-CSP 代理		PanelView Plus 终端 ⁽²⁾
	1734-AENTR 模块 ⁽²⁾		PowerFlex 755T 变频器
	PanelView Plus terminal_1 ⁽²⁾		PowerFlex 755T 变频器
	PowerFlex 755T 变频器		
	PowerFlex 755T 变频器		

(1) 该组软件安装在同一台服务器 / 计算机上。

(2) 该设备不支持 CIP Security。

创建区域至区域导管

1. 创建区域至区域导管，以便从 FactoryTalk Linx 数据服务器和 PC 区域中的工程师站将 CIP 安全连接到名为单元区域 A、B 和 C 的相应控制器区域。
- PC 区域至单元区域 A
 - PC 区域至单元区域 B
 - PC 区域至单元区域 C

图 9 - CIP Security 架构 - 导管

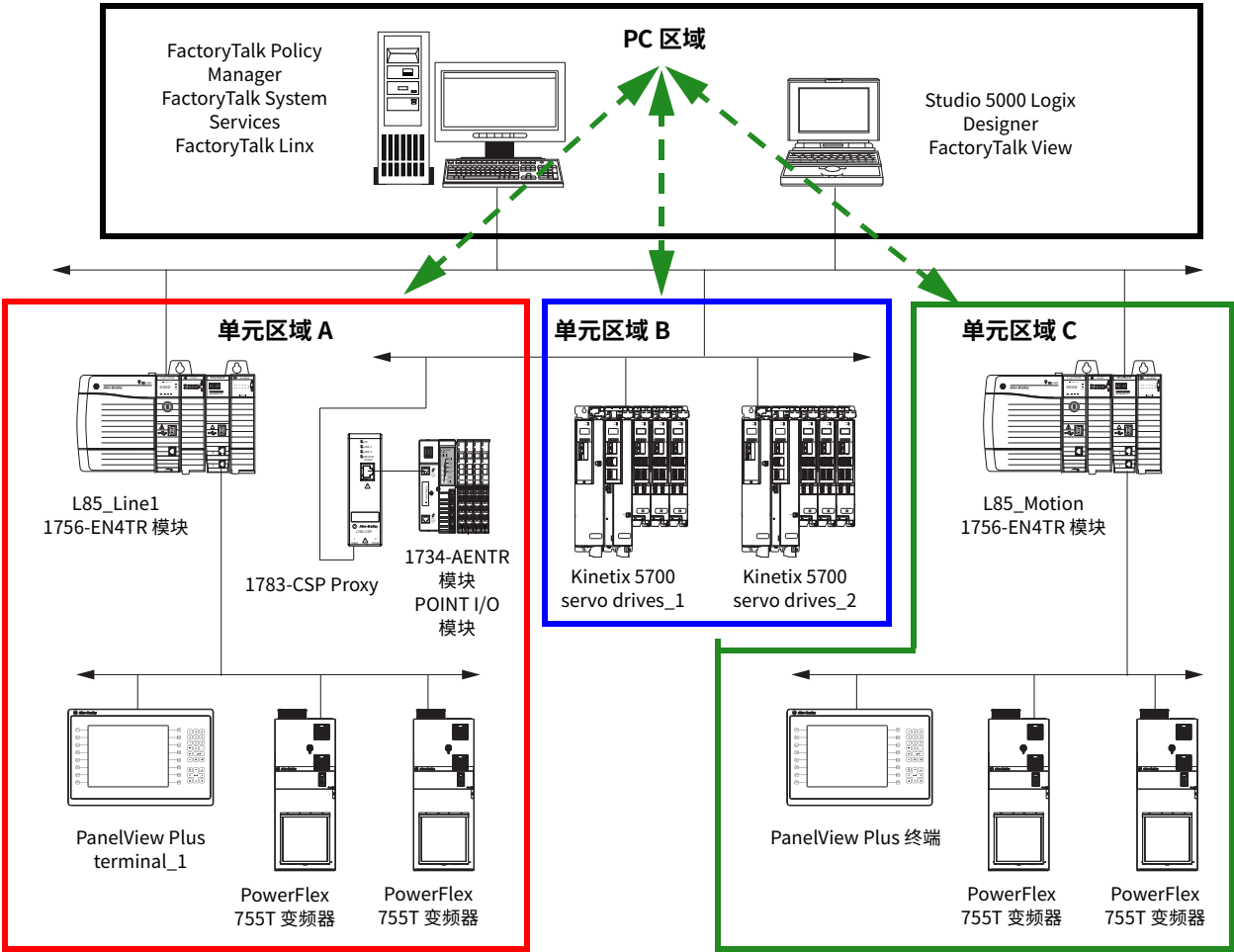


表 10 是标识和组织导管后更新的安全矩阵示例。

表 10 - 安全矩阵 - 导管

源	目标			
	PC 区域	单元区域 A	单元区域 B	单元区域 C
PC 区域	允许 ⁽¹⁾	导管 1: 区域至区域	导管 2: 区域至区域	导管 3: 区域至区域
单元区域 A	导管 1: 区域至区域	允许	拒绝	拒绝
单元区域 B	导管 2: 区域至区域	拒绝	允许	拒绝
单元区域 C	导管 3: 区域至区域	拒绝	拒绝	允许

(1) 默认路径。

配置导管安全策略

通过以下方式配置使用证书和消息完整性的导管安全策略：

- FactoryTalk Linx 软件与单元区域 A （控制器区域）中的 ControlLogix® 5580 控制器之间。
- FactoryTalk Linx 软件与单元区域 B （I/O 区域）中的 Kinetix 5700 驱动器之间。
- 通过 1756-EN4TR 通信模块，从 FactoryTalk Linx 软件到单元区域 C （控制器区域）中的 ControlLogix 5580 控制器。

或者，可以建立一个从 PC 区域到不支持 CIP Security 的设备的每个 IP 地址的允许列表。

图 10 - CIP Security 架构 - 导管安全策略

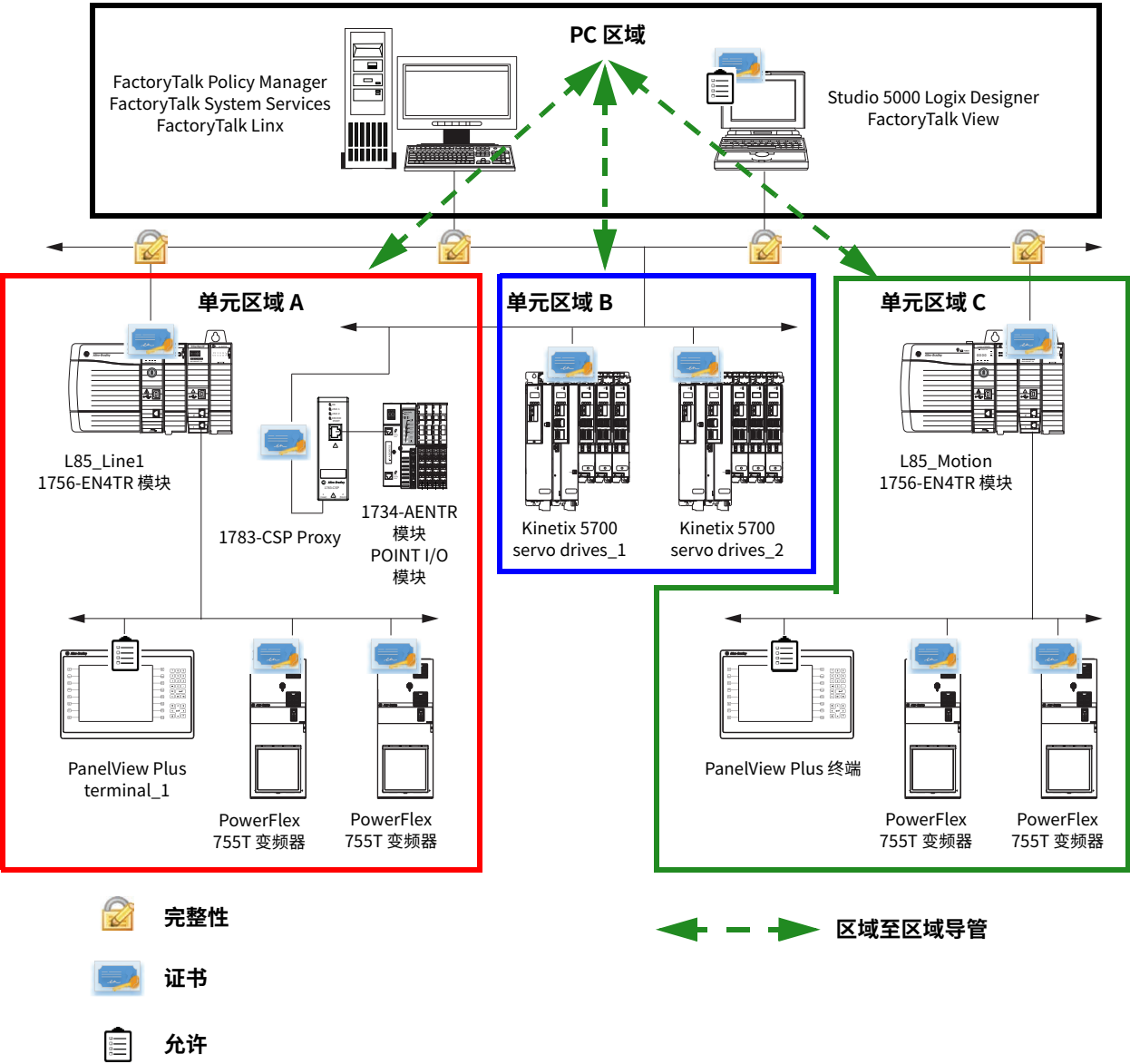


表 11 为配置导管安全策略后更新的安全矩阵示例。

表 11 - 安全矩阵 - 导管安全策略矩阵

确保 Linux 通信安全：导管 1、2 和 3		区域至区域		安全策略
区域至区域 (确保与 FactoryTalk Linx 的通信安全。)	PC 区域	单元区域 A		· 证书 · 完整性 · 保密性
	PC 区域	单元区域 B		
	PC 区域	单元区域 C		
可信 IP（允许）	区域设备至区域设备			
(不支持 CIP Security 的设备)	PC 区域 设备：FactoryTalk® Network Manager™ IP 地址： 192.168.1.100	单元区域 A - 设备	· L85_Line1 (192.168.1.8) · 1756-EN4TR 模块 (192.168.1.9) · 1783-CSP 代理 (192.168.1.10) · 1734-AENTR 模块 (192.168.1.11) · PanelView Plus terminal_1 (192.168.1.12) · PowerFlex 755T 变频器 (192.168.1.13) · PowerFlex 755T 变频器 (192.168.1.14)	
		单元区域 C - 设备	· L85_Motion (192.168.3.8) · 1756-EN4TR 模块 (192.168.3.9) · PanelView Plus 终端 (192.168.3.10) · PowerFlex 755T 变频器 (192.168.3.11) · PowerFlex 755T 变频器 (192.168.3.12)	

部署安全策略

按第 44 页所述将安全策略部署至设备。

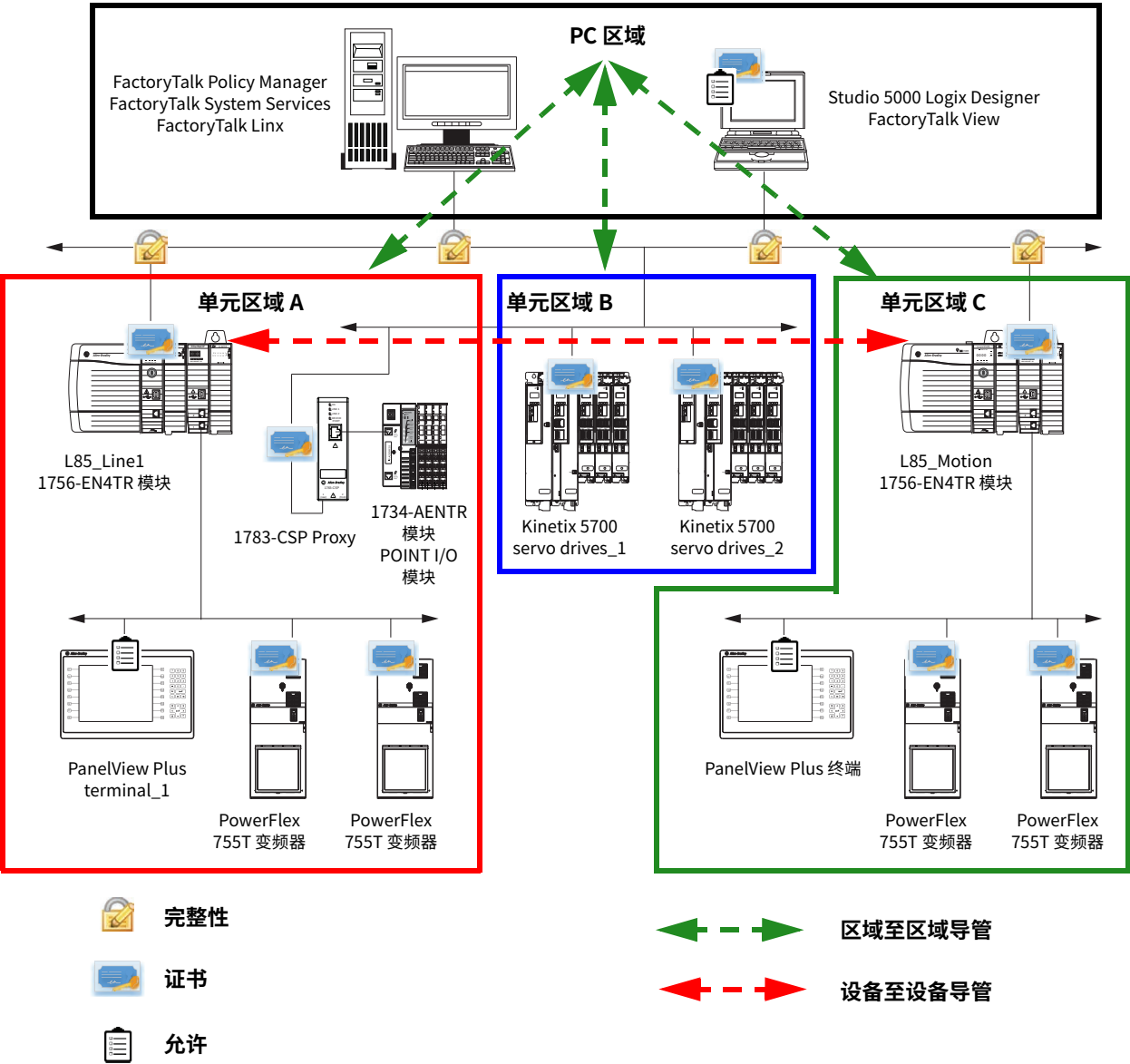
实现的第二阶段

在 CIP Security 实现的第二阶段，确保设备与设备之间的通信安全，以实现微分段。使用在第一阶段创建的现有区域。

创建设备至设备导管

创建一个设备至设备导管，以确保从单元区域 A（控制器区域）中的 ControlLogix 5580 控制器到单元区域 C（控制器区域）中的 ControlLogix 5580 控制器的 CIP 连接安全。

图 11 - CIP Security 架构 - 增加了设备至设备导管



创建区域至设备的导管

创建从单元区域 B (I/O 区域) 中的 Kinetix 5700 驱动器到单元区域 C (控制器区域) 中的 ControlLogix 5580 控制器的区域至设备导管。

图 12 - CIP Security 架构 - 增加了区域至设备导管

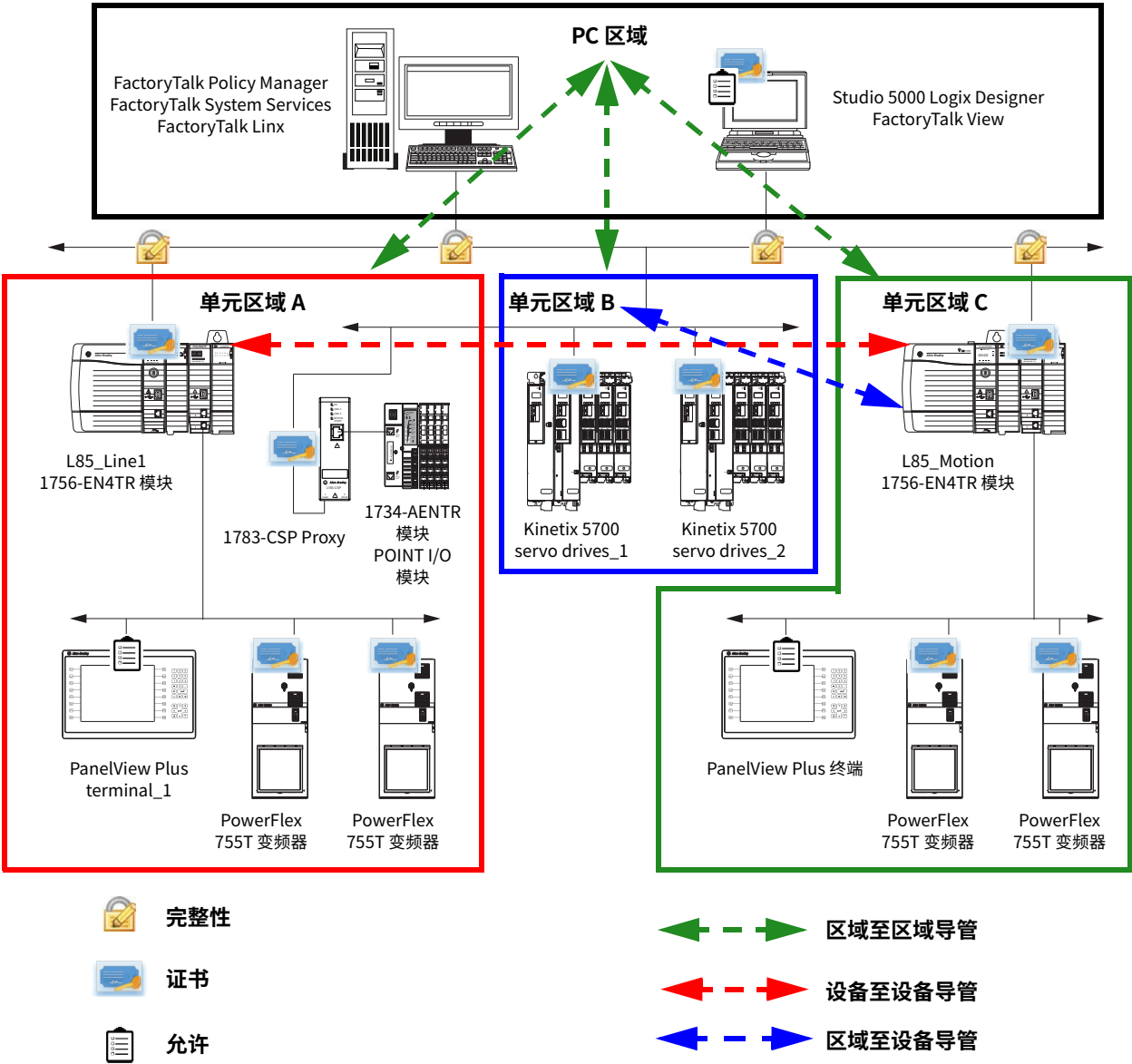


表 12 是标识和组织导管后更新的安全矩阵示例。

表 12 - 安全矩阵 - 增加了设备至设备以及区域至区域导管

源	目标			
	PC 区域	单元区域 A	单元区域 B	单元区域 C
PC 区域	允许 ⁽¹⁾	导管 1: 区域至区域	导管 2: 区域至区域	导管 3: 区域至区域
单元区域 A	导管 1: 区域至区域	允许	拒绝	导管 4: 设备至设备
单元区域 B	导管 2: 区域至区域	拒绝	允许	导管 5: 区域至设备
单元区域 C	导管 3: 区域至区域	拒绝	拒绝	允许

(1) 默认路径。

创建导管安全策略

在导管 4 和导管 5 的端点之间创建使用证书、消息完整性和数据加密的导管安全策略。

图 13 - CIP Security 架构 - 导管安全策略

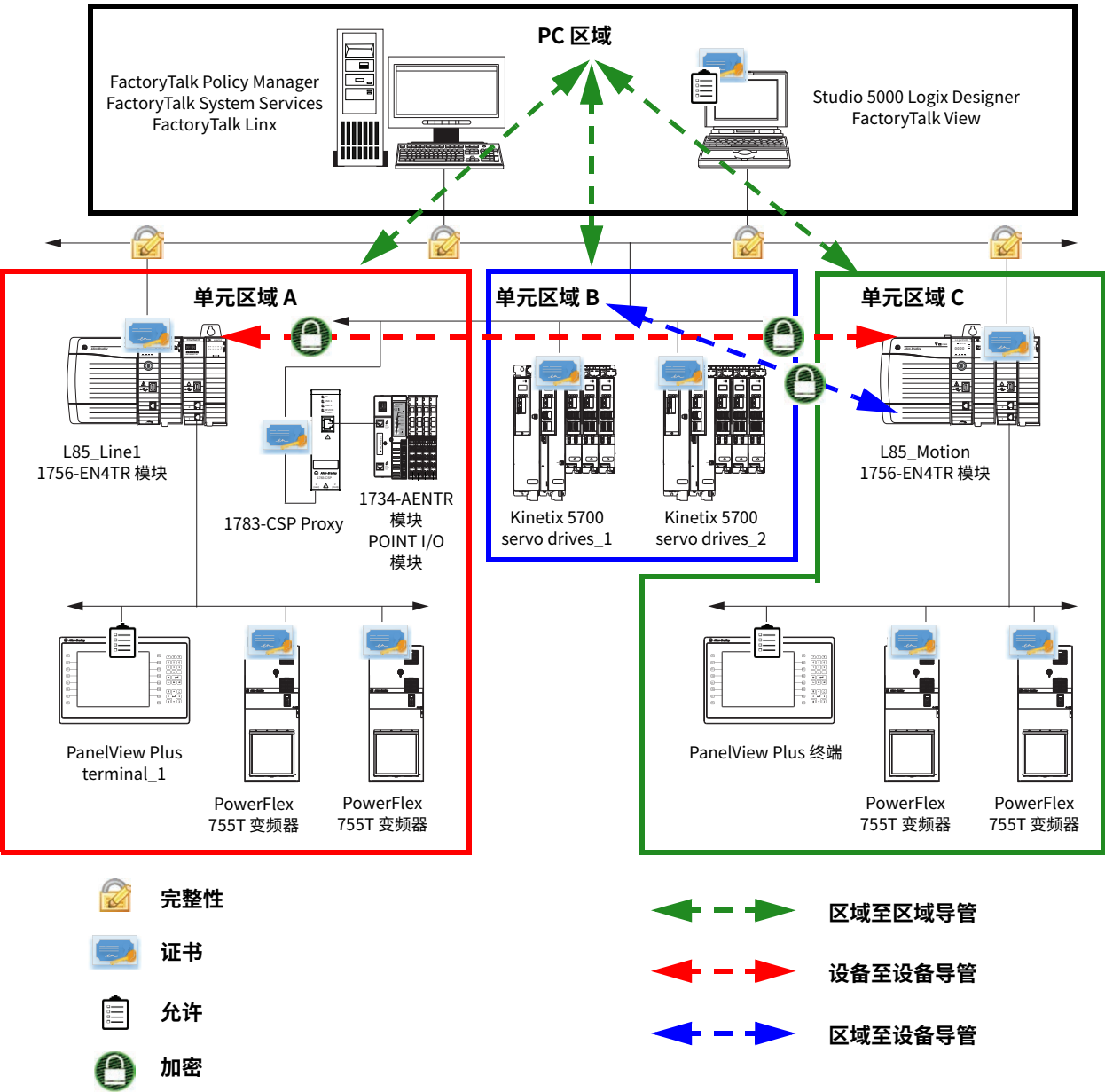


表 13 为配置导管安全策略后更新的安全矩阵示例。

表 13 - 安全矩阵 - 导管安全策略矩阵

确保 Linux 通信安全：导管 1、2 和 3	区域至区域		安全策略
区域至区域 (确保与 FactoryTalk Linx 的通信安全。)	PC 区域	单元区域 A	· 证书
	PC 区域	单元区域 B	· 完整性
	PC 区域	单元区域 C	· 保密性
安全控制器通信：导管 4	设备至设备		安全策略
(确保与发起方和目标的通信安全)	L85_Line1	L85_Motion	· 证书 · 完整性 · 保密性
安全 I/O 通信：导管 5	区域至设备		安全策略
(确保与发起方和目标的通信安全)	L85_Motion	单元区域 B	· 证书 · 完整性 · 保密性
可信 IP (允许)	区域设备至区域设备		
(不支持 CIP Security 的设备)	PC 区域 设备：FactoryTalk Network Manager IP 地址： 192.168.1.100	单元区域 A - 设备	· L85_Line1 (192.168.1.8) · 1756-EN4TR 模块 (192.168.1.9) · 1783-CSP 代理 (192.168.1.10) · 1734-AENTR 模块 (192.168.1.11) · PanelView Plus terminal_1 (192.168.1.12) · PowerFlex 755T 变频器 (192.168.1.13) · PowerFlex 755T 变频器 (192.168.1.14)
		单元区域 C - 设备	· L85_Motion (192.168.3.8) · 1756-EN4TR 模块 (192.168.3.9) · PanelView Plus 终端 (192.168.3.10) · PowerFlex 755T 变频器 (192.168.3.11) · PowerFlex 755T 变频器 (192.168.3.12)

部署安全策略

按[第 44 页](#)所述将更新后的安全策略部署至设备。

注：

数字

1783-CSP CIP Security Proxy

描述 17

A

安全策略

从设备中删除 49 - 56

安全策略属性

导管 23

区域 22

安全矩阵

导管 59

区域和设备 33, 58

安全模型

备份 47

部署 44 - 46

安全评估

执行风险评估 9

执行漏洞评估 9

执行威胁评估 9

B

备份

安全模型 47

FactoryTalk Directory 47

部署

安全模型 44 - 46

处于工作模式的控制器无法部署 24

C

CIP 桥接 27

CIP Security 属性

设备标识和身份验证 14

数据保密性 14

数据完整性和身份验证 14

CIP Security 组件 19 - 21

导管 21

区域 20

设备 19

ControlLogix 5580 控制器

描述 17

ControlLogix EtherNet/IP 通信模块 (1756-EN4TR)

描述 17

D

导管 21, 36 - 42

安全策略属性 23

安全矩阵 59

创建 37 - 41

配置 41

对策

- 设备标识和身份验证 11
- 数据保密性 11
- 数据完整性和身份验证 11

多播连接 29

F

FactoryTalk Administration Console

- 从 FactoryTalk Linx 中删除安全配置 51

FactoryTalk Directory

- 备份 47

FactoryTalk Linx

- 描述 16

FactoryTalk Policy Manager

- 从设备中删除安全策略 49 - 56
- 描述 16

FactoryTalk System Services

- 备份 47

- 恢复 48

- 描述 16

风险评估 9

G

攻击类型

- 监视数据 8
- 拒绝服务 8
- 中间人攻击 8

H

恢复

- FactoryTalk System Services 48

J

监视数据攻击 8

拒绝服务攻击 8

K

Kinetix 5300 驱动器

- 描述 17

Kinetix 5700 驱动器

- 描述 17

L

连接

- 多播 29

漏洞评估 9

P

PowerFlex 755T 变频器

- 描述 17

Q

- 区域 20, 32 - 35
 - 安全策略属性 22
 - 安全矩阵 33
 - 创建 33
 - 配置 35

S

- Studio 5000 Logix Designer
 - 描述 16
- 删除安全策略
 - 从软件应用程序中 49 - 52
 - 从设备中 53 - 56
- 设备标识和身份验证 12
 - 描述 14
 - 预共享密钥 12
 - 证书 12
- 深度防御架构 10
- 数据保密性
 - 描述 14
- 数据完整性和身份验证
 - 描述 14
- 双端口设备
 - CIP Security 限制 24

W

- 网络地址转换
 - CIP Security 限制 27
- 威胁评估 9

X

- 限值
- 无法从非安全工作站下载 25
- 限制
 - CIP 桥接 27
 - 处于工作模式的控制器无法部署 24
 - 多播连接 29
 - 工作站和控制器之间无法连接 26
 - 使用双端口设备 24
 - 使用网络地址转换 27
 - 自动设备更换 29

Y

- 预共享密钥 12

Z

- 证书 12
- 支持 CIP Security 的
 - 软件 15
 - FactoryTalk Linx 16
 - FactoryTalk Policy Manager 16
 - FactoryTalk System Services 16
 - Studio 5000 Logix Designer 16
 - 硬件 17
 - 1783-CSP CIP Security Proxy 17
 - ControlLogix 5580 控制器 17

ControlLogix EtherNet/IP 通信模块 (1756-EN4TR) 17
Kinetix 5300 驱动器 17
Kinetix 5700 驱动器 17
PowerFlex 755T 变频器 17
中间人攻击 8
自动设备更换 29

其他资源

以下文档包含有关罗克韦尔自动化相关产品的附加信息。

资源	说明
FactoryTalk Policy Manager Getting Results Guide, 出版号: FTALK-GR001 。	介绍如何安装和使用 FactoryTalk System Services 和 FactoryTalk Policy Manager。
FactoryTalk Security System Configuration Guide Quick Start, 出版号: FTSEC-QS001	介绍如何将 FactoryTalk Services Platform 与 FactoryTalk Security 结合使用。
Deploying CIP Security in a Converged Plantwide Ethernet Architecture Design Guide, 出版号: ENET-TD022	介绍安全架构的用例, 用于在工厂范围或站点范围工业自动化和控制系统 (IACS) 应用程序中设计和部署 CIP Security 技术。
System Security Design Guidelines Reference Manual, 出版号: SECURE-RM001	介绍有关如何使用罗克韦尔自动化产品提高工业自动化系统安全性的指南。
《ControlLogix 5580 和 GuardLogix 5580 控制器用户手册》, 出版号: 1756-UM543	介绍如何设计、实施和维护使用 ControlLogix® 或 GuardLogix® 控制器的工业控制系统。
ControlLogix EtherNet/IP Network Devices User Manual, 出版号: 1756-UM004	介绍 ControlLogix EtherNet/IP 通信模块如何与 Logix 5000™ 控制器配合使用, 以及如何与 Ethernet/IP 网络上的设备进行通信。
《Kinetix 5700 伺服驱动器用户手册》, 出版号: 2198-UM002	介绍在 Logix 5000 控制系统中 Kinetix® 5700 驱动器系统如何与相关联电源、单轴逆变器、双轴逆变器和附加模块配合使用。
《PowerFlex 750 系列交流变频器参考手册》, 出版号: 750-PM001	介绍如何安装、启动 PowerFlex 750 系列交流变频器以及如何如何进行故障排除。
《Kinetix 5300 伺服驱动器用户手册》, 出版号: 2198-UM005	介绍如何在 Logix 5000 控制系统中使用 Kinetix 5300 驱动系统和相关电源与附件模块。
CIP Security Proxy User Manual, 出版号: 1783-UM013	介绍如何使用 CIP Security Proxy 为不支持 CIP Security 的设备提供安全通信。
Industrial Automation Wiring and Grounding Guidelines, 出版号: 1770-4.1	提供安装罗克韦尔自动化工业系统的通用准则。
产品认证网站: rok.auto/certifications	提供符合性声明、证书和其他认证详细信息。

可访问 [rok.auto/literature](#) 查看或下载相关出版物。

罗克韦尔自动化支持

使用下列资源访问支持信息。

技术支持中心	通过操作方法视频、常见问题解答、聊天室、用户论坛和最新产品通知获取帮助。	rok.auto/support
知识库	访问知识库文章。	rok.auto/knowledgebase
本地技术支持电话号码	查找您所在国家 / 地区的技术支持热线。	rok.auto/phonesupport
文献库	查看安装指南、手册、宣传册和技术数据出版物。	rok.auto/literature
产品兼容性与下载中心 (PCDC)	下载固件、关联文件（如 AOP、EDS 和 DTM）并查看产品发布说明。	rok.auto/pcdc

文档反馈

您的意见将有助于我们改进文档，更好地满足您的要求。如有任何关于如何改进本文档的建议，请填写 rok.auto/docfeedback 上提供的表格。

Allen-Bradley、Compact 5000、CompactLogix、ControlLogix、expanding human possibility、FactoryTalk、FactoryTalk Network Manager、FLEX 5000、Kinetix、Logix 5000、POINT I/O、PowerFlex、PanelView、Rockwell Automation、RSLinx、Stratix、Studio 5000 和 Studio 5000 Logix Designer 是罗克韦尔自动化公司的商标。

CIP、CIP Security 和 EtherNet/IP 是 ODVA 公司的商标。
不属于 Rockwell Automation 的商标是其各自所属公司的财产。

罗克韦尔自动化在其网站 rok.auto/pec 上保留最新产品环境合规信息。

联系我们。    

rockwellautomation.com _____ expanding human possibility™

美洲地区：罗克韦尔自动化，南二大街 1201 号，密尔沃基市，WI 53204-2496 美国，电话：(1) 414.382.2000，传真：(1) 414.382.4444
欧洲/中东/非洲：罗克韦尔自动化，NV, Pegasus Park, De Kleetlaan 12a, 1831 布鲁塞尔，比利时，电话：(32) 2 663 0600，传真：(32) 2 663 0640
亚太地区：罗克韦尔自动化，香港数码港道 100 号数码港 3 座 F 区 14 楼 1401-1403，电话：(852) 2887 4788，传真：(852) 2508 1846
中国总部：上海市徐汇区虹梅路 1801 号宏业大厦，邮编：200233，电话：(86 21) 6128 8888，传真：(86 21) 6128 8899
客户服务电话：400 620 6620 (中国地区) +852 2887 4666 (香港地区)

出版物 SECURE-AT001B-ZH-P - 2021 年 8 月

© 2021 年 罗克韦尔自动化公司版权所有。保留所有权利。美国印刷。