

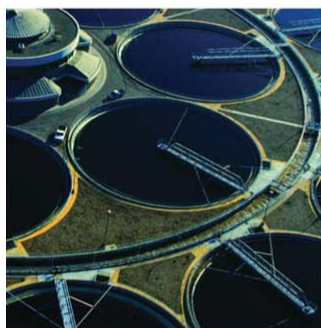
User Manual

Original Instructions

PlantPax
Distributed Control System

PlantPax Distributed Control System **Infrastructure Configuration**

System Release 4.5



Important User Information

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

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

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

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

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

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

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

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



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



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

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

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



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



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



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

Preface

Purpose of the User Manual.....	9
New and Updated Information.....	10
Manual Conventions.....	10
Default User Name.....	11
Rebranding of FactoryTalk Linx Software.....	12
Action Identifier.....	12
Configure Programs Menu.....	12
Additional Resources.....	14

Chapter 1

Configure Network Infrastructure

Overview.....	15
PlantPAx Topology Examples.....	16
VLAN Basics.....	17
Common Network Switch Configurations.....	20
Verify Workstation IP Address Settings.....	20
Configure the Switch Express Setup.....	21
Complete Switch Optimization.....	28
Distribution Switch Configuration.....	37
Enable Switch Routing.....	37
Configure EtherChannels (Link Aggregation).....	38
Configure Switch Ports.....	39
Using a Terminal Emulator (PuTTY).....	41
Enabling IP Helper.....	43

Chapter 2

Control Network Switch Configurations

Configure Smartports.....	47
Identify Connected Devices with a Port Description.....	51
I/O Network Switch Configuration.....	52
Star Topology Switch Configuration.....	53
Configure Controller Switches.....	54
Configure I/O Switches.....	55
Configure MCC Switches.....	56
Ring Topology Switch Configuration.....	58
Configure Controller Switches.....	59
Enable a DLR.....	60
Configure MCC Switches.....	62
Redundant Star Switch Configuration.....	63
Configure Controller Switches.....	64
Configure PRP Distribution.....	68
Enable PRP I/O (RedBox) Switch.....	71
Configure MCC Switches.....	72
Optimize Switches for Redundant Controllers.....	73
Configure Switch Routing.....	73
Configure a Static IP Address.....	74

Configure System Servers**Chapter 3**

Considerations.....	78
Configure the Primary Domain Controller.....	79
Configure a Secondary Domain Controller.....	86
Create a Reverse DNS Lookup Zone.....	93
Map Host Name to IP Address	96
Enable DHCP in the Primary and Secondary Controllers.....	99
Add DHCP Server Role.....	99
Configure DHCP Server.....	102
Enable DHCP Scope (Control Network)	104
Enable DHCP Scope (Supervisory Network)	107
Configure Failover.....	110
Join the Domain	113
Confirm Computers in DNS Server.....	116
Confirm Computers in DHCP Server.....	117
Create Groups and Users	118
Unit Groups	118
Role Groups	119
Area Groups	121
Create Users	123
Assign Users to a Group.....	125

**Configure Group Policy
Management****Chapter 4**

Considerations.....	131
Default Domain Controller Policy.....	133
Configuring the NTP Server	133
Configuring Windows Time Service	139
Enforcing the Domain Controller Policy	140
Default Domain Policy	143
Configuring an NTP Client.....	143
Configuring Windows Time Service	147
Configuring Password Strength.....	148
Configuring Account Lockout Policy	150
Configuring Kerberos Policy	154
Configuring an Interactive Logon.....	155
Enforcing the Domain Policy.....	158
PlantPAx Users Policy Object.....	160
Define Group Access Level.....	160
USB Drive Protection	161
Configure Portable Device Enumerator Service	163
Software Access Restriction	165

Configure FactoryTalk Components	Chapter 5	
	Considerations.....	167
	Configure the FactoryTalk Directory	169
	Enable Windows Firewall	171
	Define Network Directory	172
	Use FactoryTalk Activation to Apply Licenses.....	175
	Open Activation Manager.....	175
	Use FactoryTalk Patches From the PCDC	177
Configure FactoryTalk Security	Chapter 6	
	Considerations.....	183
	Configure FactoryTalk Users and Groups	185
	Assign User Domain to FactoryTalk Directory.....	185
	Create Internal Users and Groups.....	191
	Define FactoryTalk System Policies	193
	Use Default Terminal Client	193
	Use the Same FactoryTalk Log On.....	194
	Restrict Application Authorization	195
	Audit Security Actions.....	196
	Define the Security System Policy.....	197
	Define FactoryTalk Product Policies	199
Create Permission Sets.....	200	
Configure the Controller	Chapter 7	
	Consideration	203
	Use Architect for Controller Initiation.....	205
	Change Controller Properties	207
	Configure Network Adapters	210
	Synchronize the Project.....	212
	Configure RSLinx Classic Software	213
	Download the Controller.....	216
	Enable Controller Security.....	217
	Create a Controller Logical Name	219
	Configure Authority Identifier	220
	Configure Communication Restrictions.....	223
	Configure Data Restrictions.....	224
	Configure Code Restrictions	225

	Chapter 8	
Configure Time Synchronization	Considerations.....	233
	Configure UTC Time Source	234
	Configure Internet Time Synchronization.....	234
	NTP to PTP Clock Conversion	236
	Configure GPS Time Synchronization	236
	Configure PTP Time Synchronization for Ethernet Bridges	239
	Enable Switch Port Modes	240
	Configure PTP Time Synchronization for Controllers.....	241
	Chapter 9	
Configure the Process	Considerations.....	243
Automation System Server (PASS)	Configure Servers on PASS	245
	Configure the Application	245
	Configure the HMI Server	247
	Primary HMI Server.....	247
	Configure the Data Server.....	250
	Configure the Alarm and Event Server	254
	Commit Project.....	256
	Configure Redundancies.....	257
	Enable HMI Redundancy	257
	Enable Data Server Redundancy	266
	Shortcut Configuration Paths	267
	Redundant ControlLogix Controller.....	274
	Enable Alarm and Event Redundancy	279
	Create Alarm and Event Database	281
	Define HMI Security	284
	Configure FactoryTalk SE Security	284
	Configure PanelView Plus	293
	Create a FactoryTalk View ME Project.....	293
	Configure FactoryTalk View ME Security	300
	Configure Time Synchronization for PanelView Terminals ..	306
	Download the Application	309

Configure an Application Server Information Server (AppServ- Info)

Chapter 10

Considerations.....	313
FactoryTalk Historian	313
FactoryTalk VantagePoint	313
Configure Historian SE Server Collective	315
Create a Firewall Rule for Primary Historian Server	315
Create a Firewall Rule for Secondary Historian Servers	318
Change the Historian Identification	319
Set Security Settings	321
Create a Server Collective	327
Configure a Historian SE Server.....	331
Create a Historian Server.....	331
Create a Synchronization Path.....	336
Configure a Node Interface	342
Configure Primary Node Interface Server.....	342
Configure Secondary Node Interface Server	358
Configure FactoryTalk Live Data Connectors	358
Configure a FactoryTalk Live Data Primary Connector.....	359
Configure a FactoryTalk Live Data Secondary Connector....	362
Confirm Unit Failover Diagnostics	370
Configure Performance Monitor Interface	373
Create PIPerfMon System User.....	373
Configure the PIPerfMon Interface	375
Import PIPerfMon Digital State	379
Create PIPerfMon Interface Health Points	382
Monitor PIPerfMon Interface	386
Enable Performance Monitor	387
Adding PIPerfMon User	387
Adding PIPerfMon Firewall Rule	390
Enabling PIPerfMon Counter Service	395
Configure FactoryTalk Historian Connectivity.....	396
View PI Builder Excel Add-in	398
Configure FactoryTalk VantagePoint Historian Tags	399

Chapter 11

Considerations.....	403
Configure Diagnostic Settings.....	405
View Audit Log	407

Configure Asset Management (AppServ-Asset)

Appendix A

Access the Attachments

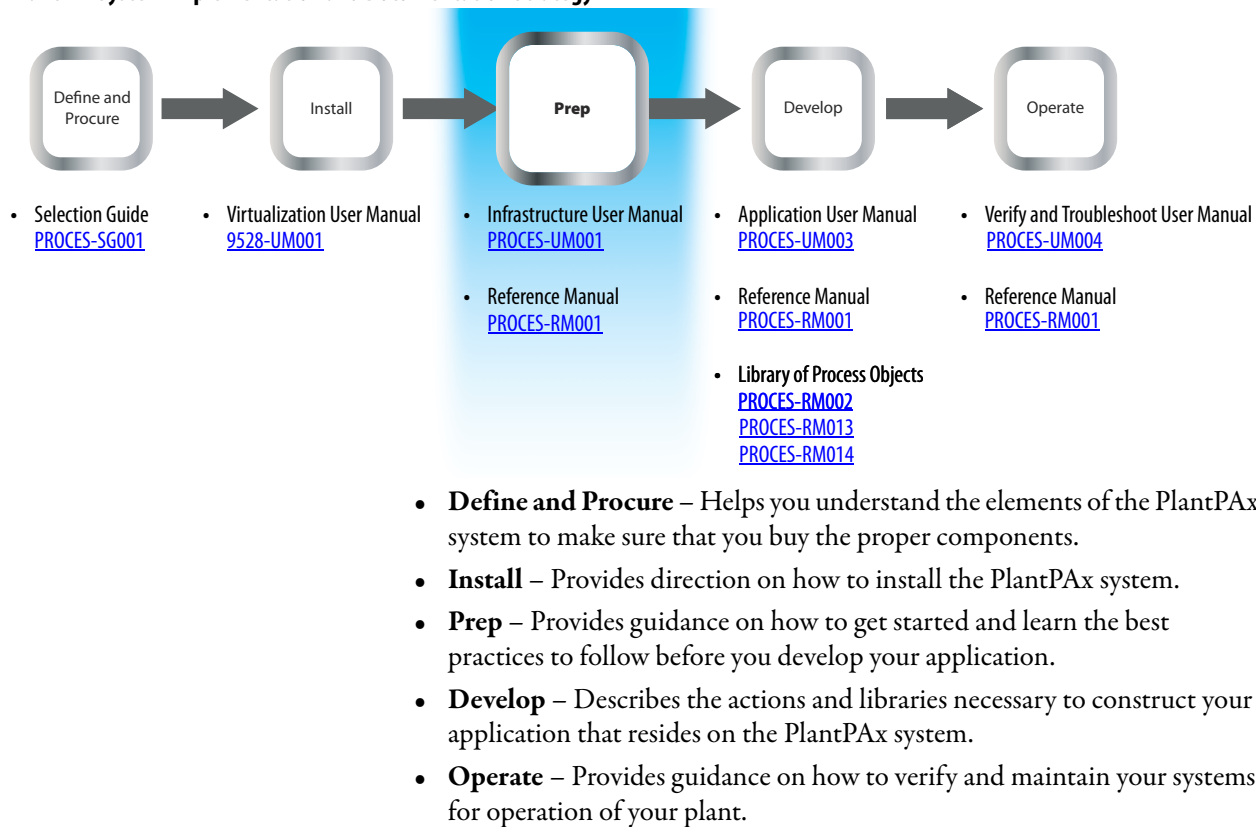
Open Content	409
How to Use Attachments	410

Define a Workgroup and DeskLock Utility	Appendix B
	Enable the Windows DeskLock Utility (optional) 413
Firewall Configurations	Appendix C
	Common Ports 417
	Rockwell Automation TCP/UDP Ports 417
	Index
 421

The PlantPAx® system provides a modern approach to distributed control by using common technology (integrated architecture) shared with all other automation disciplines within the plant. This approach creates a seamless information flow across the plant to create optimization opportunities and enables a Connected Enterprise.

Our scalable platform provides you with the flexibility to implement a system appropriate for your application. [Figure 1](#) shows the documents (this manual in the highlighted section) that are available to help design and implement your system requirements.

Figure 1 - PlantPAx System Implementation and Documentation Strategy



Purpose of the User Manual

This manual provides screen facsimiles and step-by-step procedures to configure infrastructure components for your system requirements. While flexibility and scalability are among the strengths of the PlantPAx system, we offer suggestions, such as how to set IP addresses and naming conventions, to help you get started. We suggest that you perform the tasks in the order that is outlined in each chapter. However, we explain each procedure from the start to help you reference specific topics if you choose to skip around to other chapters.

Each chapter has a flowchart that summaries the topics, similar to a mini Table of Contents. See [page 10](#) for descriptions of the tools that are used in the documentation.

New and Updated Information

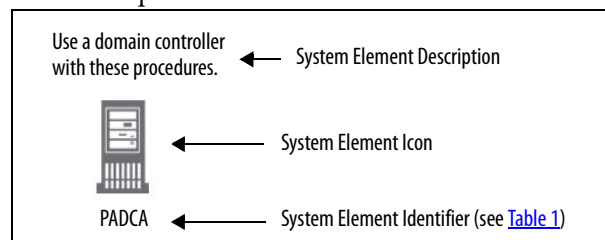
This table contains the changes that are made to this revision.

Topic	Page
PlantPAx infrastructure revised with three network layers: Supervisory, Control, and I/O.	16
Procedures added for security exception for CRYPTO version of Stratix® switches.	22
Control network switch configurations added to Chapter 1.	37
Terminal emulator interface and Port Link Aggregation (EtherChannel) procedures added.	41
PlantPAx system common topologies added to Chapter 2.	46
I/O Network switch configuration procedures include Star, Ring, and Redundant Star.	52
Parallel Redundant Protocol (PRP) and Redbox functionality added for I/O Network.	63
Reverse DNS Lookup Zone aids database search for computer name via IP address.	93
IP address scope and range added for Control and Supervisory Networks.	104, 107
Group policy procedures include units, roles, and areas.	118, 119, 121
Password strength, account lockout, network authentication policies added to group policy management.	148, 150, 154
Procedures added to import roles and areas.	187, 189
Shortcut configuration paths added for enabling redundant controllers.	267
Security codes revised for user permissions on workstations.	288
PIPerMon interface procedures added to enhance evaluation of system performance.	373

Manual Conventions

For instructional purposes, this manual uses visual tools to complement the procedures. Icons that represent system elements are shown at the start of a section to help identify the system element that is being configured in the steps.








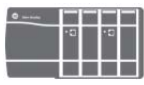
The abbreviation for an element is listed with the icon for identification as shown in the example.



See [page 11](#) for visual naming conventions.

See [Table 1](#) for descriptions and abbreviations of the system element icons.

Table 1 - Visual Naming Conventions

Icon	Description	Abbreviation Element Names	Topic Page
	Stratix switch	<ul style="list-style-type: none"> Stratix 5400 or Stratix 5410 Layer 2 access switch Stratix 5700 Layer 2 access switch 	16, 21, 29, 31, 33, 35, 38, 53, 59, 55, 56, 58, 63, 64, 68, 71, 72
	Stratix switch	<ul style="list-style-type: none"> Stratix 5400 or Stratix 5410 Layer 3 distribution switch 	16, 21, 29, 31, 33, 35, 37, 39, 63, 73, 231, 232
	PlantPAx Domain controllers	<ul style="list-style-type: none"> PADCA⁽¹⁾ - PlantPAx parent domain controller PADCB⁽²⁾ - PlantPAx child domain controller 	79, 86, 93, 99, 102, 116, 118, 133, 140, 143, 148, 150, 154, 155, 158, 160, 161, 163, 231, 232, 234, 344, 373
	PlantPAx workstations	<ul style="list-style-type: none"> OWS01⁽³⁾ - Operator workstation EWS01⁽³⁾ - Engineering workstation 	16, 20, 113, 167, 177, 185, 191, 193, 197, 199, 205, 207, 210, 212, 213, 217, 231, 232, 236, 239, 234, 245, 247, 254, 261, 281, 284, 288, 293, 379, 386, 387, 390, 395, 396, 398, 405, 411, 413
	PlantPAx Application servers	<ul style="list-style-type: none"> ASIS01 - AppServ-Info SQL server ASIH01 - AppServ-Info Historian server ASIV01 - AppServ-Info VantagePoint® server ASAM01 - AppServ-Asset Management server ASBM01 - AppServ-Batch server ASEWS01 - AppServ-Engineering Workstation server ASOWS01 - AppServ-Operator Workstation server 	16, 37, 38, 39, 113, 116, 167, 231, 232, 315, 319, 321, 324, 326, 327, 331, 334, 336, 342, 346, 370, 375, 379, 382, 386, 390, 395, 399, 405
	Firewall	Firewall	231
	PASS (Process Automation System Server)	<ul style="list-style-type: none"> PASS01 - FactoryTalk® directory PASS02A⁽¹⁾ - Primary HMI server PASS02B⁽²⁾ - Secondary HMI server 	16, 175, 239, 257, 260, 284, 331, 334, 336, 342, 349, 358, 359, 362, 367, 370
	Logix controllers	<ul style="list-style-type: none"> LGXC01 - Controller LGXC02 - Controller 	16, 58, 59, 63, 64, 68, 73, 231, 232, 248, 250, 252, 267, 269, 274

(1) A = Parent and/or Primary element

(2) B = Child and/or Secondary element

(3) EWS and OWS are used throughout the manual but the same procedures apply for AppServ-EWS and AppServ-OWS.

Default User Name

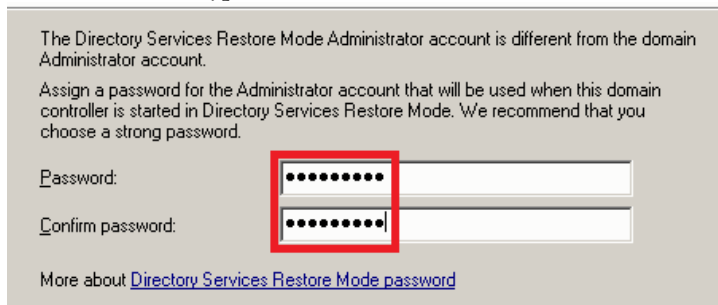
In this manual, we use ‘Admin’ and ‘Administrator’ as referenced user names in sample screen examples. But, we recommend that you do not use these user names in production.

Rebranding of FactoryTalk Linx Software


As of version 6.00, RSLinx® Enterprise software is known as FactoryTalk Linx software.


Action Identifier

Dialog boxes have **red** boxes to identify areas that require some type of user action, such as to type text or click 'Next'.

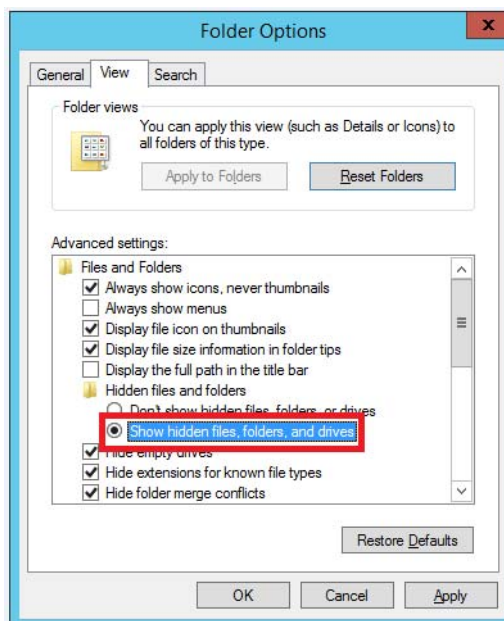


Configure Programs Menu

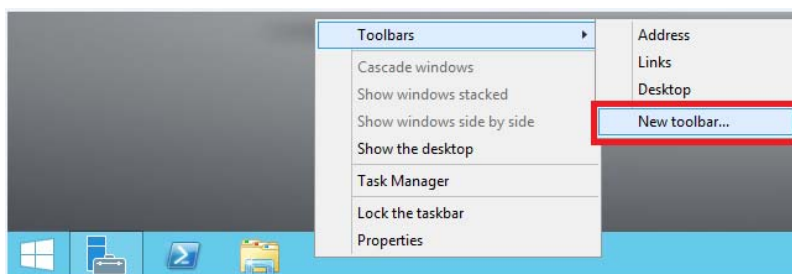
We strongly suggest that you perform the following procedure in the system computers to group folders under 'Programs' on the taskbar. When complete, you access Windows and software folders by clicking the Programs  symbol.

1. Click the Windows  symbol.
2. Click Control Panel and choose Folder Options.

The Folder Options dialog box appears.



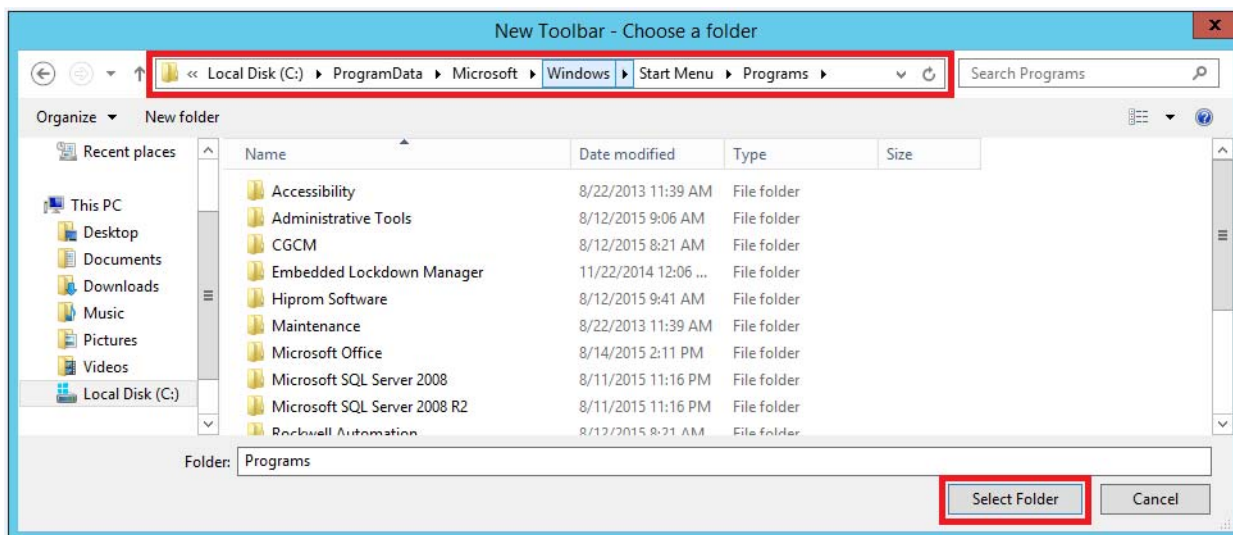
3. On the View Tab, select 'Show hidden files, folders, and drives' and click OK.
4. Right-click in the taskbar, click Toolbars, and choose New Toolbar.



5. On the New Toolbar window, designate a path for your Programs folder.

For example:

C:\ProgramData\Microsoft\Windows\StartMenu\Programs.



6. Click Select Folder.

Additional Resources

These documents contain additional information that concern-related products from Rockwell Automation.

Resource	Description
PlantPAx Distributed Control System Selection Guide, publication PROCES-SG001	Provides basic definitions of system elements and sizing guidelines for procuring a PlantPAx system.
PlantPAx Distributed Control System Reference Manual, publication PROCES-RM001	Provides characterized recommendations for implementing your PlantPAx system.
PlantPAx Distributed Control System Application Configuration User Manual, publication PROCES-UM003	Describes procedures to start development of your PlantPAx distributed control system.
Rockwell Automation Library of Process Objects, publication PROCES-RM002	Provides information on how to use the Rockwell Automation Library of Process Objects.
Rockwell Automation Library of Process Objects: Logic Instructions Reference Manual, publication PROCES-RM013	Provides controller codes and tags for Rockwell Automation Library objects. The objects are grouped by family and attached as Microsoft Excel files to the manual PDF file.
Rockwell Automation Library of Process Objects: Display Elements Reference Manual, publication PROCES-RM014	Provides common display elements for the Rockwell Automation Library. For improved accessibility, the elements are combined into one manual.
Activate Rockwell Software® Products, publication FTA-QS002	Explains how FactoryTalk Activation generates activation files and distributes them over the Internet to activate software.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Describes tested and validated industrial network architectures, recommendations and best practices, including network resiliency and security
Resilient Converged Plantwide Ethernet Architecture Technical Data, publication ENET-TD010	Describes design considerations to implement a scalable and secure CPwE architecture that helps maximize plant efficiency.
Stratix Managed Switches User Manual, publication 1783-UM007	Describes how to set up, configure, and troubleshoot Stratix switches.
Embedded Switch Technology Reference Architectures, publication ENET-RM003	Provides design recommendations for connecting device-level topologies to larger, switch networks comprised of Layer 2 access switches. Document also covers the implementation of embedded switch technology within the Converged Plantwide Ethernet (CPwE) Cell/Area zone. The Cell/Area zone is where the device-level topologies connect Industrial Automation and Control System (IACS) end-devices into the Cell/Area zone.
Securely Traversing IACS Data Across the Industrial Demilitarized Zone Technical Data, publication ENET-TD009	Describes requirements and design considerations to deploy an Industrial Demilitarized Zone (IDMZ) within Industrial Automation and Control System (IACS) plant-wide architectures.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Explains the infrastructure components that allow this open network to communicate seamlessly throughout a plant, from shop floor to top floor.
Integrated Architecture® and CIP Sync Configuration manual, publication IA-AT003	Explains CIP Sync technology and how you can synchronize clocks within the Rockwell Automation® Integrated Architecture® system.
PlantPAx Virtualization User Manual, publication 9528-UM001	Describes the catalog numbers and details for using virtual image templates to configure virtual machines.

You can view or download publications at <http://www.rockwellautomation.com/literature/>. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Configure Network Infrastructure

Overview

A traditional distributed control system (DCS) is typically limited to a single model option for servers, workstations, and network switches. A traditional DCS provides specific configurations that are based on closed and fixed networks. This traditional approach makes it difficult to manage IT support and integrate with business systems.

The PlantPAx® system leverages a more modern approach, being open to commercial off-the-shelf servers, workstations, and servers. The PlantPAx system supports the adoption of the latest IT technology for automation, including virtualization. The use of virtualization breaks the dependency between your server and workstation system elements from the specific hardware that hosts those elements. By rationalizing to a common IT infrastructure, companies can mitigate security risks and improve uptime to help protect people, assets, and information.



However, without specific guidance, poor infrastructure configuration can cause system performance and functionality of your control system to be degraded. The PlantPAx System Infrastructure User Manual steps you through the procedures that are necessary to prepare your system infrastructure, inclusive of operating systems and network configuration.

The performance of the PlantPAx system is dependent upon following the sizing guidelines and application rules that are provided by the PlantPAx Reference Manual. These rules and guidelines are developed through a process called characterization.

Characterization is the activity of measuring system performance against key operational criteria called Critical System Attributes (CSA). CSAs provide specific recommendations for application sizing and system performance. Follow the instructions that are contained in this manual to help make sure that your control system is built as prescribed by the PlantPAx Reference Manual and characterization.

If you have more complex requirements, you can take advantage of the flexibility of the PlantPAx system. For more information, see [Distributed Control Systems](#) under the Products webpage.

The Converged Plantwide Ethernet (CPwE) Design and Implementation Guide provides a broader set of manufacturing focused reference architectures.

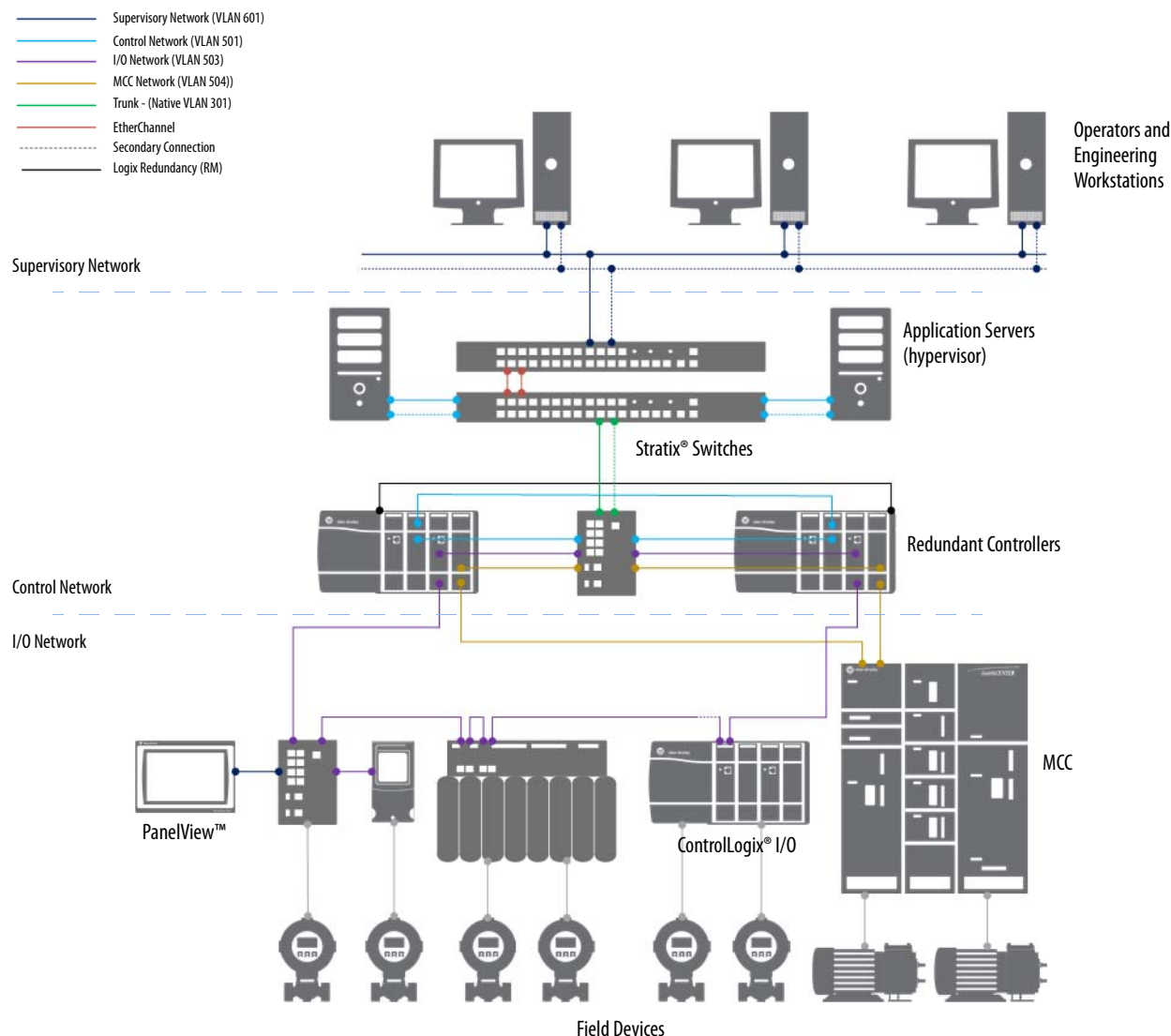
The CPwE manual helps accelerate the deployment of standard networking technologies and convergence of manufacturing and enterprise/business networks. You also can engage technical specialists by using Network and Support Services from Rockwell Automation®.

PlantPax Topology Examples

This manual describes how to install infrastructure components, including switches and routers, to serve as a blueprint for commissioning a PlantPax network.

[Figure 2](#) is an example of a PlantPax system topology for high availability. The illustration comprises different network layers, including Supervisory, Controller, and I/O. Each of these network layers is described in [Chapter 2](#).

Figure 2 - PlantPax Architecture Example



VLAN Basics

A VLAN (virtual local area network) creates network segmentation that forms network groups that are identified by VLAN IDs. The grouping of computers into VLANs enables the switches and routers to control the flow of information on a network.

IMPORTANT Network Address Translation (NAT) is another way to enable network segmentation by using switches and routers. But, we do **not** provide NAT guidelines in this manual.

Switches are inter-connected through trunk ports. Trunk ports send information from multiple VLANs between switches.

A dedicated VLAN called native VLAN is defined on trunk ports. A native VLAN transports, by default, all VLANs on a trunk port. But, a native VLAN is isolated because of security concerns of mixing a native VLAN with access and management VLANs. The native VLAN is not to have any assigned IP addresses. By default, the native VLAN ID is 1 but it is recommended to change it. For example, the native VLAN is assigned a VLAN ID of 301 in the example in [Table 2 on page 18](#).

All computers, controllers, and I/O modules are connected through access ports. Access ports are assigned to a VLAN within the ID range of 501...509 and 601...603 depending on the device and your architecture.

We recommend implementing physical security, like plugging unused ports and disabling ports that are not going to be used. For more information on physical security recommendations, see the PlantPAx Distributed Control System Reference Manual, publication [PROCES-RM001](#).

IMPORTANT It is recommended to use the Crypto firmware for Stratix switches to add additional levels of security. The procedures in this section require the Crypto firmware.

Example: 172.18.0.20/24

The instructions in this manual use IP addresses that have a CIDR (Classless Inter-domain Routing), which contains a slash mark before a number. We recommend that you use the number (24) that means that the first 24 bits of the IP address constitutes the network address. In the example, the network mask is configured to 255.255.255.0 for the routing functionality to work.

Subnets are used to segment the devices in a network into smaller groups. The IP address and associated subnet mask are unique identifiers for the switch in a network. The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs.

IMPORTANT Make sure that the IP address that you assign to the switch is not being used by another device in your network.

[Table 2](#) describes typical VLANs and media access control (MAC) address ranges that are suggested for use on the PlantPAx system. More VLANs can be used depending on your configuration.

The following pages describe how to configure network segmentation with switches on the Control and Supervisory networks.

Table 2 - Descriptions for VLANs and Ethernet Address Ranges⁽¹⁾

VLAN ID (Name)	EtherNet/IP Address Range		Description
1	—	—	Not used
300 (Management VLAN) ⁽²⁾	172.18.0.1		Default gateway
	172.18.0.2	172.18.0.9	VLAN routing – switch addresses ⁽³⁾
	172.18.0.10	172.18.0.253	Application – switch addresses
301 (Native VLAN)	—	—	Not to have any assigned IP addresses
501 (Control network)	172.18.1.1		Default gateway
	172.18.1.2	172.18.1.9	VLAN routing
	172.18.1.10	—	Domain/DNS primary server
	172.18.1.11		Domain/DNS secondary server
	172.18.1.12	172.18.1.99	Servers and workstations (DHCP)
	172.18.1.100	172.18.1.253	Ethernet interface to controllers for HMI and system communication
502...509 (I/O network)	172.18.[2...].1	172.18.[...9].1	Default gateway
	172.18.[2...].2	172.18.[...9].9	VLAN routing
	172.18.[2...].10	172.18.[...9].253	Ethernet interface between controllers and I/O modules (fixed)
601 (Supervisory network - wired network)	172.20.1.1	172.20.1.1	Default gateway
	172.20.1.2	172.20.1.9	VLAN routing
	172.20.1.10	172.20.1.25	Workstation interface
602 (Supervisory network - wireless network)	172.20.2.1	172.20.2.1	Default gateway
	172.20.2.2	172.20.2.9	VLAN routing
	172.20.2.10	172.20.2.253	Mobile interface
602 (External - untrusted network) Note: From IDMZ (industrial demilitarized zone)	172.20.3.1	172.20.3.1	Default gateway
	172.20.3.2	172.20.3.9	VLAN routing
	172.20.3.10	172.20.3.253	External interface

(1) The referenced IP Addresses can be changed for your system requirements.

(2) All networks do not use a dedicated management VLAN, but it is a good practice. Many times, a supervisory VLAN is the same VLAN as the management VLAN.

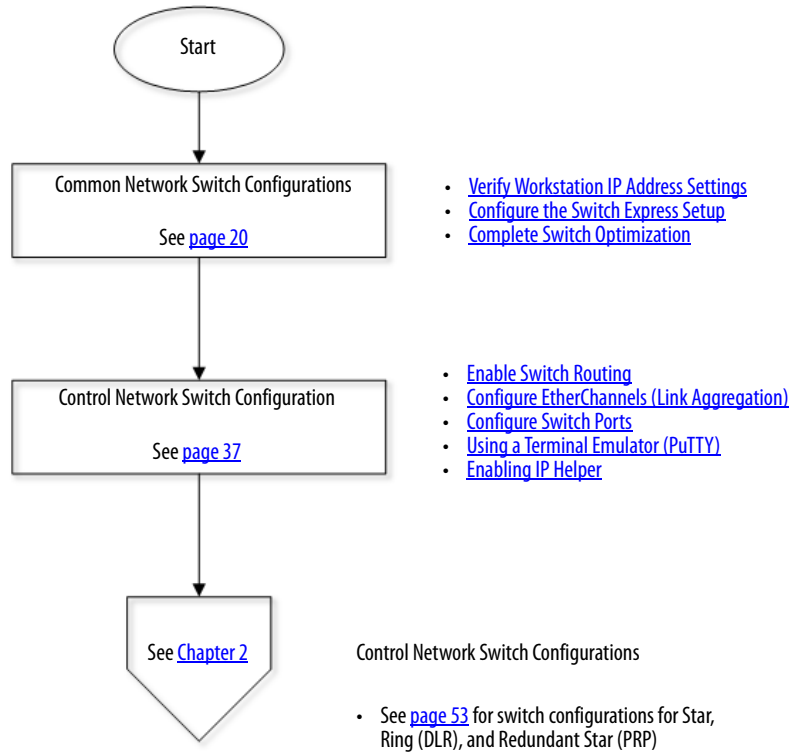
(3) If there are more than eight Layer 3 switches on your system, more IP addresses must be reserved.

IMPORTANT

One network range is assigned per VLAN only. For example, the 172.18.1.xxx network range is assigned to VLAN 501. [Table 2](#) identifies nine VLANs for access ports to provide logical segregation of your system. More VLANs can be used, if necessary.

[Figure 3](#) lists the configuration topics that are described in this chapter. Click the page number or the links for quick access to specific information in each subsection.

Figure 3 - PlantPAx Network Infrastructure Workflow



Common Network Switch Configurations


Use an Engineering Workstation with these procedures.



This section describes how to configure the Express Setup for each Stratix switch. We recommend that you complete the tasks in the order that they are listed. These tasks help to define IP addresses, create and assign VLANs, and enable faster network convergence time with Rapid PVST+.⁽¹⁾

Verify Workstation IP Address Settings

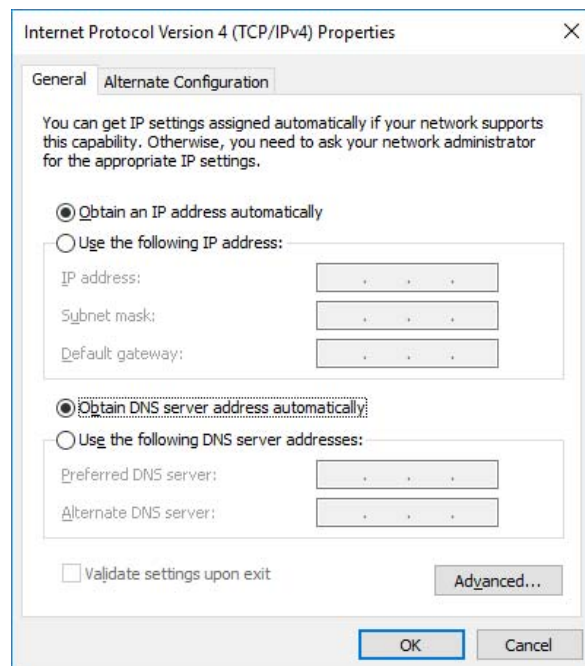
Before you start switch setup, you must verify that **no** fixed IP address is assigned to the workstation that is being used to configure the switch. You want the switch to manage the IP address configuration in your computer. Complete these steps.

1. Click the Windows  symbol.
2. Click Control Panel and choose Network and Sharing Center>Change adapter settings.

The Network Connections dialog box appears.

3. Right-click the network and choose Properties.
4. Double-click Internet Protocol Version 4 (TCP/IPv4).

The Internet Protocol Version 4 Properties dialog box appears.



5. Select Obtain an IP address automatically and Obtain DNS server address automatically, and click OK.

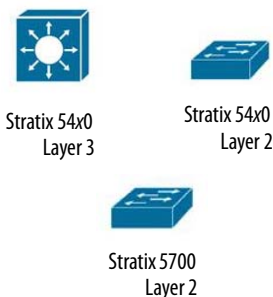
You are ready to assign an IP address to the switch by using the express setup. See [page 21](#).

(1) Default mode (MST) is comparably the same performance as RPVST+, just a different standard.

Configure the Switch Express Setup

You **must** configure Switch Express Setup for **each** switch in your system. The settings enable the switches to operate as managed switches with a default configuration that supports industrial automation.

Use Layer 2 and Layer 3 switches with these procedures.



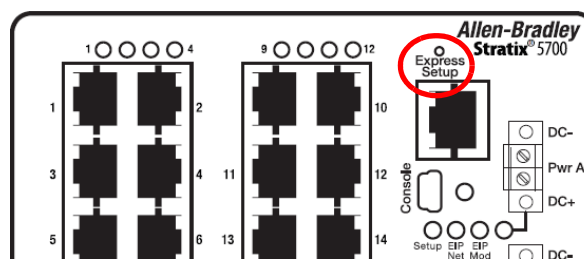
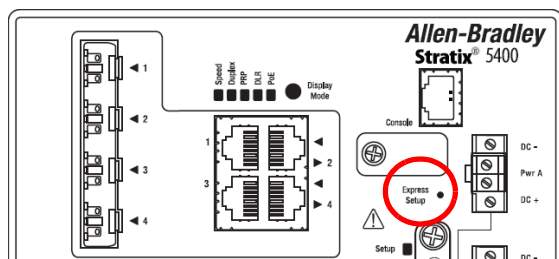
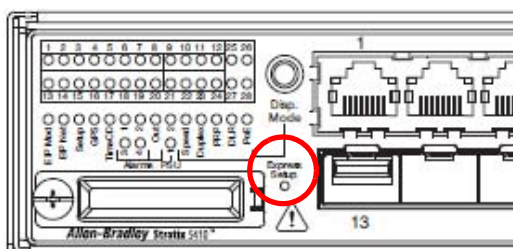
IMPORTANT We walk you through how to configure a 5410 Stratix switch. The steps are basically the same for different switch types. Make sure that for each switch you repeat the steps on pages [21...36](#).

Initiate Express Setup

The following steps require a switch with factory defaults. An out-of-box switch is ready for these steps. You can reset an existing switch by pressing the Express Setup button for 16...20 seconds to default switch settings. After a restart, the switch can be initialized.

1. On the Ethernet switch, press once on the Express Setup button (as identified on the devices by red circles).

TIP The Express Setup button is recessed in the hole. Use a small tool or a paper clip to reach the button.



2. Connect a network cable from your workstation to the flashing switch port.

Continue with [Configure Security Exception on page 22](#).

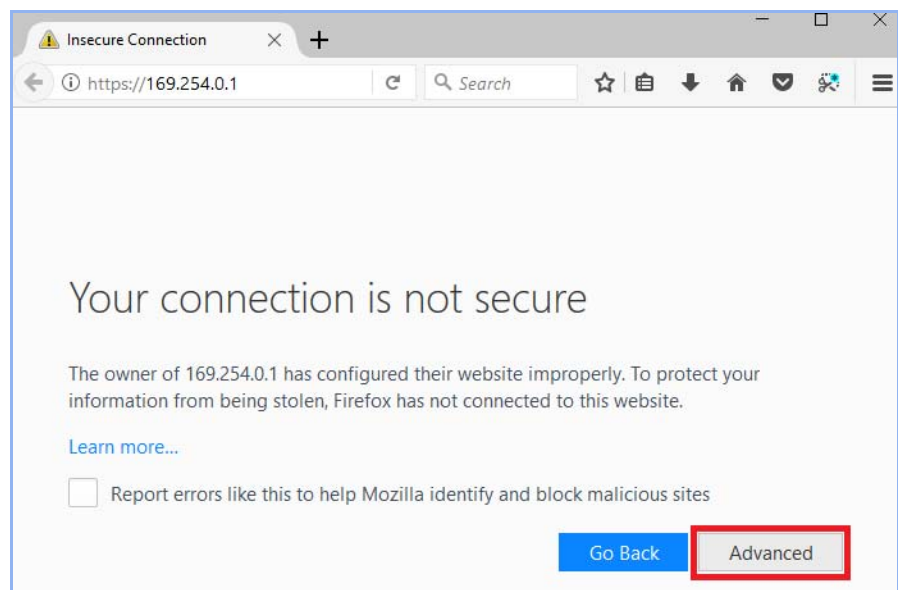
Configure Security Exception

We recommend that you use the Crypto version of Stratix switches. This version provides a self-signed certificate to each switch. You **must** add a security exception for the application to initialize each switch.

IMPORTANT Our recommended web browsers are Internet Explorer and Mozilla Firefox.

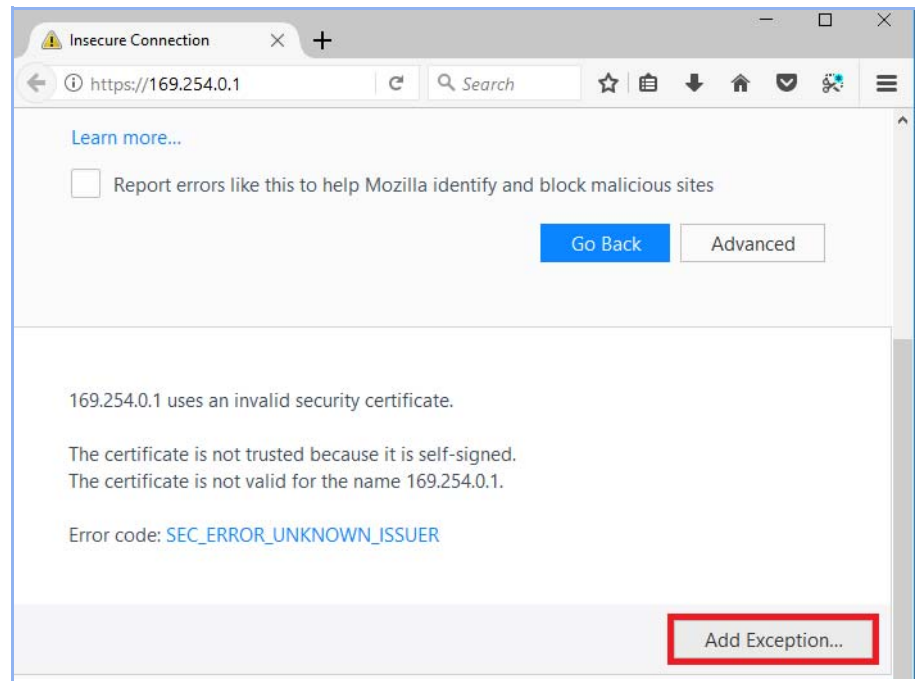
1. Start a web browser session.
2. Type the IP address 169.254.0.1 into the browser and press Enter to navigate to the switch that you are setting up.

Follow the browser message prompts in steps [3...5](#).

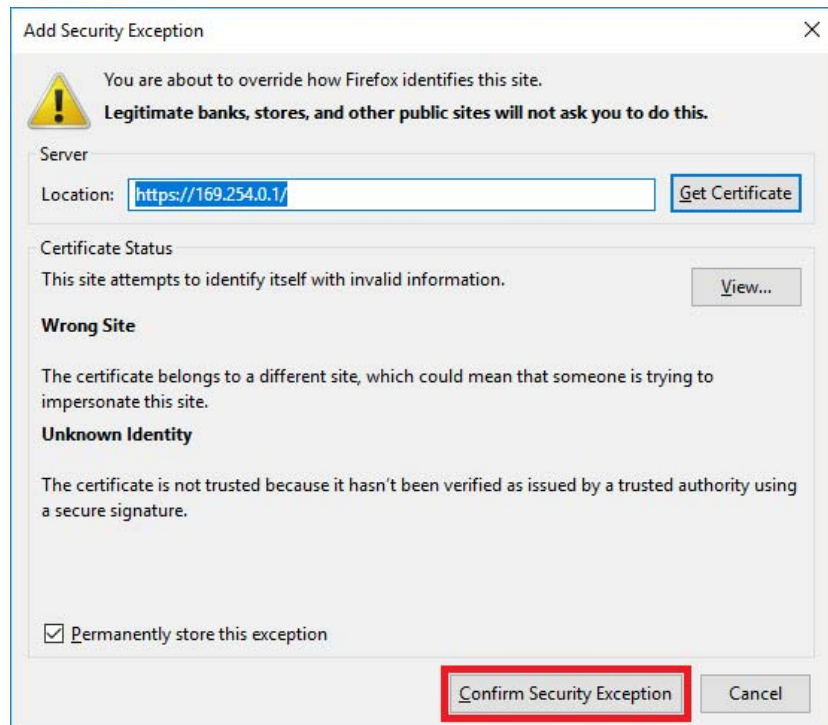


3. Click Advanced.

4. Click Add Exception.

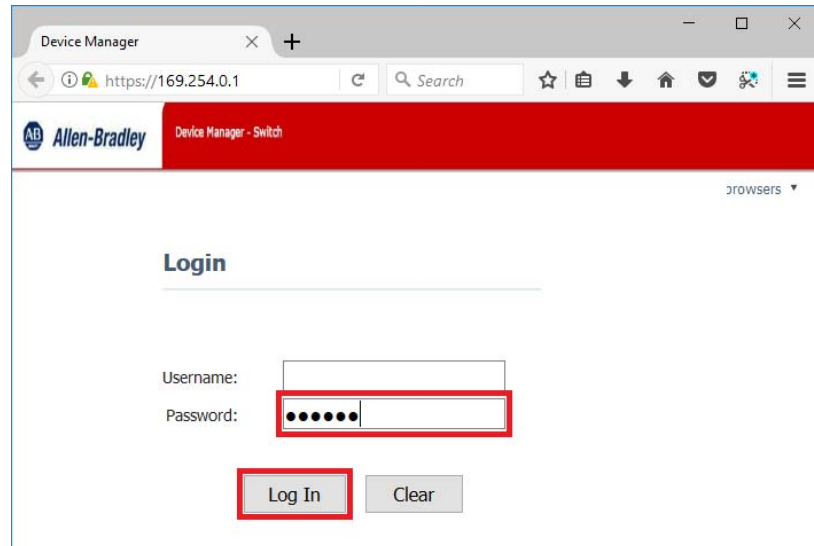


5. Click Confirm Security Exception.



- On the switch Login page, leave the Username blank and type 'switch' for the default password.

TIP The 'switch' password lets you continue to the Device Manager for additional steps. We recommend that you change the default password in step 2 on [page 25](#).



- Click Log In.

The Device Manager dialog box appears.

Continue to [Configure a Switch in Device Manager on page 25](#).

Configure a Switch in Device Manager

You must complete this section for each switch in your system to define settings for managed switches. The Device Manager has two sections: Network Settings and Advanced Settings (see [page 26](#)).

The Network Settings portion of the dialog box provides the ability to perform the following:

- Name the switch
- Select the VLAN
- Set IP addresses
- Create a password (to replace the 'switch' default).

The screenshot shows the 'Express Setup' page for the Allen-Bradley Stratix 5410 Solution Device Manager. The 'Network Settings' section is expanded, showing the following configuration:

- Host Name: SW001
- Management Interface (VLAN): 300
- IP Assignment Mode: ☒ Static ☐ DHCP
- IP Address: 172.18.0.1 / 255.255.255.0
- Default Gateway: 172.18.0.1
- NTP Server: 172.18.1.10
- User: admin
- Password: [masked]
- Confirm Password: [masked]

1. Type the switch configuration that is similar to the example shown in the illustration and the IP addresses in [Table 3](#).

Table 3 - Management Network IP Addresses

Host Name	Management (VLAN)	IP Address	Mask	Default Gateway	NTP Server ⁽¹⁾
SW001	300 (management)	172.18.0.1	255.255.255.0	172.18.0.1	172.18.1.10

(1) NTP server can be a different address according to the Time Synchronization application option.

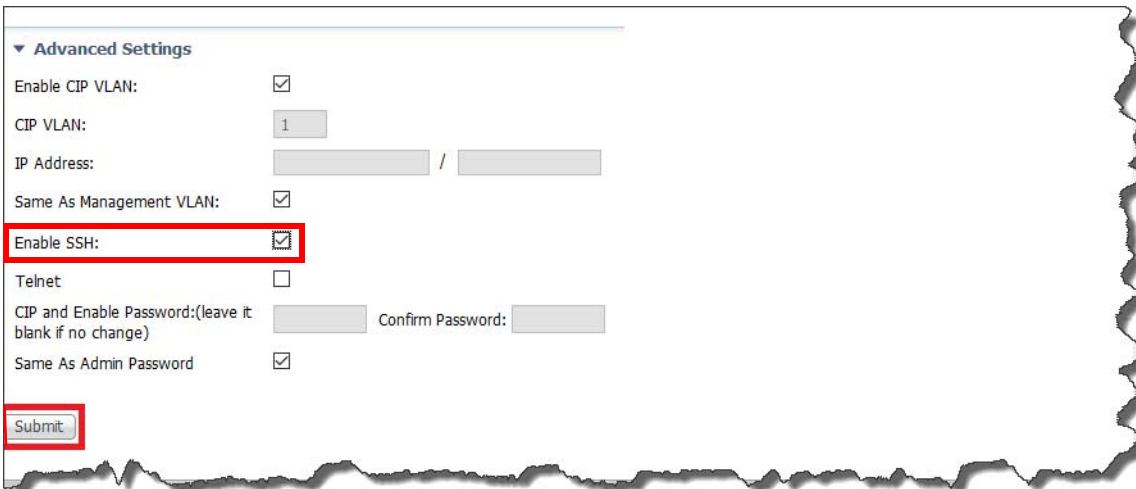
IMPORTANT The IP addresses and default gateway for the 5410 switch example are for illustration purposes only.

2. Type a user name.
Change the default 'admin'.
3. Type a password (which replaces the default 'switch').
Retype the password to confirm your entry.

4. In the Advanced Settings, make sure that you click the SSH (secure shell) checkbox.

SSH provides more security for remote connections than Telnet by providing strong encryption.

Must be checked —



Advanced Settings

Enable CIP VLAN: ☒

CIP VLAN: 1

IP Address: /

Same As Management VLAN: ☒

Enable SSH: ☒

Telnet: ☐

CIP and Enable Password:(leave it blank if no change)

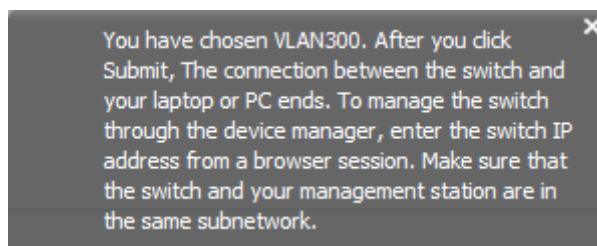
Confirm Password:

Same As Admin Password: ☒

Submit

5. Click Submit.

A message appears.



See [Table 4 on page 27](#) to configure additional managed switches in your system.

6. [Table 4](#) shows the IP addresses to be used with these procedures for each switch in your system.

Table 4 - Network IP Addresses

Host Name (Switch Type)	Management (VLAN)	IP Address	Mask	Default Gateway	NTP Server ⁽¹⁾
SW010	300 (Management)	172.18.0.10	255.255.255.0	172.18.0.1	172.18.1.10
SW020		172.18.0.20			
SW022		172.18.0.22			
SW030		172.18.0.30			
SW040		172.18.0.40			
SW042		172.18.0.42			
SW043		172.18.0.43			
SW044		172.18.0.44			

(1) NTP server can be a different address according to the Time Synchronization application option.

Complete Switch Optimization

After you have completed the Express Setup procedures for all your system switches, you must log in to each switch. The following pages describe how to optimize switch operation for these functions:

- [Create a VLAN](#)
- [Enable CIP VLAN](#)
- [Enable Rapid PVST+](#)
- [Enable Precision Time Protocol \(PTP\)](#)
- [Enable Simple Network Management Protocol \(SNMP\)](#)

Login to Switches

Use your login name and password to access a desired switch.

1. On the workstation that is being used, change your network adapter address to a fixed mode by following steps on [page 21](#) through [page 27](#).

Choose an IP address under the management network range (172.18.0.xxx)/255.255.255.0/172.18.0.1. See suggestions in [Table 3](#) and [Table 4](#).

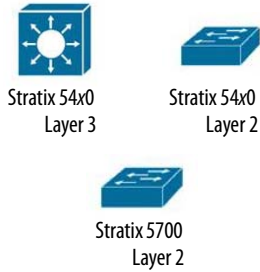
2. Connect to another switch port.
3. Log into the switch by using the same information that you entered on the Device Manager on [page 25](#).

The screenshot shows a web browser window titled "Device Manager" with a single tab. The address bar contains "https://172.18.0.1". The page header features the Allen-Bradley logo and the text "Device Manager - Switch". Below the header, there is a "Login" section with a horizontal line. Underneath, there are two input fields: "Username:" with the value "admin" and "Password:" with masked characters. A "Log In" button is located below the password field, and a "Clear" button is to its right. The "Log In" button is highlighted with a red rectangular box.

4. Click Log In and proceed to [page 29](#).

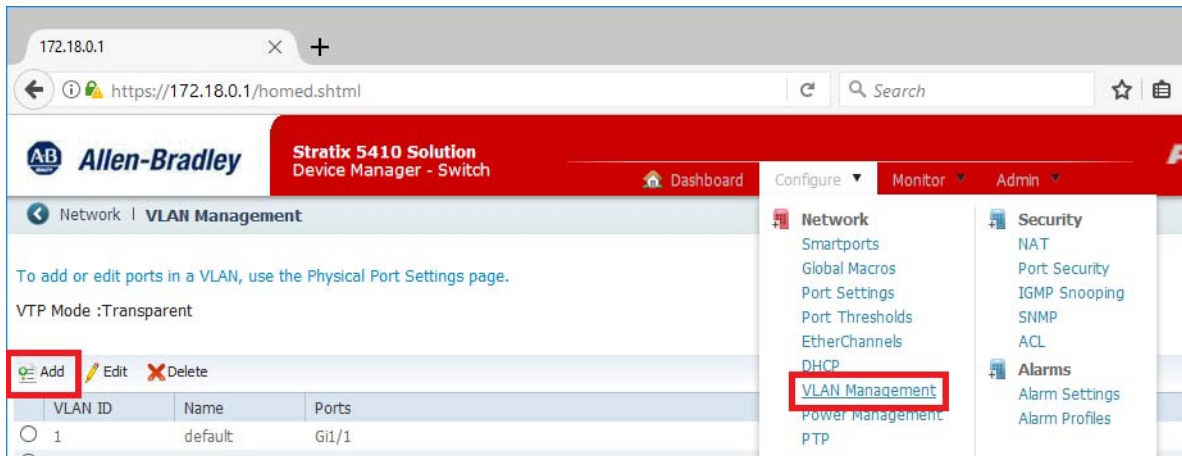
Create a VLAN

Use Layer 2 and Layer 3 switches with these procedures.



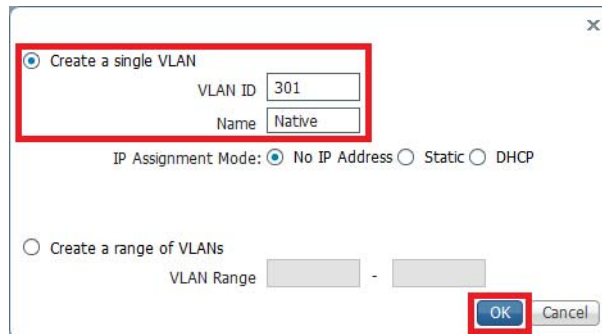
IMPORTANT This procedure requires that the VLAN and IP addresses are assigned as outlined in [Table 2 on page 18](#). Do **not** use VLAN 1. The following example is for switch SW001.

1. From the main menu of the Device Manager, click Configure and choose Network>VLAN Management.



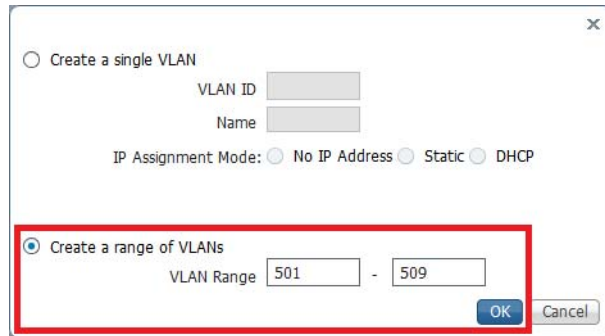
2. Click Add.
3. Create the native VLAN ID and click OK.

Our example is 301.



IMPORTANT A native VLAN is separate from the infrastructure VLANs as well as the other CIP VLANs that are used.

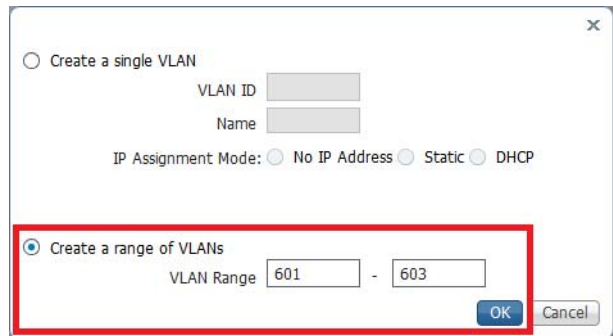
4. Repeat [step 2](#) and create a range of VLANs (501...509 and 601...603).



☐ Create a single VLAN
 VLAN ID
 Name
 IP Assignment Mode: ☐ No IP Address ☐ Static ☐ DHCP

☒ Create a range of VLANs
 VLAN Range -

OK Cancel



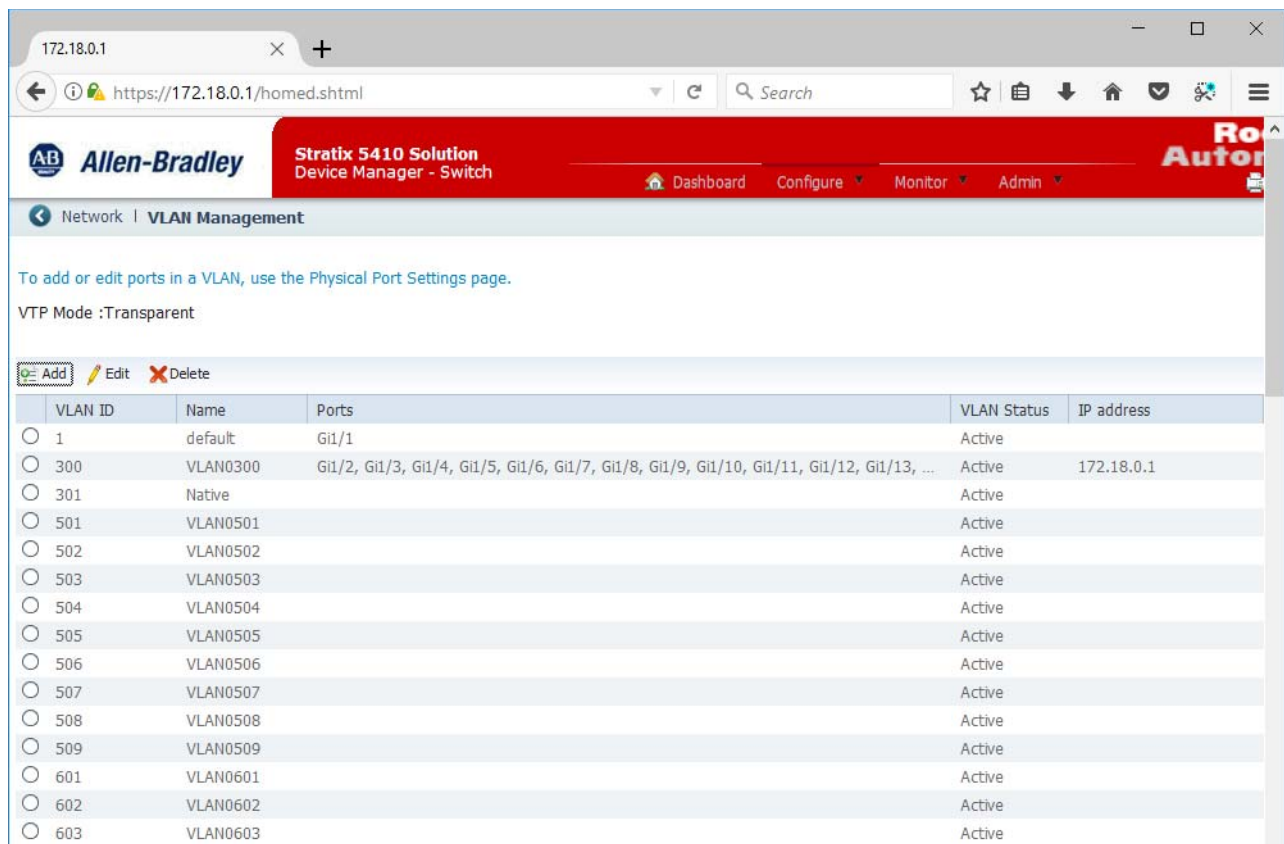
☐ Create a single VLAN
 VLAN ID
 Name
 IP Assignment Mode: ☐ No IP Address ☐ Static ☐ DHCP

☒ Create a range of VLANs
 VLAN Range -

OK Cancel

5. Click OK.

The VLANs appear as listed in the graphic.



172.18.0.1

https://172.18.0.1/homed.shtml

Allen-Bradley Stratix 5410 Solution Device Manager - Switch

Dashboard Configure Monitor Admin

Network | VLAN Management

To add or edit ports in a VLAN, use the Physical Port Settings page.

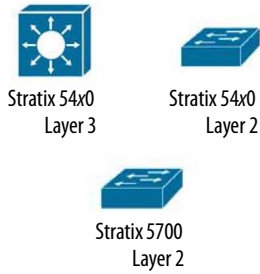
VTP Mode :Transparent

Add Edit Delete

VLAN ID	Name	Ports	VLAN Status	IP address
1	default	Gi1/1	Active	
300	VLAN0300	Gi1/2, Gi1/3, Gi1/4, Gi1/5, Gi1/6, Gi1/7, Gi1/8, Gi1/9, Gi1/10, Gi1/11, Gi1/12, Gi1/13, ...	Active	172.18.0.1
301	Native		Active	
501	VLAN0501		Active	
502	VLAN0502		Active	
503	VLAN0503		Active	
504	VLAN0504		Active	
505	VLAN0505		Active	
506	VLAN0506		Active	
507	VLAN0507		Active	
508	VLAN0508		Active	
509	VLAN0509		Active	
601	VLAN0601		Active	
602	VLAN0602		Active	
603	VLAN0603		Active	

Enable CIP VLAN

Use Layer 2 and Layer 3 switches with these procedures.



The CIP VLAN is used to create infrastructure diagnostics and configurations in the application level. For our example, CIP VLAN is isolated from the management VLAN (300).

[Table 5](#) shows example IP addresses to be associated with the switches for CIP VLAN.

Table 5 - Example CIP VLAN Configuration⁽¹⁾

Host Name	CIP (VLAN)	IP Address	Mask
SW020	501 (Control network)	172.18.1.200	255.255.255.0
SW022		172.18.1.202	
SW023		172.18.1.203	
SW030		172.18.1.210	
SW040		172.18.1.220	
SW042		172.18.1.222	
SW043		172.18.1.223	
SW044		172.18.1.224	
SW045		172.18.1.225	

(1) If there are more than eight switches on your system, more IP Addresses must be reserved. Additional switch IP Addresses start with a higher number.

Complete these steps to configure CIP VLAN for each applicable switch.

1. From the main menu of the switch Device Manager, click the Admin tab and choose Device Management>Express Setup.

2. In the Advanced Settings section, type the information as shown in [Table 5](#).

172.18.0.20

https://172.18.0.20/homed.shtml

Allen-Bradley Stratix 5700 Solution Device Manager - Switch

Dashboard Configure Monitor Admin

Device Management | Express Setup

Select device initial setup mode: Express Setup

Network Settings

Host Name: SW020

Management Interface (VLAN): 300

IP Assignment Mode: ☒ Static ☐ DHCP

IP Address: 172.18.0.20 / 255.255.255.0

Default Gateway: 172.18.0.1

NTP Server: 172.18.1.10

Advanced Settings

Enable CIP VLAN: ☒

CIP VLAN: 501

IP Address: 172.18.1.200 / 255.255.255.0

Same As Management VLAN: ☐

CIP and Enable Password:(leave it blank if no change) Confirm Password:

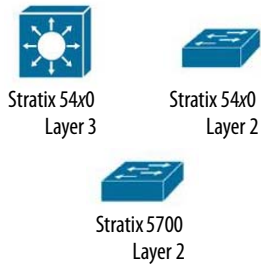
Submit

© 2009-2017 Rockwell Automation, Inc. ALL RIGHTS RESERVED. Alarms 0 12 0 0

3. Click Submit.

IMPORTANT SW001 and SW010 (Stratix 5410 switches) do not enable CIP VLAN because these switches are not used in the controller I/O configuration.

Use Layer 2 and Layer 3 switches with these procedures.

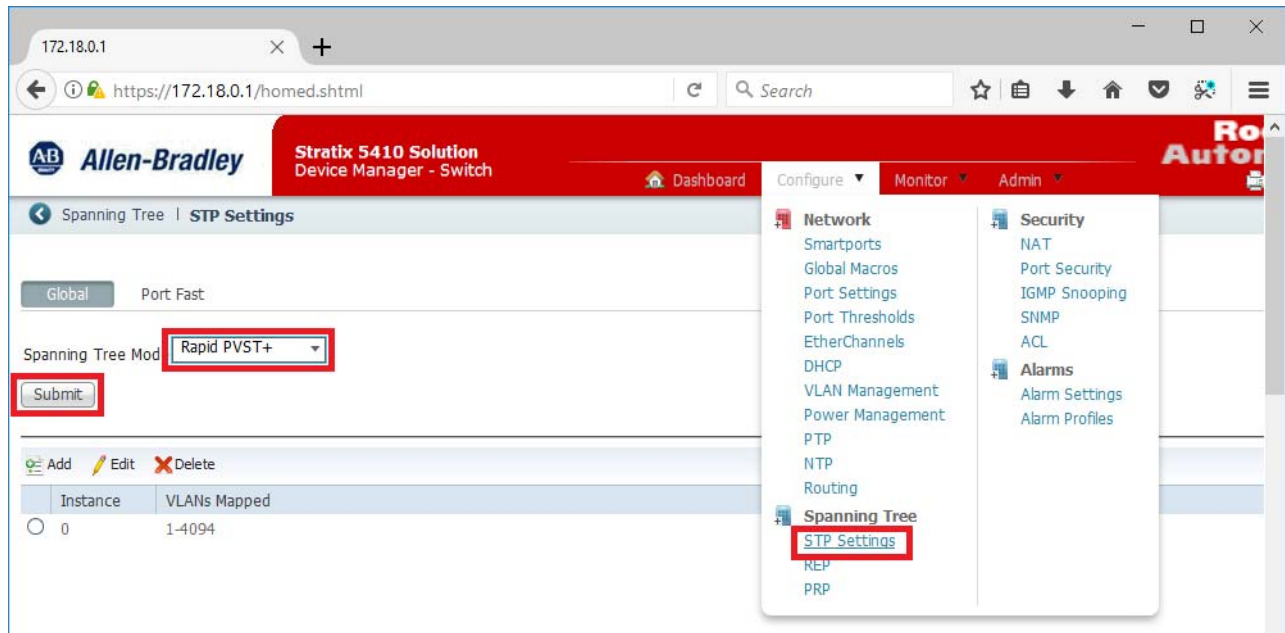


Enable Rapid PVST+

Complete these steps for all switches to enable Rapid Per-VLAN Spanning Tree Plus (Rapid PVST+). This functionality provides better convergence time for communication.

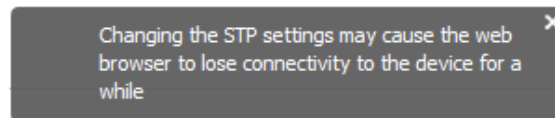
IMPORTANT This procedure requires that the VLAN and IP addresses are assigned as outlined in [Table 4 on page 27](#). The following example is for SW001.

1. From the main menu of the switch Device Manager, click Configure and choose Network>Spanning Tree>STP Settings.

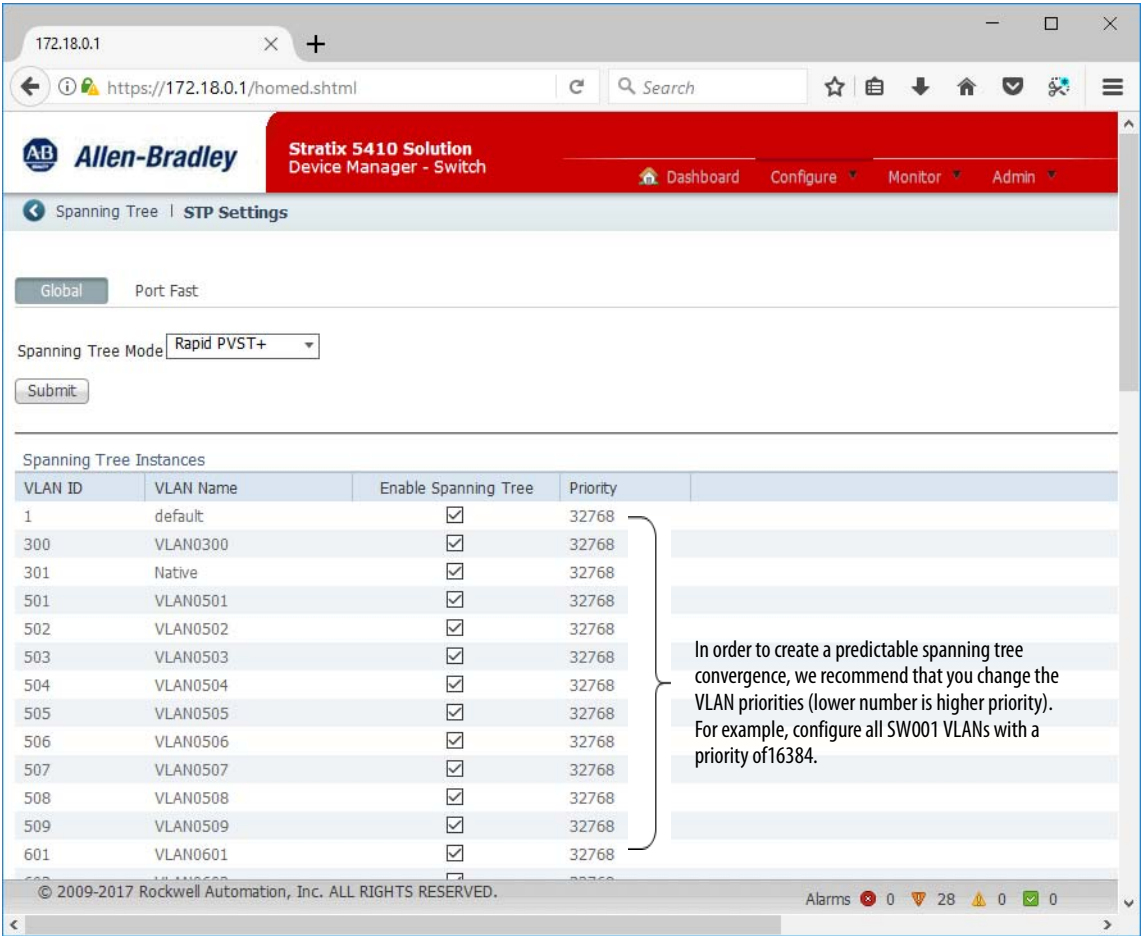


2. Select Rapid PVST+ from the Spanning Tree Mode pull-down, and click Submit.

A warning message appears.



The Spanning Tree of all the VLANs is enabled.



IMPORTANT Do not enable Rapid PVST+ if you have non-Cisco/Stratix switches on your network. The use of Rapid PVST+ with non-Cisco/Stratix switches could result in a longer convergence time after a fault has occurred.

Use Layer 2 switches with these procedures.

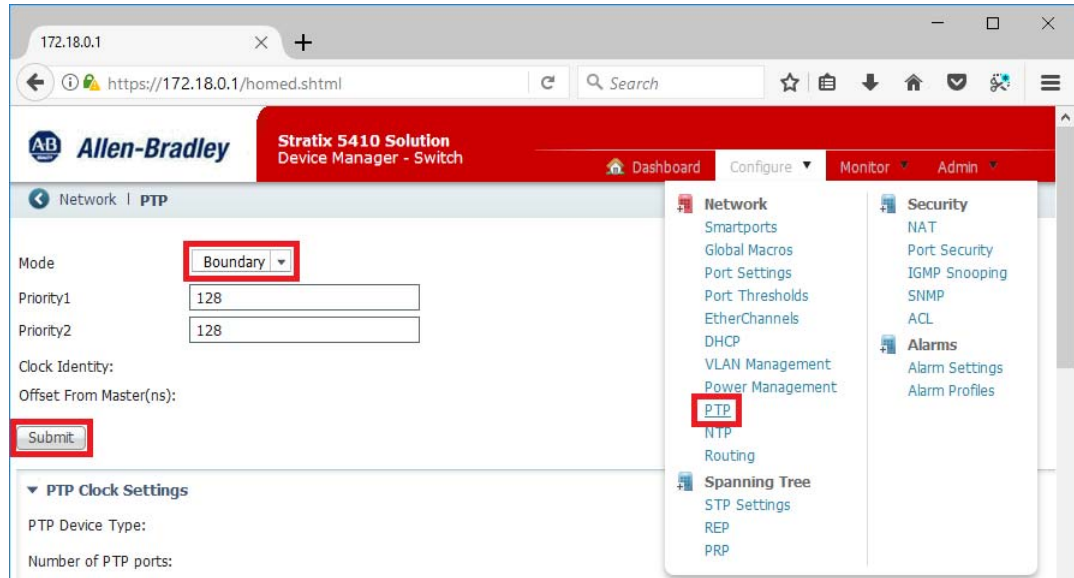


Enable Precision Time Protocol (PTP)

PTP functionality is necessary for end devices to operate in the same time frame as with the clock that is deemed the Grandmaster clock. This section describes how to enable PTP in switch ports.

For details on time synchronization, see [Chapter 8](#).

1. From the main menu of the switch Device Manager, click Configure and choose Network>PTP.



2. Do one of the following from the Mode pull-down depending on the switch that is used:
 - For the 5400 switch, select NTP-PTP clock and type Priority 1 and Priority 2
 - For the 5700 switch, select Boundary.

By default, PTP is enabled for the ports.
3. Click Submit.

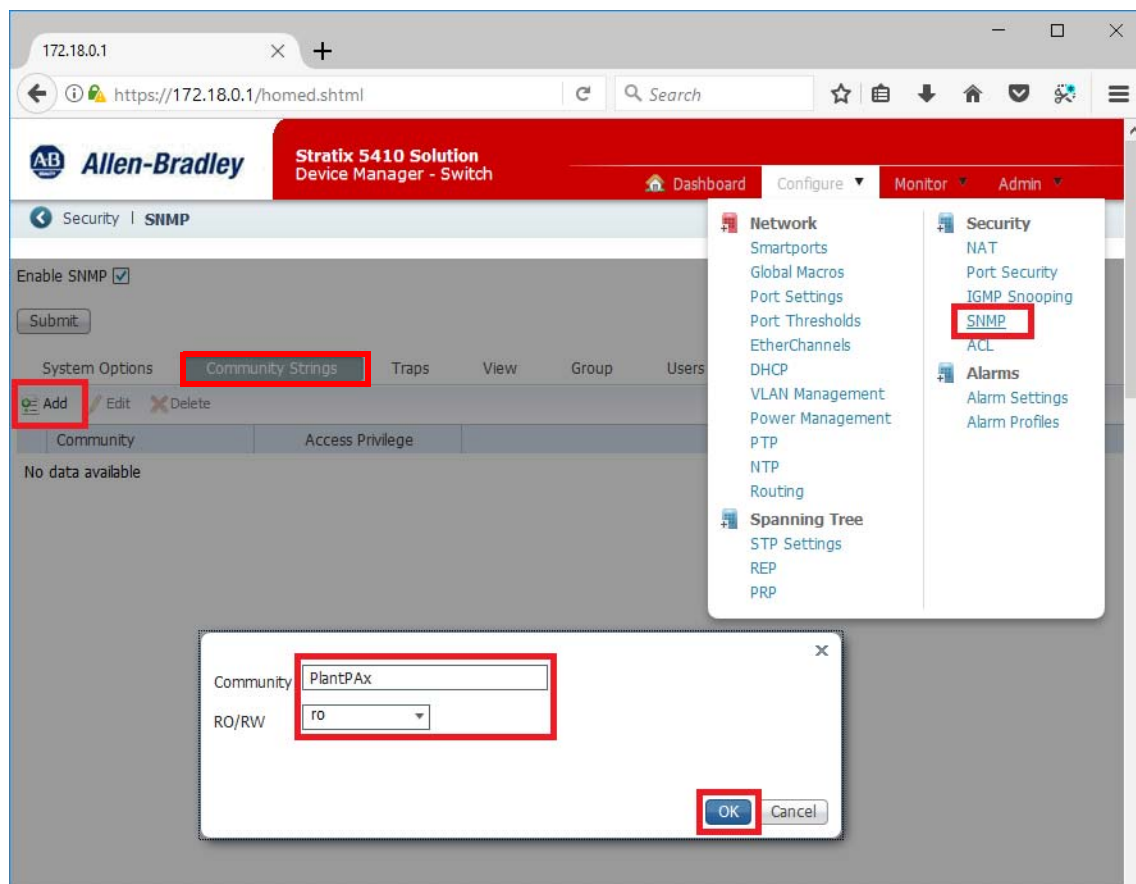
IMPORTANT Boundary clock is required when using a PRP network topology or a DLR redundant gateway. By selecting boundary clock, it's necessary to configure the VLAN ID to be propagated (for example, 300) under device clock details in the device manager or via the terminal emulator interface (CLI).

Device Clock Details								
Device Time Source:		NTP						
Device Clock Time:								
Port Name	State	Enable	Delay Request Interval	Announce Timeout	Announce Interval	Sync Interval	Sync Fault Limit	Vlan Id
Gi1/1	SLAVE	<input checked="" type="checkbox"/>	5	3	1	0	500000	300
Gi1/2	PASSIVE...	<input checked="" type="checkbox"/>	5	3	1	0	500000	300
Gi1/3	MASTER	<input checked="" type="checkbox"/>	5	3	1	0	500000	300

Enable Simple Network Management Protocol (SNMP)

Enable SNMP to provide connectivity for FactoryTalk® AssetCentre inventory discovery and FactoryTalk® Network Manager™. Complete these steps.

1. From the main menu of the switch Device Manager, click Configure and choose Security>SNMP.



2. Click Community Strings.
3. Click Add.
A popup window appears.
4. Type a community string in the Community text field.
Our example shows 'PlantPax'.
5. Use the default of 'ro' (read-only) from the RO/RW pull-down menu.
6. Click OK.

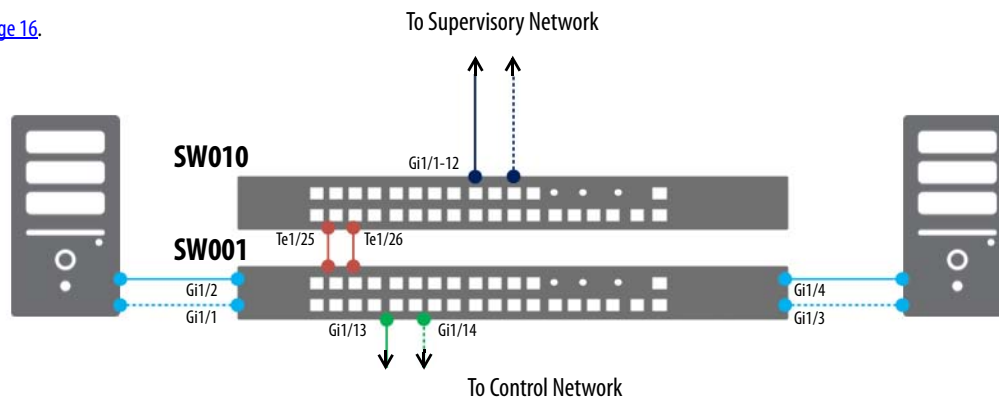
IMPORTANT You must repeat the steps on pages [21](#)...[36](#) for each switch in your PlantPax system.

Distribution Switch Configuration

The Control Network is aptly named for its control of switches between the Supervisory Network and the I/O Network. If different subnets are applicable, Control Network switches serve as distribution switches to perform routing.

Figure 4 - Control Network Switches

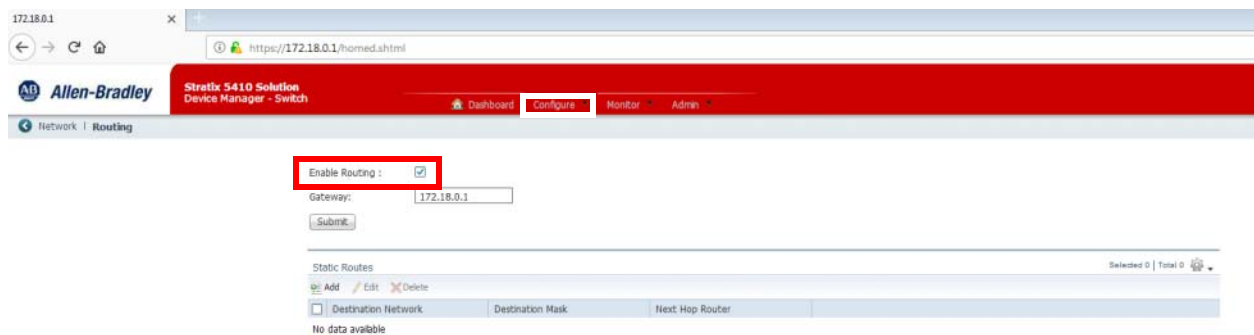
For color legend, see [page 16](#).



Enable Switch Routing

Complete these steps to enable routing for the SW001 switch. While switches apply VLAN segmentation and forward data within a VLAN on the same network, routers send data between multiple VLANs and connect different networks. Routers act as dispatchers to choose the best path to travel for faster, efficient communication.

1. From the main menu of the Device Manager, click Configure and choose Routing.



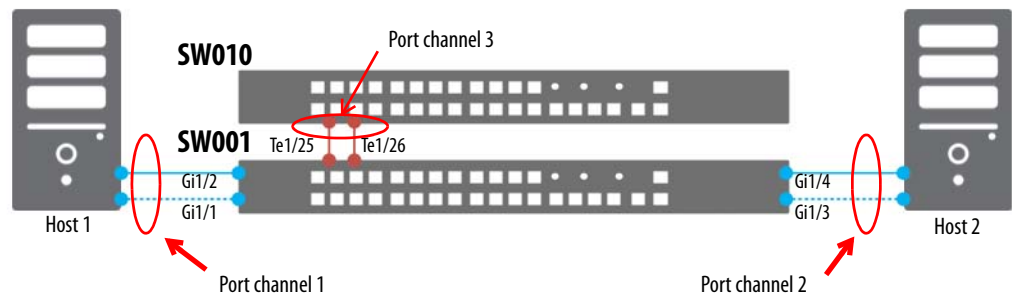
2. Click Enable Routing
3. Validate the gateway is set to 172.18.0.1
4. Click Submit.

Configure EtherChannels (Link Aggregation)

Port link aggregation, also called EtherChannel, lets you combine multiple Ethernet ports to improve the aggregated file transfer speed. Link aggregation also provides redundancy if one of the links fails

An aggregation group combines a number of physical ports to create a single data path. This single data path shares the traffic load among the member ports in the group.

For color legend, see [page 16](#).



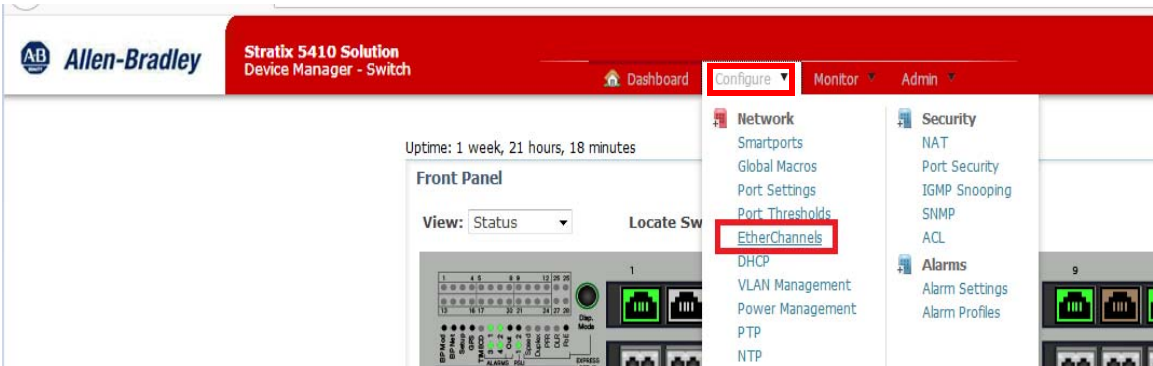
[Table 6](#) identifies EtherChannel ports.

Table 6 - Control Network Access

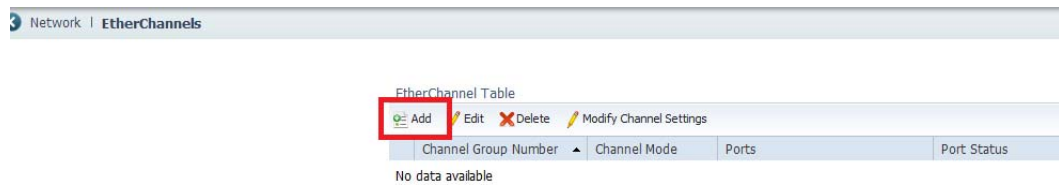
Port	Role	VLAN
Gi1/1 ... Gi1/2 (EtherChannel Po1)	Desktop for Automation	501 (Control network)
Gi1/3 ... Gi1/4 (EtherChannel Po2)		
Gi1/5 ... Gi1/24	Switch for Automation	301 (Native VLAN)
Te1/25 ... Te1/26 (EtherChannel Po3)		
Te1/27 ... Te1/28	—	—

Complete these steps to configure the EtherChannels for SW001 and for the Layer 2 switches that link back to SW001.

1. On the Device Manager, click Configure and choose EtherChannels.



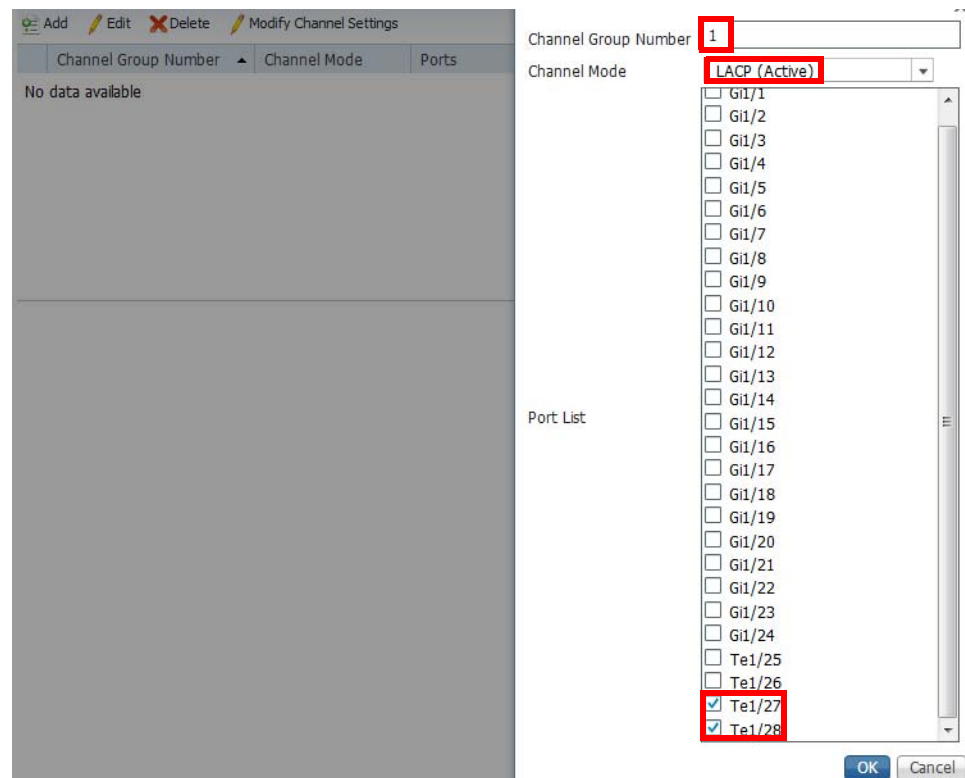
2. Click the Add button.



3. Type a group number for the EtherChannel.

4. From the Channel Mode pull-down, select LACP (Active).

5. In the Port List, select the ports that are used for the EtherChannel.



6. Click OK.

Configure Switch Ports

The greater the number of available ports the more additional devices, as necessary, you can add to your PlantPAx system.

See [page 38](#) for an illustration and a table with port descriptions.

Complete these steps to configure ports.

1. On the Device Manager, click Configure and choose Port Settings.

2. Select an EtherChannel port and click Edit.

Network | Port Settings

Physical Port Table

Edit

	Port Name	Description	Port Status	Speed	Duplex	Media Type
<input type="radio"/>	Gi1/1		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/2		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/3		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/4		●	Auto-1000Mb/s	Auto-Full	10/100/1000BaseTX
<input type="radio"/>	Gi1/5		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/6		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/7		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/8		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/9		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/10		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/11		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/12		●	Auto	Auto	10/100/1000BaseTX
<input type="radio"/>	Gi1/13		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/14		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/15		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/16		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/17		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/18		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/19		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/20		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/21		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/22		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/23		●	Auto	Auto	Not Present
<input type="radio"/>	Gi1/24		●	Auto	Auto	Not Present
<input type="radio"/>	Te1/25		●	10000Mb/s	Full	Not Present
<input type="radio"/>	Te1/26		●	10000Mb/s	Full	Not Present
<input checked="" type="radio"/>	Po1		●	Auto	Auto	
<input type="radio"/>	Te1/27		●	10000Mb/s	Full	SFP-10GBase-SR
<input type="radio"/>	Te1/28		●	10000Mb/s	Full	SFP-10GBase-SR

3. Do the following to configure the port:

- Type a port description
- Click the Administrative Mode pull-down and select Trunk
- Change the Access VLAN and Native VLAN to 'Native 301'

Edit Physical Port

Port Name: Po1

Description: Port Group 1 SW001 to SW010 (Range: 1-200 Characters)

Administrative: ☒ Enable

Speed: 10000Mb/s

Duplex: Full

Auto MDIX: ☒ Enable

Media Type:

Administrative Mode: Trunk

Access VLAN: Native-301

Allowed VLAN:
☒ All VLANs
☐ VLAN IDs
(e.g., 2,4)

Native VLAN: Native-301

OK Cancel

d. Click OK

4. Repeat steps 1..3 on SW001 to create an EtherChannel port for each Layer 2 switch that is to be connected.
5. Follow the same steps on the Layer 2 switches to complete the EtherChannel.

Using a Terminal Emulator (PuTTY)

Besides the Device Manager, the Cisco IOS command-line interface (CLI) enables you to configure, monitor, and maintain Cisco switches. The CLI interface is not available via a web browser like the Device Manager. Therefore, you must configure a terminal emulator to use the CLI interface.



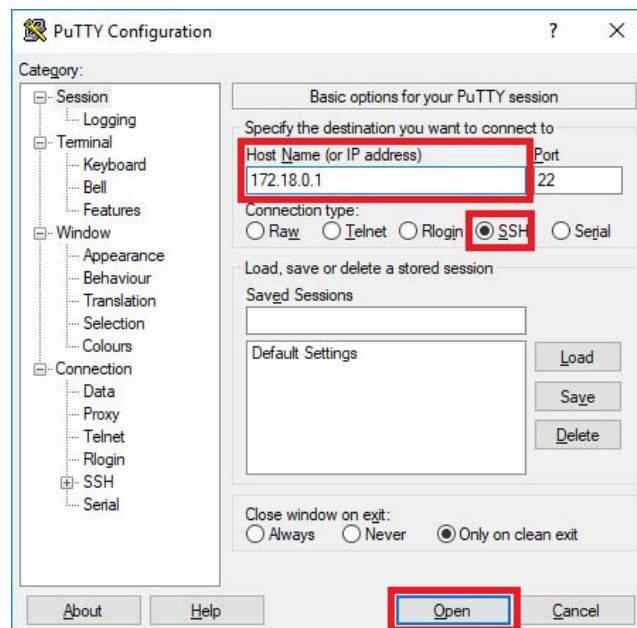
We recommend that you use a terminal emulator, such as PuTTY, to access the CLI interface. PuTTY is an open-source software that is available with source code, which a group of volunteers develops and supports.

IMPORTANT Access the switch by using a Secure Shell (Ethernet) connection (SSH) or via a Console (Serial) Port. By using SSH, it's necessary to be connected through a management VLAN (300).

Complete these steps for an **Ethernet connection**.

TIP The following steps are for enabling an SSH (secure shell) connection. See [page 42](#) if you are using a Serial connection.

1. From the PuTTY Configuration dialog box, click the Session category.
2. Type a host name or an IP address.

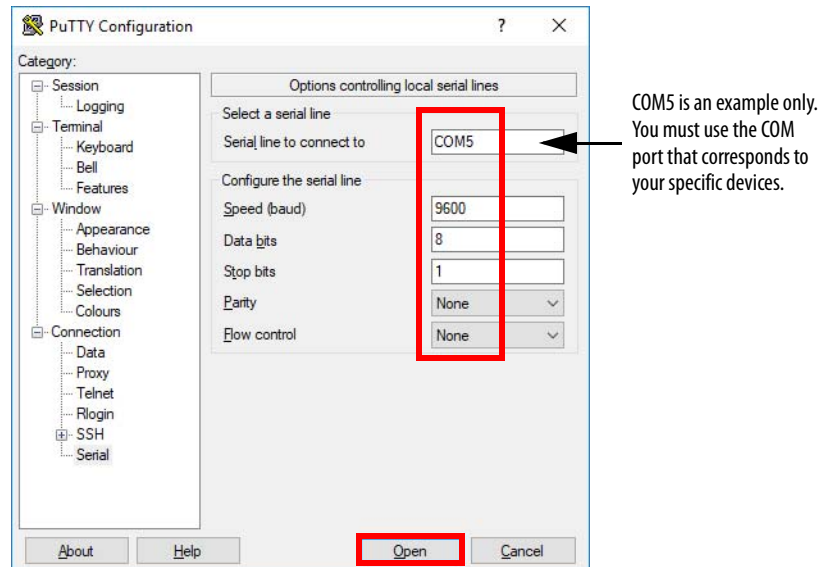


3. Select SSH and click Open.

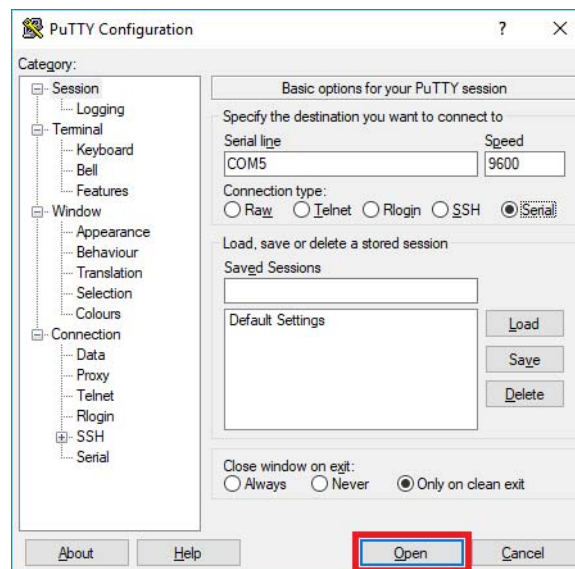
Complete these steps for a **Serial connection**.

TIP Skip this procedure if you are enabling an SSH connection, which is explained on [page 41](#).

1. From the PuTTY Configuration dialog box, click the Serial category.



2. Use the dialog box options as shown and click Open.



When you click Open with either connection procedure (SSH or Serial), the Cisco CLI appears.

Enabling IP Helper

In this section, we are configuring the IP helper-address for each VLAN, which uses the system DHCP servers. An IP helper-address command is required when the DHCP server is connected to a different subnet.

Complete these steps to configure SW010 (as shown on [page 39](#)).

1. Repeat steps 1...2 on [page 41](#) or steps 1...2 on [page 42](#) if you are using an Ethernet or Serial connection to access the command line interface (CLI).

When you click Open with either connection procedure (SSH or Serial), the command interface appears.

On the terminal emulator interface (CLI), type the text exactly as shown in boldface for each prompt. Press Enter after each entry.

2. Type the following to login.
login as: **admin**
Using keyboard-interactive authentication.
Password:

3. Enable configuration mode.
SW001#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.

4. Copy and paste the information in [Table 7](#) into a text editor, such as Notepad.

Table 7 - Routing Configuration

SW001
!
interface Vlan601
ip helper-address 172.18.1.10 redundancy 172.18.1.11
!
interface Vlan602
ip helper-address 172.18.1.10 redundancy 172.18.1.11
!
interface Vlan603
ip helper-address 172.18.1.10 redundancy 172.18.1.11

5. In a text editor, edit the configuration according to application requirements.
6. Copy from the text editor, and paste into the terminal emulator configuration software.

IMPORTANT Do not use the Ctrl+V command to paste the data into the PuTTY software. Right-click the mouse to paste the information in one, single file.

7. Type **end** and press Enter.

8. At the SW001# prompt, type **copy running-config startup-config**.

IMPORTANT If you do not execute [step 8](#) your configuration is lost during a power cycle.

9. Confirm the routing status by using the terminal emulator interface.
SW001#**show running config**

Control Network Switch Configurations

This chapter describes switch configurations for several topologies depending on your application requirements. Each of these topologies for a PlantPAx® system is explained separately to provide illustrations and procedures for the necessary port settings on the Control Network.

Topologies, and respective pages, include the following:

- Star, see [page 52](#)
- Ring (redundant DLR), see [page 58](#)
- PRP (redundant Star), see [page 63](#)

Regardless of your experience with switch configuration, we recommend that you follow the procedures on how to select the correct type of ports for devices, starting on [page 47](#).

This chapter includes illustrations and procedures on how to configure redundant media. Port aggregation links two Ethernet ports to provide redundancy if one of the links fails.

Before You Begin

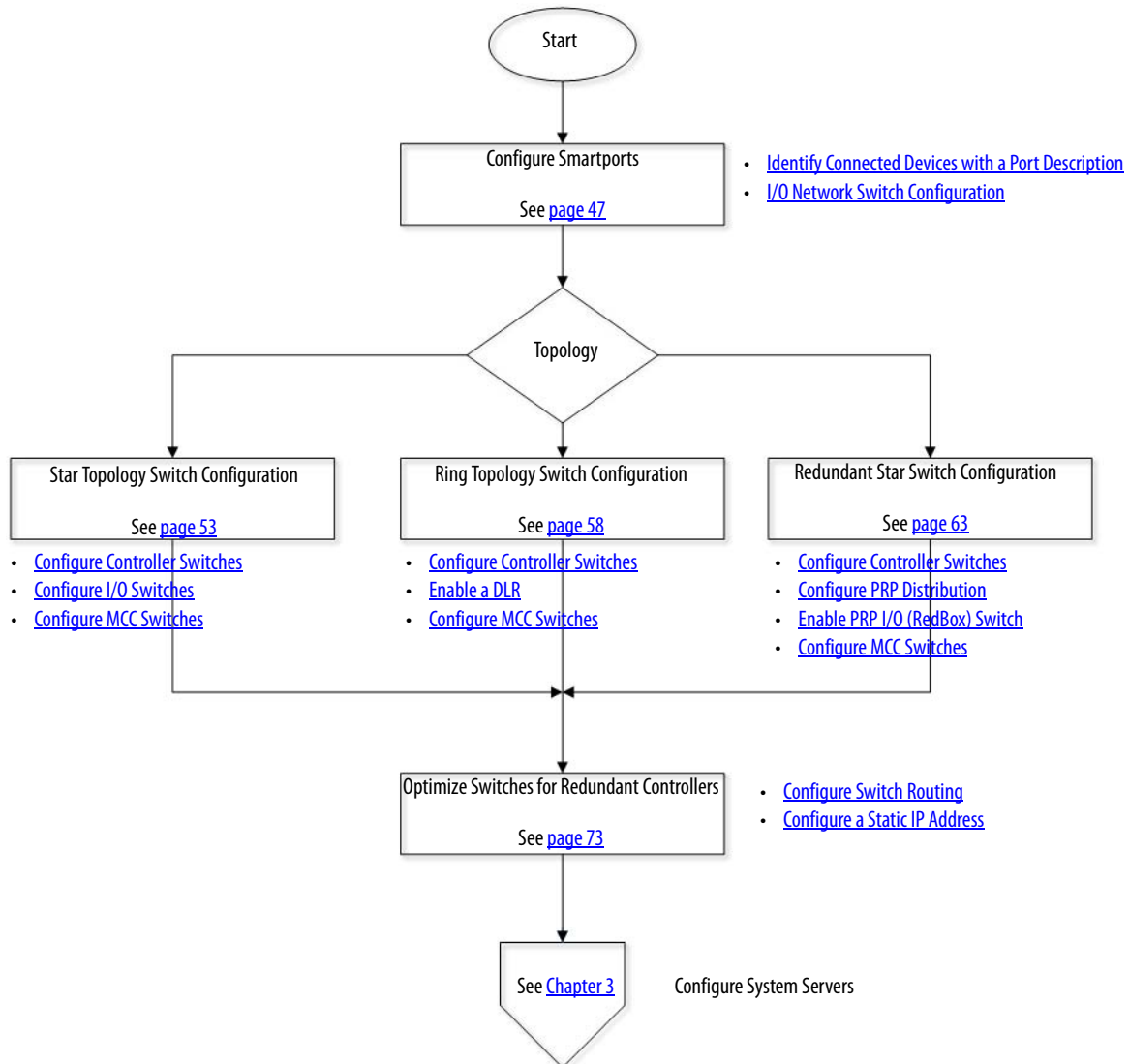
Before starting the procedures in this chapter, you must complete common network configuration for **all** switches in your PlantPAx system. See [Chapter 1](#) for how to initiate switches.

Managed switch configuration includes the following:

- Switch Express Setup
- VLAN segmentation
- Rapid PVST+
- Precision Time Protocol (PTP)
- Simple Network Management Protocol (SNMP)
- Switch routing

[Figure 5](#) lists the topics that are described in this chapter. Click the page number or the links for quick access to specific information in each subsection.

Figure 5 - PlantPAx Topology Configuration Workflow



Configure Smartports

Device Manager is a web-based management tool for configuring, monitoring, and troubleshooting individual switches. You can display Device Manager from anywhere in your network through a web browser. Device Manager displays real-time views of switch configuration and simplifies configuration tasks with features such as Smartports.

Smartports help designate the ports that are pre-defined for the application. Port roles are based on the type of devices to be connected to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to computers.

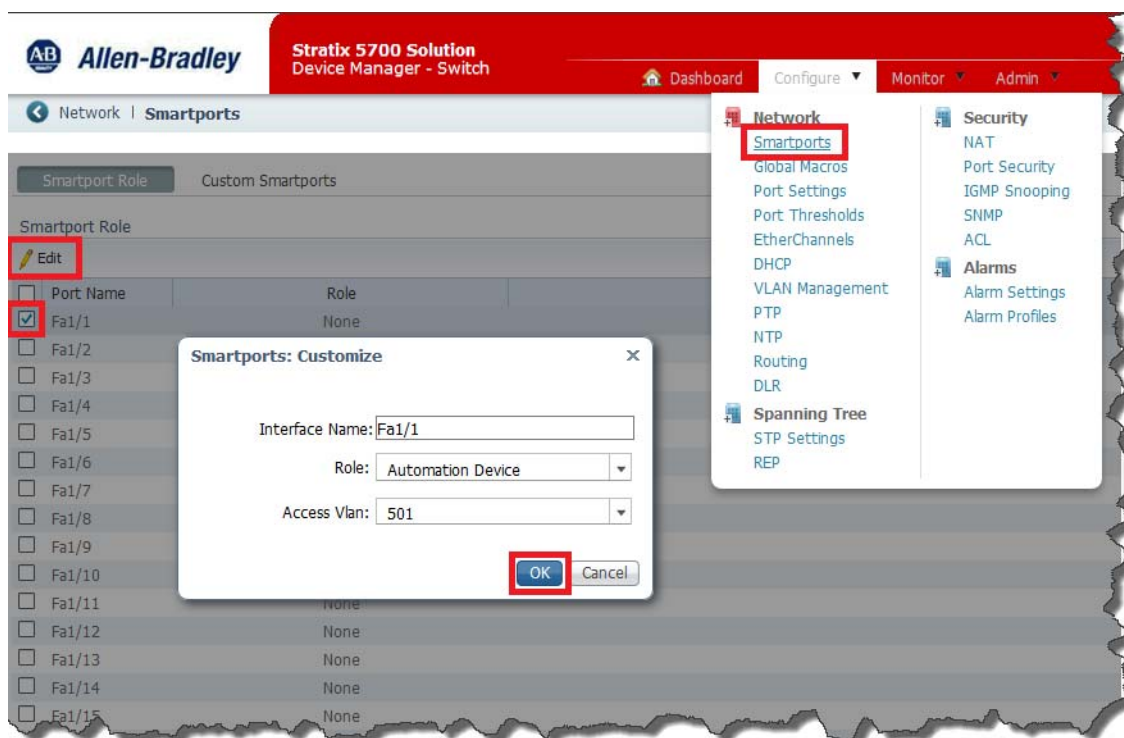
[Table 8](#) describes the port types that are selected with procedures in this section.

Table 8 - Available Ports

Smartport	Description
Automation Device	<p>The Automation Device Smartport is used for any EtherNet/IP devices. Devices include controllers, HMI displays, distributed I/O, and so forth. The Automation Device Smartport enables the following features:</p> <ul style="list-style-type: none"> • Sets the port to host mode that enables Spanning Tree PortFast and BPDU Guard • Enables port security (one MAC address per port) • Sets the VLAN number • Enables the automation QoS policy • Configures the output queues • Enables the alarm profile • Disables Cisco Discovery Protocol (CDP)
Multipoint Automation device	<p>Apply this role to ports connected to multipoint EtherNet/IP devices, such as multipoint EtherNet/IP devices arranged in a linear or daisy chain topology. You also can use this role for Device Level Ring (DLR). The following devices apply:</p> <ul style="list-style-type: none"> • 1783-ETAP module (for connection to the device port only) • Unmanaged switches (such as the Stratix® 2000) • Managed switches with Rapid Spanning Tree Protocol (RSTP) disabled: <ul style="list-style-type: none"> – Port is set to Access mode – No port security – Optimize queue management for CIP™ traffic
Desktop for Automation	<p>The Desktop for Automation Smartport can be used for computers on the Cell/Area zone EtherNet/IP network. Do not use this port role for any systems that run virtual machines without turning off the port security configuration. This Smartport enables the following features:</p> <ul style="list-style-type: none"> • Sets the port in access mode • Set the VLAN number • Enables port security (one MAC address per port) • Enables Spanning Tree PortFast • Enables Spanning Tree BPDU Guard • Enables the automation QoS policy • Sets the alarm profile • Provides up to two MAC addresses per port (physical computer and virtual machine)
VM-Desktop for Automation	<p>Apply this role to ports connected to computers that run virtualization software. This port role can be used with devices that run two MAC addresses.</p> <p>IMPORTANT: Do not apply the Virtual Desktop for Automation role to ports that are connected to switches, routers, or access points.</p> <p>VM-Desktop for Automation enables the following features:</p> <ul style="list-style-type: none"> • Sets the port access mode • Enables port security (two MAC addresses per port) • PortFast is enabled • Set the VLAN number • CIP-PTP-Traffic Policy enabled
Switch for Automation	<p>The Switch for Automation Smartport is used on ports that connect to other managed Ethernet switches that support STP (Spanning Tree Protocol). This port role enables the following features:</p> <ul style="list-style-type: none"> • Sets the port in trunk mode • Sets the native VLAN • Sets Spanning Tree to use a point-to-point link • Sets the port to trust QoS policy • Configures the output queues • Sets the alarm profile

Complete these steps to configure Smartports. This procedure must be repeated for **each** switchport based on the devices that you are using.

1. From the main menu of the switch Device Manager, click Configure and choose Network>Smartports.
2. Select the desired ports and click Edit.



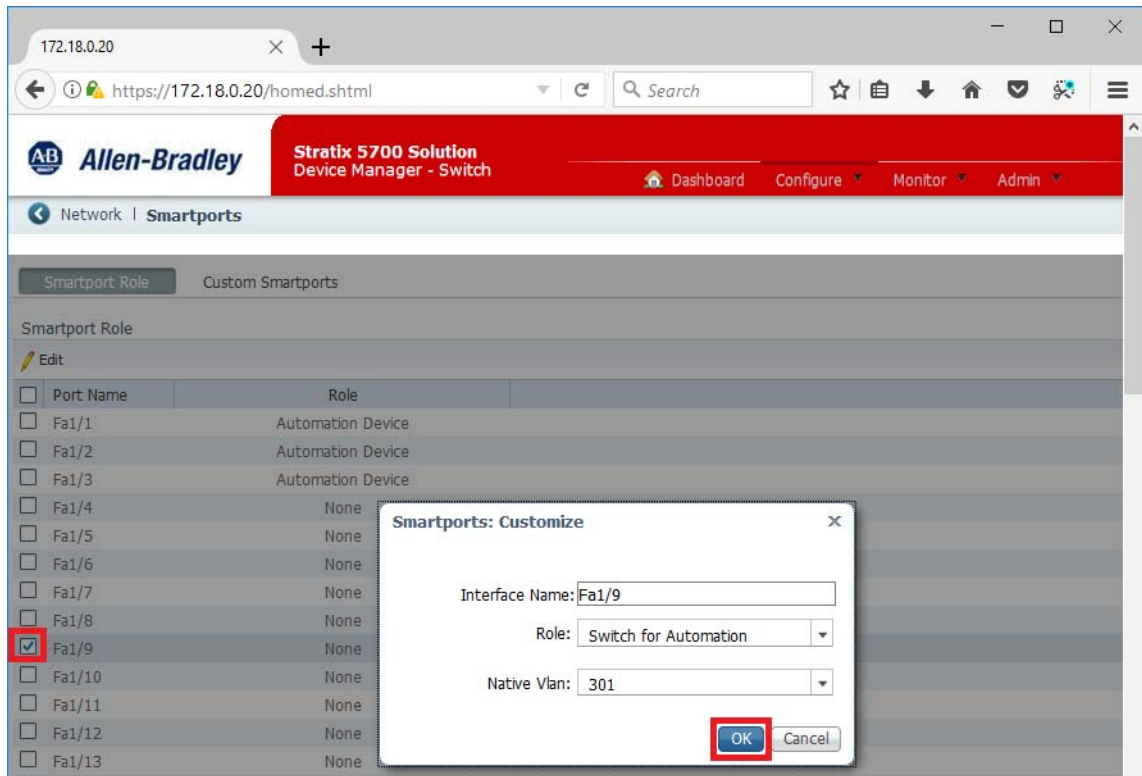
3. Select a desired role from the Role pull-down menu.
4. Select an Access VLAN or Native VLAN based on the use as described in [Table 8 on page 47](#).

For example:

VLAN 501 – Control network

5. Click OK.

6. Select another Smartport from the Role pull-down menu, and click OK.



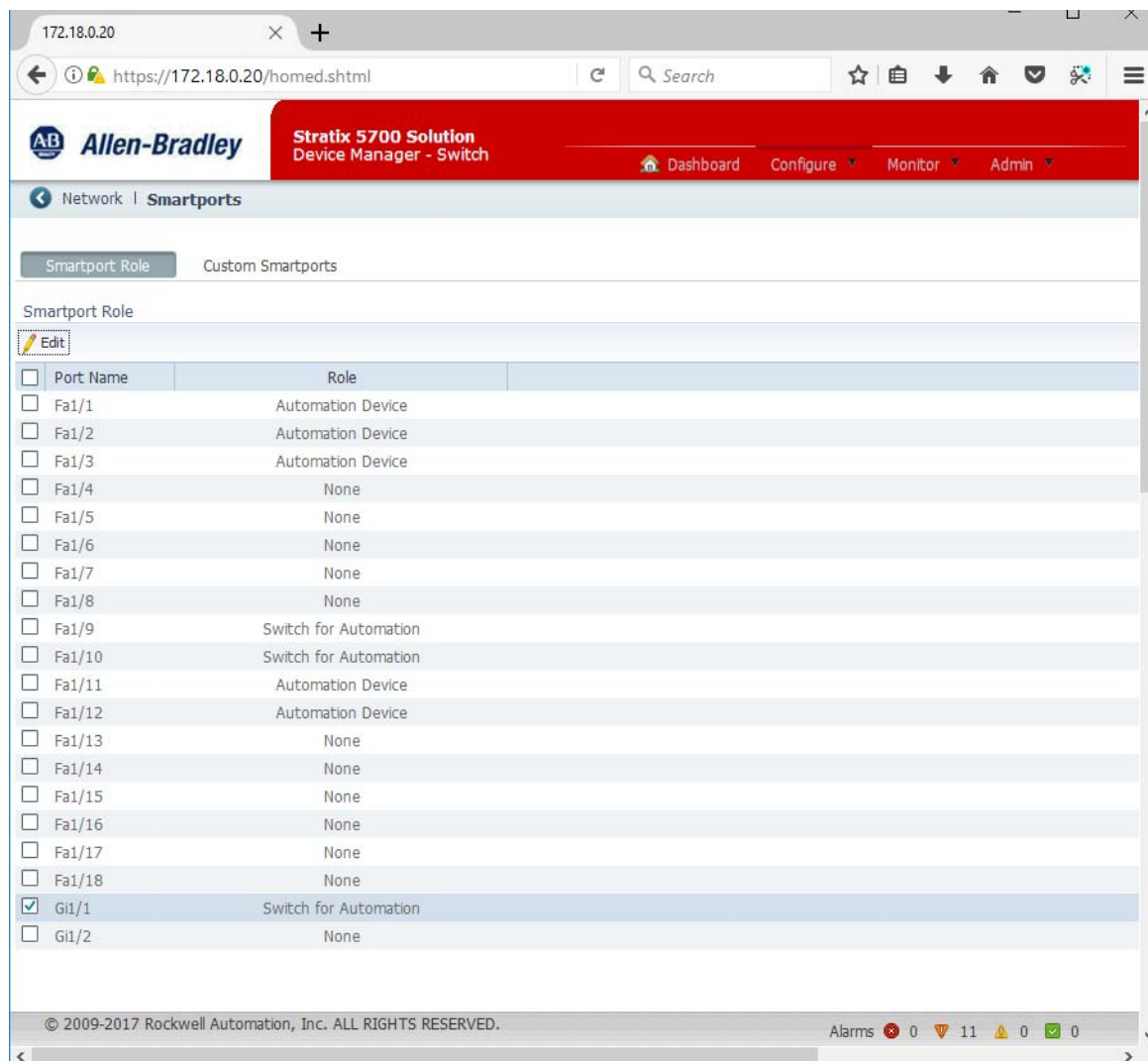
7. Select each port, click Edit, and type a Native VLAN.

For example:

VLAN 301 – Trunk

8. Repeat [step 6](#) and [step 7](#) for each port that is being used.

IMPORTANT If you have a virtualized system, connect the hypervisor to a port with the Desktop for Automation role.

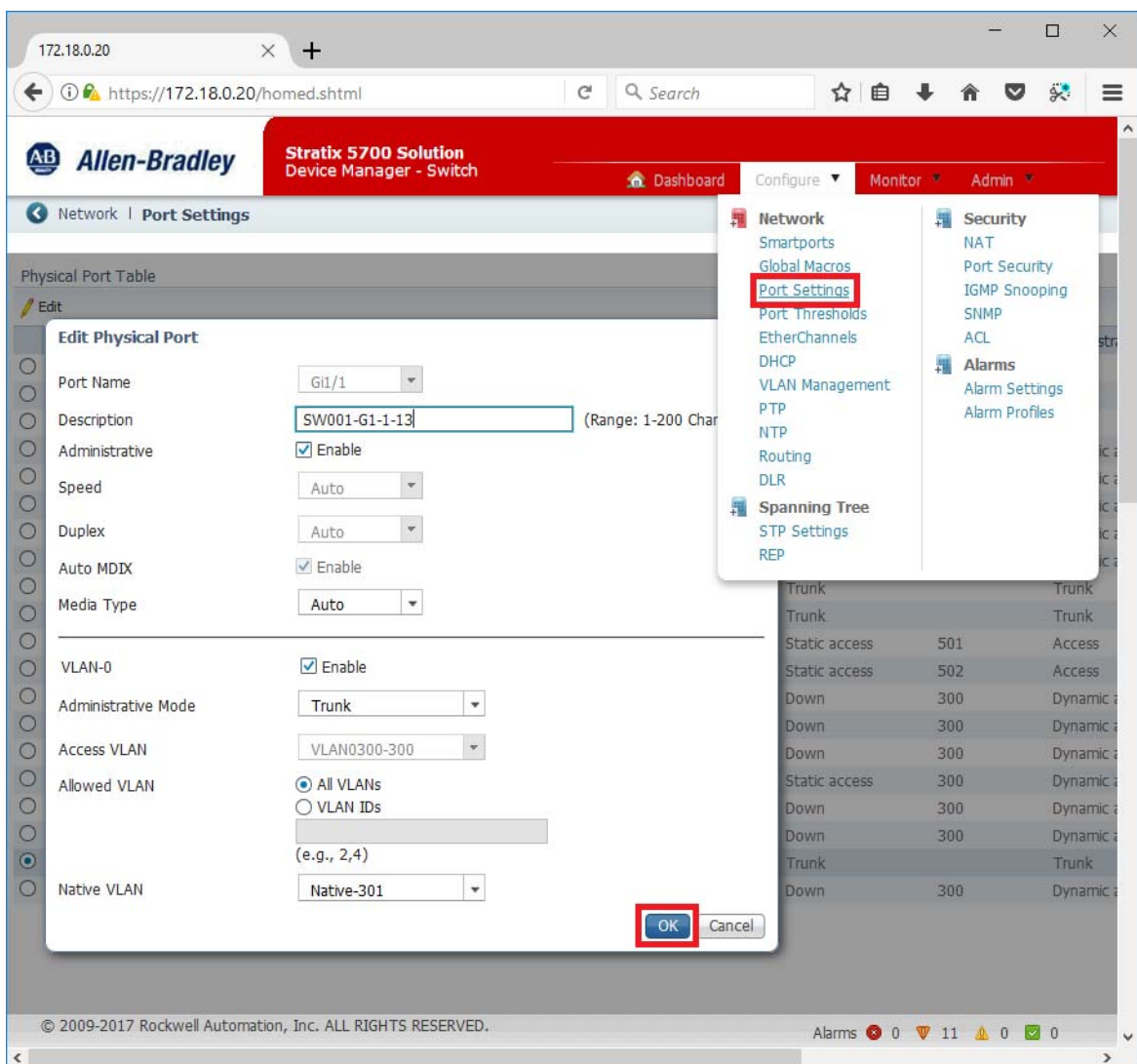


Identify Connected Devices with a Port Description

Port settings define the application requirements. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port must be compatible with the port settings of the connected device.

We recommend that you configure each switch port with a port description to help with diagnostics and maintenance. Complete these steps.

1. From the main menu of the switch Device Manager, click Configure and choose Network>Port Settings.
2. Select a port and click Edit.



3. We recommend that in the Description text box, type the connected device.
4. Click OK.

The switch description is listed next to the port name.

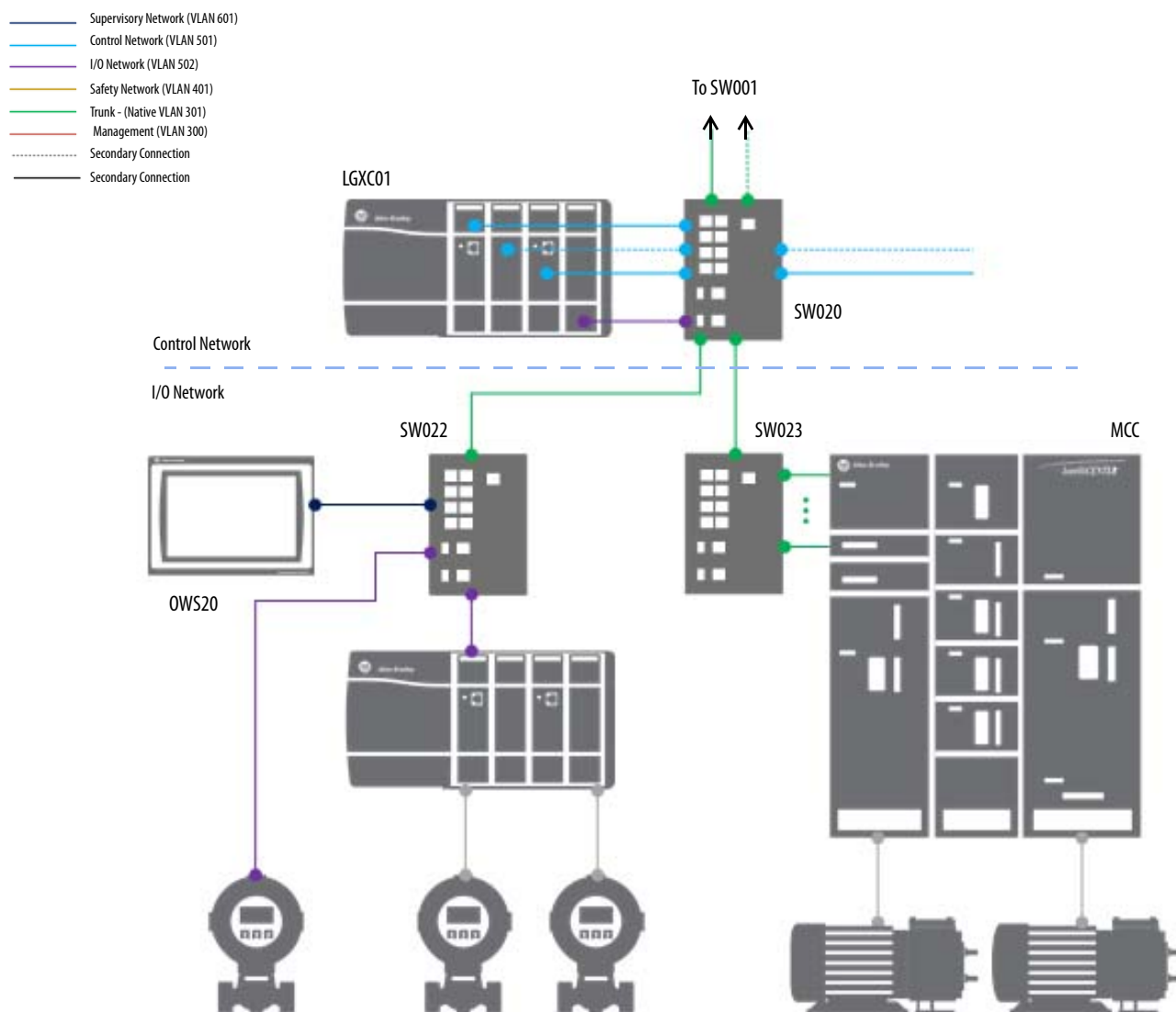
I/O Network Switch Configuration

This section describes three topologies on the I/O Network, starting with a Star configuration. The switches that are used for each are described in their respective sections. Each section includes set up for controller, I/O, and MCC switches.

See the following pages for basic PlantPAx topologies:

- Star, [page 53](#)
- Device Level Ring, [page 58](#)
- Redundant Star, [page 63](#)

Figure 6 - Control and I/O Network



Star Topology Switch Configuration

Use Layer 2 switches with these procedures.



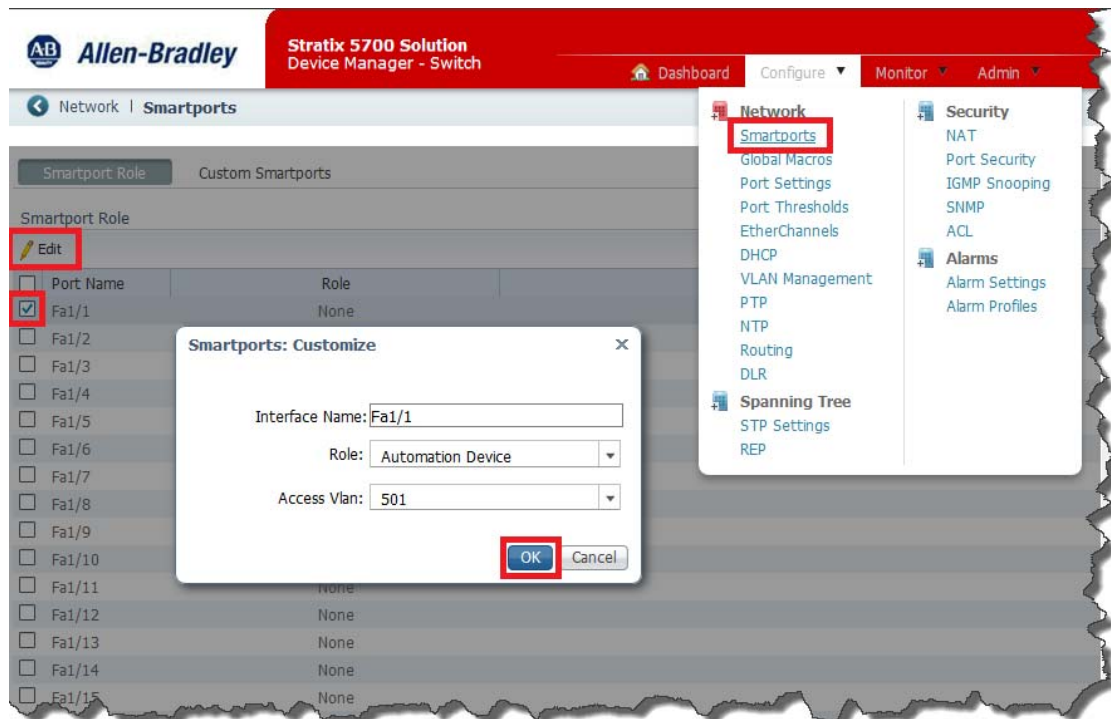
Stratix 5700 switch

Access switches serve as an uplink from the servers to the workstations. Layer 2 switches also send packets at the controller level from the end devices. With multiple network levels, access switches control the flow of information to make sure that packets are delivered to the correct network level. Complete these steps.

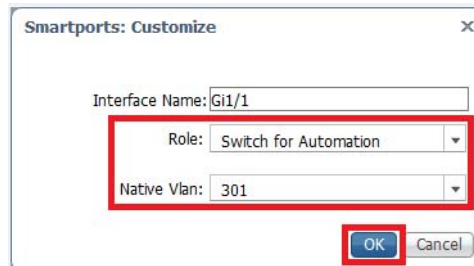
1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.

IMPORTANT See [page 47](#) for Smartport descriptions.

2. Select the desired ports and click Edit.



3. Select a desired role from the Role pull-down menu.



Example I/O configurations:

VLAN 301 – Trunk

4. Click OK.

Use Layer 2 switches with these procedures.



Stratix 5700 switch

Configure Controller Switches

Complete these steps to configure SW020 and SW021 switches to route data from I/O Network (Level 1) devices.

For color legend, see [page 52](#).

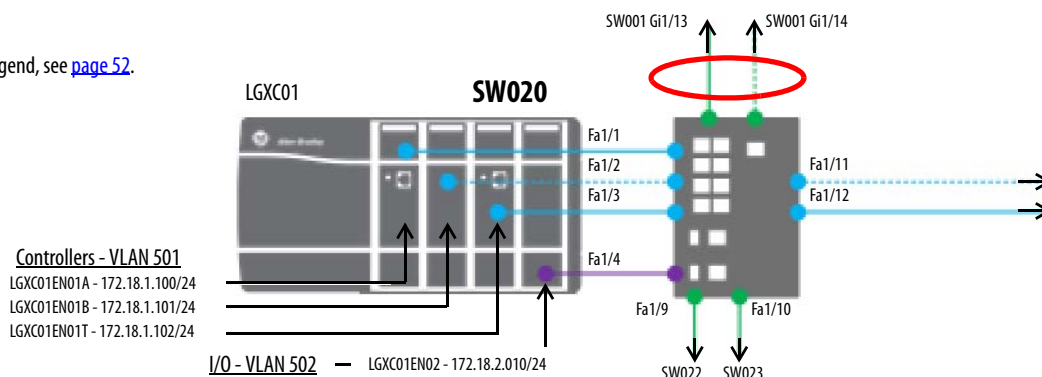


Table 9 - Control Network - Control Star

Port	Role	VLAN	SW020
Fa1/1	Automation Device	501 (Control Network)	LGXC01EN01A
Fa1/2			LGXC01EN01B
Fa1/3			LGXC01EN01T
Fa1/4		502 (I/O Network)	LGXC01EN02
Fa1/5...Fa1/8	—	—	—
Fa1/9	Switch for Automation	Trunk (Native VLAN 301)	SW022-G1/1
Fa1/10			SW023-G1/1
Fa1/11...Fa1/12	Automation Device	501 (Control Network)	SIS01EN01A
Fa1/13...Fa1/18	—	—	SIS01EN01B
Gi1/1 ⁽¹⁾	Switch for Automation	Trunk (Native VLAN 301)	SW001-G1/13
Gi1/2 ⁽¹⁾		—	SW001-G1/14

(1) Ports Gi1/1 and Gi1/2 must be configured as an EtherChannel to connect to SW001.

1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.
2. Select the desired ports and click Edit.
3. Select a desired role from the Role pull-down menu and click OK.
4. Use information in [Table 9](#) to configure switch ports.
5. Select the desired ports and click OK.

Use Layer 2 switches with these procedures.



Stratix 5700 switch

For color legend, see [page 52](#).

Configure I/O Switches

In our example, the SW022 switch is used for the I/O connection and the OWS/EWS access connection.

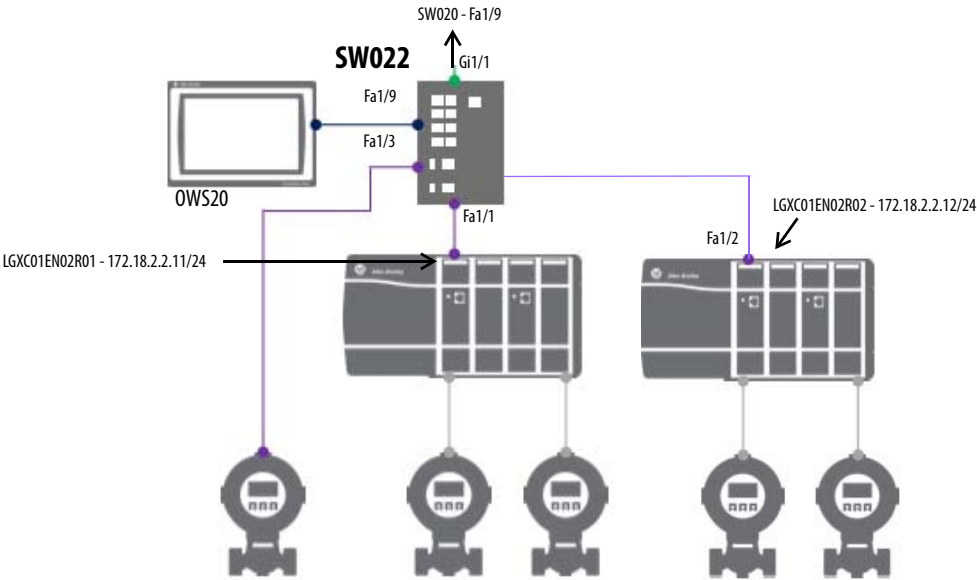


Table 10 - I/O Network - I/O Star

Port	Role	VLAN	SW022
Fa1/1	Automation Device	502 (I/O Network)	LGXC01EN02R01
Fa1/2			LGXC01EN02R02
Fa1/3			LGXC01EN02FM01
Fa1/4...Fa1/8			—
Fa1/9	Desktop for Automation	501 (Control Network)	OWS20
Fa1/10...Fa1/18	—	—	—
Gi1/1	Switch for Automation	Trunk (Native VLAN 301)	SW020 Fa1/9
Gi1/2	—	—	—

1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.

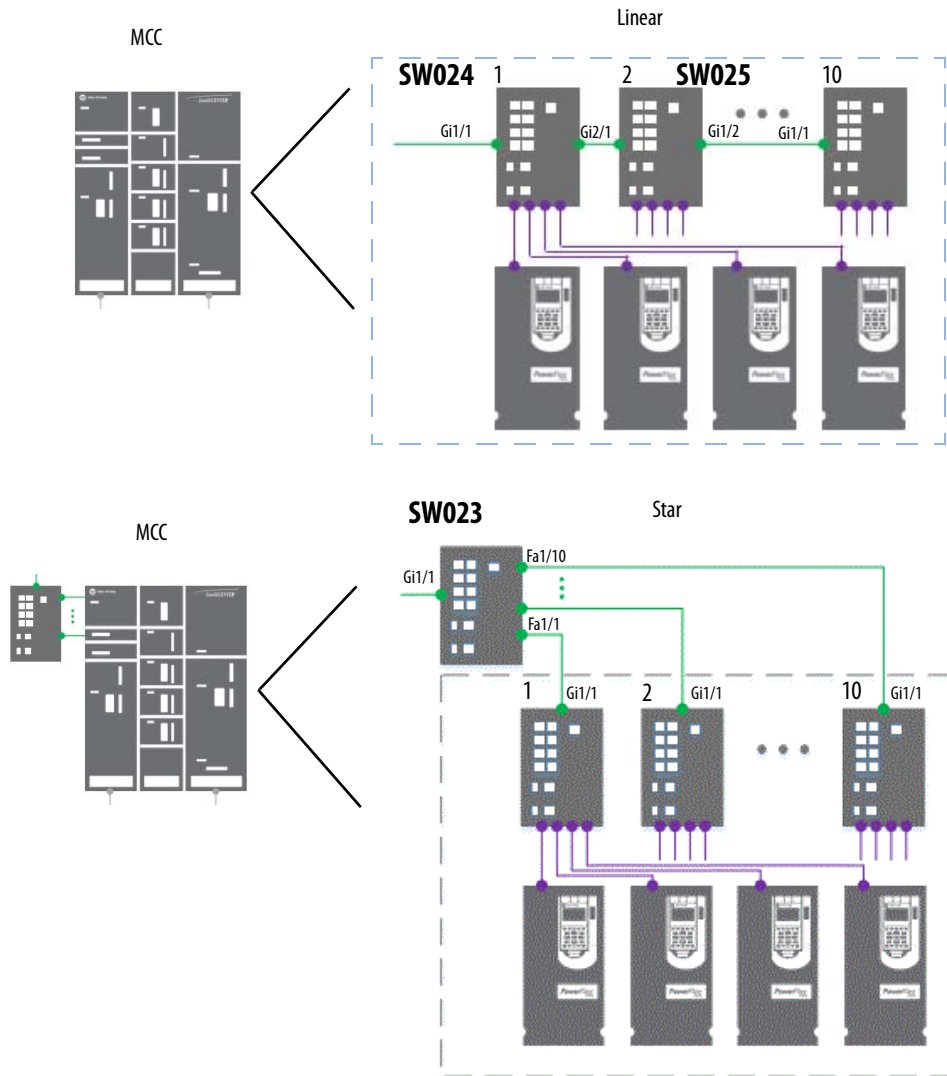
IMPORTANT See [page 47](#) for Smartport descriptions.

2. Select the desired ports and click Edit.
3. Select Switch for Automation from the Role pull-down and click OK.
4. Use the information in [Table 10](#) to configure switch ports.

Configure MCC Switches

Complete these steps to configure a Linear or Star topology for motor control center (MCC) devices.

For color legend, see [page 52](#).



1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.

IMPORTANT See [page 47](#) for Smartport descriptions.

2. Select the desired ports and click Edit.
3. Select a role type from the Role pull-down and click OK.

4. Use the information in [Table 11](#) and [Table 12](#) to configure switch ports.

Table 11 - I/O Network - MCC Linear/Star

Port	Role	VLAN	SW024 - Linear
Fa1/1...Fa1/15	Automation Device	502 (I/O Network)	—
Fa1/16	Desktop for Automation	300 (Management)	—
Fa1/17...Fa1/18	—	—	—
Gi1/1	Switch for Automation	Trunk (Native VLAN 301)	SW020-F1-10
Gi1/2			SW025-G1-1

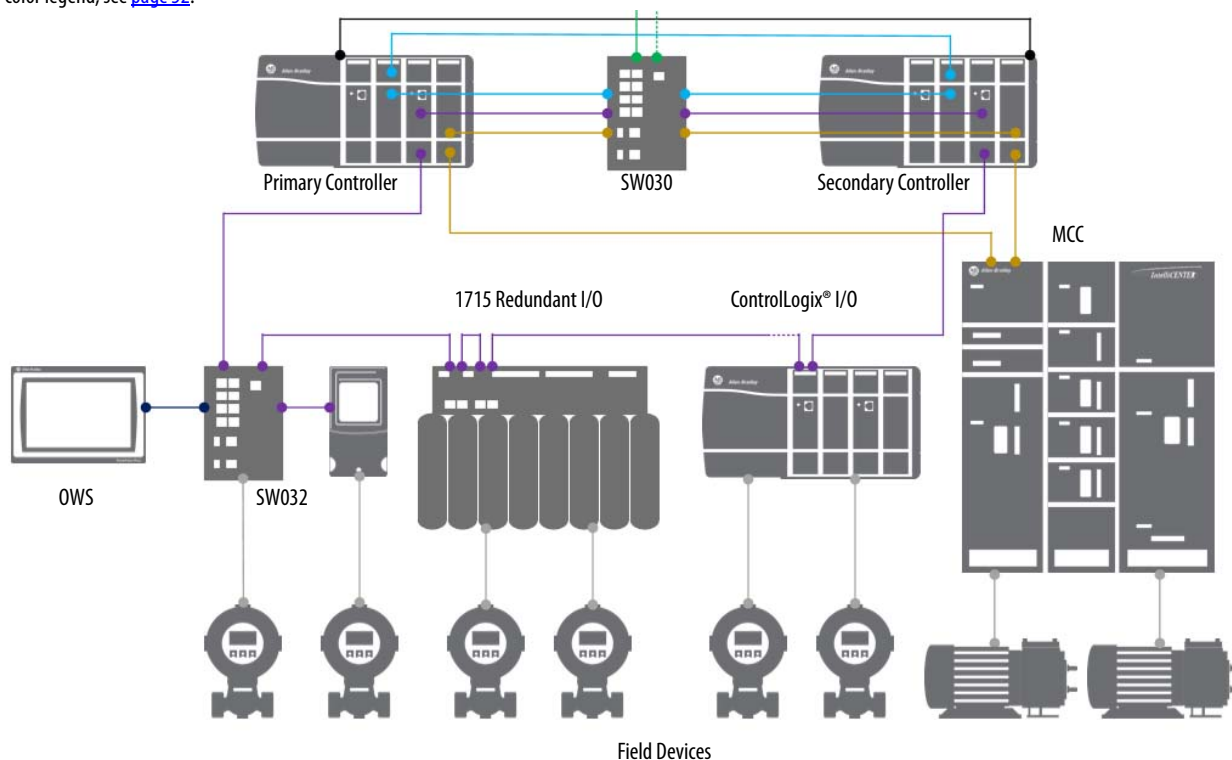
Table 12 - I/O Network - MCC Star (Additional)

Port	Role	VLAN	SW023 - Star
Fa1/1...Fa1/15	Switch for Automation	301 (Native VLAN)	—
Fa1/16	Desktop for Automation	300 (Management)	—
Fa1/17...Fa1/18	—	—	—
Gi1/1	Switch for Automation	301 (Native VLAN)	SW020-F1-10
Gi1/2	—	—	—

Ring Topology Switch Configuration

This section details the switch configuration for a Ring topology by using a Device Level Ring (DLR) on the I/O Network.

For color legend, see [page 52](#).



A DLR topology is a device-level network topology that helps prevent a loss of communication between devices if a fault occurs. Multiport EtherNet/IP devices equipped with DLR technology connect directly to neighboring nodes and form a ring topology at the end devices. If a break in the line is detected, the network provides an alternate routing of the data to help recover the network at fast rates.

All end devices that are tightly coupled to a controller must be a part of the same embedded switch topology. This peer-to-peer architecture reduces the physical amount (and therefore cost) of cabling.

Enhanced diagnostics built into DLR-enabled products identify the point of failure, helping to speed maintenance and reduce mean time to repair.

For more information, see the Embedded Switch Technology Reference Architectures, publication [ENET-RM003](#).

Configure Controller Switches

Complete these steps to select the switch ports for SW030.

For color legend, see [page 52](#).

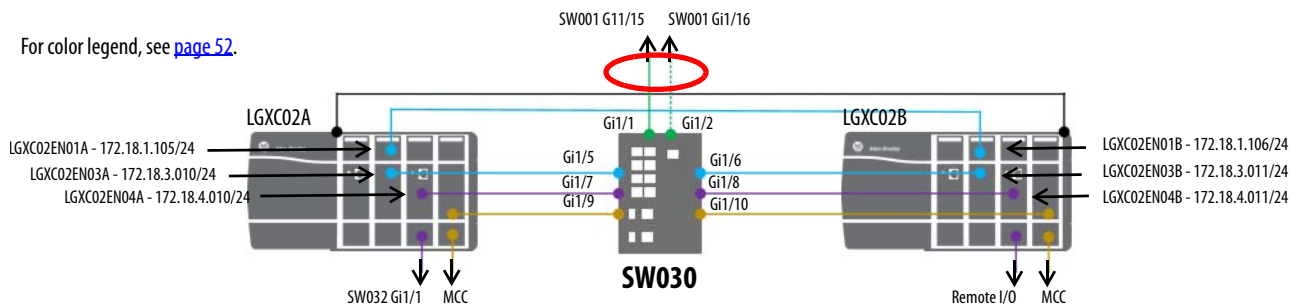


Table 13 - Control Network - Control DLR

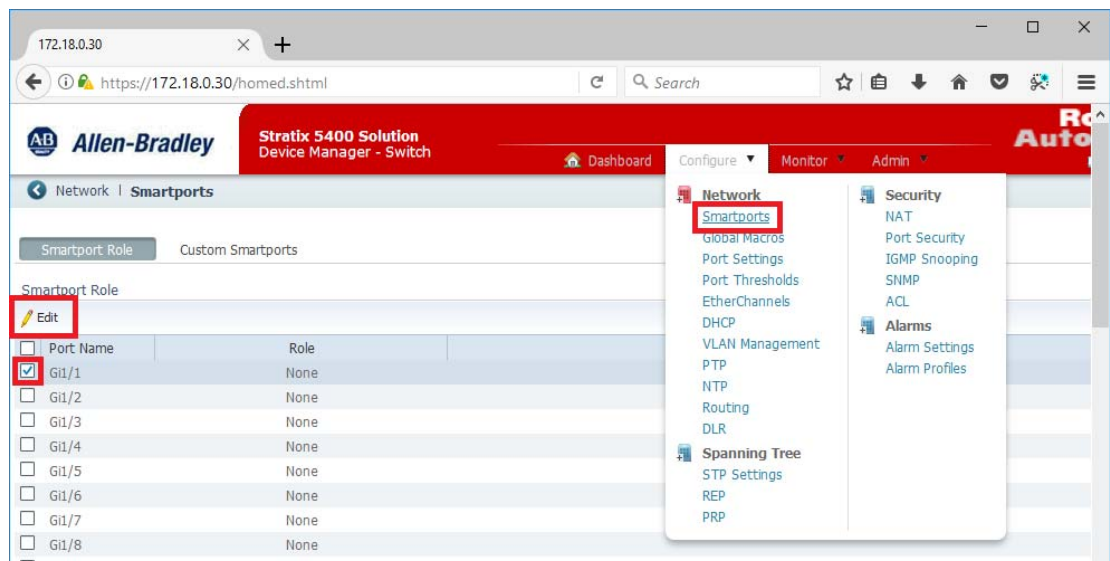
Port	Role	VLAN	SW030
Gi1/1 ⁽¹⁾	Switch for Automation	Trunk (Native VLAN 301)	SW001-Gi1/15
Gi1/2 ⁽¹⁾			SW001- Gi1/16
Gi1/5	Automation Device	501 (Control Network)	LGXC02EN01A
Gi1/6			LGXC02EN01B
Gi1/7		503 (I/O Network)	LGXC02EN03A
Gi1/8			LGXC02EN03B
Gi1/9		504 (MCC Network)	LGXC02EN04A
Gi1/10			LGXC02EN04B

(1) Ports Gi1/1 and Gi1/2 must be configured as an EtherChannel to connect to SW001.

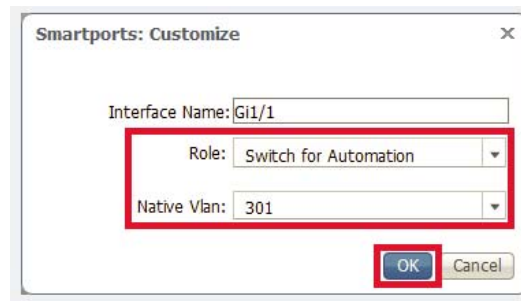
- From the main menu of the Device Manager, click Configure and choose Network>Smartports.

IMPORTANT See [page 47](#) for Smartport descriptions.

- Select the desired ports and click Edit.



3. Select Switch for Automation from the Role pull-down.



4. Select a Native Vlan and click OK.
5. Use the information in [Table 13](#) to configure switch ports.

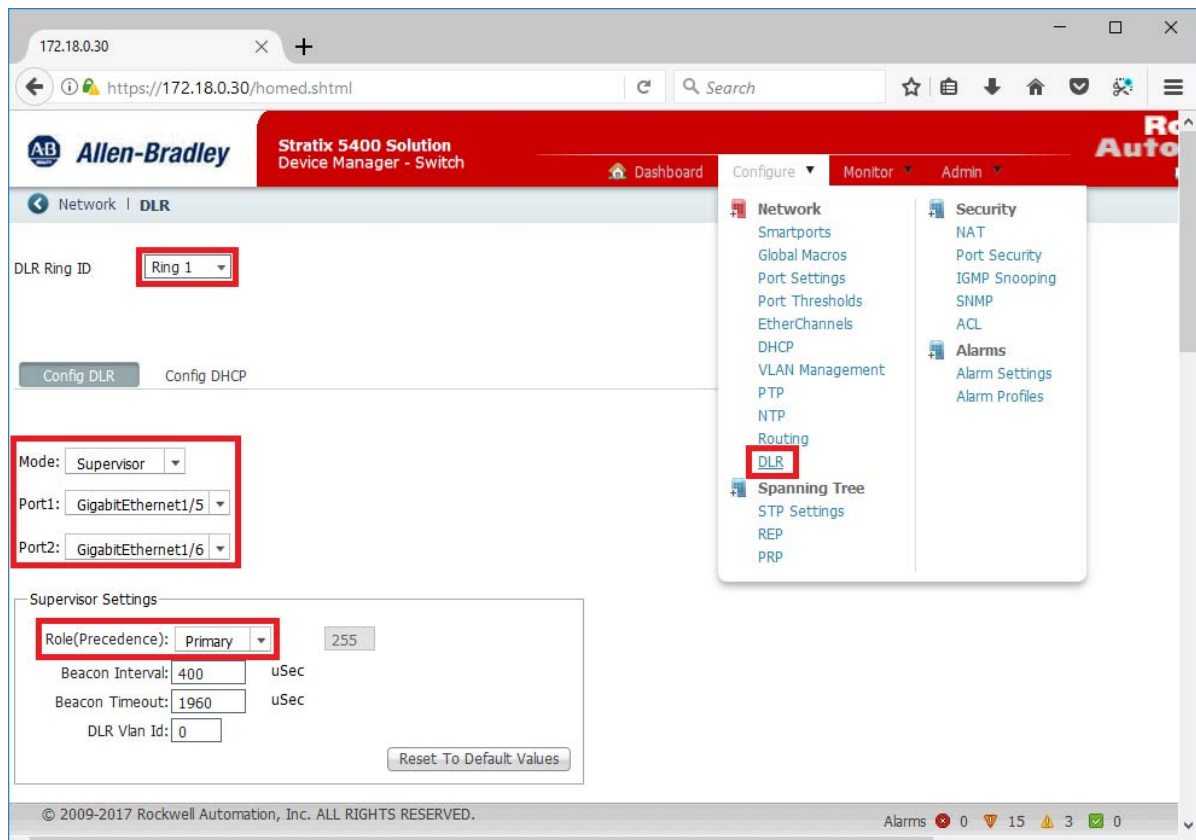
Enable a DLR

Our single DLR example in this section is between the controllers and access switch (SW030) for server-to-controller communication.

1. From the main menu of the Device Manager, click Configure and choose Network>DLR.

IMPORTANT See [page 47](#) for Smartport descriptions.

2. Select Ring 1 from the DLR Ring ID pull-down.



3. Select Supervisor from the Mode pull-down.

4. Select the ports.

5. Select Primary for the Role (Precedence) pull-downs.

Continue to the next gateway section by scrolling down the DLR dialog box.

Configure MCC Switches

Complete these steps to configure SW033 and SW034 switches on a DLR network.

For color legend, see [page 52](#).

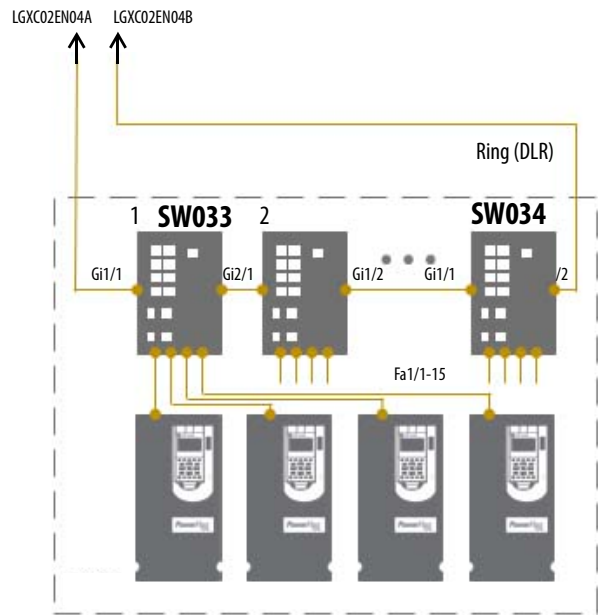


Table 14 - I/O Network - MCC DLR

Port	Role	VLAN	SW033 - Ring	SW034 - Ring
Fa1/1...Fa1/15	Automation Device	504 (MCC Network)	Device tag	Device tag
Fa1/16	Desktop for Automation	300 (Management) ⁽²⁾	—	—
Fa1/17...Fa1/18	—	—	—	—
Gi1/1	Switch for Automation ⁽¹⁾	Trunk (Native VLAN 301)	LGXC02EN04A	SW033 - Gi1/2
Gi1/2			SW034 - Gi1/1	LGXC02EN04B

(1) Ports Gi1/1 and Gi1/2 must be configured for DLR.
(2) Optional.

1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.

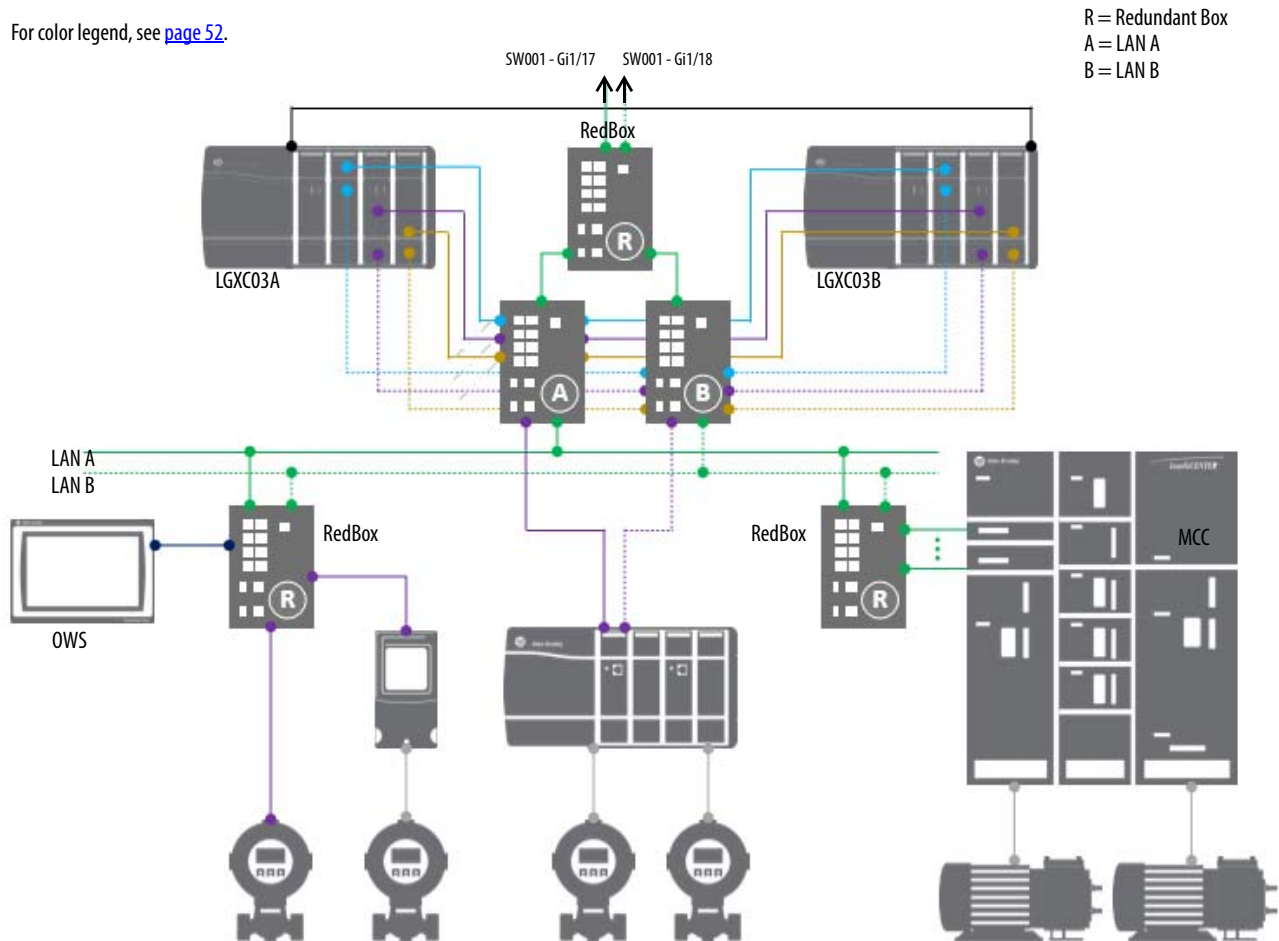
IMPORTANT See [page 47](#) for Smartport descriptions.

2. Select the desired ports and click Edit.
3. Select a role type from the Role pull-down and click OK.
4. Use the information in [Table 14](#) to configure switch ports.

Redundant Star Switch Configuration

This section details the switch configuration for a Redundant Star topology with a Parallel Redundancy Protocol (PRP) on the I/O Network.

For color legend, see [page 52](#).



PRP is available on Stratix 54x0 switches. PRP offers alternative network topologies for interconnecting EtherNet/IP devices. PRP technology builds redundancy into the end devices so that network infrastructure can be duplicated by using standard components, such as managed and unmanaged switches.

IMPORTANT You must use a 1756-EN2TP, PRP communication module for PRP topologies.

For more information, see the Stratix Managed Switches User Manual, publication [1783-UM007](#).

Configure Controller Switches

Complete these steps to select the switch ports for redundant switches. The PRP switch is referred to as a RedBox.

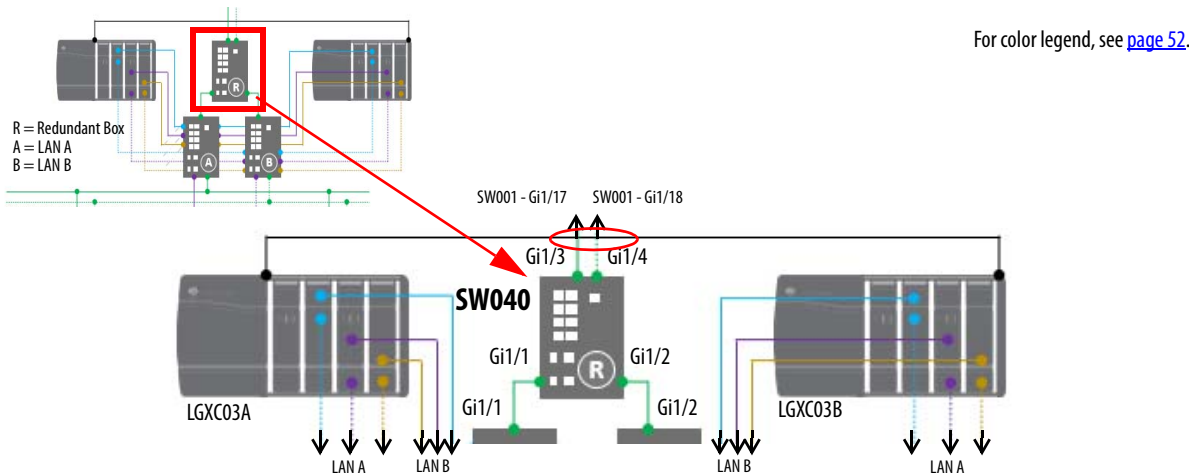


Table 15 - Control Network - Control PRP

Port	Role	VLAN	SW040
Gi1/1	Switch for Automation	Trunk (Native VLAN 301)	SW042 - Gi1/1
Gi1/2			SW043 - Gi1/1
Gi1/3 ⁽¹⁾			SW001-Gi1/17
Gi1/4 ⁽¹⁾			SW001-Gi1/18
Gi1/5...Gi1/20			—

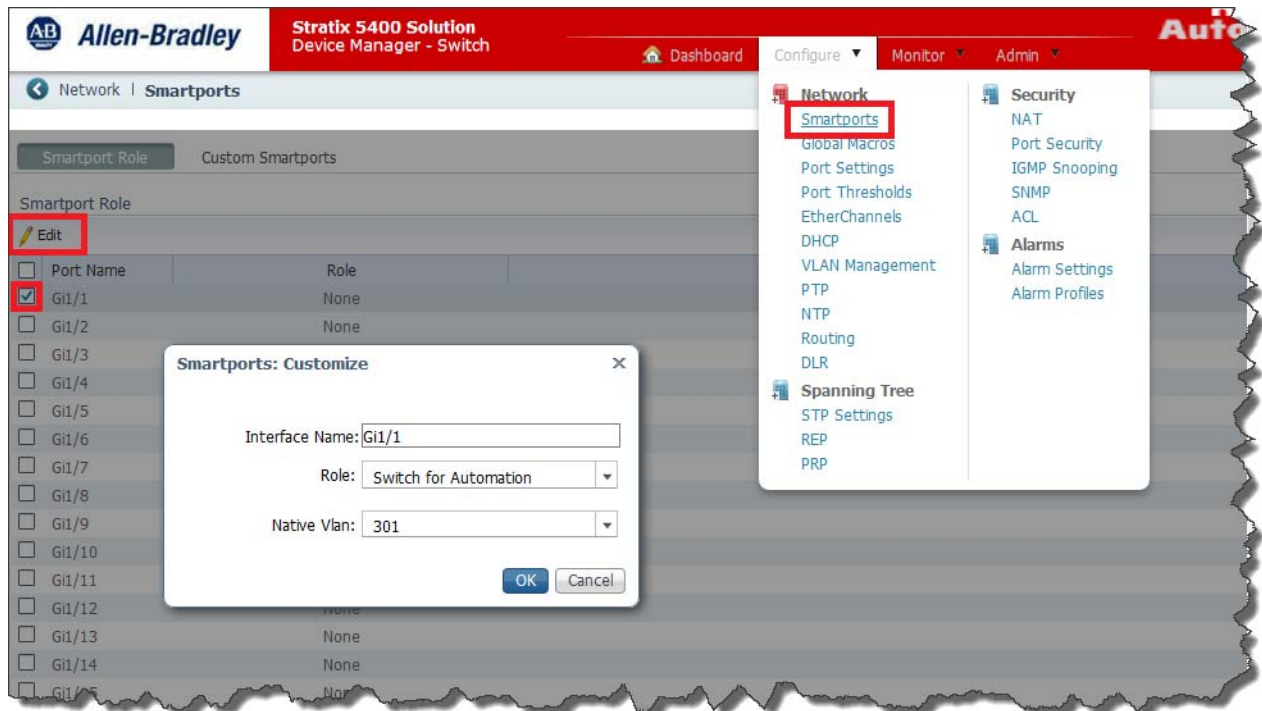
(1) Ports Gi1/3 and Gi1/4 must be configured as an EtherChannel to connect to SW001.

IMPORTANT You must use a 1756-EN2TP, PRP communication module for PRP topologies.

1. From the main menu of the Device Manager, click Configure and choose Network>Smartports.

TIP See [page 47](#) for Smartport descriptions.

2. Select the desired ports and click Edit.



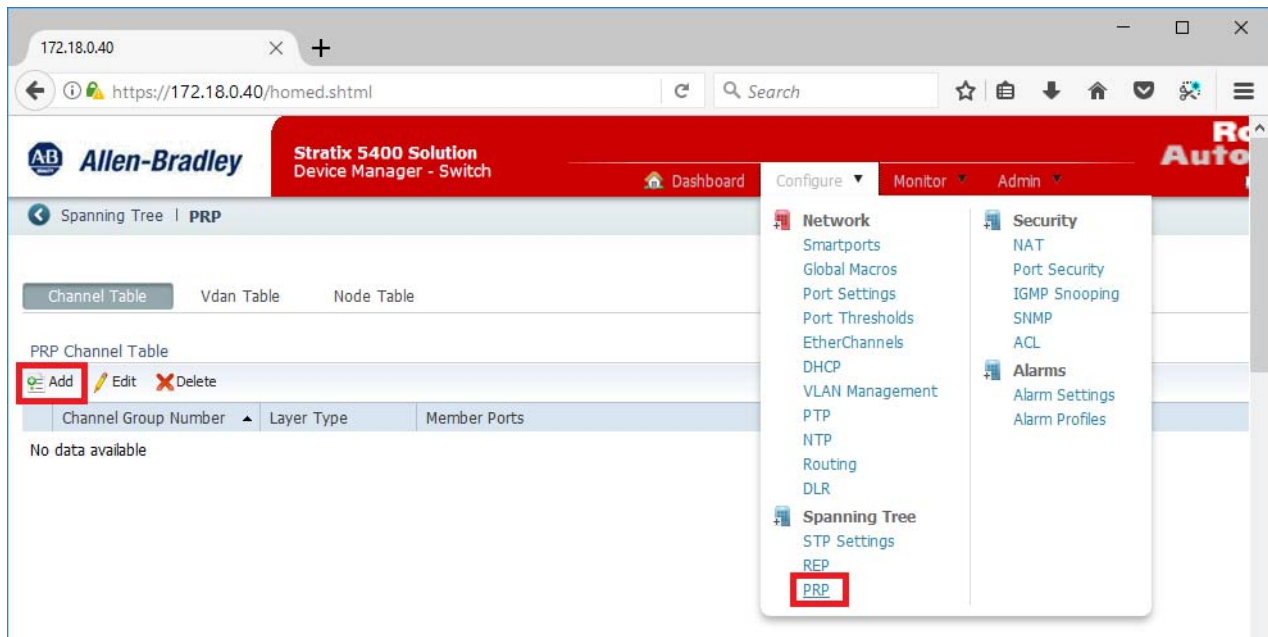
3. Select Switch for Automation from the Role pull-down.
4. Select a Native Vlan and click OK.
5. Use the information in [Table 15](#) to configure switch ports.

Enable PRP (RedBox) Switch

A RedBox switch allows non-PRP devices to be added to both LANs. Devices that are connected to both LANs through a RedBox are called Virtual Doubly Attached Nodes (VDANs). VDANs do not have media redundancy between the device and the RedBox, however, media redundancy exists on the LAN A/LAN B side of the RedBox.

Complete these steps.

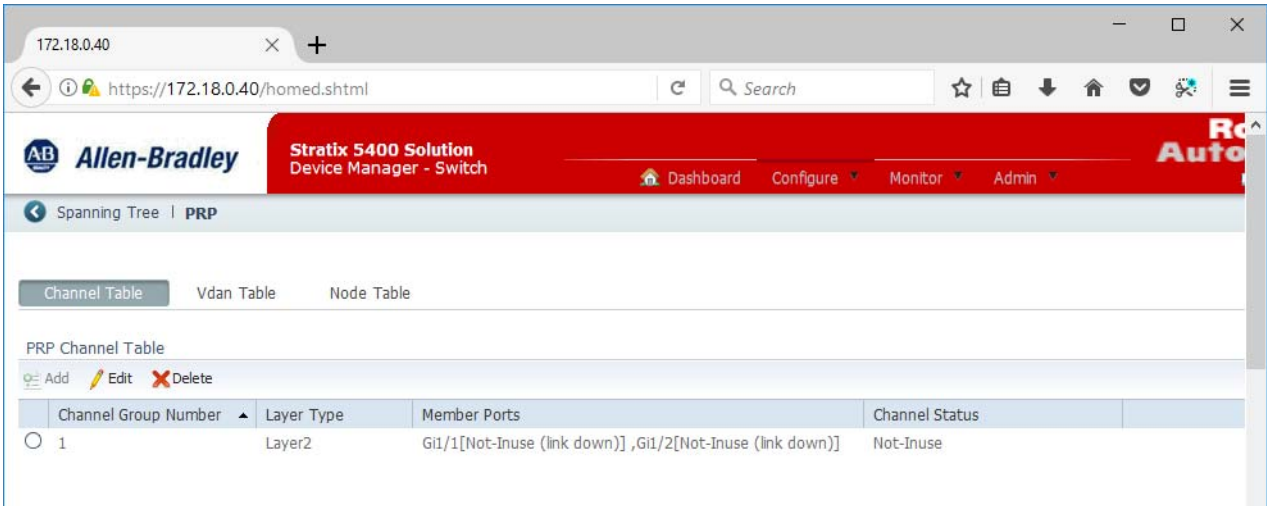
1. From the main menu of the Device Manager, click Configure and choose Configure>PRP.



2. Click Add and select Trunk from the Administrative Mode pull-down.

3. Select All VLANs for the Allows VLAN.
4. Select Native-301 from the Native VLAN pull-down.

5. Click OK.



Configure PRP Distribution

The two ports for each PRP device are attached to two separated networks of similar topology to minimize downtime and enhance high availability.

For color legend, see [page 52](#).

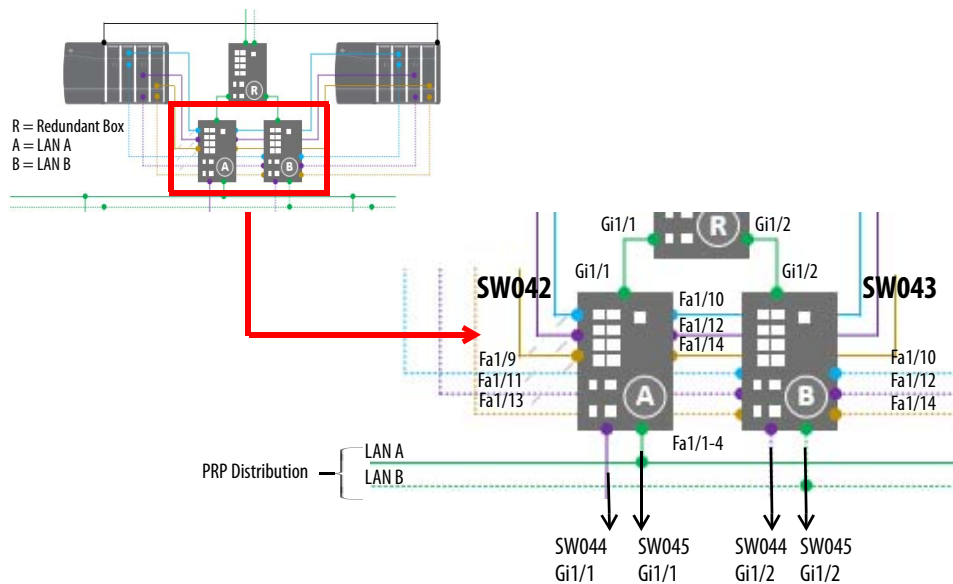
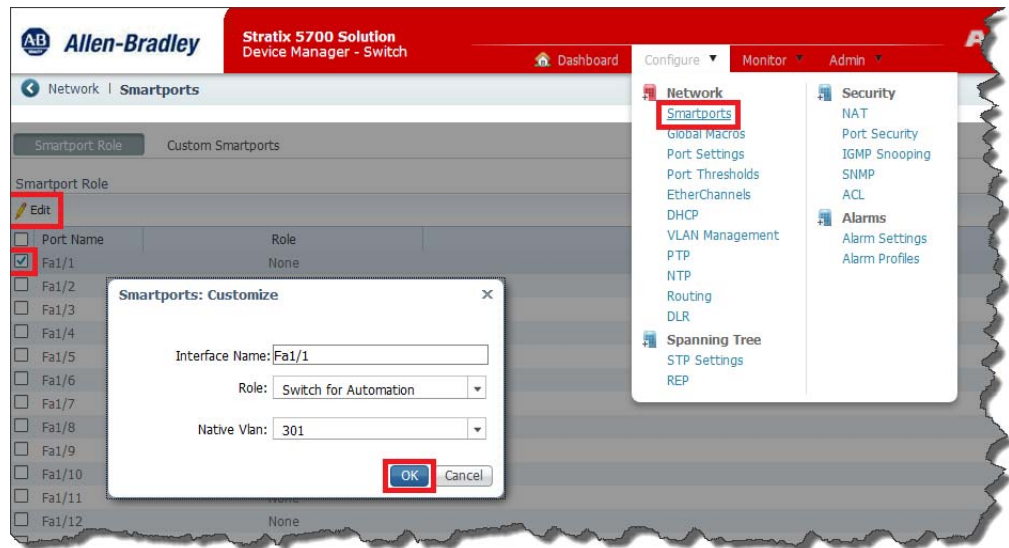


Table 16 - I/O Network - Control PRP

Port	Role	VLAN	SW042 (LAN A)	SW043 (LAN B)
Fa1/1	Switch for Automation	301 (Native VLAN - Trunk)	SW044 - Gi1/1	SW044 - Gi1/2
Fa1/2			SW045 - Gi1/1	SW045 - Gi1/2
Fa1/3-4			—	—
Fa1/5...Fa1/8	—	—	—	—
Fa1/9-10	Multiport Automation	501 (Control Network)	LGXC03A	LGXC03B
Fa1/11-12		505 (I/O Network)		
Fa1/13-14		506 (MCC Network)		
Fa1/15...Fa1/18	—	—	—	—
Gi1/1	Switch for Automation	301 (Native VLAN - Trunk)	SW040 - Gi1/1	SW040 - Gi1/2

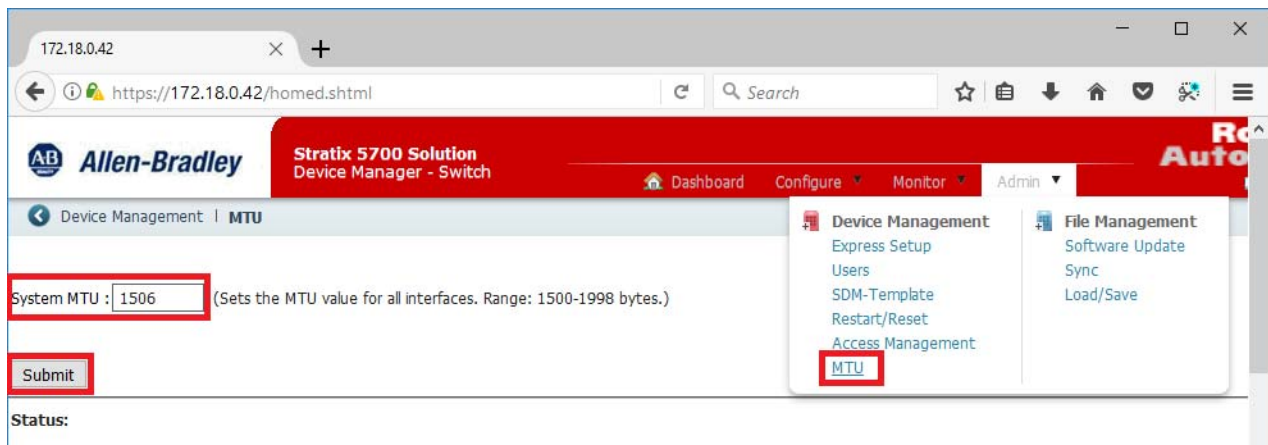
1. From the main menu of the Device Manager, click Configure and choose Smartports.



2. Select the desired ports and click Edit.
3. Select Switch for Automation from the Role pull-down.
4. Select a Native Vlan and click OK.
5. Use the information in [Table 16](#) to configure switch ports.

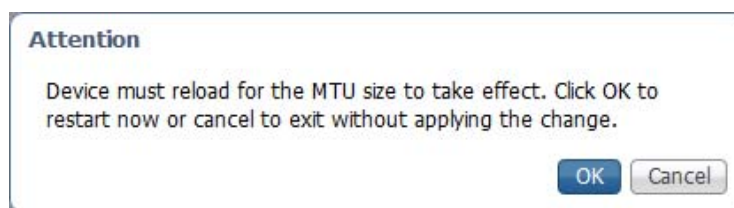
IMPORTANT The next procedure must be performed to configure the MTU (maximum transmission) for each distribution switch in your application. The PRP architecture can support a maximum of seven hops.

6. From the main menu of the Device Manager, click Admin and choose MTU.



7. Select an MTU value and click Submit.

A warning message appears.



8. Click OK to restart.

Enable PRP I/O (RedBox) Switch

This section describes how to configure a redundant switch on the PRP I/O Network.

For color legend, see [page 52](#).

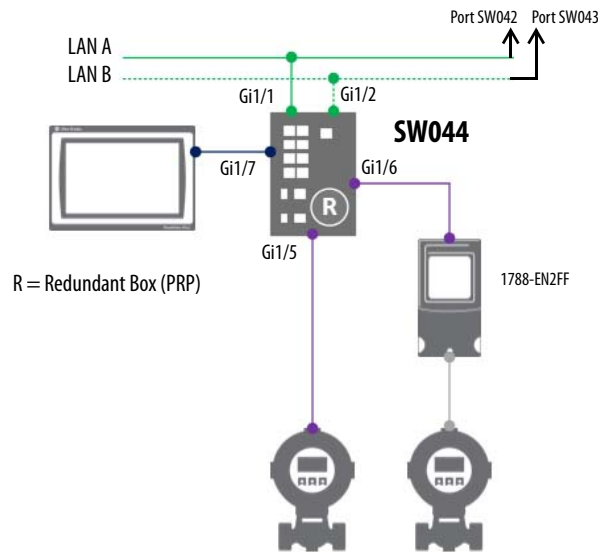
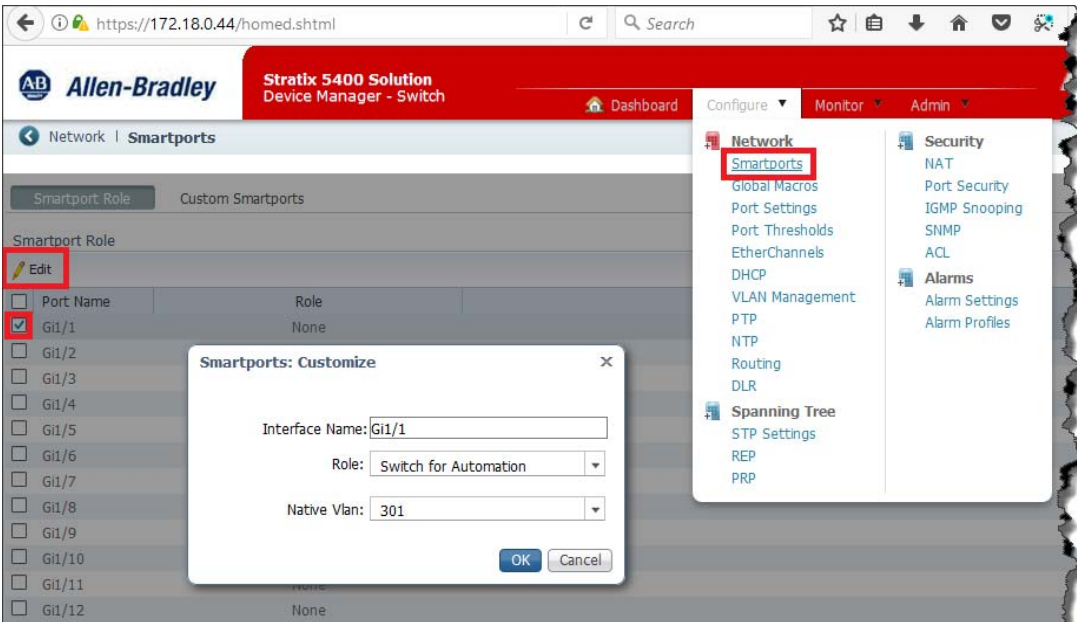


Table 17 - I/O Network - PRP

Port	Role	VLAN	SW044
Gi1/1...Gi1/2	Switch for Automation	Trunk (Native VLAN 301)	SW042, SW043
Gi1/3...Gi1/4	—	—	—
Gi1/5...Gi1/9	Automation Device	505 (I/O Network)	—
Gi1/10...Gi1/20	—	—	—

1. From the main menu of the Device Manager, click Configure and choose Smartports.



2. Select the desired ports and click Edit.
3. Select Switch for Automation from the Role pull-down.
4. Select a Native Vlan and click OK.
5. Use the information in [Table 17](#) to configure switch ports.

Configure MCC Switches

This section describes how to configure MCC-level switches for a Redundant Star (PRP) topology.

For color legend, see [page 52](#).

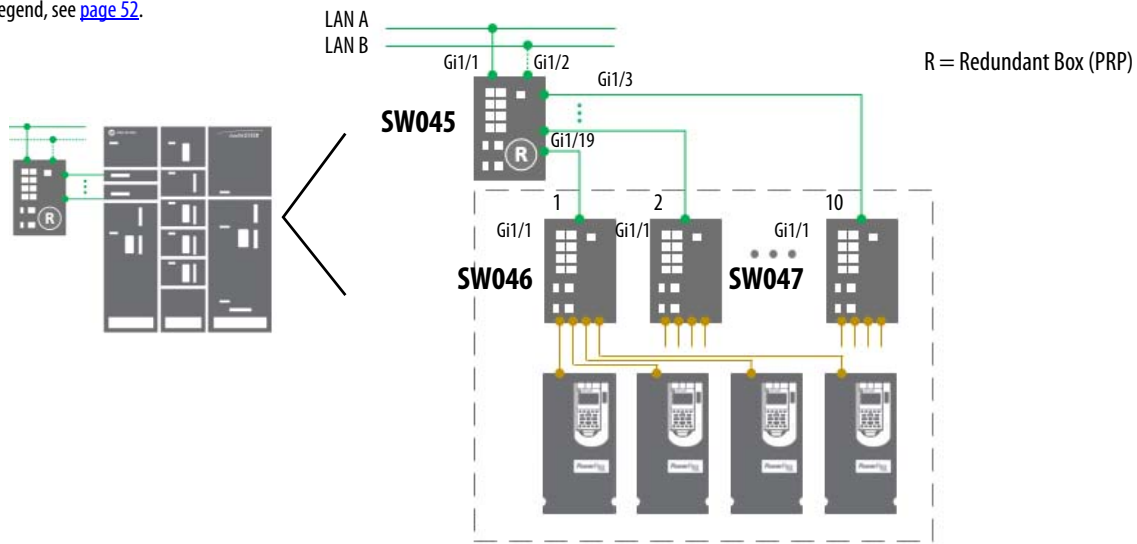


Table 18 - I/O Network - MCC PRP

Port	Role	VLAN	SW045
Gi1/1...Gi1/19	Switch for Automation	Trunk (Native VLAN 301)	Switch tag
Gi1/20	Desktop for Automation	300 (Management)	—

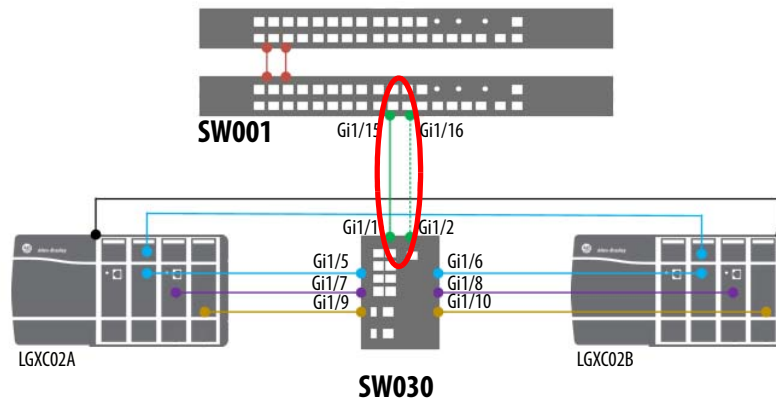
1. From the main menu of the Device Manager, click Configure and choose Smartports.
2. Select the desired ports and click Edit.
3. Select Switch for Automation from the Role pull-down.
4. Select a Native Vlan and click OK.
5. Use the information in [Table 18](#) to configure switch ports.

Optimize Switches for Redundant Controllers

This section describes how to configure routing at the controller level to reduce multitasking. This functionality minimizes the Internet Group Management Protocol (IGMP) members on the control level.

IMPORTANT This configuration can be executed only in one switch. Moving the default gateway to the controller level requires changes in the upper level (CLI).

For color legend, see [page 52](#).



Configure Switch Routing

Complete these steps to change the VLAN IP address to modify the gateway address. This example shows the VLAN IP address is changing from 172.18.2.1 to 172.18.2.2. The same configurations are required for additional VLANs and subnets.

1. From the Device Manager, click Configure and choose VLAN Management.
2. Select the VLAN that you are changing, and click Edit.

+ Add ✎ Edit ✕ Delete		
VLAN ID	Name	Ports
<input type="radio"/> 1	default	Te1/27
<input type="radio"/> 300	VLAN0300	Gi1/13,
<input type="radio"/> 301	Native	
<input type="radio"/> 501	VLAN0501	Po3, Po
<input checked="" type="radio"/> 502	VLAN0502	
<input type="radio"/> 503	VLAN0503	
<input type="radio"/> 504	VLAN0504	
<input type="radio"/> 505	VLAN0505	
<input type="radio"/> 506	VLAN0506	
<input type="radio"/> 507	VLAN0507	
<input type="radio"/> 508	VLAN0508	
<input type="radio"/> 509	VLAN0509	

3. In the IP Address text box, type the new IP address.

To add or edit ports in a VLAN, use the Physical Port Settings page.

VTP Mode :Transparent

Add Edit Delete

VLAN ID	Name	Ports
<input type="radio"/> 1	default	Te1/27, Te1/28
<input type="radio"/> 300	VLAN0300	Gi1/13, Gi1/14, Gi1/15
<input type="radio"/> 301	Native	
<input type="radio"/> 501	VLAN0501	Po3, Po4
<input checked="" type="radio"/> 502	VLAN0502	
<input type="radio"/> 503	VLAN0503	
<input type="radio"/> 504	VLAN0504	

VLAN ID: 502

Name: VLAN0502

IP Assignment Mode: ☐ No IP Address ☒ Static ☐ DHCP

IP Address: 172.18.2.2 / 255.255.255.0

OK Cancel

4. Click OK.

Configure a Static IP Address

Complete these steps to configure a VLAN with a static IP address.

1. From the main menu of the Device Manager, click Configure and choose Routing.
2. Click Enable Routing.

Allen-Bradley Stratix 5400 Solution Device Manager - Switch

Dashboard Configure Monitor Admin

Network | Routing

Enable Routing : ☒

Gateway: 172.18.0.1

Submit

Static Routes

Add Edit Delete

Destination Network	Destination Mask	Next Hop Router
No data available		

Network

- Smartports
- Global Macros
- Port Settings
- Port Thresholds
- EtherChannels
- DHCP
- VLAN Management
- PTP
- NTP
- Routing**
- DLR

Spanning Tree

- STP Settings
- RCD

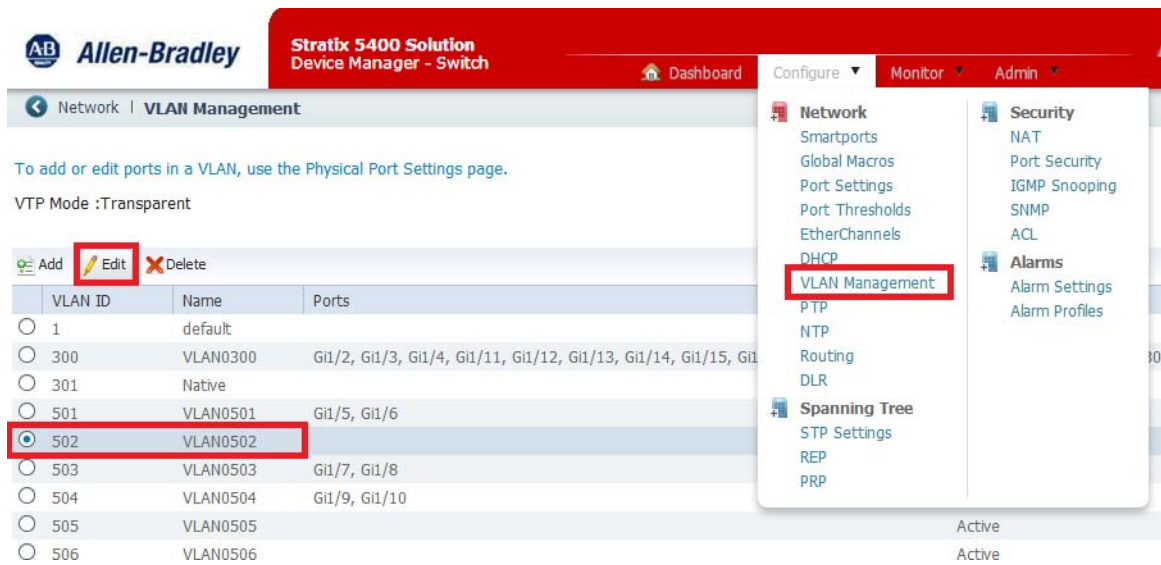
Security

- NAT
- Port Security
- IGMP Snooping
- SNMP
- ACL

Alarms

- Alarm Settings
- Alarm Profiles

- Return to the main menu of the Device Manager, click Configure and choose VLAN Management.



- Click Edit and choose an I/O Network VLAN.
See [page 18](#) for a list of VLAN descriptions.
- Select Static and type an IP address followed by a network mask.

The screenshot shows the VLAN configuration dialog box. The 'VLAN ID' is 502, 'Name' is VLAN0502, and 'IP Assignment Mode' is set to Static. The IP address is 172.18.2.1 and the network mask is 255.255.255.0.

- Click OK.

Notes:

Configure System Servers

This chapter describes how to configure a Windows domain, which centralizes the administration of users, policies, and security. Use of a Windows domain also improves performance, especially for larger systems. We recommend that all PlantPAx® system servers and workstations be a member of a domain.

A domain is a collection of computers that share rules and procedures. These computers comprise a central directory database, which is the active directory. The sharing of network objects creates a unified base to manage users, groups, and security settings.

Procedures in this chapter explain how to build a Windows domain named System. The System domain is a child domain of parent domain PlantPAx. Hence, the following fully qualified domain namespace:

System.PlantPAx.local

This domain forms a domain tree that's rooted at PlantPAx. Your Windows active directory implementation (for example forest), can include one tree or be composed of multiple trees.

When a Windows secondary domain is created, the following operations occur:

- Secondary domain is verified
- Domain controller in the primary domain is located (referenced) and the secondary domain time is synchronized
- Two-way transitive trust relationships between the secondary domain and the primary domain are established
- Existing Active Directory Schema and Configuration containers are replicated to the secondary domain controllers.

IMPORTANT To perform tasks in this chapter, you must verify the naming conventions of your computers or use the names as shown in the examples. You cannot change computer names in the middle of the procedures for any domain controller.

Rockwell Automation® does not support the installation of application software on a computer that is configured as a domain controller.

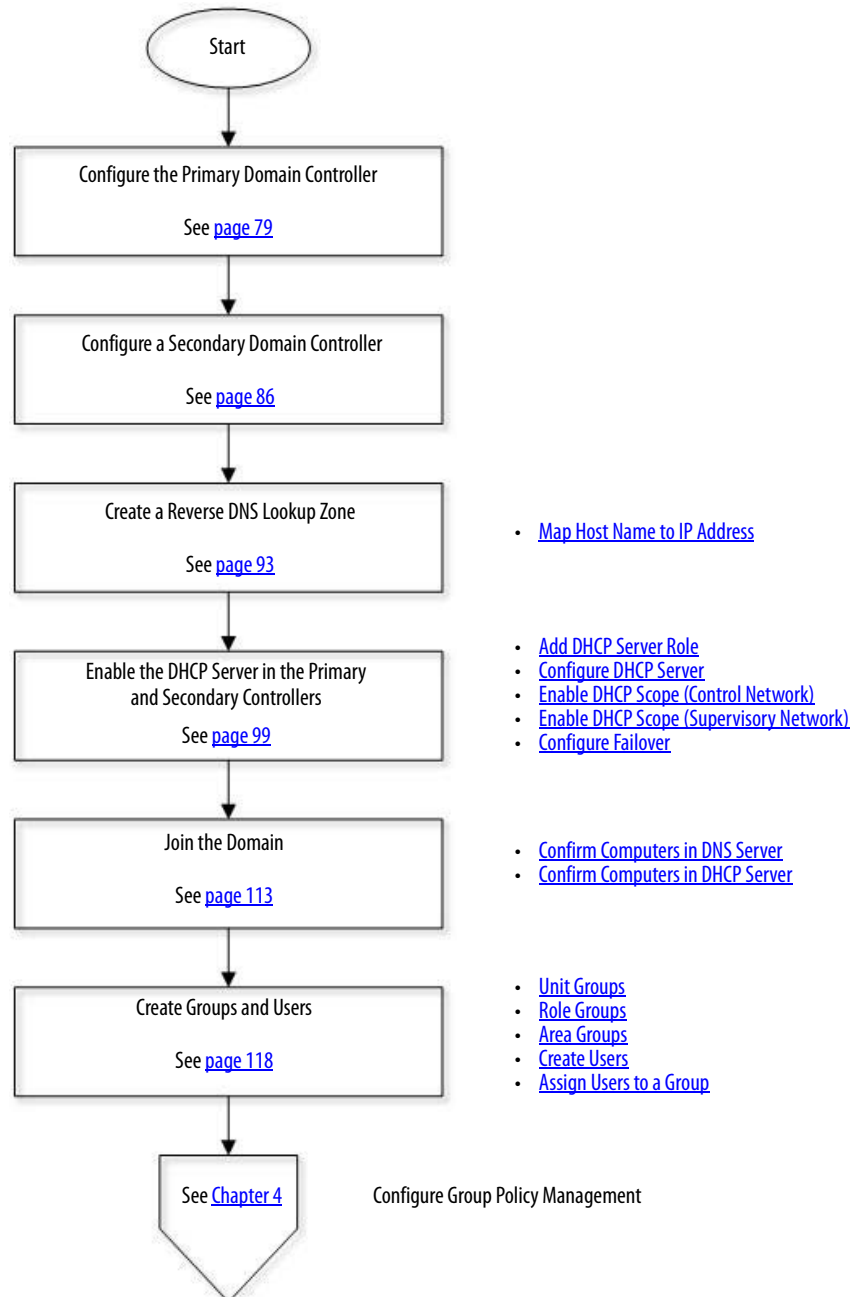
For additional server recommendations, see the PlantPAx Distributed Control System Reference Manual, publication [PROCES-RM001](#).

Considerations

Consider the following suggestions before starting this chapter:

- We assume that your active directory (forest) exists and that a hosting primary domain, such as PlantPAX.local, exists as well. The domain names that are used herein are only arbitrary to denote a respective hierarchy that works for you.
- Our recommendation is to use domain controllers. But, if you want to create a workgroup, see the procedures in [Appendix B](#).
- This chapter describes how to set up a dedicated domain for your PlantPAX system. If you are adding your PlantPAX system to an existing domain and DHCP server, skip to [page 99](#) for details.

Figure 7 - PlantPAX System Server Workflow



Configure the Primary Domain Controller


For high availability, primary and secondary domain controllers are required. Complete these steps to configure a primary domain controller.

IMPORTANT Before you begin to configure a primary domain controller, you must assign a fixed IP address to the domain controller, such as 172.18.1.10.

Use a domain controller with these procedures.



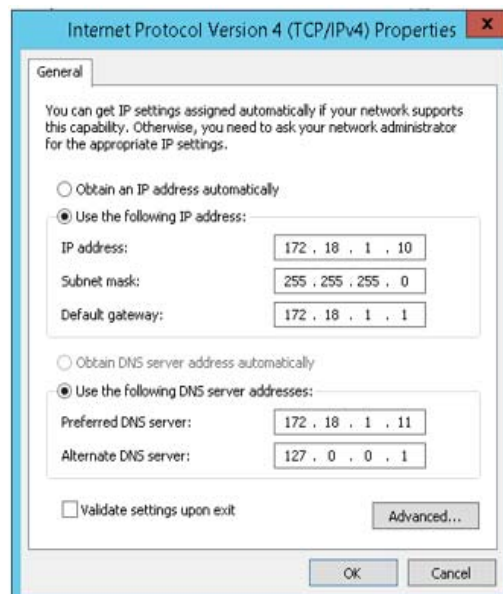
Primary Controller
(PADCA)

1. Click the Windows  symbol.
2. Click Control Panel and choose Network and Sharing Center>Change adapter settings.

The Network Connections dialog box appears.

3. Right-click the network and choose Properties.
4. Double-click Internet Protocol Version 4 (TCP/IPv4).

The Internet Protocol Version 4 Properties dialog box appears.



5. Type an IP address, default gateway address, and a Preferred DNS (Domain Name System) server address.

IMPORTANT You could receive Windows Event Log errors related to the Preferred DNS server (for example 172.18.1.11). However, these errors go away when you add the DNS server.

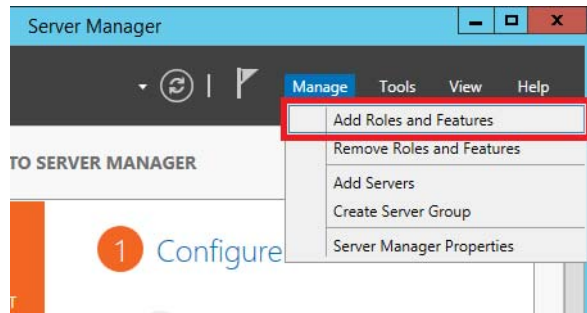
127.0.0.1 is a special purpose address that is reserved for use on each computer (computer loopback address).

Typically, the alternate DNS server is your secondary domain controller.

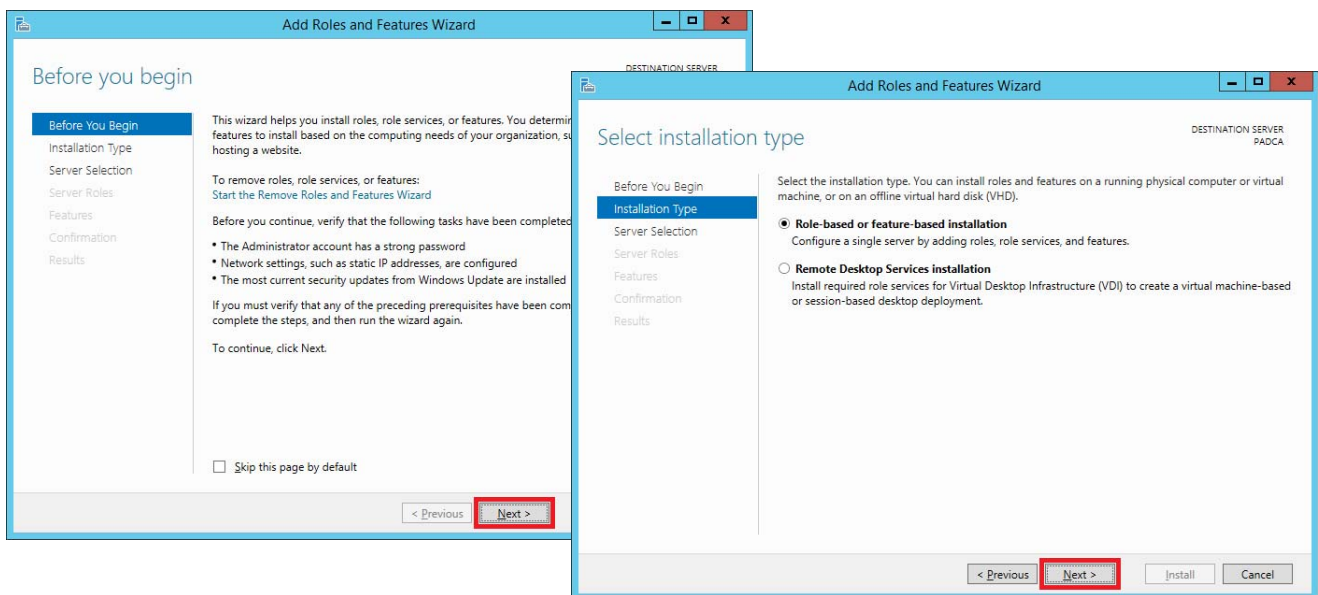
6. Click OK.

After defining the IP address, complete these steps to configure the primary domain controller.

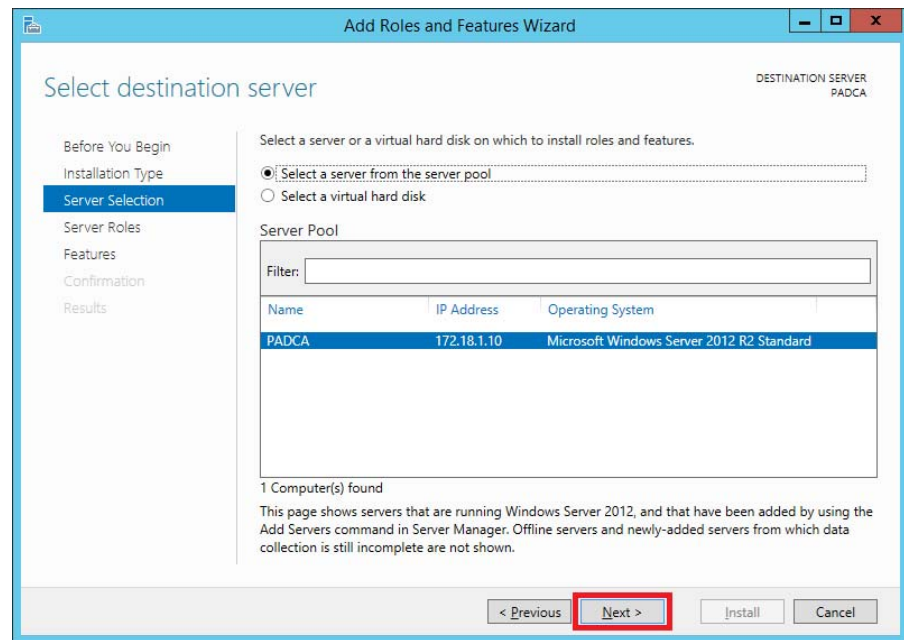
1. From the Server Manager, click Manage and choose Add Roles and Features.



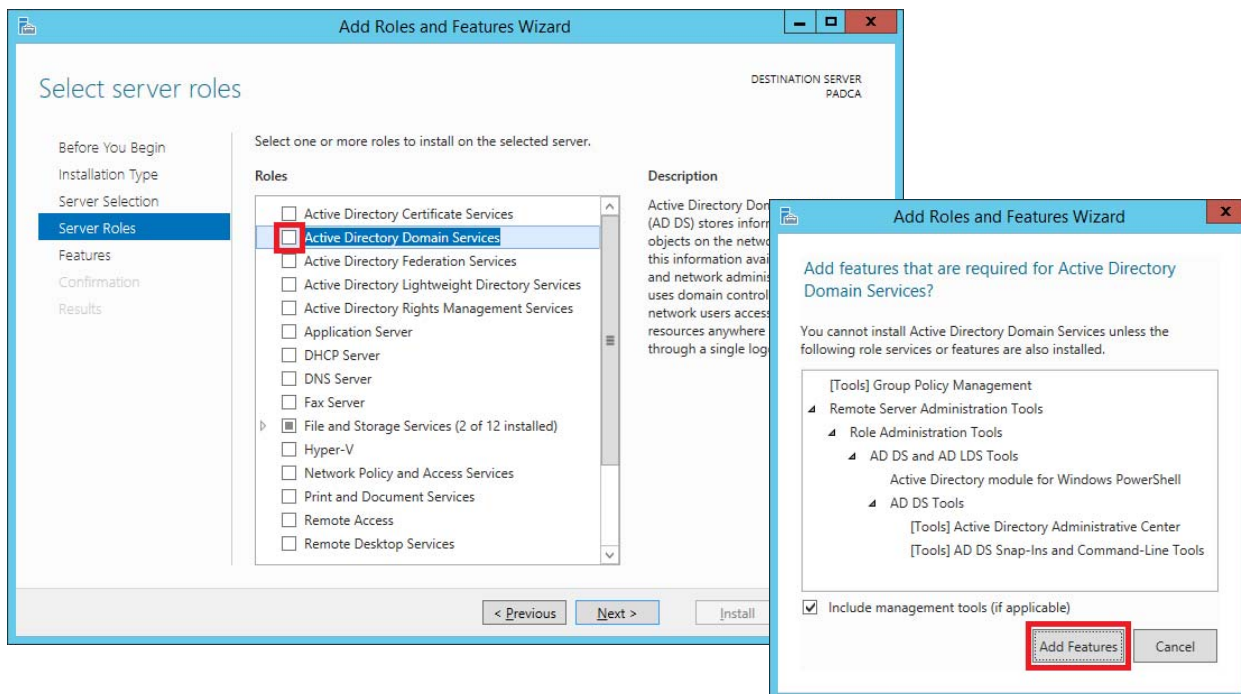
2. Click Next on each of the successive installation wizard dialog boxes for the following:
 - Review Before You Begin
 - Select Installation Type



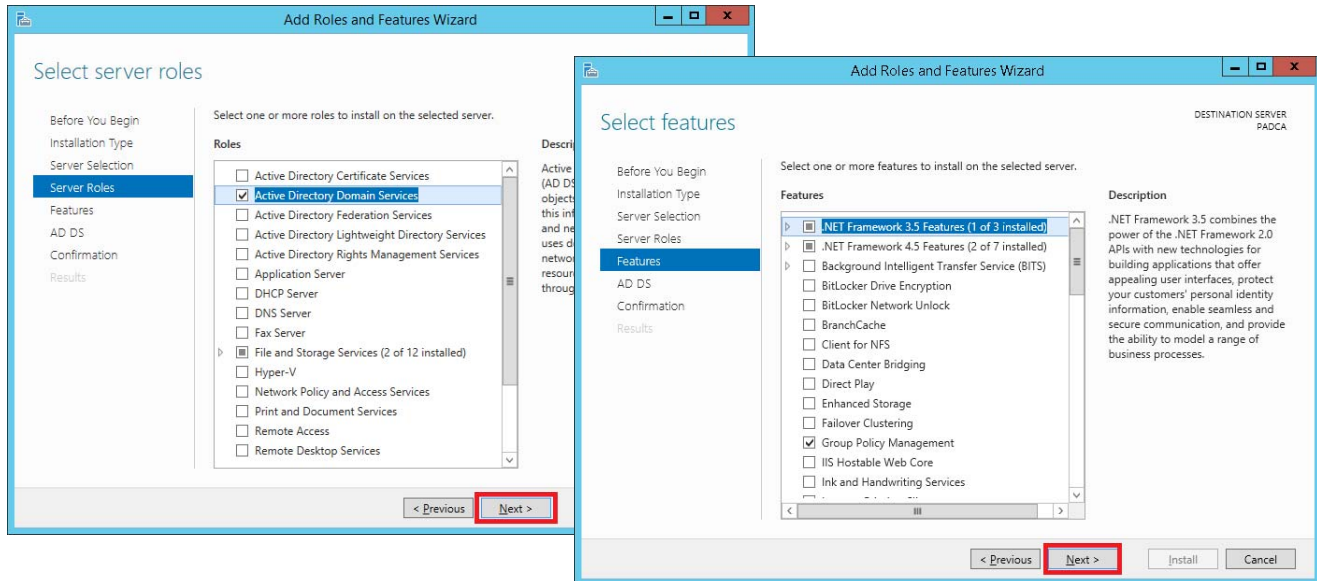
3. Click 'Select a server from the server pool' and select your primary domain (PADCA in the example).
4. Click Next.



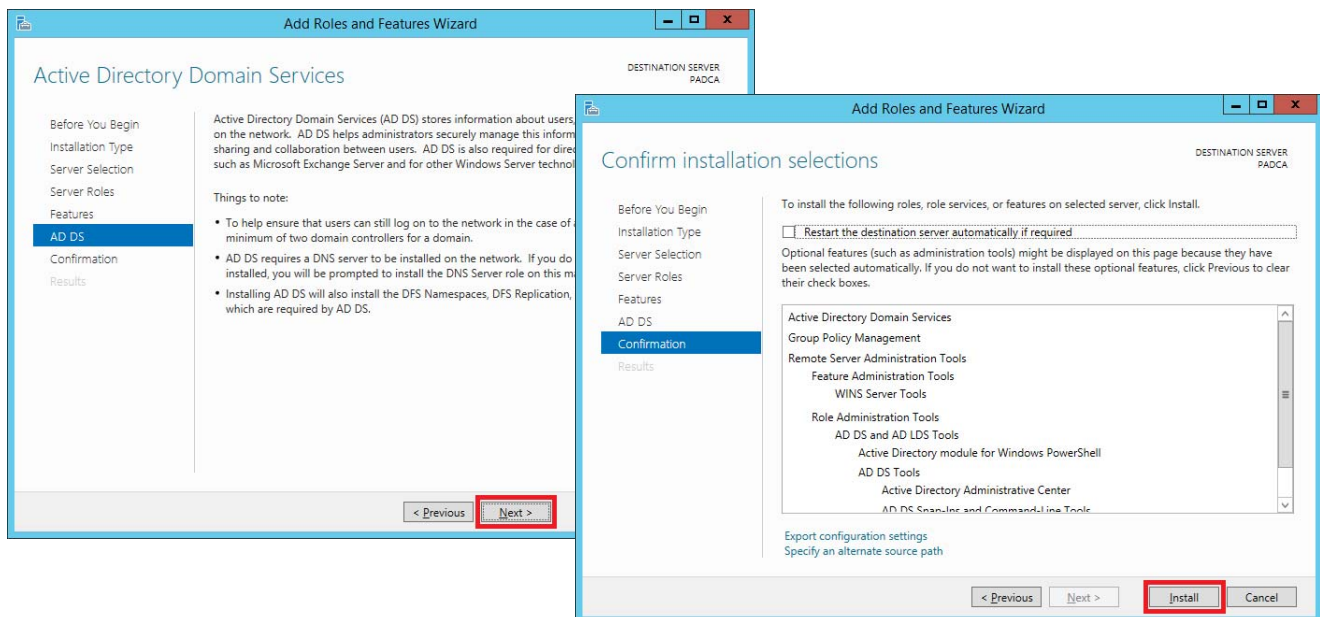
5. Choose Active Directory Domain Services, and then click Add Features.



6. Make sure 'Active Directory Domain Services' is checked and click Next.
7. Make sure the Features selections match as shown, and click Next.



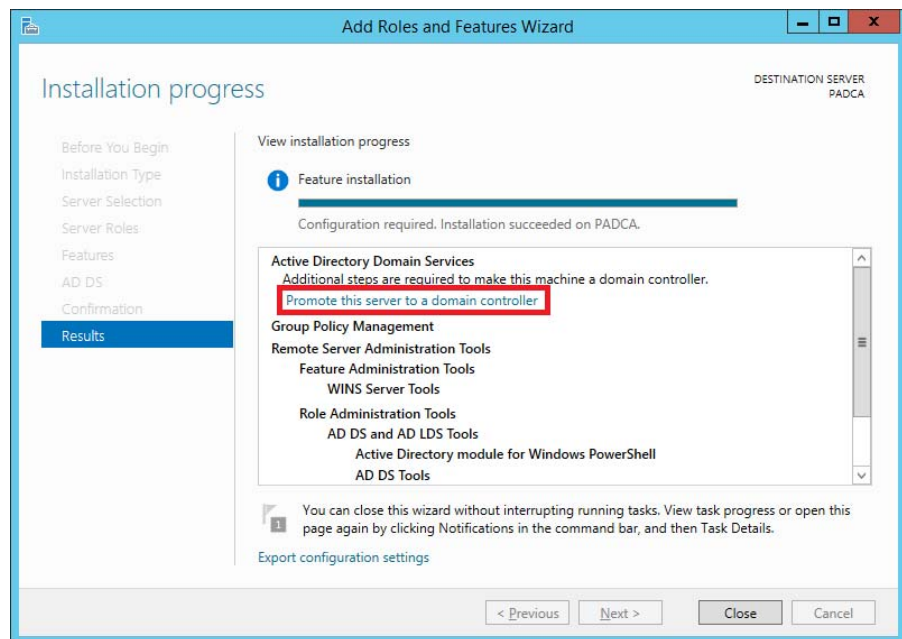
8. Make sure AD DS is highlighted and click Next.



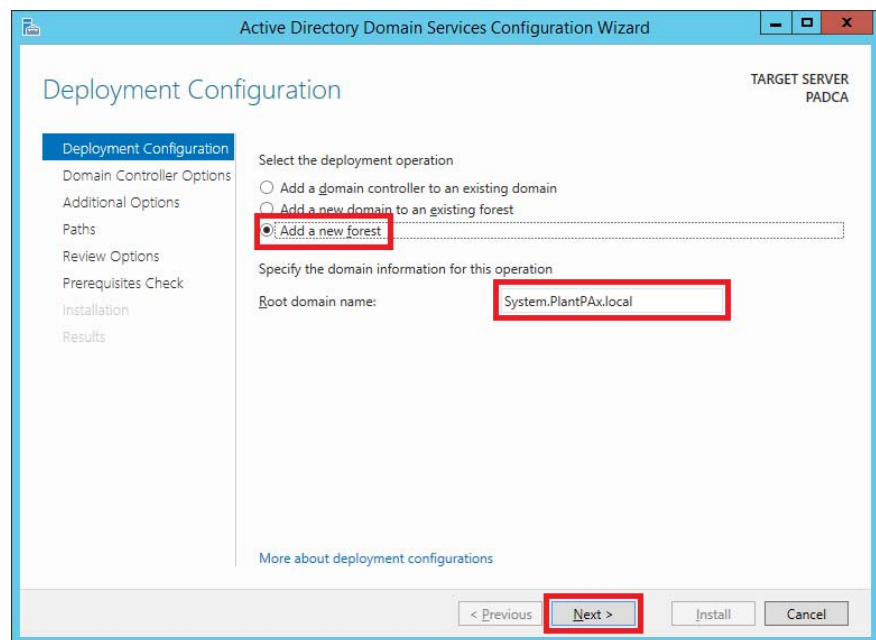
9. On Confirmation, make sure 'Restart the destination server automatically if required' is **not** checked.
10. Click Install.

The installation can take a few minutes. Do **not** close the Wizard.

11. Click Promote this server to a domain controller.



12. On the Configuration wizard, select Add a new forest, and type a root domain name.



13. Click Next.

14. Type the Directory Services Restore Mode (DSRM) password, confirm the password, and click Next.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
PADCA

Deployment Configuration
Domain Controller Options
 DNS Options
 Additional Options
 Paths
 Review Options
 Prerequisites Check
 Installation
 Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

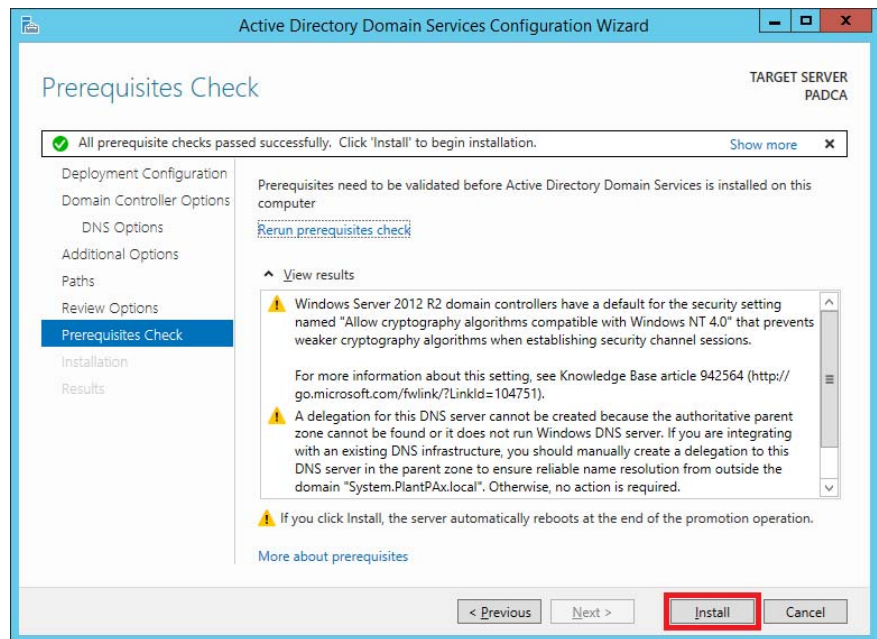
Confirm password:

[More about domain controller options](#)

< Previous **Next >** Install Cancel

IMPORTANT We recommend that you document these credentials and store them in a secure location. For security, the domain controller verifies passwords for all users and computers in the PlantPAx network. The domain controller also authenticates the installation and upgrade of network software.

15. Do not specify DNS Delegation options and click Next.
16. In the NetBIOS™ Domain Name text box, make sure the domain name is 'System' and click Next.
17. Click Next on the successive two windows to do the following:
 - Accept the location of the AD DS database, log files, and SYSVOL
 - Review selections

18. Click Install.

The installation can take a few minutes before the computer automatically restarts.

Configure a Secondary Domain Controller

Use a domain controller with these procedures.




Secondary Controller (PADC)

The secondary domain controller is a replication of the Active Directory (AD) and runs the alternate DNS server. We recommend that you configure a second domain controller as a backup to the primary domain for high availability.

You **must** assign a fixed IP address to the secondary domain controller.

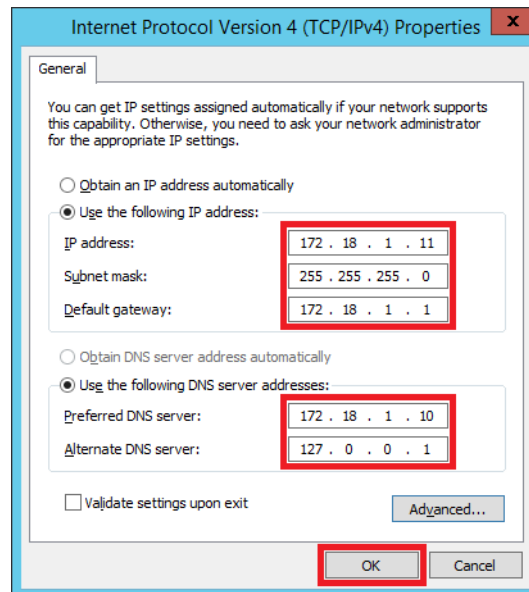
Complete the following steps.

1. Click the Windows  symbol.
2. Click Control Panel and choose Network and Sharing Center>Change adapter settings.

The Network Connections dialog box appears.

3. Right-click the network and choose Properties.
4. Double-click Internet Protocol Version 4 (TCP/IPv4).

The Internet Protocol Version 4 Properties dialog box appears.



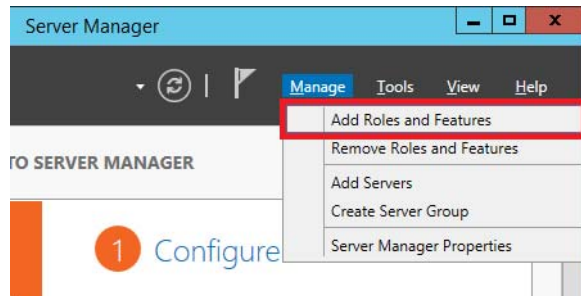
5. Type an IP address that matches the primary domain controller IP address as the preferred DNS server.

This secondary domain server is the alternate DNS server for the system infrastructure.

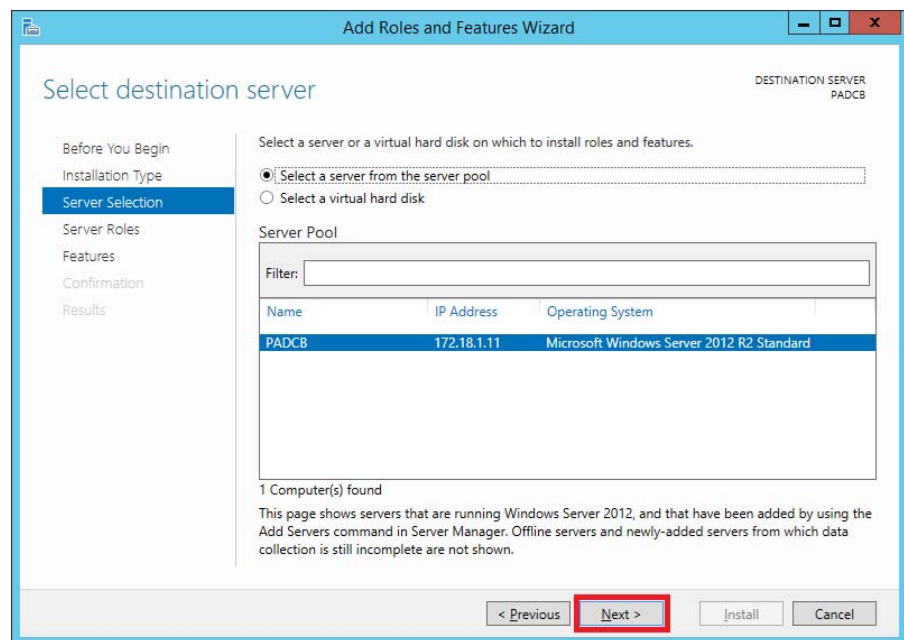
6. Click OK.

After defining the IP address, complete these steps to create the secondary domain.

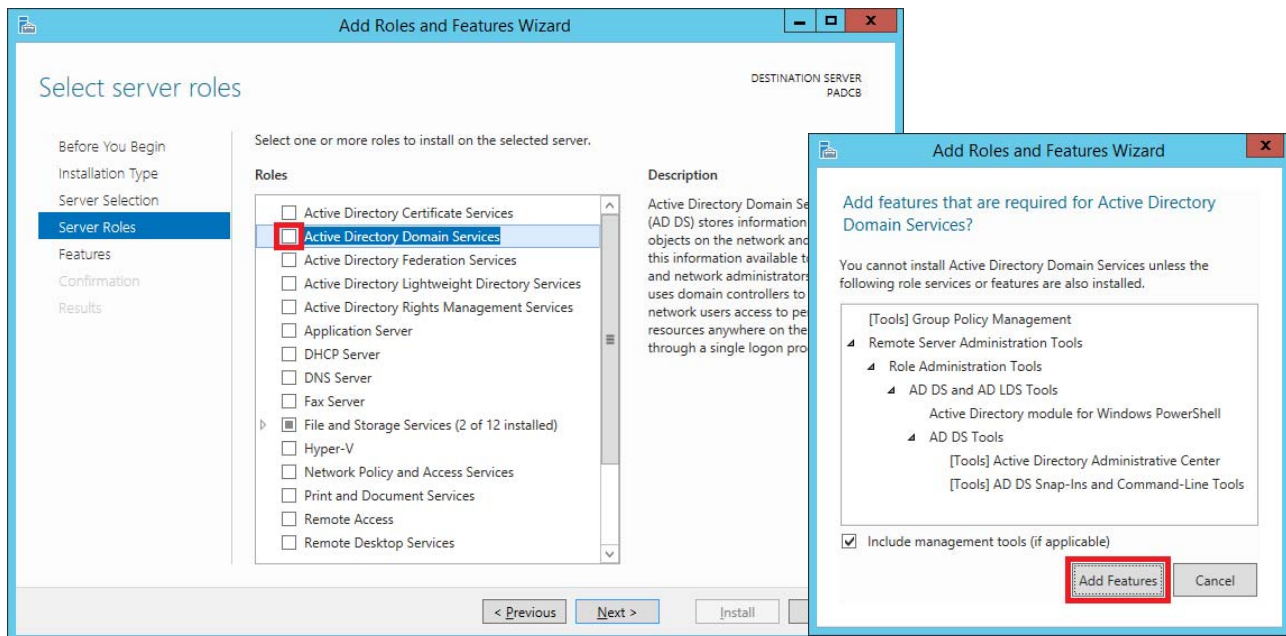
1. From the Server Manager, click Manage and choose Add Roles and Features.



2. Click Next on each of the successive dialog boxes to do the following.
 - Verify that certain tasks have been completed
 - Select an installation type
3. Click Select a server from the server pool, and select your secondary domain (PADCB in the example).
4. Click Next.



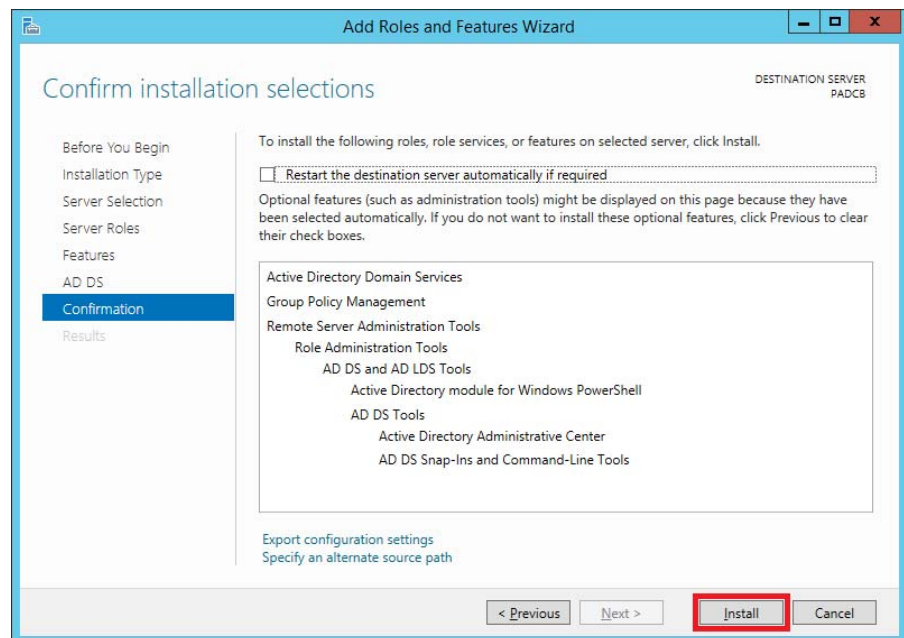
5. Click Active Directory Domain Services, and then click Add Features.



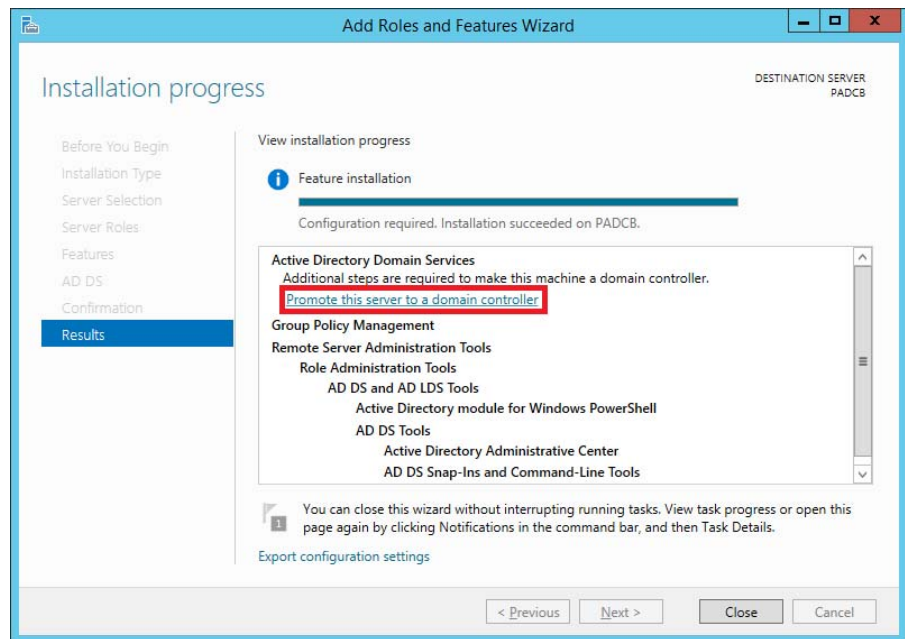
6. Click Next on each of the successive dialog boxes to do the following.

- Verify selected server role
- Confirm installation selections
- Verify 'Things to note' concerning AD DS

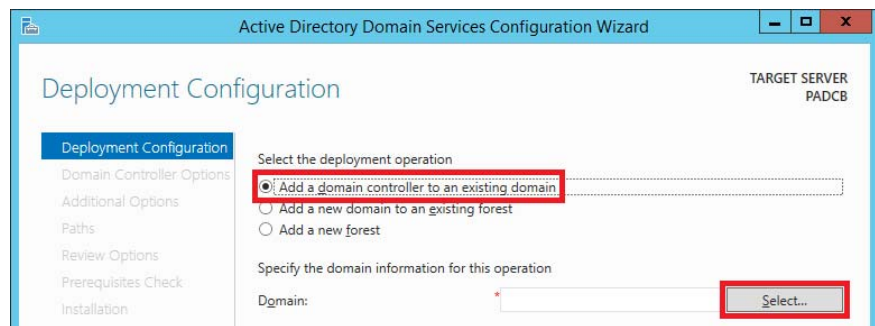
7. Confirm your installation selections and click Install.



8. Click Promote this server to a domain controller.

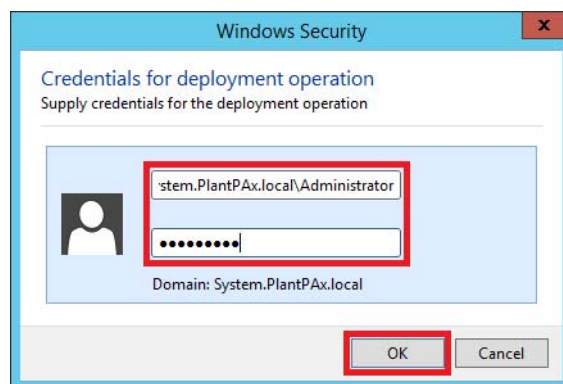


9. Click Add a domain controller to an existing domain and click Select.



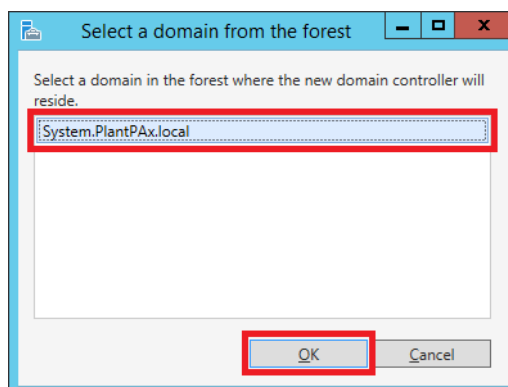
10. Type a user name under the domain.

For example, System.PlantPAx.local\Administrator

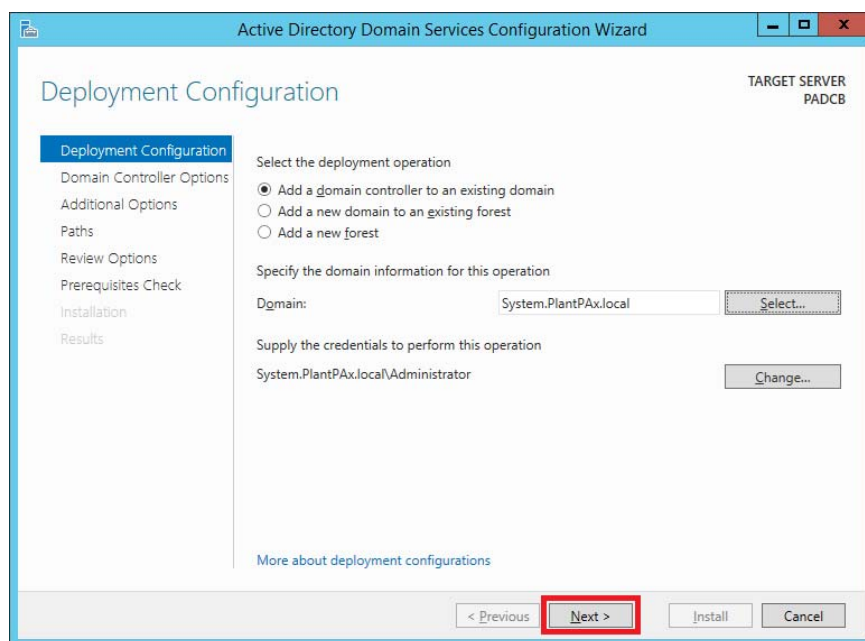


11. Type a password and click OK.

12. Select the domain and click OK.



13. On the Configuration wizard, click Next.



14. Type the Directory Services Restore Mode (DSRM) password, confirm, and click Next.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Domain Controller Options' step. The left sidebar lists the steps: Deployment Configuration, Domain Controller Options (selected), DNS Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Specify domain controller capabilities and site information'. It includes checkboxes for 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). The 'Site name' dropdown is set to 'Default-First-Site-Name'. Below this, the text says 'Type the Directory Services Restore Mode (DSRM) password'. There are two password fields: 'Password:' and 'Confirm password:', both containing masked characters (dots). A red rectangle highlights these two password fields. At the bottom, there are navigation buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'. The top right corner indicates 'TARGET SERVER PADCB'.

15. Click Next on the DNS Options window.

Ignore the warning message.

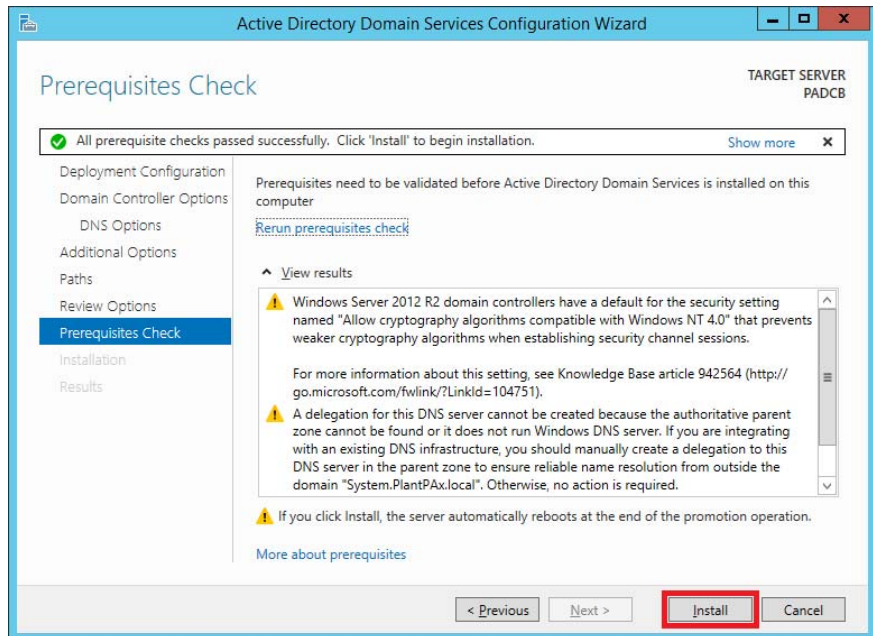
16. From the Replicate from pull-down menu, select PADCA.System.PlantPax.local.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Additional Options' step. The left sidebar lists the steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options (selected), Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Specify Install From Media (IFM) Options' and 'Specify additional replication options'. Under 'Specify Install From Media (IFM) Options', the 'Install from media' checkbox is unchecked. Under 'Specify additional replication options', the 'Replicate from:' dropdown menu is set to 'PADCA.System.PlantPax.local'. A red rectangle highlights this dropdown menu. At the bottom, there are navigation buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'. The top right corner indicates 'TARGET SERVER PADCB'.

17. Click Next on each of the successive windows for the following:

- Accept the location of the AD DS database, log files, and SYSVOL
- Review selections

18. Click Install.



The computer automatically restarts.

Create a Reverse DNS Lookup Zone

Use a domain controller with these procedures.



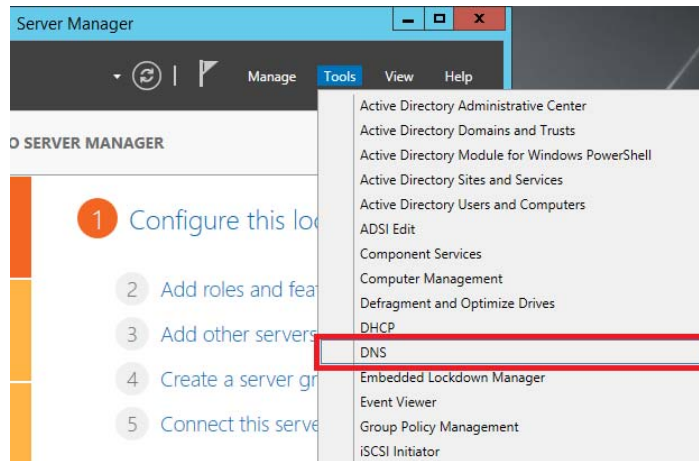
A reverse lookup zone provides the ability to search a database for a computer name based on its IP address. This process is contrary to how a Domain Name System (DNS) was originally designed. Ordinarily, DNS lookups are forward lookups, which are searches via a DNS of another computer that is stored in the host record. The IP address is usually the resource for a response.

To define how a DNS name is indexed with an assigned IP address for a reverse lookup, you must program a special domain (in-addr.arpa). Subdomains within the in-addr.arpa domain reverse the address order by using a pointer (PTR) record that is mapped to the IP address. Thus, the domain name is found in the query.

Complete these steps to add a reverse lookup zone.

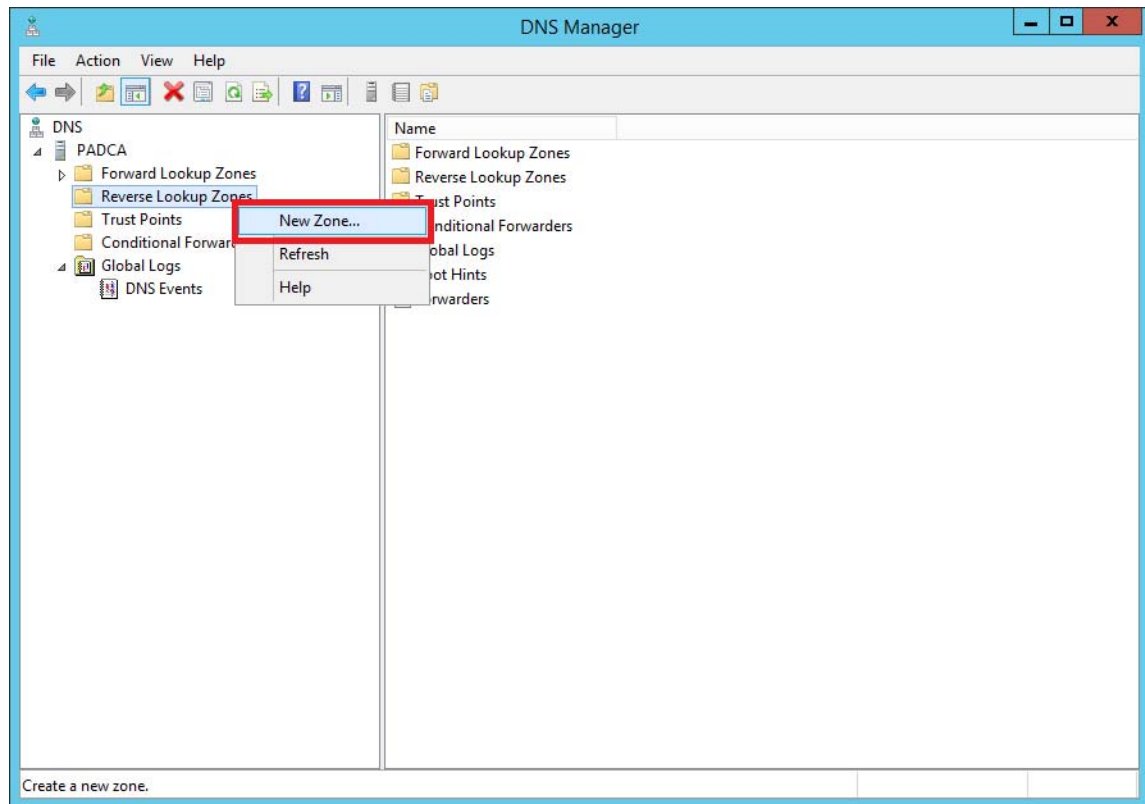
IMPORTANT The Active Directory installation wizard does not automatically add a reverse lookup zone to the server. The PTR records are not necessary to operate an Active Directory, but these records must be mapped to IP addresses for a reverse lookup zone. See [page 96](#) for the procedure.

1. From the Server Manager, click Tools and choose DNS.

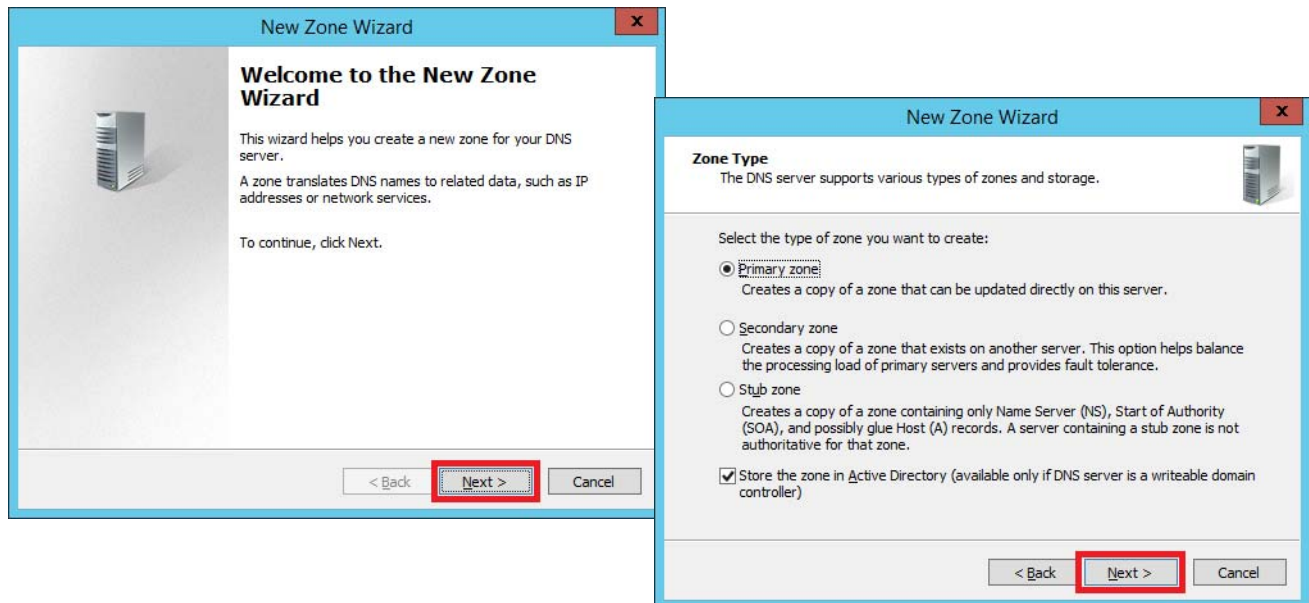


The DNS Manager dialog box appears.

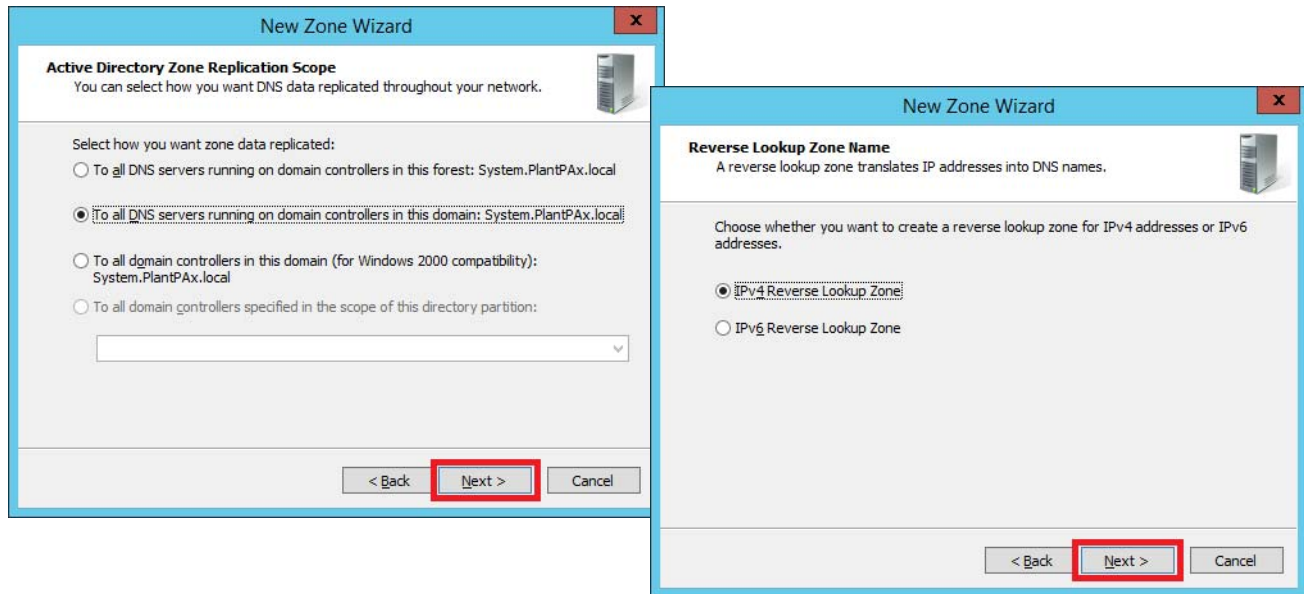
2. Open the primary server (PADCA), right-click Lookup Zones and choose New Zone.



Wizard installation screens appear to create a zone for your DNS server.

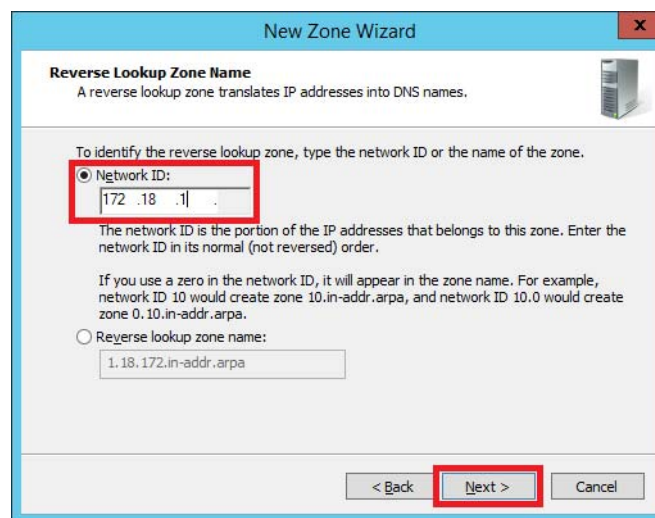


3. Click Next twice to use defaults



4. Click Next twice to use defaults.
5. Type the network ID of an IP address or the zone name.

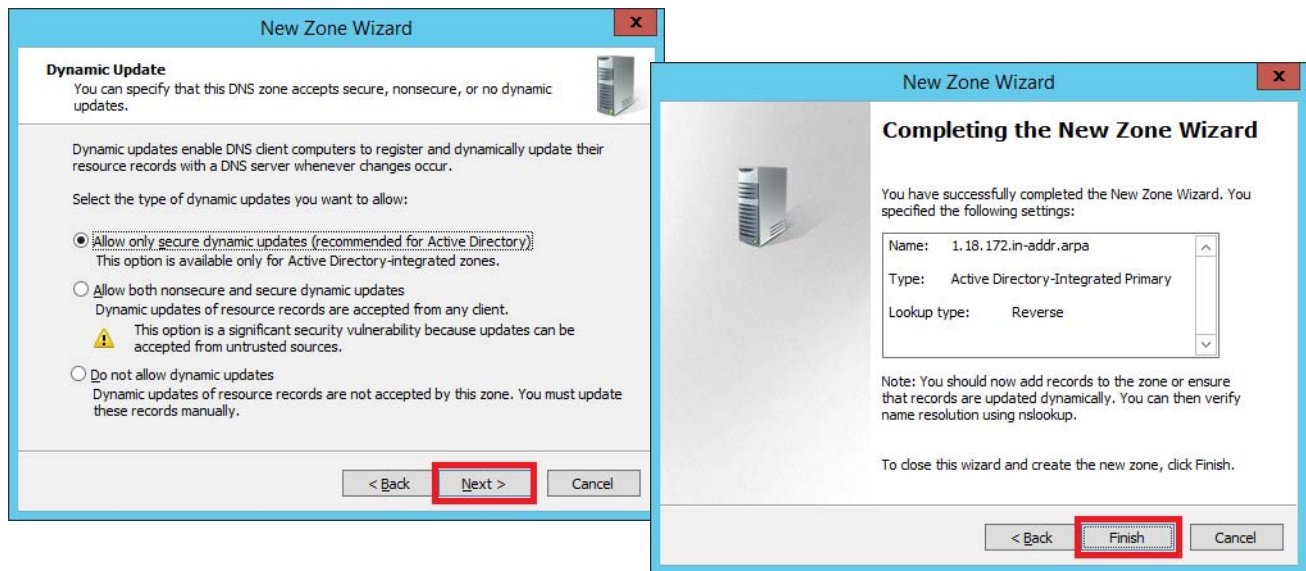
IMPORTANT Type the network ID portion of the IP address in the normal (not reversed) order.



The zone translates the IP address into DNS names.

6. Click Next.

7. Click Next and Finish to complete the zone installation.

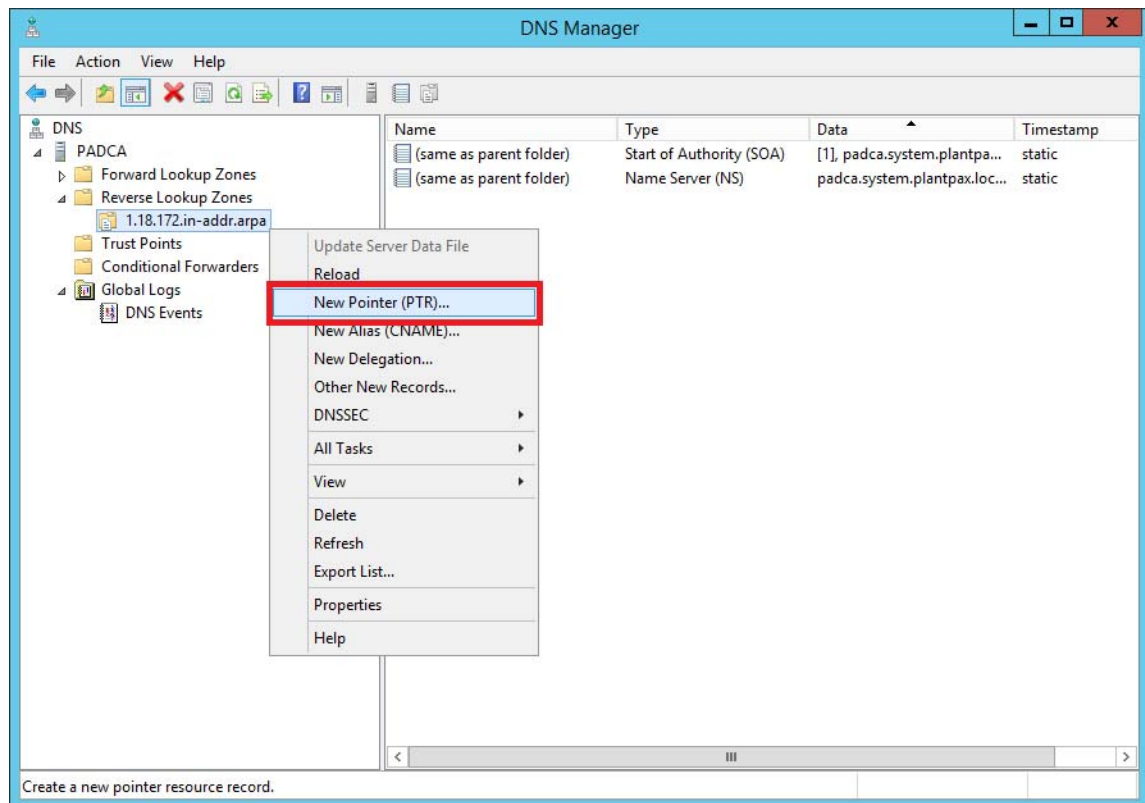


Map Host Name to IP Address

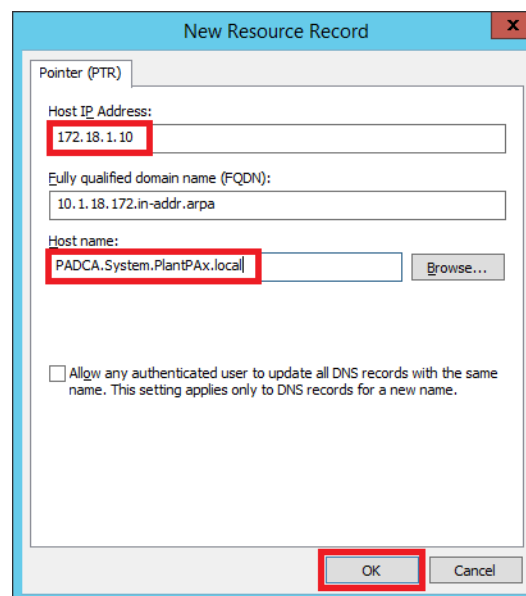
Complete these steps to create a pointer (PTR) record that associated the DNS name to the IP address. During a search, the IP address is reversed to find the associated DNS name.

1. From the Server Manager, click Tools and choose DNS.
The DNS Manager dialog box appears.
2. Open the primary server (PADCA) and Reverse Lookup Zones folders and right-click the subdomain.

3. Choose New Pointer (PTR) from the pull-down menu.

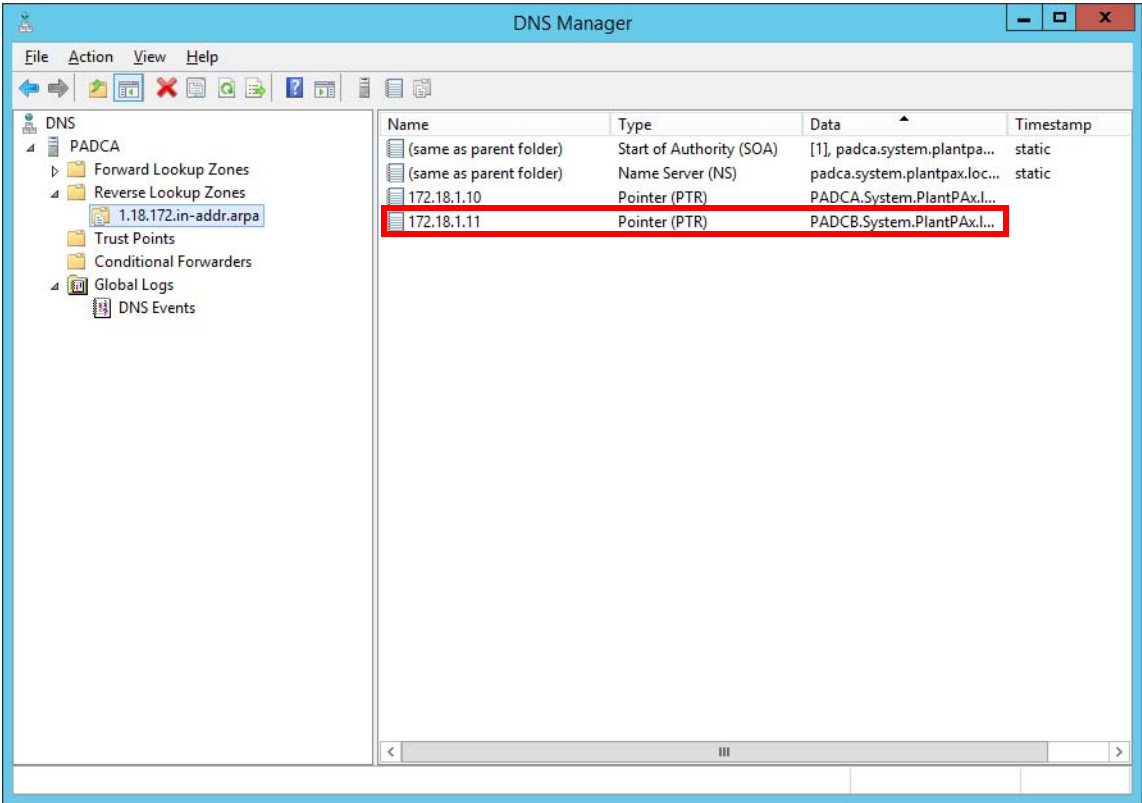


The New Resource Record dialog box appears.

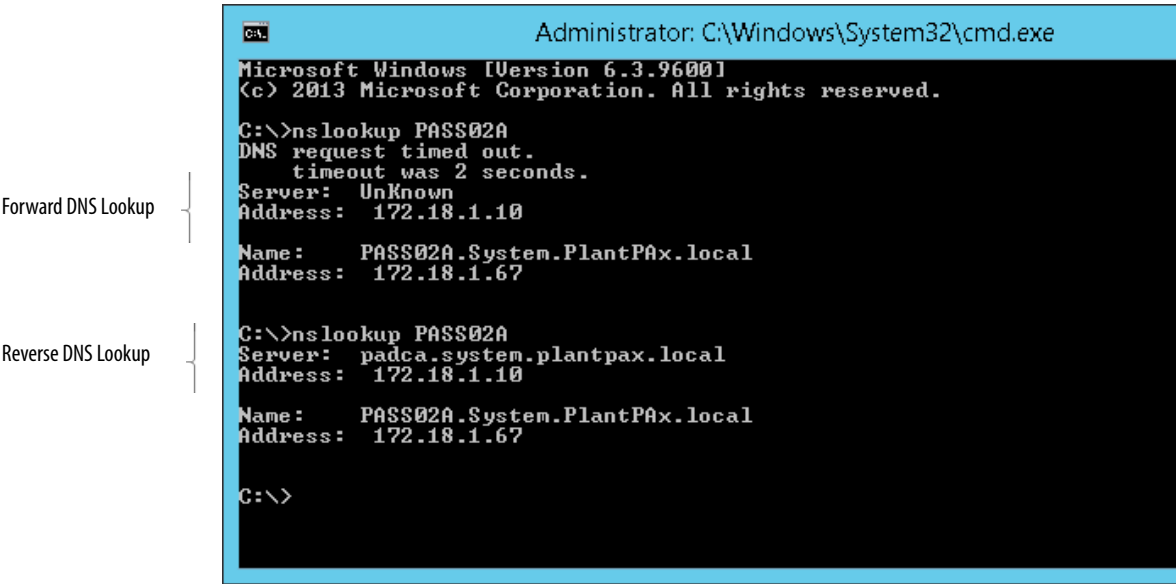


4. Type an IP address in the normal (not reversed) order.
5. Click Browse and select the host name on the primary server.
6. Click OK.

7. Repeat [step 1...step 6](#) for 'secondary' servers.



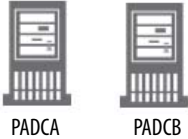
The example shows results for a DNS Lookup forward search and a DNS Lookup reverse search.



IMPORTANT Repeat the steps in the Control Network for the supervisory.

Enable DHCP in the Primary and Secondary Controllers

Use a primary and a secondary domain controller with these procedures.



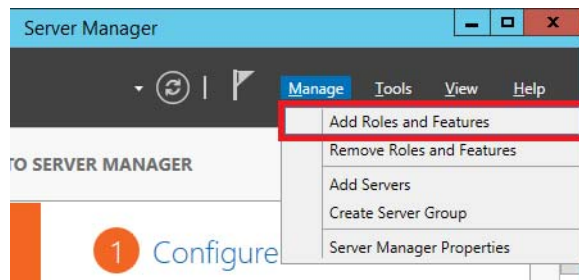
There are two ways of configuring IP addresses: static (manually) or dynamic (via server). Both options are supported within a PlantPAx system. By using the Dynamic Host Configuration Protocol (DHCP) server, you do not need fixed IP addresses for application servers and workstations. But, you **must** define a range and the system manages the IP addresses and names. We are applying DHCP in PlantPAx computers only.

Add DHCP Server Role

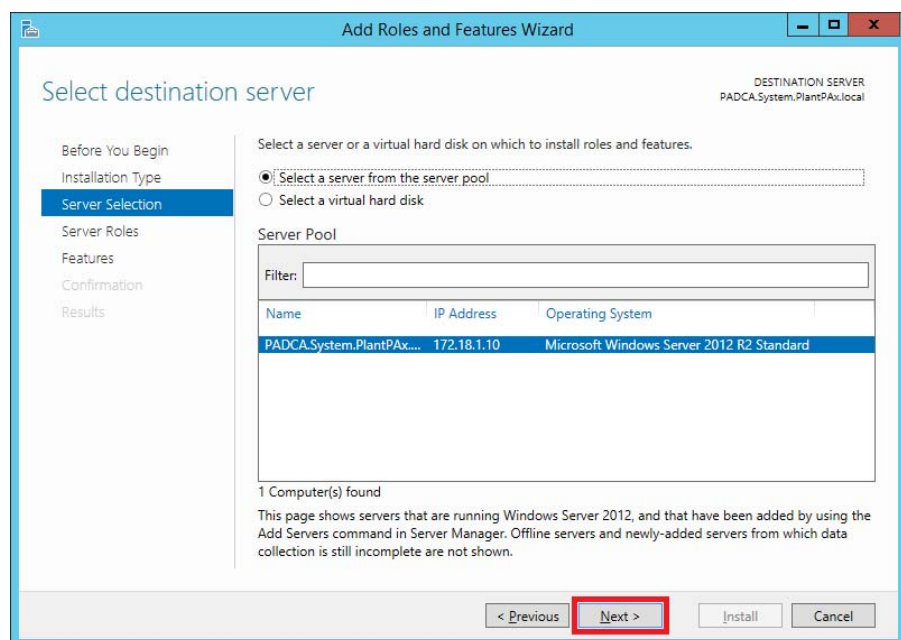
If adding DHCP server roles for the domain controllers, you must do this procedure for the primary and secondary servers.

In the primary domain, complete the following steps.

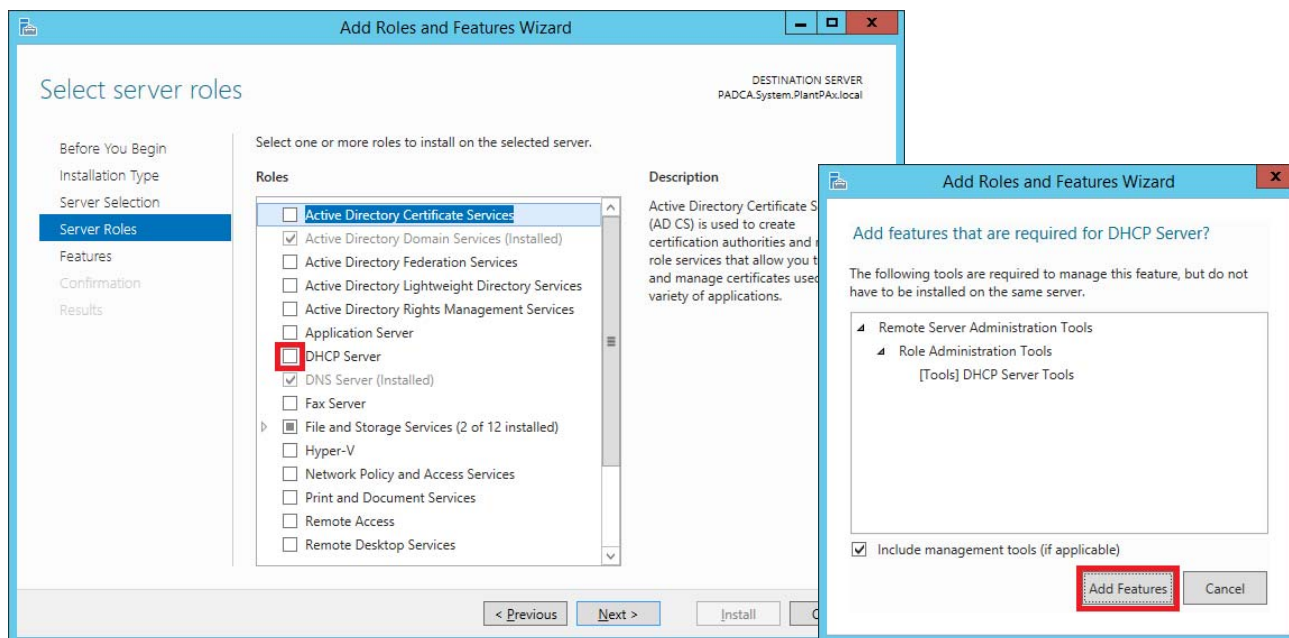
1. From the Server Manager, click Manage and choose Add Roles and Features.



2. Click Next on each of the successive windows to do the following:
 - Verify that certain tasks have been completed
 - Select an installation type
3. Click Select a server from the server pool, select the desired server (PADCA and PADC), and click Next.



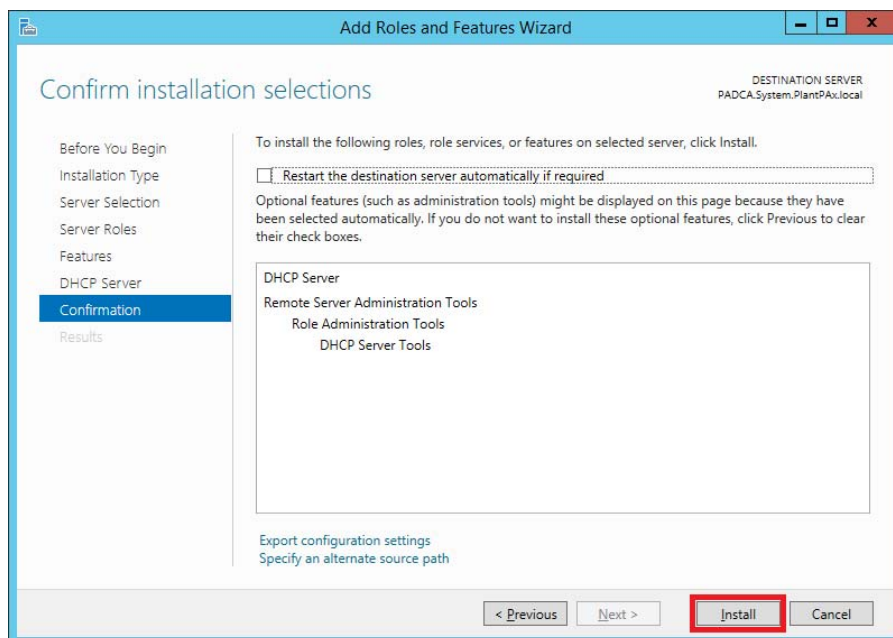
4. Select DHCP Server and click Add Features.



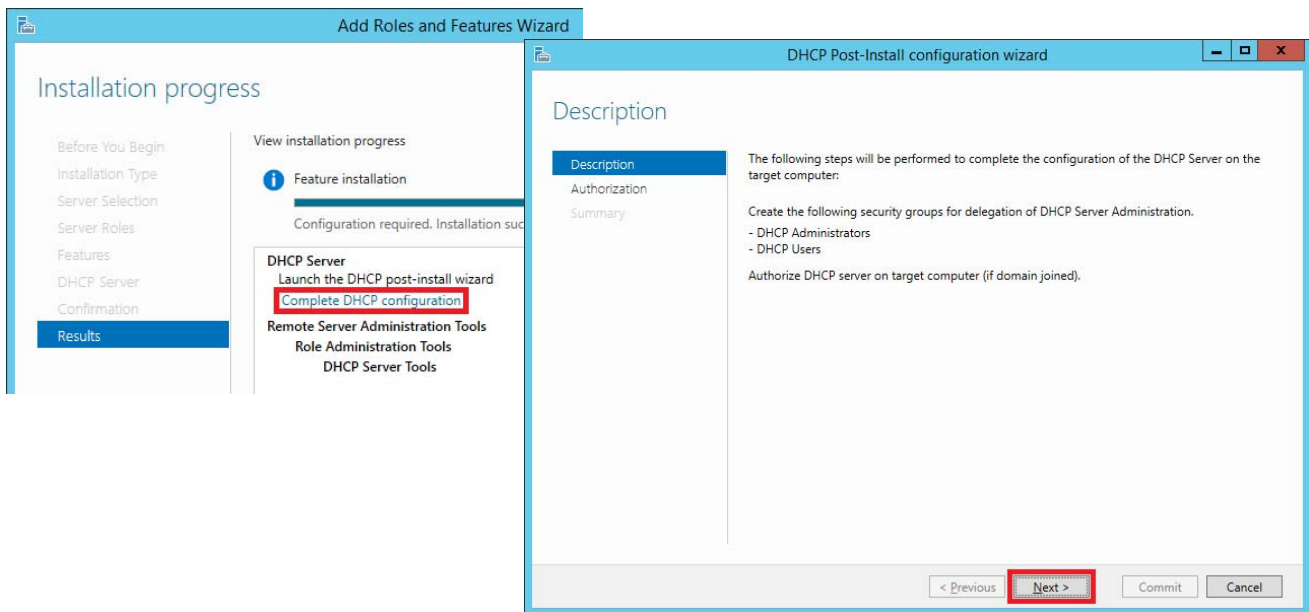
5. Click Next on each of the successive dialog boxes to do the following:

- Verify selected server role
- Confirm installation selections
- Verify 'Things to note' concerning DHCP server

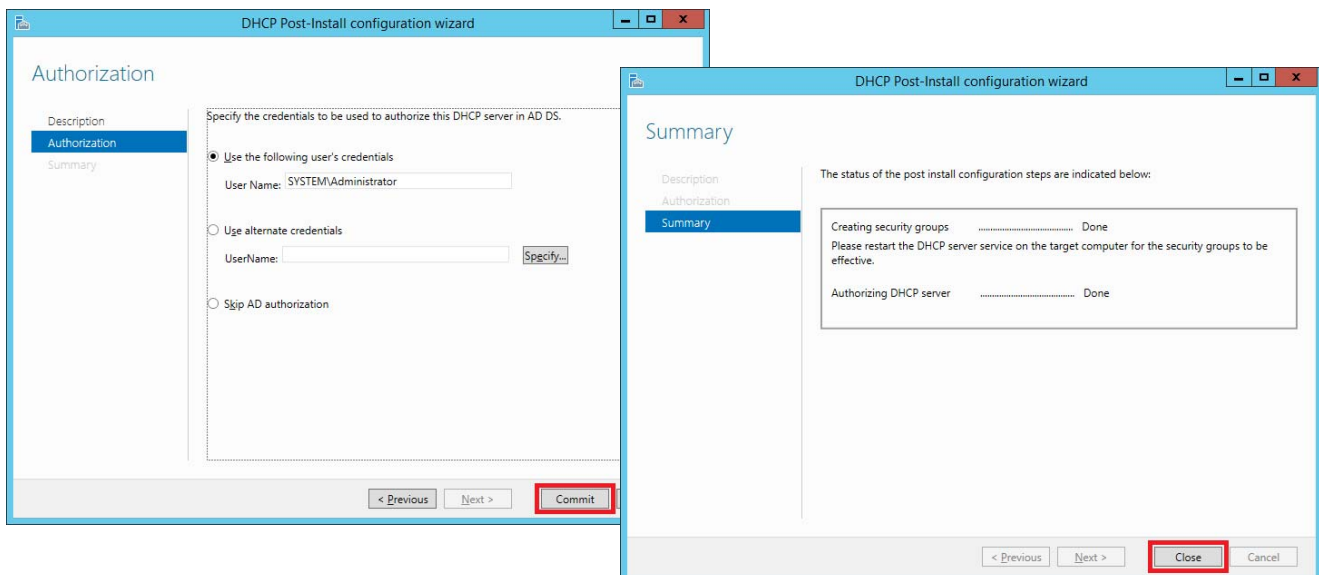
6. To confirm installation selections, click Install.



7. Click Complete DHCP configuration. The DHCP PostInstall configuration wizard window appears.
8. Click Next.



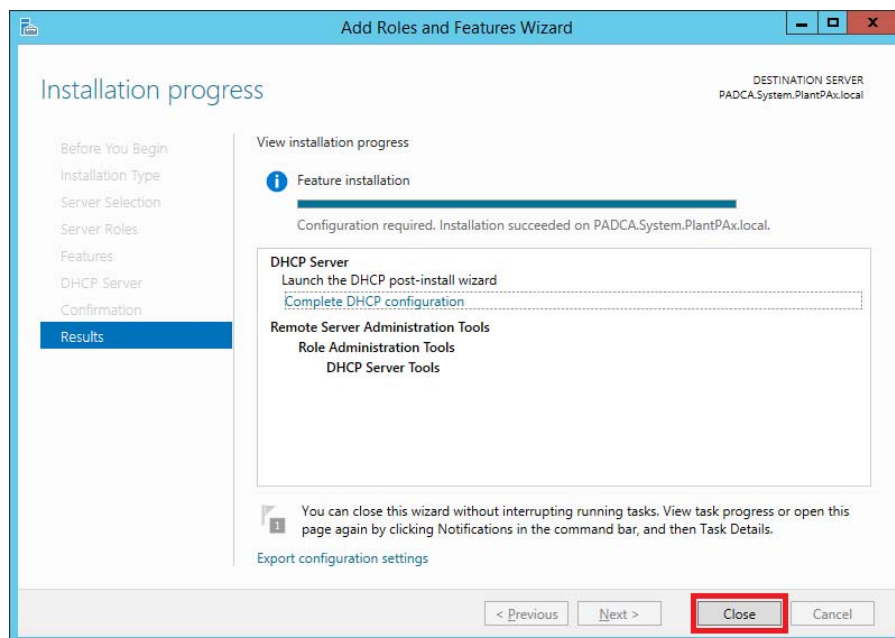
9. Click Commit to authorize the configuration and then click Close.



The DHCP Post-Install configuration wizard window closes.

IMPORTANT Authorize DHCP servers to help avoid damage that is caused by running incorrect configurations or by using the wrong network with DHCP servers.

10. In the Add roles and Features Wizard window, click Close.



11. Repeat step 1 through step 10 to add the secondary server (PADCB).

Configure DHCP Server

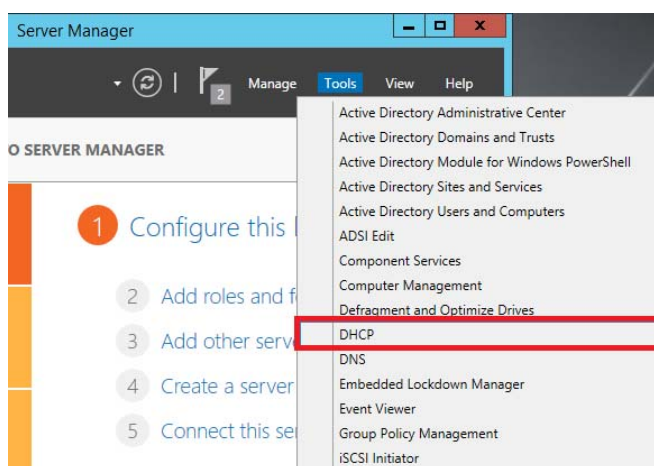
Complete the following steps to configure the DHCP server.

1. From the Server Manager, click Tools and choose DHCP.

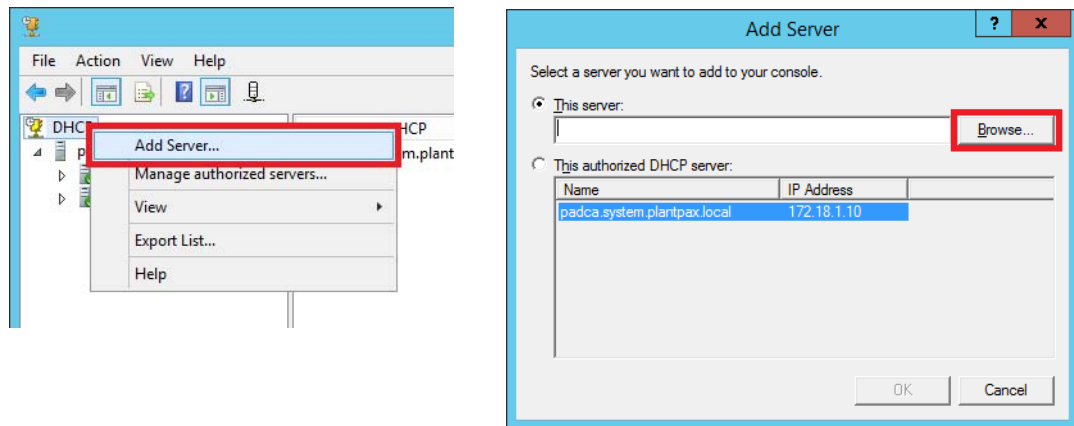
Use a primary domain controller with these procedures.



PADCA

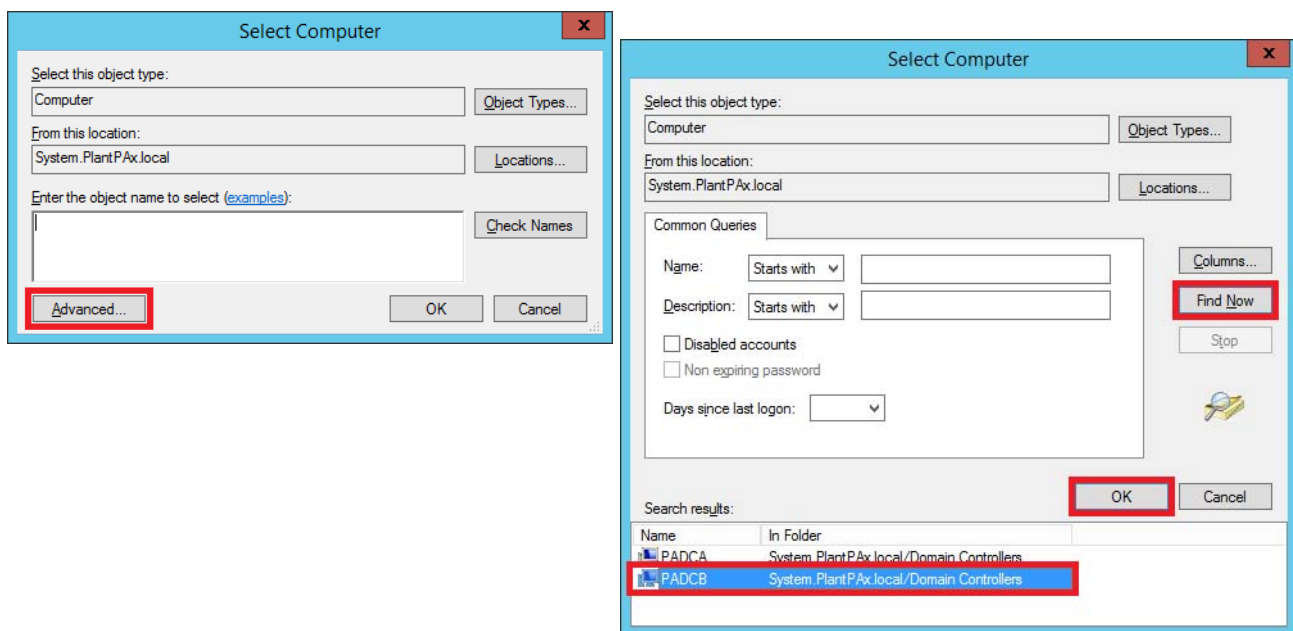


2. Right-click DHCP and choose Add Server.
3. To find the primary domain controller, click Browse.



The Add Computer dialog box appears.

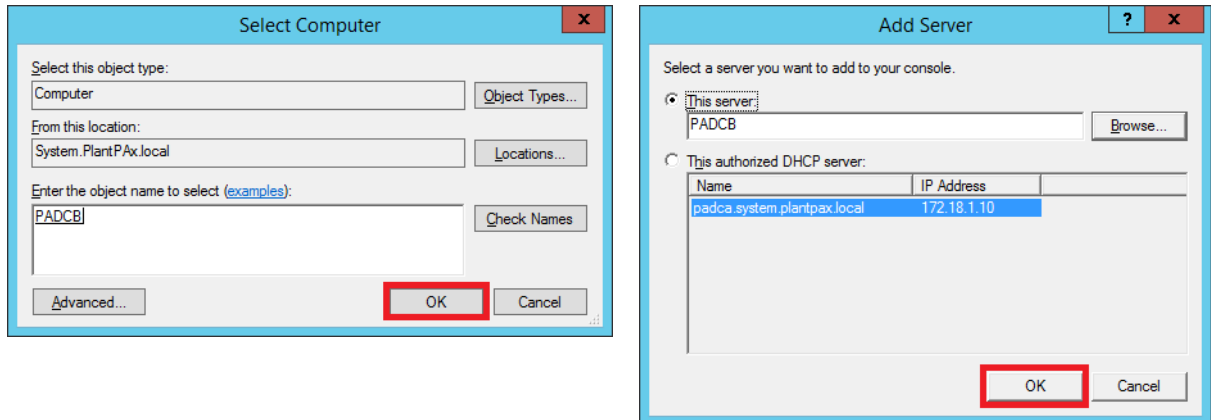
4. Click Advanced and then Find Now for the secondary domain controller.



The domain controller servers appear in the Search results.

5. Select the PADCB server and click OK.

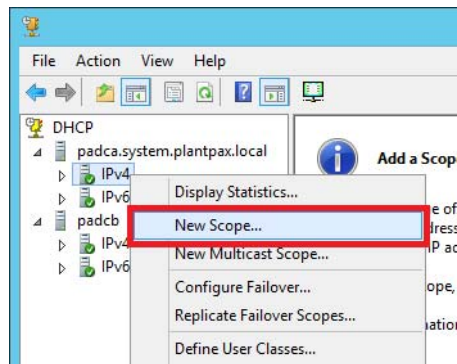
6. To add the secondary domain controller, click OK on the following dialog boxes.



Enable DHCP Scope (Control Network)

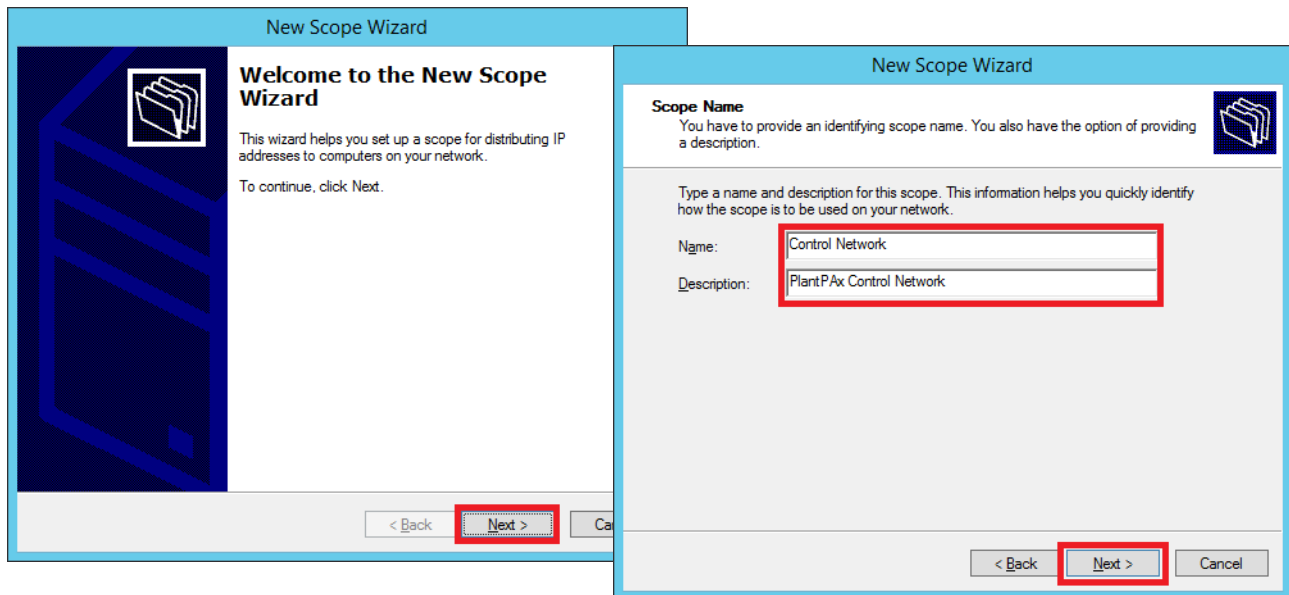
Complete these steps to define the IP address range for the domain controllers. A scope distributes the IP addresses to the computers on your network.

1. From the Server Manager, click Tools and choose DHCP.
2. In the Primary Domain, right-click on IPv4 and choose New Scope.

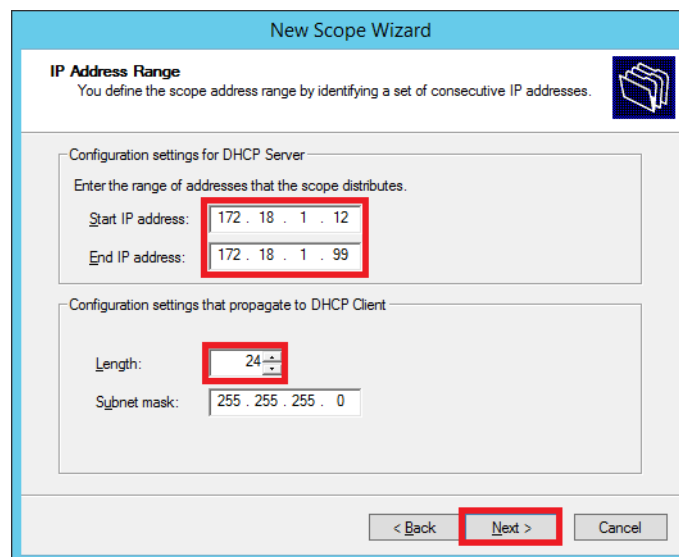


- Click Next, type Control Network.

A description is optional.



- Click Next.
- Type the Start and End IP address range.



- Select a CIDR value from the Length pull-down arrows, and click Next.

The number, such as 24 in the example, represents 24 bits on the network mask. The last 8 bits on the address are used to identify the device on the network.

- Click Next on each of the successive dialog boxes to accept the defaults:
 - Add Exclusions and Delay
 - Lease Duration
 - Confirm 'Configure DHCP Options now'

8. Type the gateway IP address that is used in this VLAN and click Add. The gateway address is added to the list.
9. Click Next.

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: **Add**

Remove

Up

Down

Next >

10. To select the alternate DNS server, type the secondary domain controller IP address and click Add. The IP address is added to the list.

TIP The primary IP address is already in the list (172.18.1.10 in the example).

11. Click Next.

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name: IP address: **Add**

Resolve

Remove

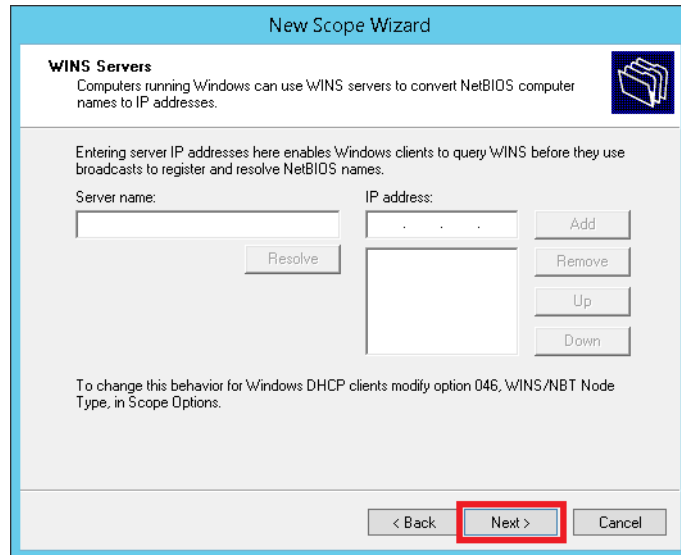
Up

Down

Next >

The WINS Servers dialog box appears.

12. (Optional) To enable WINS servers, type an IP address for a server and click Add. The IP address is added to the list.
13. Click Next.



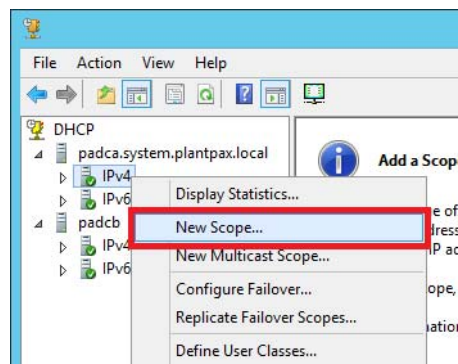
The Activate Scope dialog box appears.

14. To activate the Scope, click Next and then Finish.

Enable DHCP Scope (Supervisory Network)

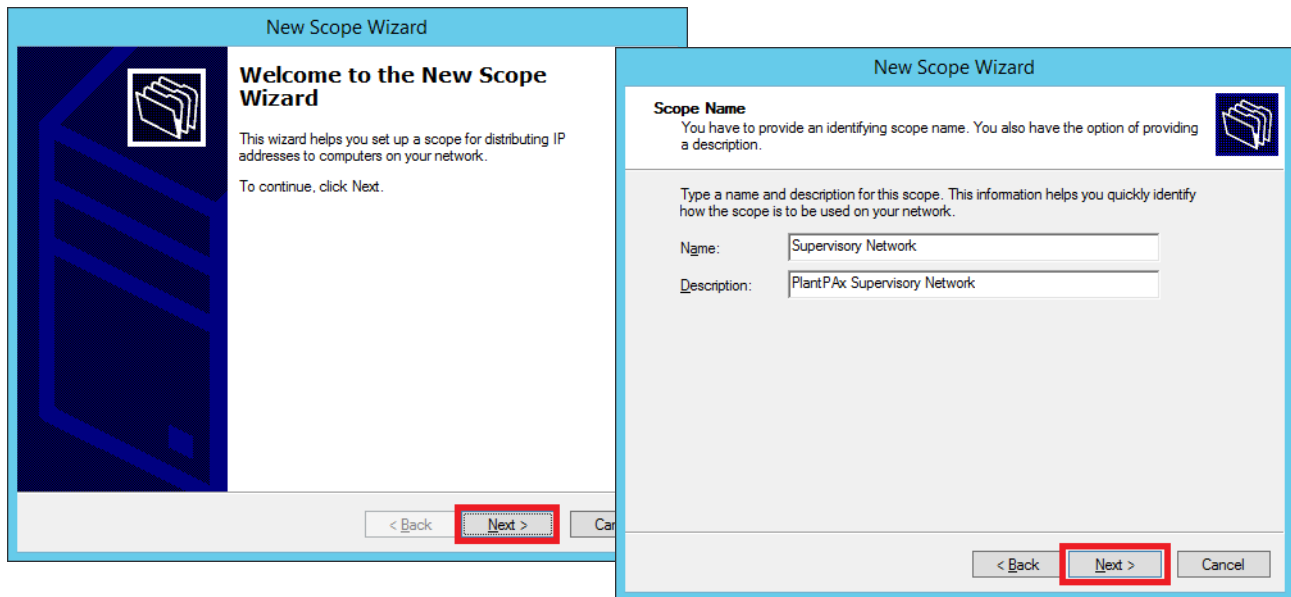
Complete these steps to define the IP address range for the Supervisory Network.

1. From the Server Manager, click Tools and choose DHCP.
2. In the Primary Domain, right-click on IPv4 and choose New Scope.

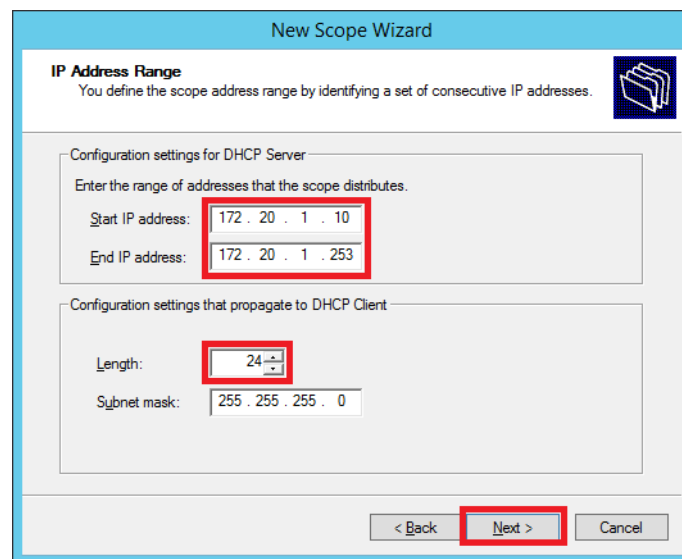


- Click Next, type Supervisory Network.

A description is optional.

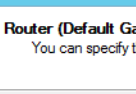


- Click Next.
- Type the Start and End IP address range.



- Select a CIDR value from the Length pull-down arrows, and click Next.
The number, such as 24 in the example, represents 24 bits on the network mask. The last 8 bits on the address are used to identify the device on the network.
- Click Next on each of the successive dialog boxes to accept the defaults:
 - Add Exclusions and Delay
 - Lease Duration
 - Confirm 'Configure DHCP Options now'

8. Type the gateway IP address that is used in this VLAN and click Add. The gateway address is added to the list.
9. Click Next.



Router (Default Gateway)

You can specify the routers, or default gateways.

To add an IP address for a router used by clients

IP address:

172 . 20 . 1 . 1

Add

Remove

Up

Down

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

. . .	Add
172.20.1.1	Remove
	Up
	Down

< Back **Next >** Cancel

- To select the alternate DNS server, type the secondary domain controller IP address and click Add. The IP address is added to the list.

TIP The primary IP address is already in the list (172.18.1.10 in the example).

11. Click Next.

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

<input type="text" value="172 . 18 . 1 . 11"/>	<input type="button" value="Add"/>
<input type="text" value="172.18.1.10"/>	<input type="button" value="Remove"/>
	<input type="button" value="Up"/>
	<input type="button" value="Down"/>

< Back Next > Cancel

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

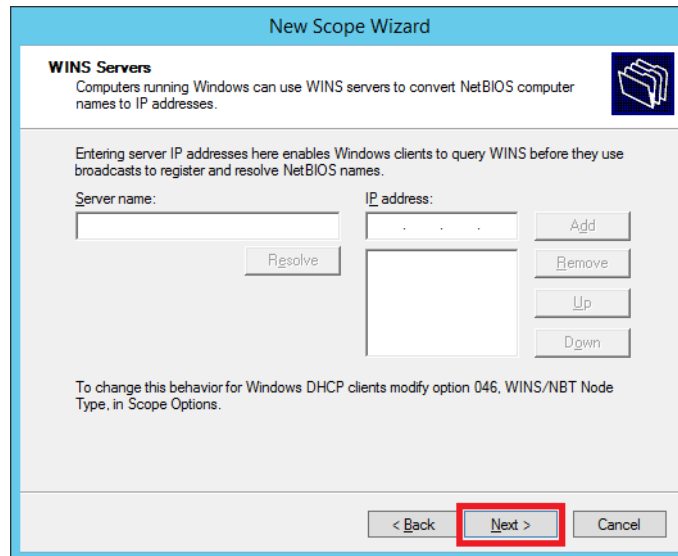
Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="..."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<div>172.18.1.10 172.18.1.11</div>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

The WINS Servers dialog box appears.

12. (Optional) To enable WINS servers, type an IP address for a server and click Add. The IP address is added to the list.
13. Click Next.



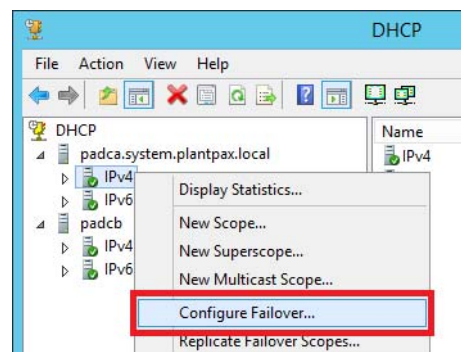
The Activate Scope dialog box appears.

14. To activate the Scope, click Next and then Finish.

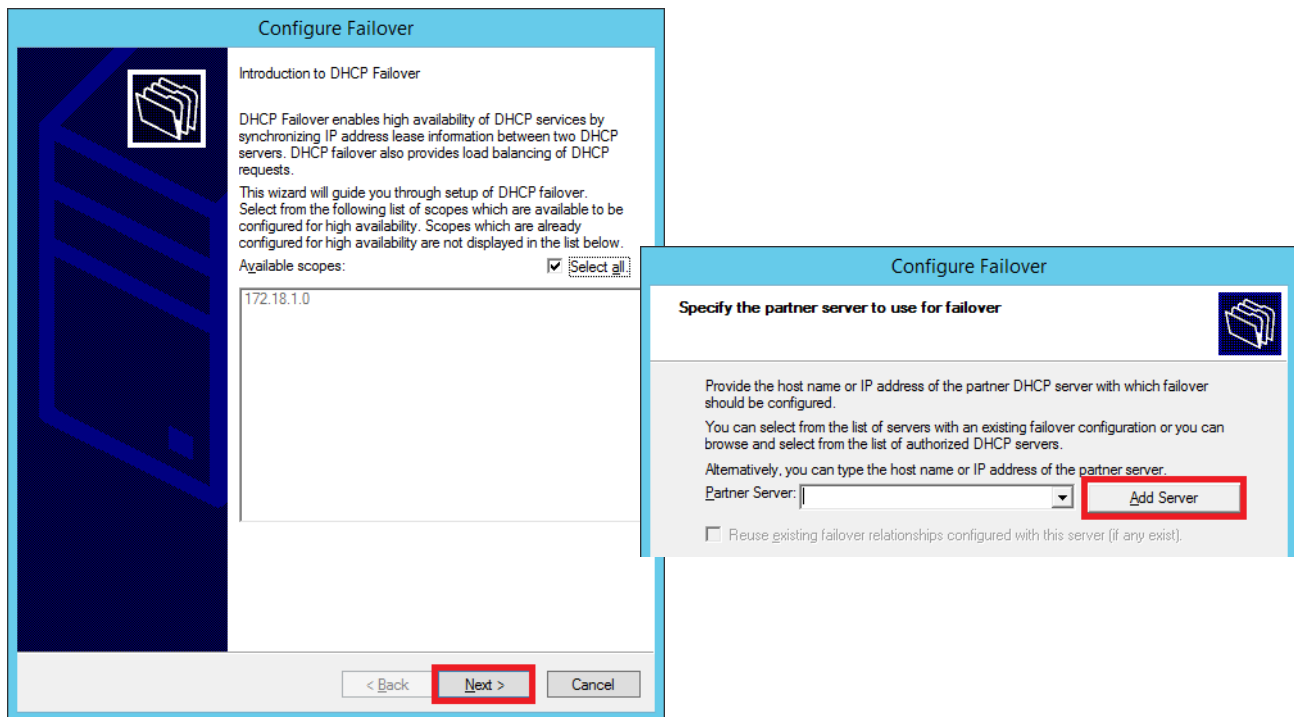
Configure Failover

Complete these steps to configure high availability for your domain controllers.

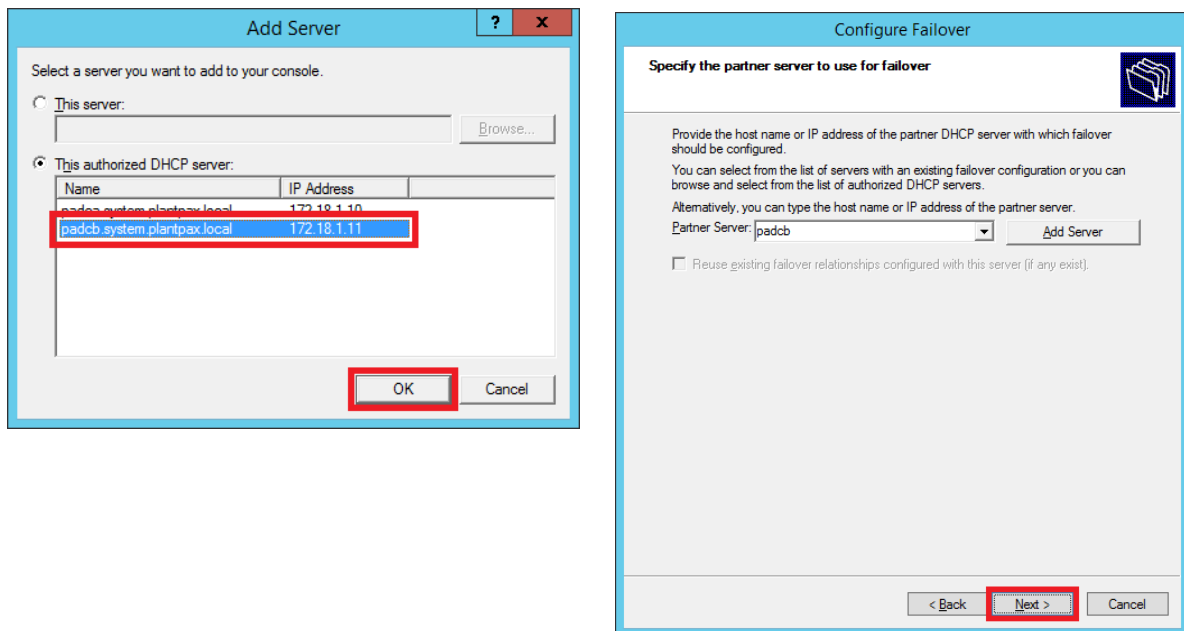
1. From the Server Manager, click Tools and choose DHCP.
2. In the Primary Domain, right-click on IPv4 and choose Configure Failover.



3. Click Next and then Add Server.



4. Select the backup server, select 'padcb', click OK, and then Next.



5. Select Hot standby from the Mode pull-down, and type a shared secret.

Configure Failover

Create a new failover relationship

Create a new failover relationship with partner padcb

Relationship Name: padca.system.plantpax.local-padcb

Maximum Client Lead Time: 1 hours 0 minutes

Mode: Hot standby

Hot Standby Configuration

Role of Partner Server: Standby

Addresses reserved for standby server: 5 %

☐ State Switchover Interval: 60 minutes

☒ Enable Message Authentication

Shared Secret: *****

< Back Next > Cancel

6. Click Next.
7. Click Finish and Close.

Configure Failover

Failover will be set up between padca.system.plantpax.loc... and padcb with the following parameters.

Scopes:

172.18.1.0

Relationship Name: padca.system.plantpax.loc...

Maximum Client Lead Time: 1 hrs 0 mins

Mode: Hot standby

State Switchover Interval: Disabled

Hot Standby Configuration

Role of Partner Server: Standby

Addresses reserved for standby: 5 %

< Back Finish Cancel

Configure Failover

Progress of failover configuration.

The log below shows the progress of the various tasks for configuring failover including any errors encountered.

Add scopes on partner serverSuccessful

Disable scopes on partner serverSuccessful

Creation of failover configuration on partner serverSuccessful

Creation of failover configuration on host serverSuccessful

Activate scopes on partner serverSuccessful

Configure failover successful.

Close


Proceed to [page 113](#) to group the settings for the workstations and servers under one authority.

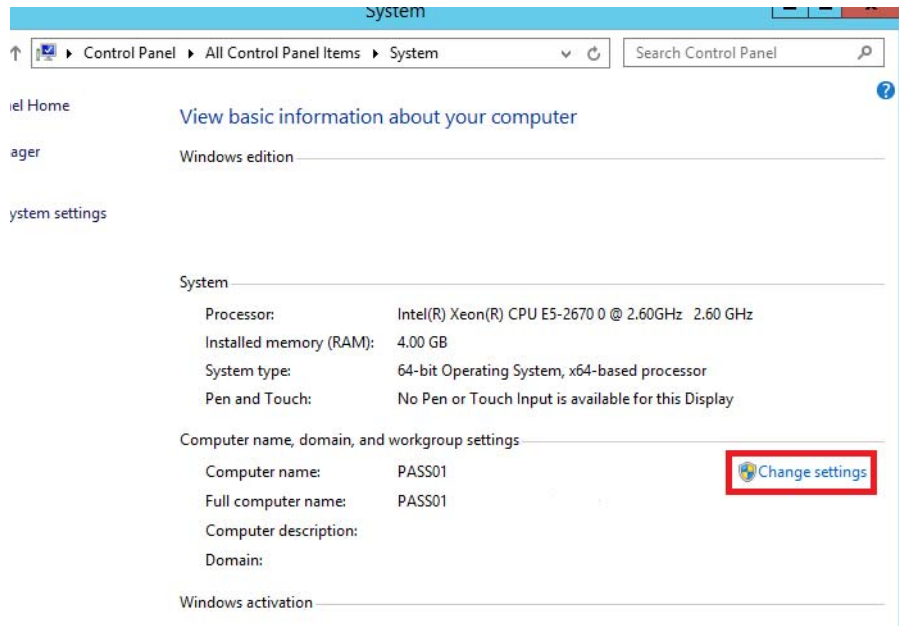
Join the Domain

Use all servers and workstations with these procedures.

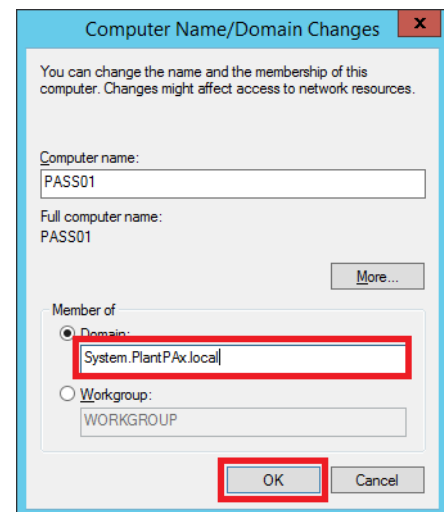
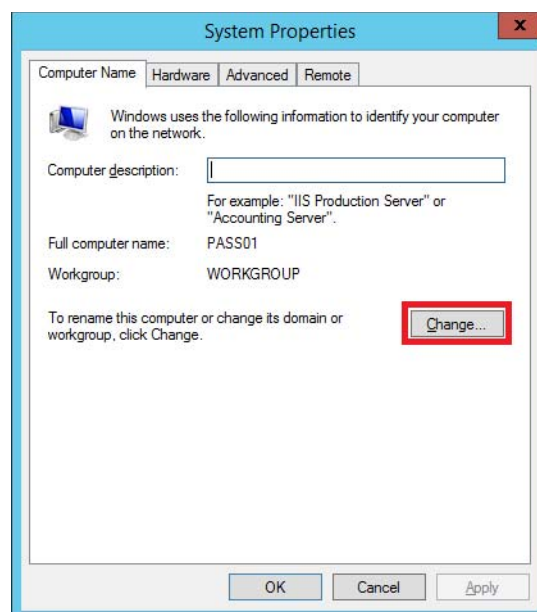


When you join the system elements into a single domain, the control and communication of the infrastructure is seamless. The domain centralizes all administrative settings for the workstations and servers in your application.

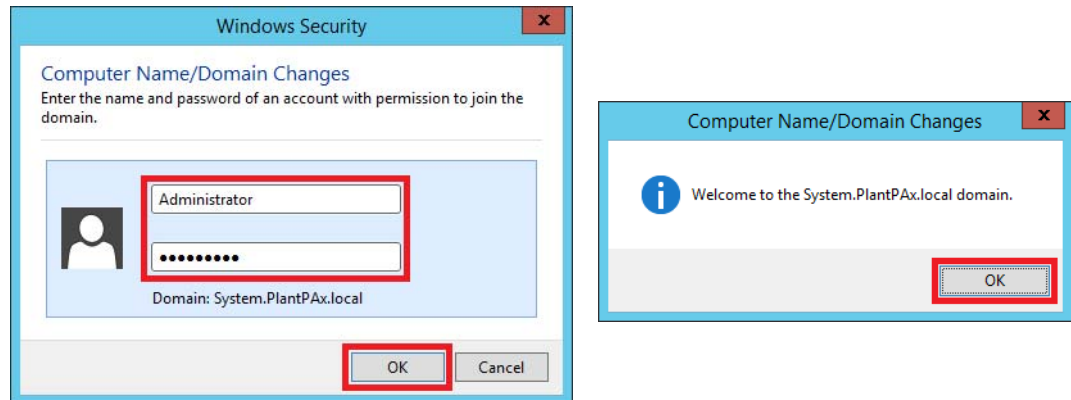
1. Click the Windows  symbol.
2. Click Control Panel and choose System > Change Settings.



3. Click Change, select Domain, and then type the domain name and click OK.

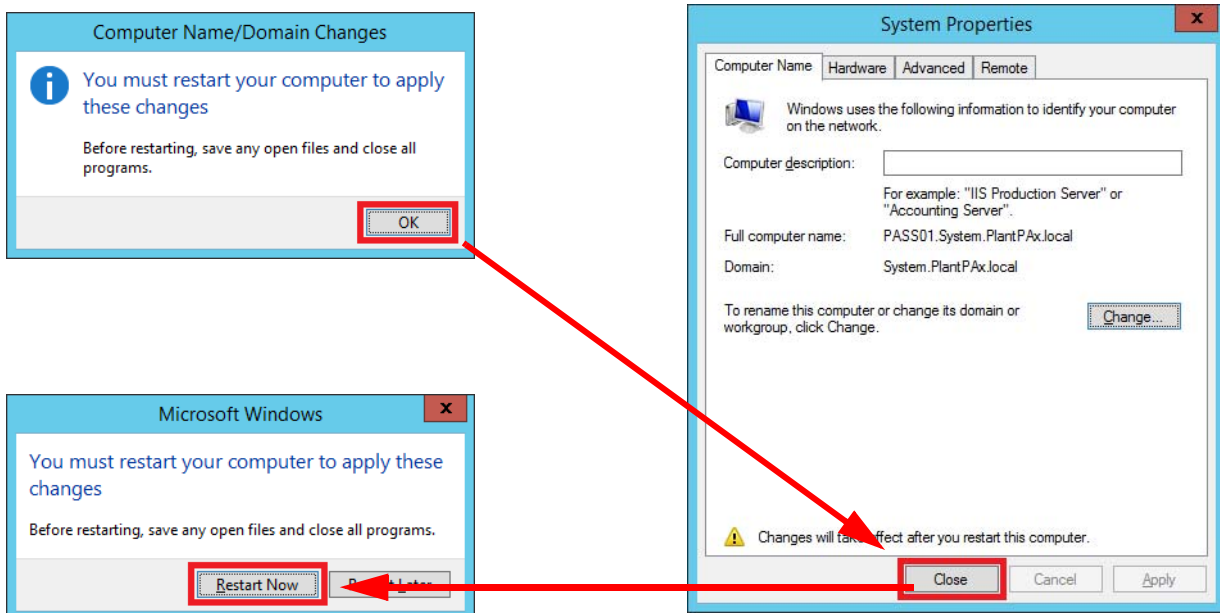


4. Type a user name and password to add this computer to the domain and click OK on the dialog boxes.



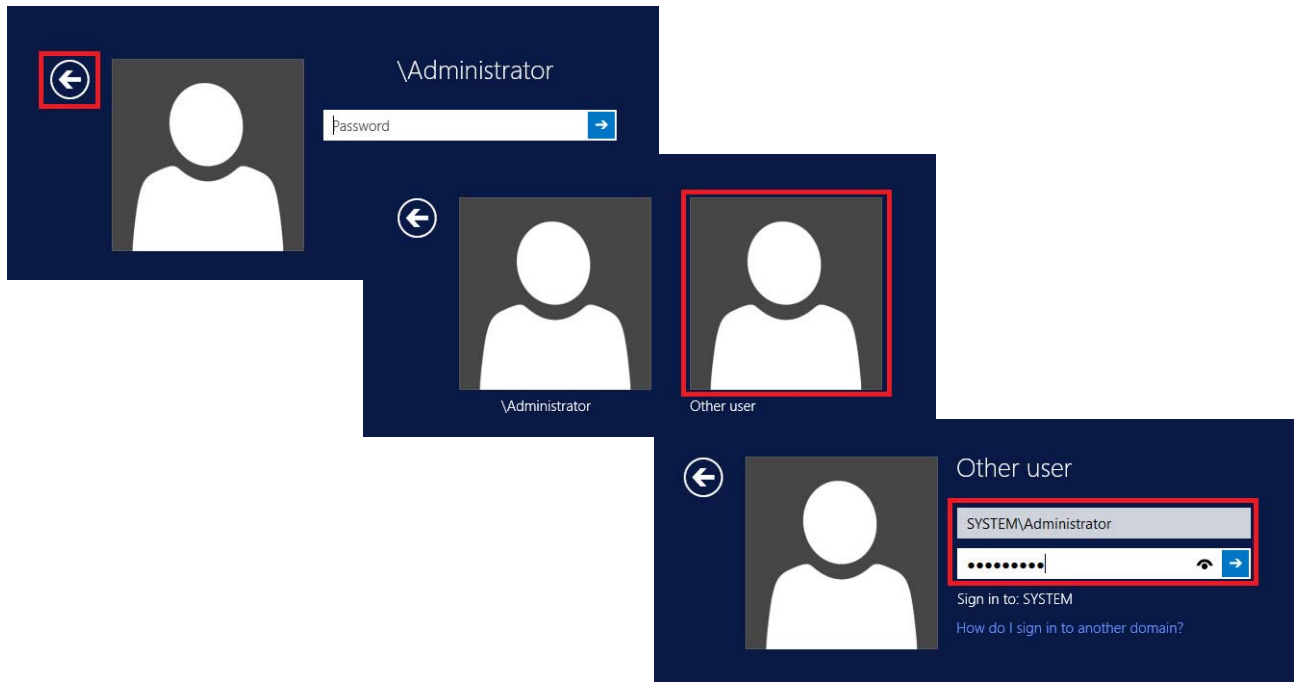
If you have the correct access, the computer is accepted into the domain.

5. To accept the changes and restart the computer, do the following:
 - Click OK in the first warning dialog box
 - Click close in the Systems Properties dialog box
 - Click Restart Now in the second warning dialog box



6. After restarting the computer, press Ctrl+Alt+Delete to log in.

7. Click Switch User, choose Other User, and type [Domain Name]\user, such as System\Administrator, followed by the password.



8. Repeat [step 1](#) through [step 7](#) for all system computers.

Use the primary server with these procedures.



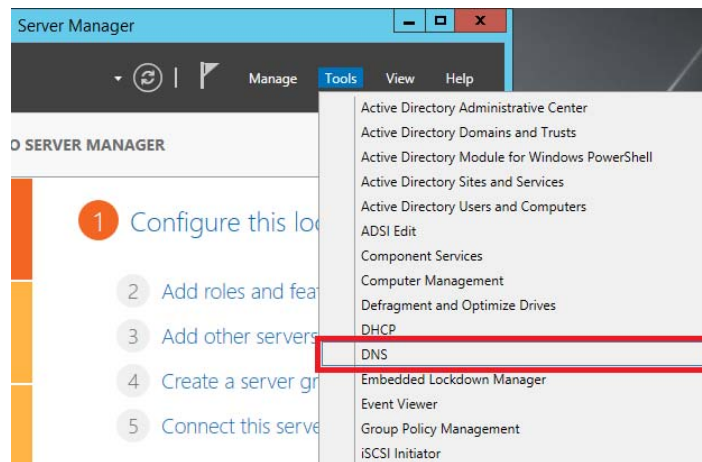
PADCA

Confirm Computers in DNS Server

When all system computers are in the domain, you can confirm the addresses on the Domain Controller DNS server.

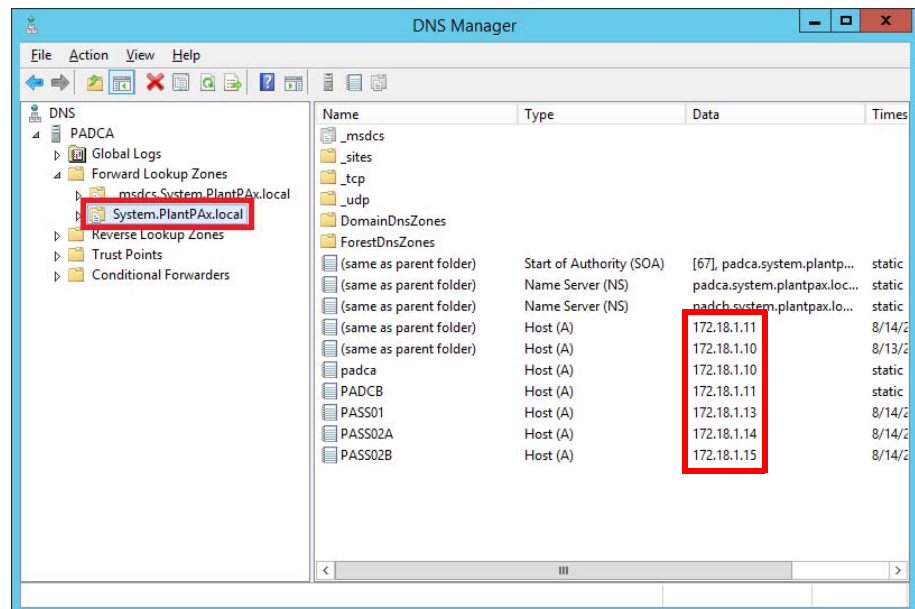
Complete the following steps.

1. From the Server Manager, click Tools and choose DNS.



The DNS Manager dialog box appears.

2. Select DNS><primary domain>>Forward Lookup Zone><primary domain name> (System.PlantPAx.local in our example).



The Data column displays the IP addresses.

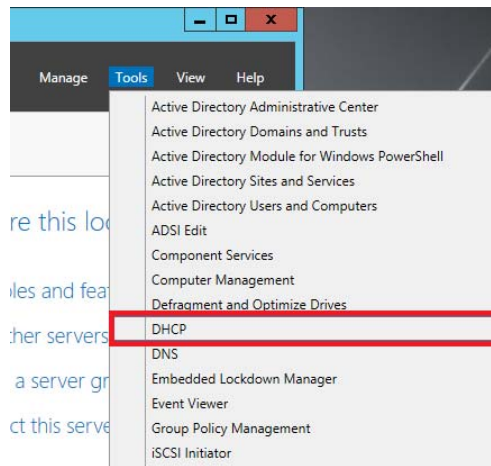
IMPORTANT The same IP address is not expected for more than one server or workstation.

Confirm Computers in DHCP Server

You can confirm all computers in the DHCP server by accessing the Address Leases folder.

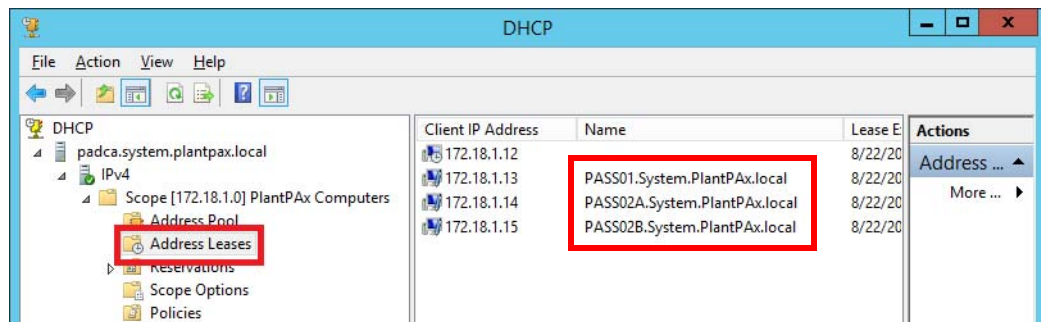
Complete the following steps.

1. From the Server Manager, click Tools and choose DHCP.



The DHCP dialog box appears.

2. Select DHCP > <domain controller> > IPv4 > Scope > Address Leases.



The Name column lists the computers.

IMPORTANT The IP address that is assigned to all system computers needs to match the IP addresses in the DNS list.

Proceed to [page 118](#) to place the users and groups into the Active Directory.

Create Groups and Users

Use a domain controller with these procedures.

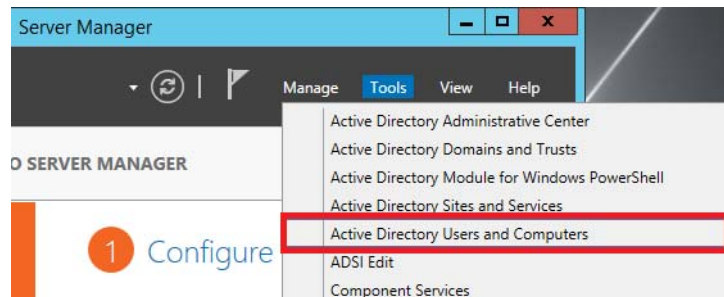


From operators and maintenance personnel to engineers, the domain controller manages groups in the active directory. The procedures describe how to create groups for units, roles, and areas per your application requirements.

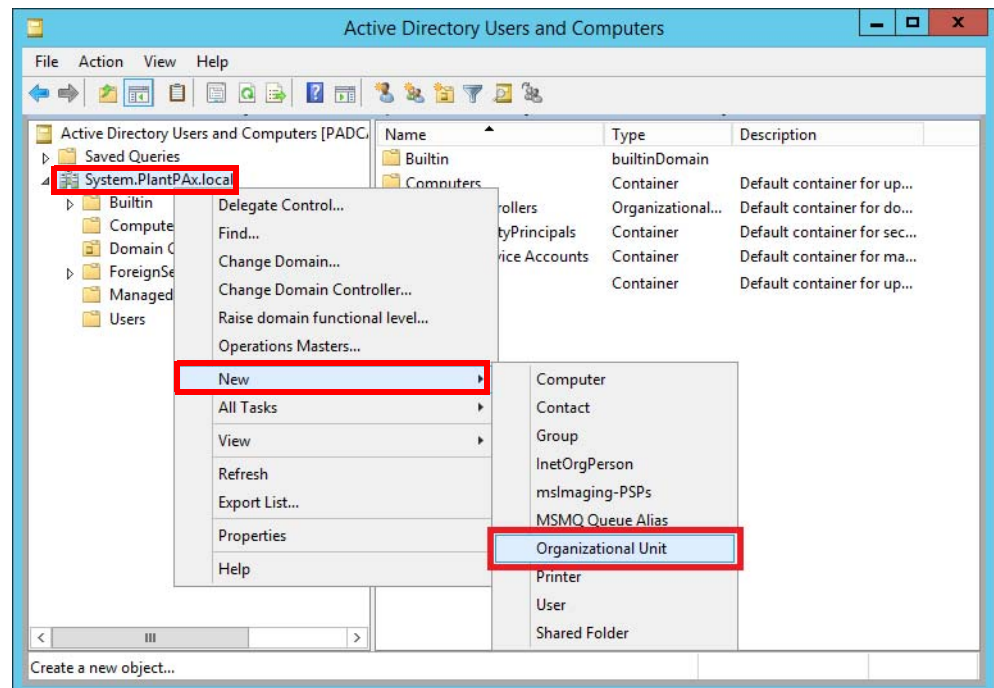
Unit Groups

Complete these steps.

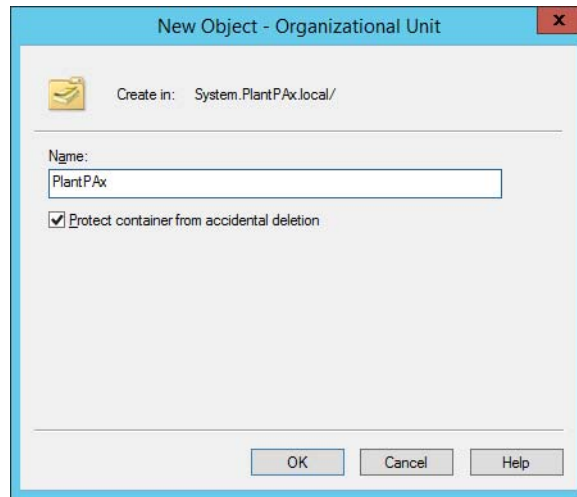
1. From the Server Manager, click Tools and choose Active Directory Users and Computers.



2. On the Active Directory Users and Computers dialog box, expand the domain folder (System.PlantPAx.local).
3. Right-click the domain and choose New>Organizational Unit.

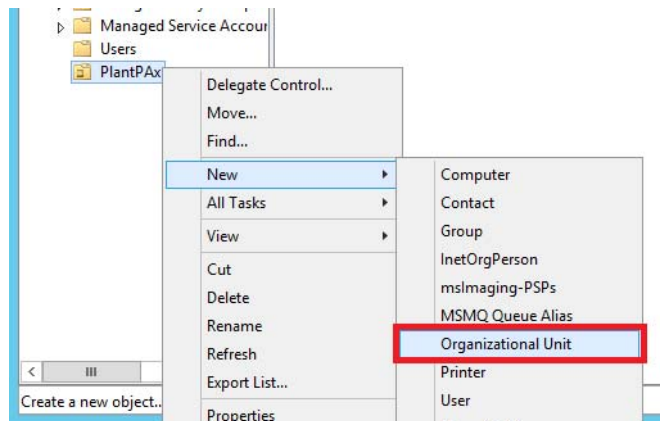


4. Type the group name and click OK.



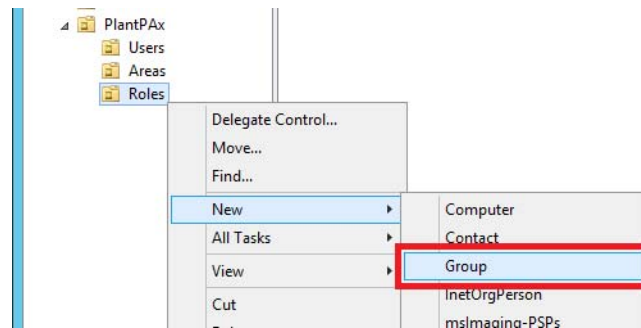
Role Groups

1. To define the roles for the group, right-click the group name and choose New>Organizational Unit.

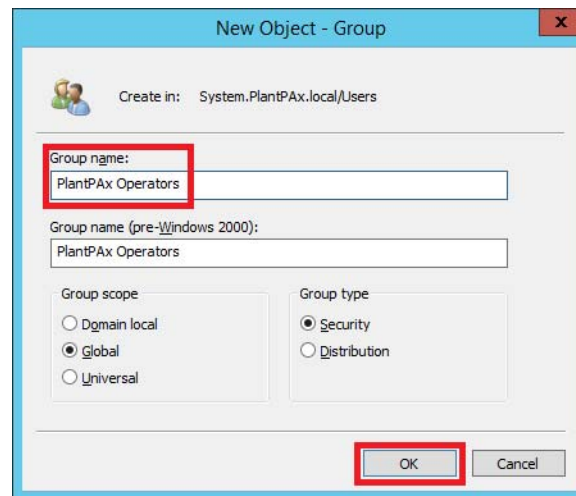


2. Under the PlantPAx Organizational Unit, create these three units:
 - Users
 - Areas
 - Roles

3. Right-click Roles and choose New>Group.



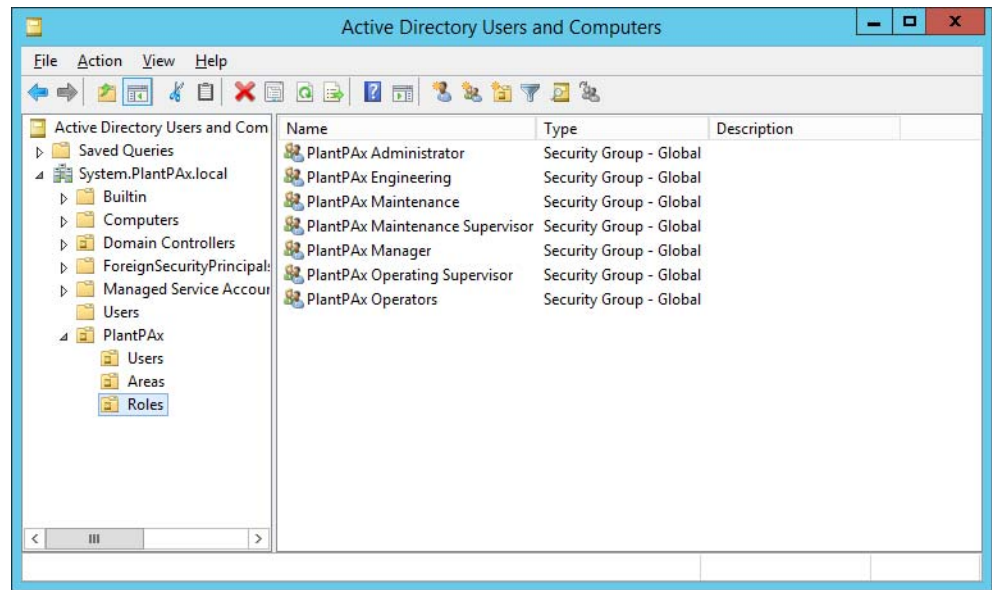
4. Type the group name and click OK.



5. Repeat [step 4](#) for all application groups, including the following:

- PlantPAx Operating Supervisor
- PlantPAx Maintenance
- PlantPAx Maintenance Supervisor
- PlantPAx Manager
- PlantPAx Engineering
- PlantPAx Administrator

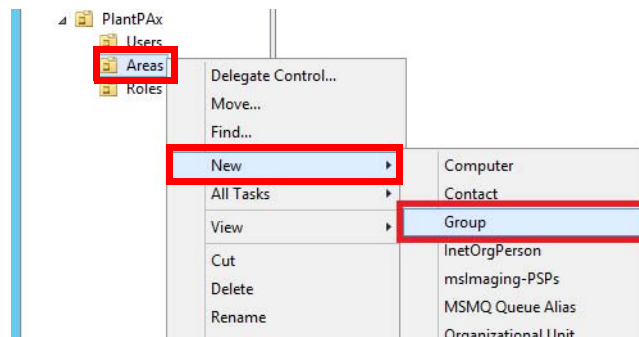
6. Create the roles for all group application, including as shown:



Area Groups

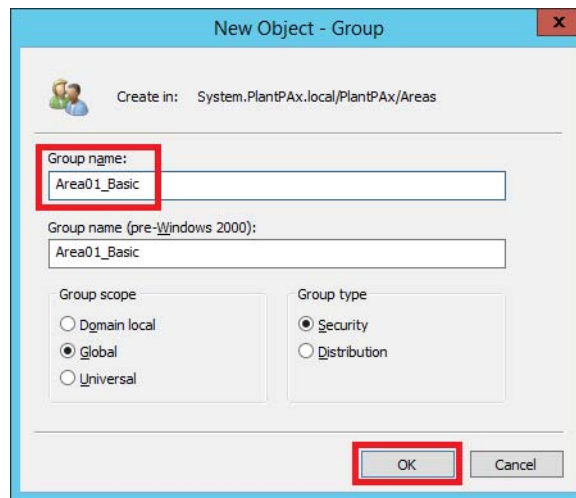
Complete these steps to define specific areas based on the group.

1. On the Active Directory Users and Computers dialog box (with the Users folder still selected), right-click New and choose User.



The New Object Group dialog box appears.

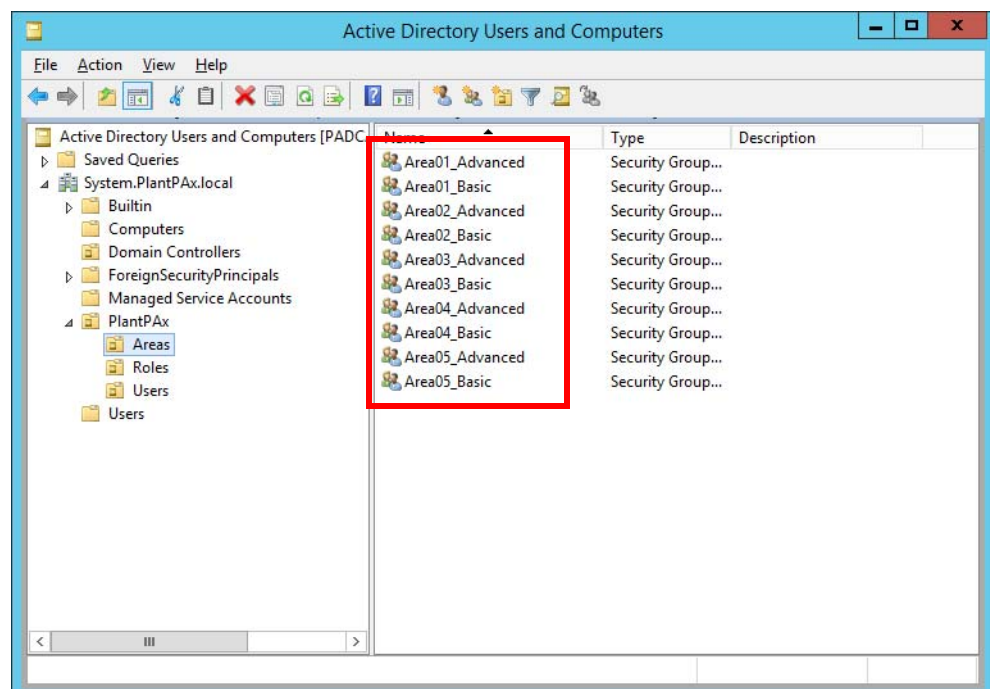
2. Type an object name for the group and use the defaults for scope and type.



3. Click OK.
4. Repeat [step 2](#) but for the group name type Area01_Advanced.
5. Click OK.

IMPORTANT We do not recommend using generic area names like Area01. Be specific ('Packaging', 'Molding', and so on), but create two types—Basic and Advanced—for each area.

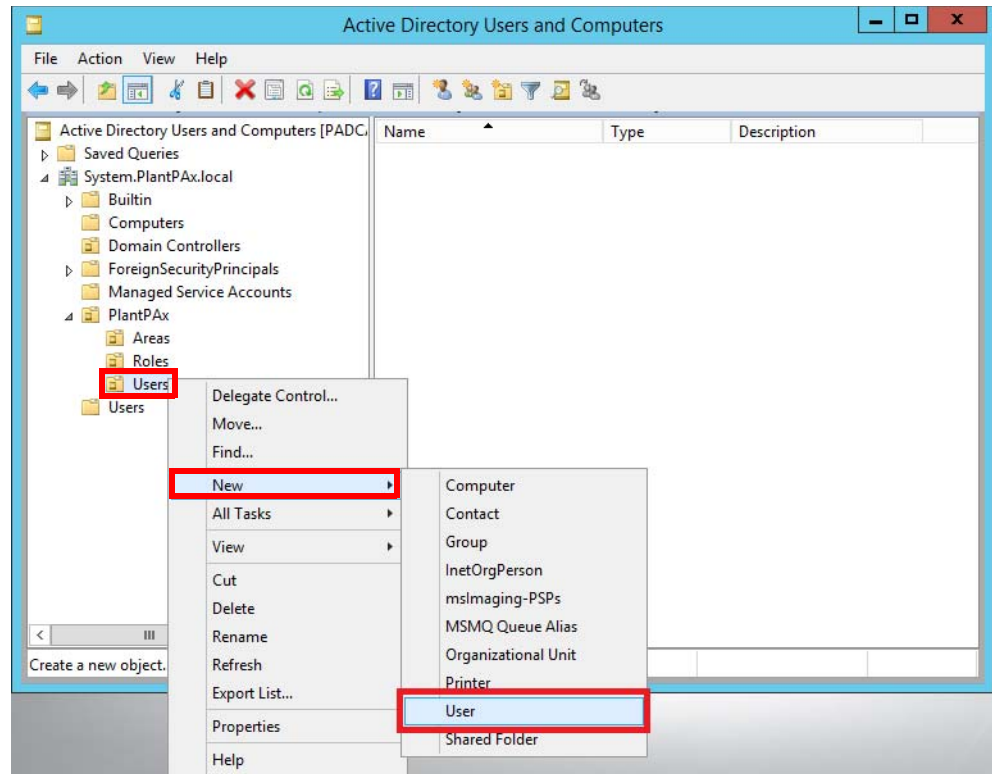
6. Repeat [step 2](#) for each area of the plant.



Create Users

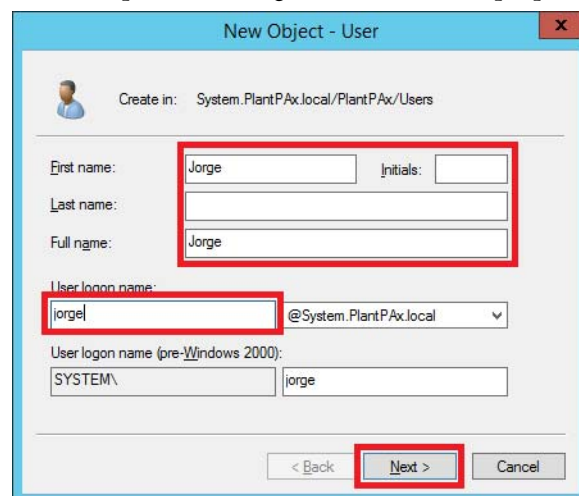
Complete these steps to enter personnel names into the domain controller.

1. On the Active Directory Users and Computers dialog box, click the domain and expand the group (PlantPAx).
2. Right-click Users and choose New> User.



The New Object User dialog box appears.

3. Type the name of a user and initials.
- Our example shows 'Jorge' for instructional purposes only.



IMPORTANT We do not recommend using 'generic users' such as 'Operator' or 'Admin' to share on the system.

4. Type a user login name and click Next.
5. Type the initial user password and repeat to confirm the entry.

6. Click 'User must change password at next logon' and click Next.

This procedure gives a user a unique password that, for security purposes, a user can change any time.

TIP You can consider checking the 'Password never expires' checkbox to help prevent from being locked out if the password expires.

7. Click Finish.

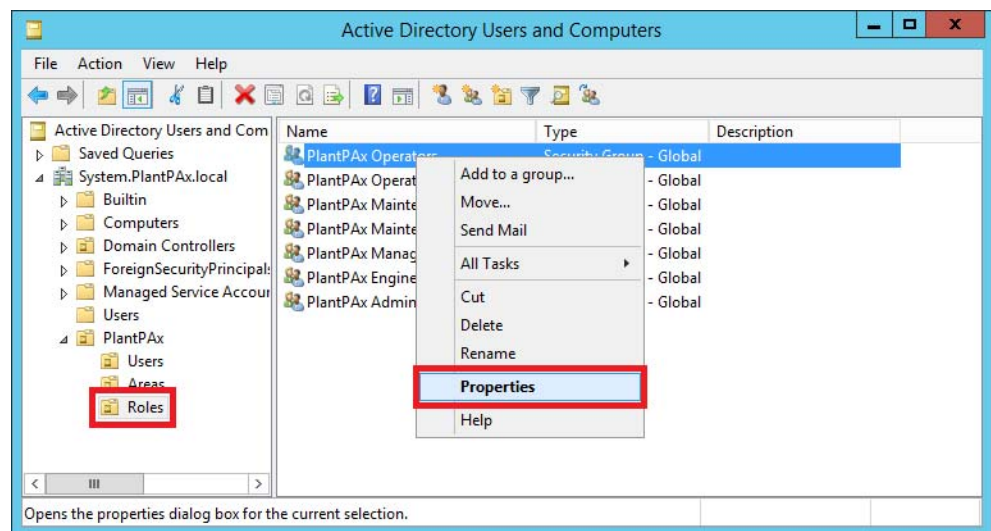
Assign Users to a Group

The created users are not yet members of any group. Complete the following steps to assign the users to a group.

Assign a User to the PlantPAx Operators Group

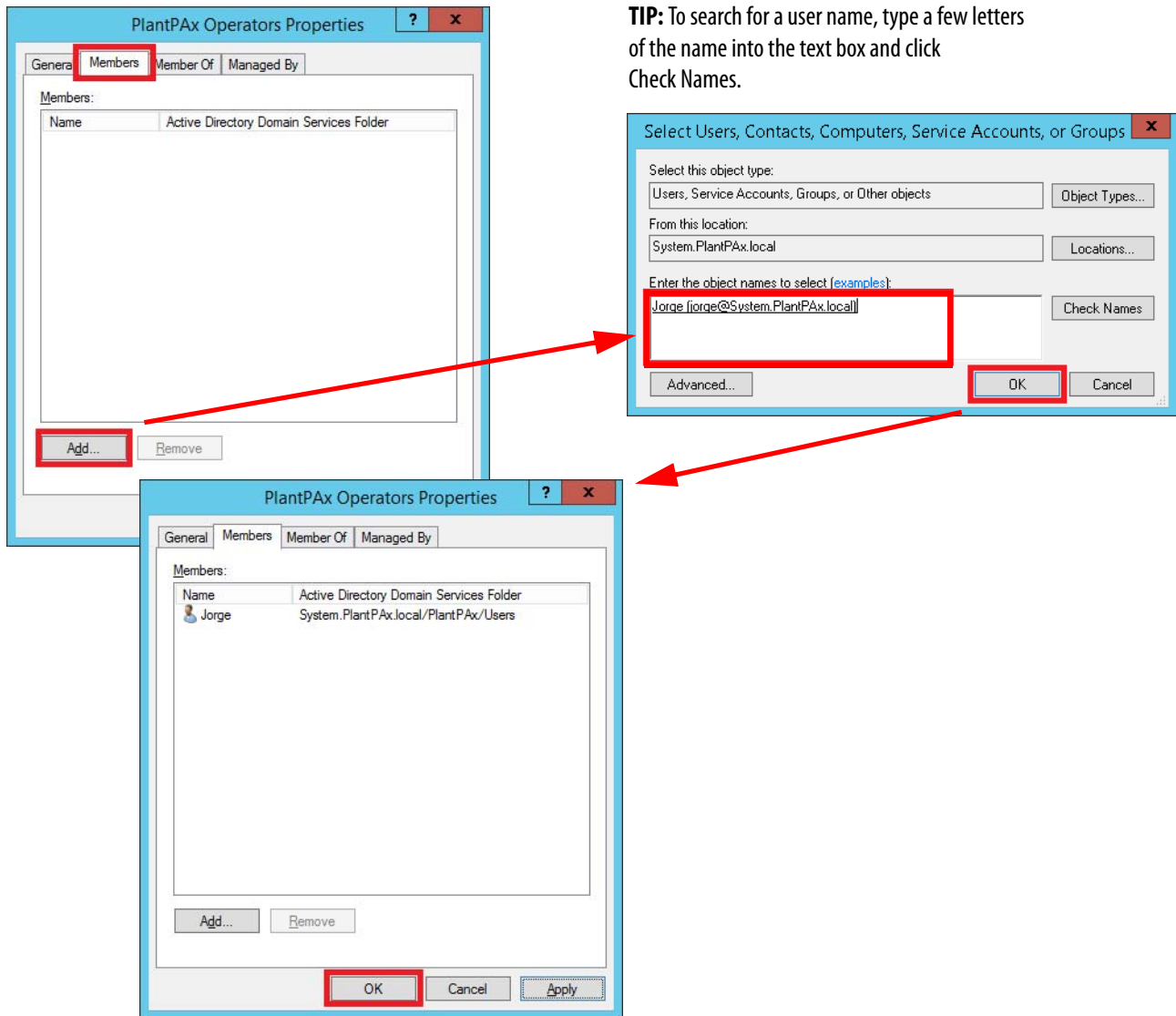
In this section, individual users are assigned to the PlantPAx Operators group. The same procedures apply to assign users to other groups.

1. In the Active Directory Users and Computers window, open the group folder. (PlantPAx is our example).
2. Click Roles, right-click a group, and choose Properties.



3. In the PlantPAx Operators Properties dialog box, click the Members tab.
This tab shows the members of the PlantPAx Operators group. (Our example shows no members.)
4. Click Add.
5. Type the user name (Jorge in our example) in the text box and click OK.
6. Repeat step 4 and step 5 to add users.

TIP: To search for a user name, type a few letters of the name into the text box and click Check Names.



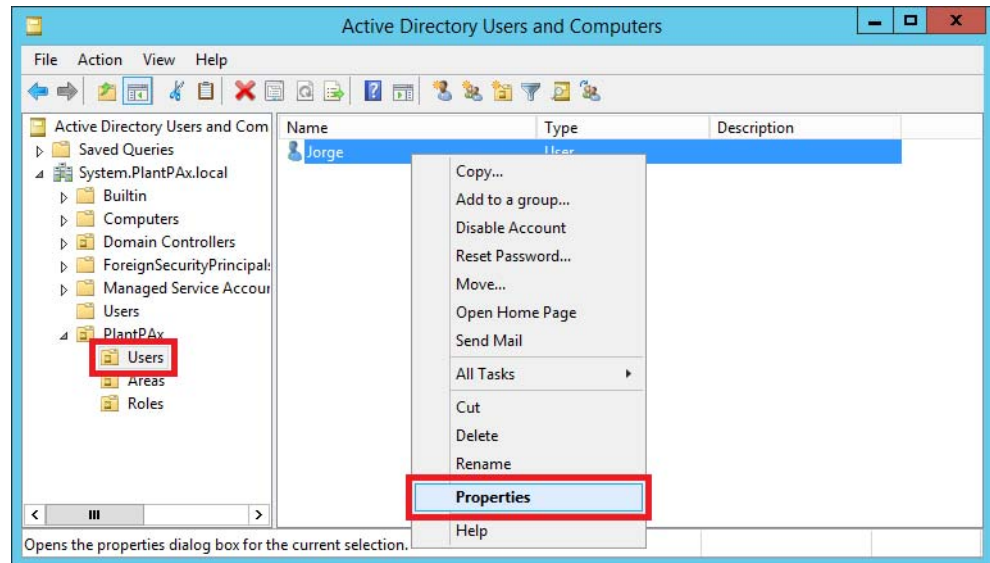
The PlantPAx Operators Properties dialog box shows all users that you added in the previous steps. (Jorge in our example.)

IMPORTANT Do not use more than one PlantPAx group for a single user to help prevent being denied access. The following dialog boxes show how to identify members that are assigned to groups.

7. Click OK to close the group Properties dialog box.

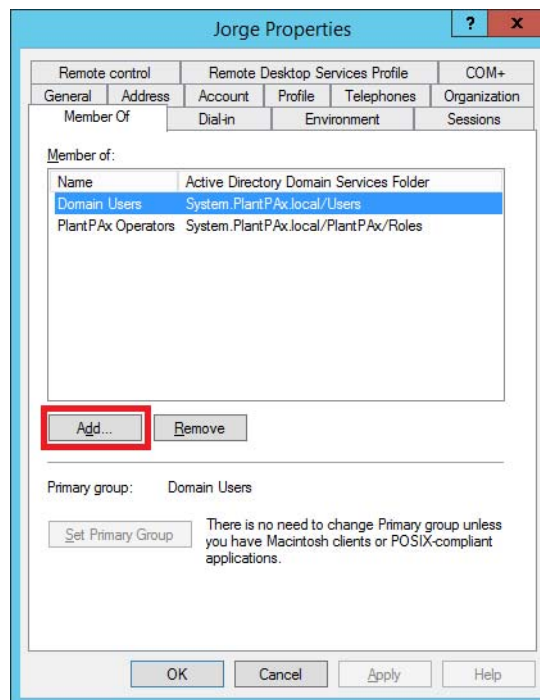
The following steps assign a user to a group by using the group properties.

8. In the Active Directory Users and Computers window, click the Users folder, right-click on an individual user name (Jorge in our example) and choose Properties.

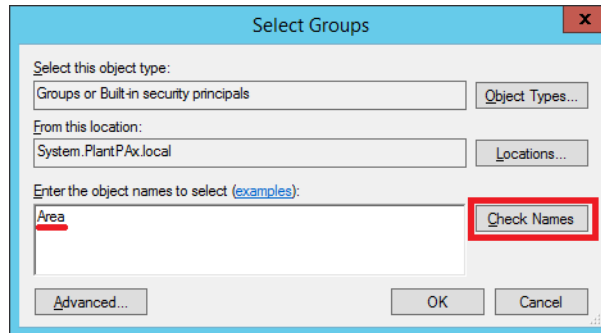


The Properties dialog box for the selected user appears.

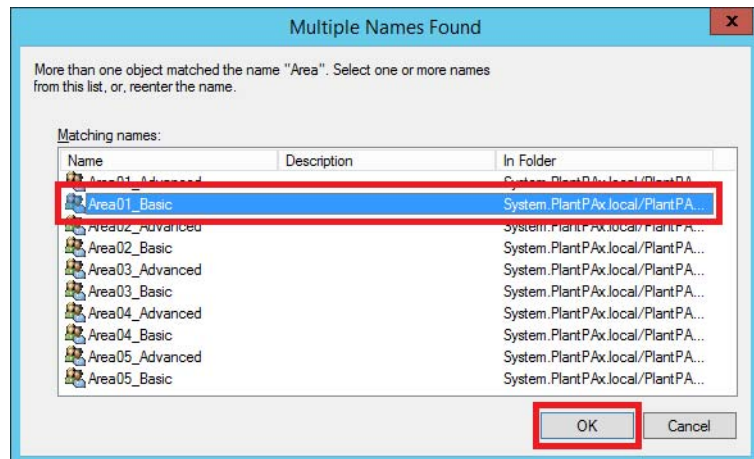
9. Click Add to add users to areas of the application.



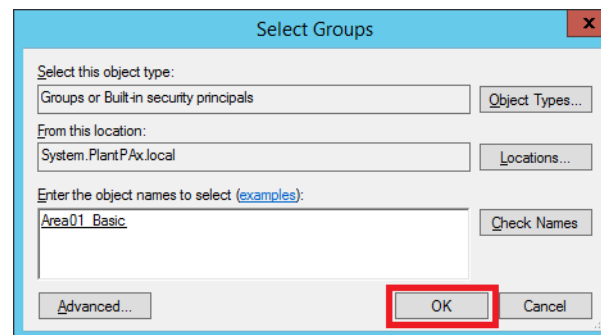
10. From the Select Groups dialog box, type an object name.
'Area' is our example as entered on [page 122](#).



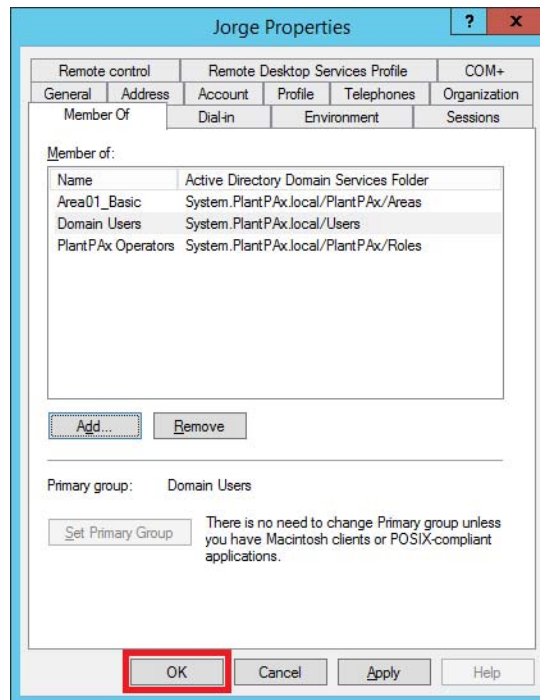
11. Click Check Names.
12. Select an object from the list and click OK.



13. Click OK.



A Properties dialog box appears for the personnel name (for example, Jorge) that is being added as a 'member of' a group.



14. Click OK.

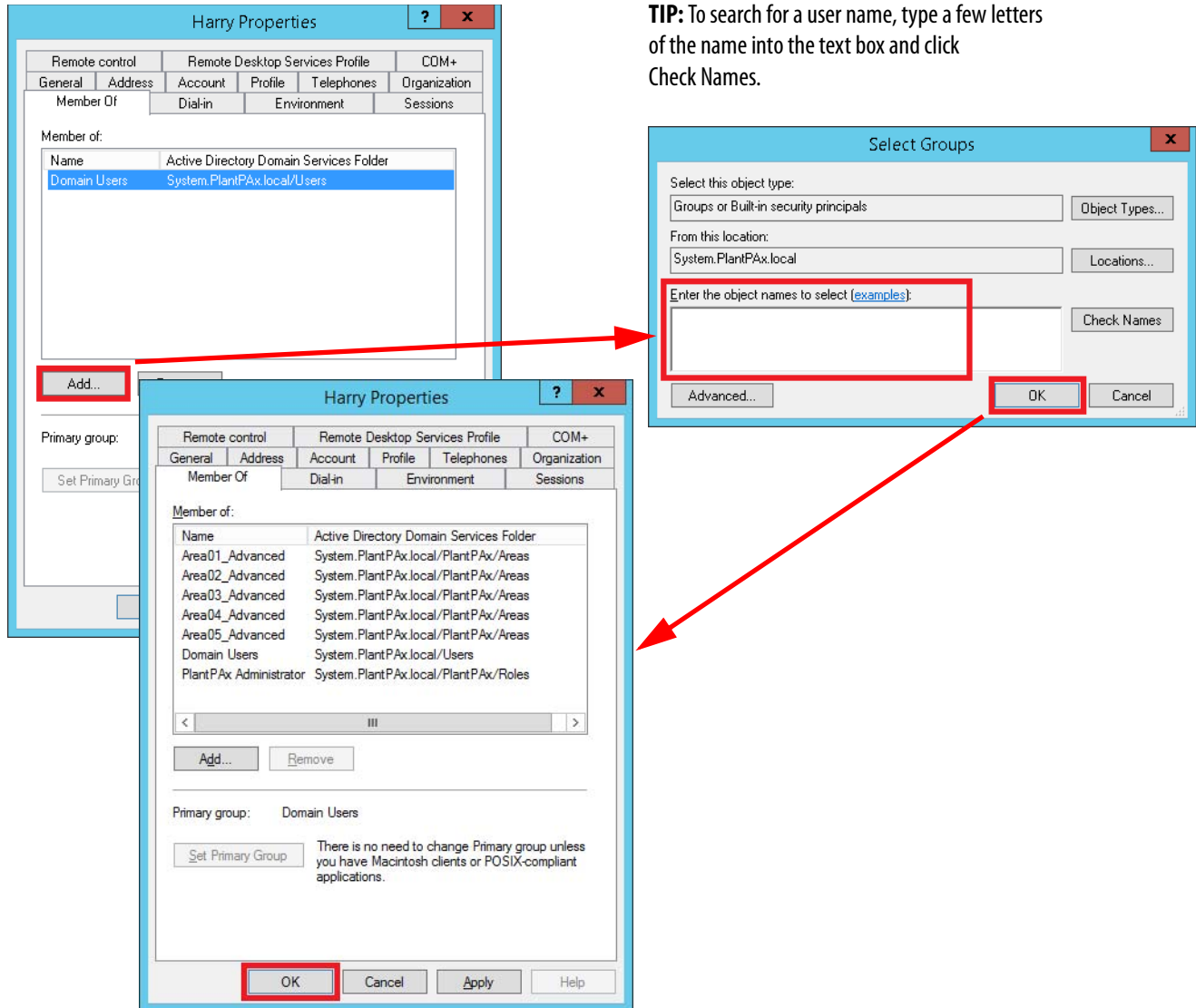
Assign a User to the PlantPAx Administrator Group

IMPORTANT In the previous procedure, a user was added to a group by using the group properties. In this procedure, a user is added to a group by using the individual user properties. Our example is 'Harry'.

1. In the Active Directory Users and Computers dialog box, choose the Users folder, right-click on a user (Harry in our example) and choose Properties.

The Properties dialog box appears and 'Harry' is not a member of any groups.

2. Click Add.
3. Type the group name in the text box and click OK.



TIP: To search for a user name, type a few letters of the name into the text box and click Check Names.

'Harry' is now a member of the PlantPAx Administrator group. Harry is an Advanced user to all areas.

4. Click OK.

IMPORTANT We recommend for a production environment to disable the Windows Administrator account and use a new PlantPAx Administrators Users Group. Do not use default passwords.

Configure Group Policy Management

We recommend group policy management as a part of the infrastructure design. Policies help reduce the maintenance and complexity when you add new users and computers into the PlantPAx® system. Once that you have configured specific policies on a domain controller, you do not have to configure the same policies on the domain computers.

The policies determine what users can and cannot do, such as password maintenance or to restrict folder access. The same approach applies for how to define server maintenance.

By carefully planning the control of multiple policies in the Active Directory environment, you can reduce the cost of system ownership. Group Policy Objects (GPOs) administer the set of policies that centralize all settings.

This chapter describes procedures to manage configurations for your domain controller. The optional techniques include the following:

- Windows Time Service with an NTP server
- Password strength configuration
- Lockout policy configuration
- Interactive logon configuration
- Group access level definition
- USB drive protection

The settings that are outlined are recommendations; your business, IT, and security requirements could require additional policies.

[Figure 8 on page 132](#) shows the topics that are described in this chapter.

Considerations

Consider the following suggestions before starting this chapter:

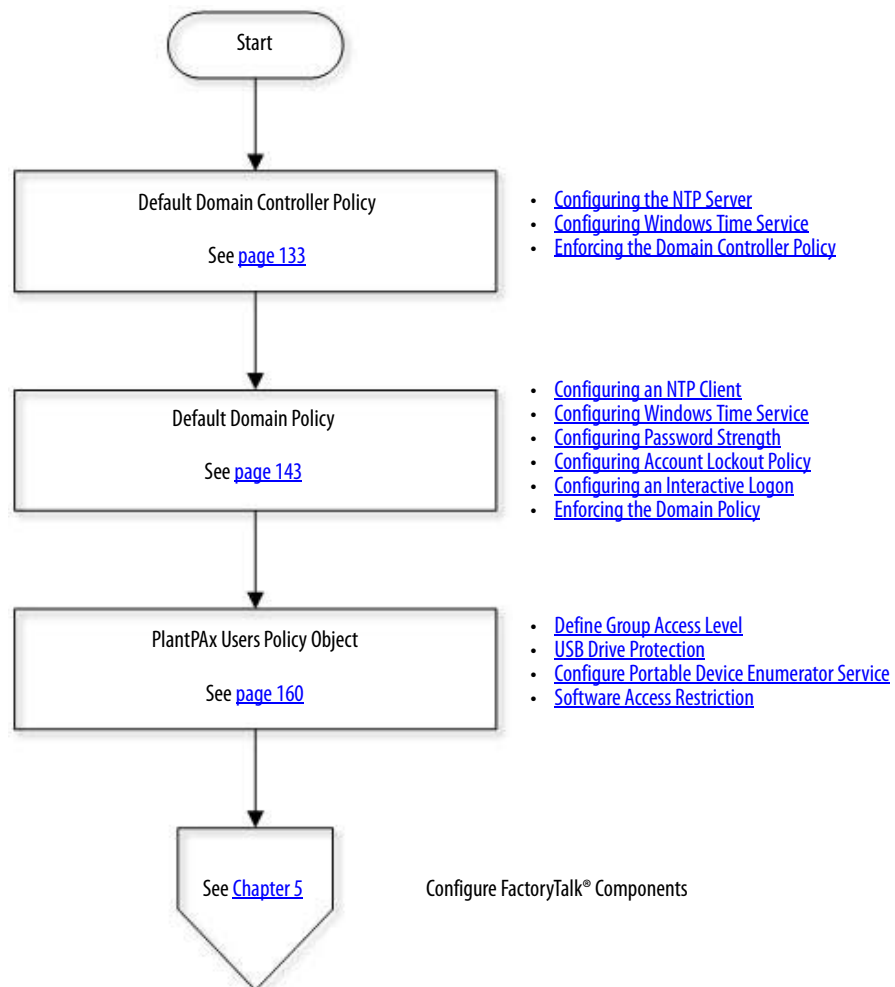
- Although this chapter offers optional configurations for domain controllers, we strongly encourage the use of the techniques for a centralized administration.
- This layer of protection does **not** supersede any anti-virus protection or other protection methods. It is best practice to have antivirus software that is installed on your PlantPAx servers and workstations.

See Knowledgebase Answer ID 35330 at

<http://www.rockwellautomation.custhelp.com> for more information on compatibility and considerations when you install antivirus software.

[Figure 8](#) contains the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 8 - Group Policy Management Workflow



Default Domain Controller Policy

Use a domain controller with these procedures.




This section describes how to configure Windows Time Service as a Network Time Protocol (NTP) server and client. The domain is responsible to propagate and enforce the clock time to the domain computers. This policy functionality helps verify that all computers are synchronized with the NTP server.

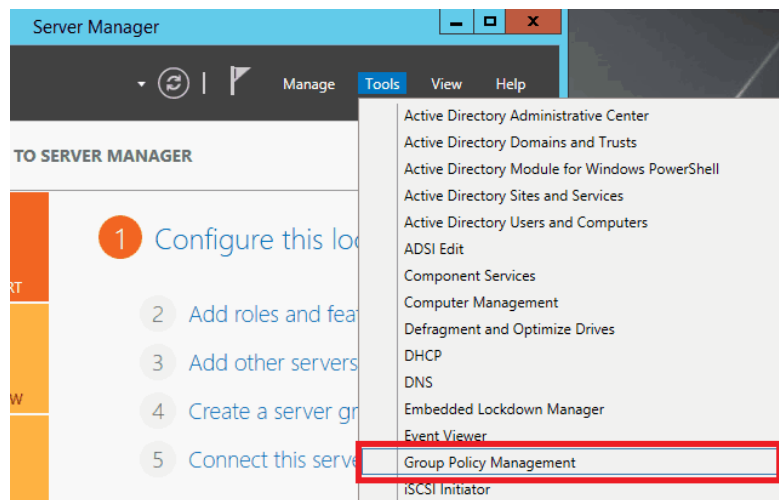
For your convenience, the procedures are presented in these subsections:

- [Configuring the NTP Server](#)
- [Configuring Windows Time Service](#)
- [Enforcing the Domain Controller Policy](#)

Configuring the NTP Server

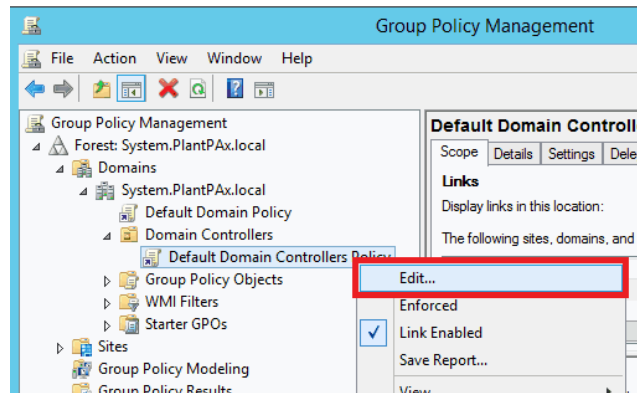
Complete these steps to edit the default domain policy to define the NTP server.

1. Click  to open the Server Manager.
2. Click Tools and choose Group Policy Management.



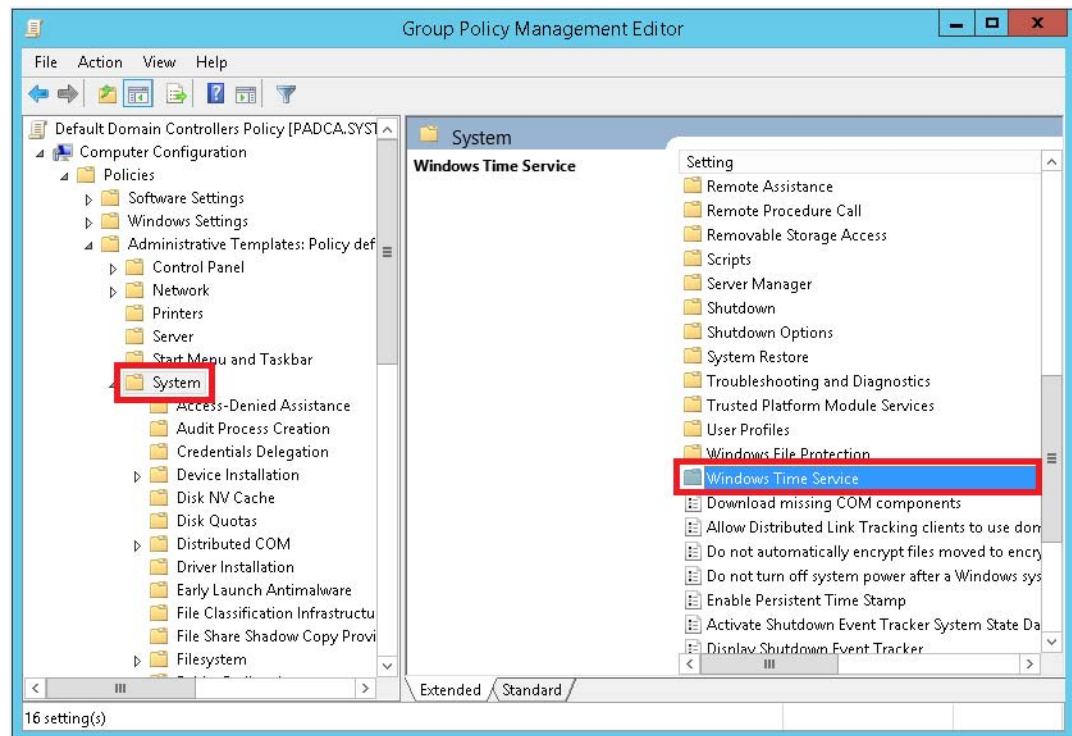
The Group Policy Management dialog box appears with the system domain.

3. Right-click Default Domain Controllers Policy and choose Edit.



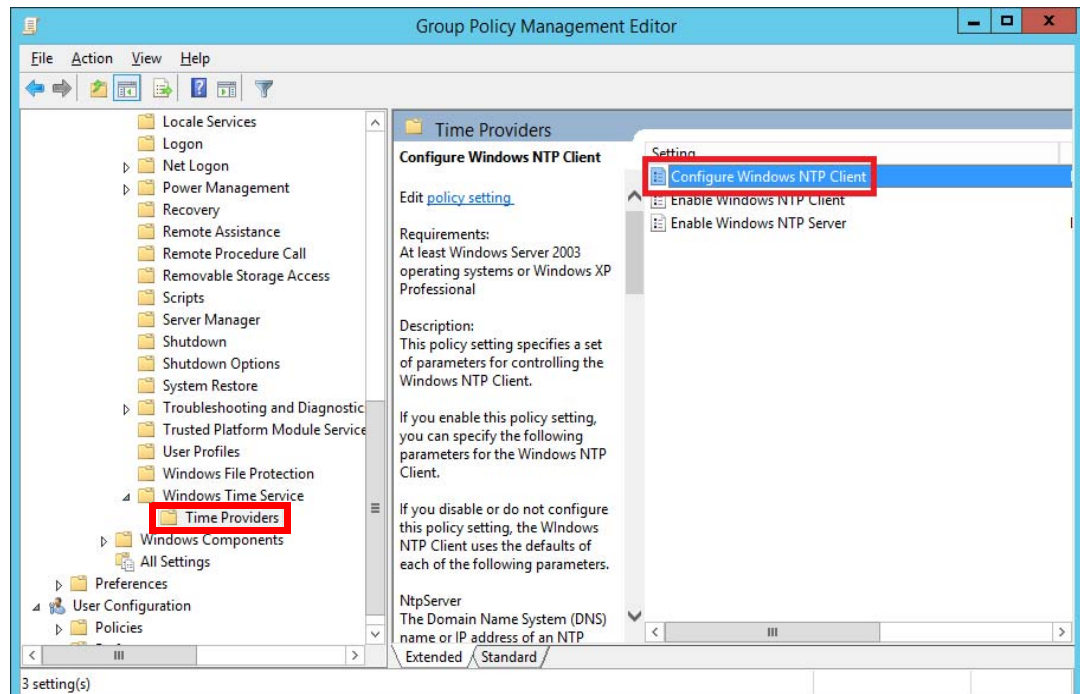
The Group Policy Management Editor dialog box appears.

4. Click to expand the Computer Configuration folder and choose Policies>Administrative Templates.
5. In the System folder, click Windows Time Service.



6. Click to expand Windows Time Service and click Time Providers.

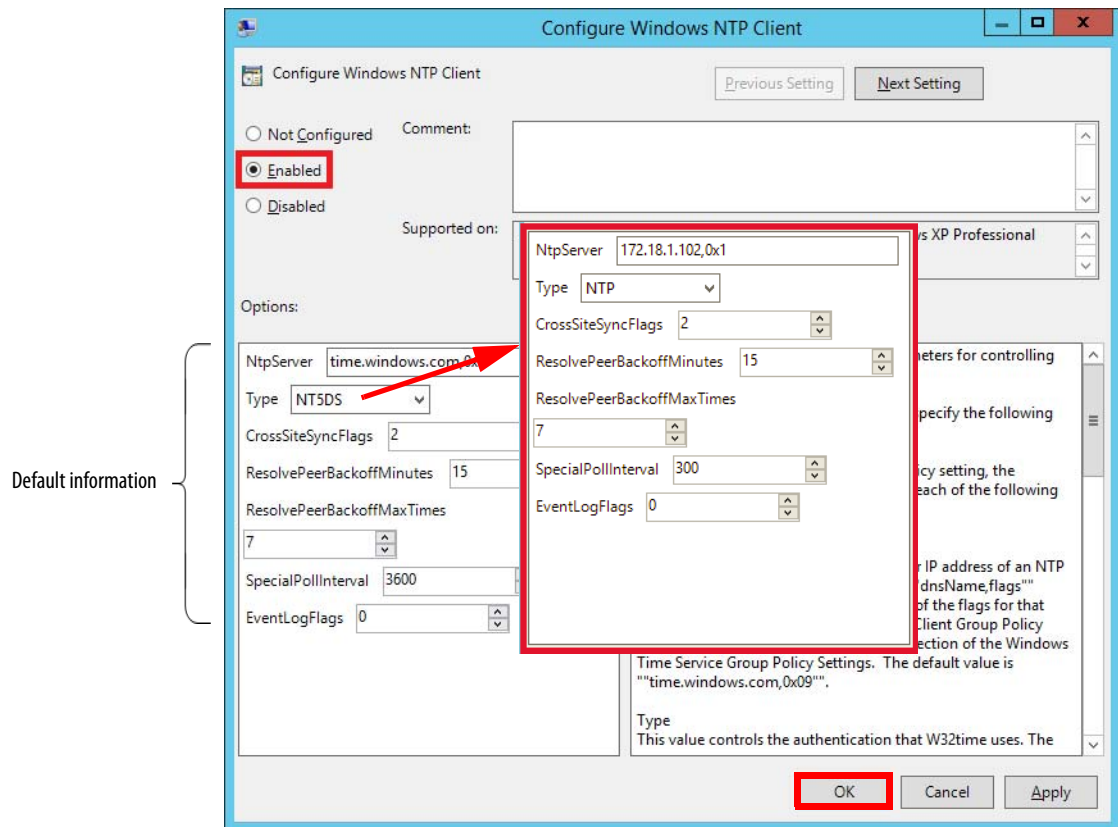
7. In the Time Providers folder, choose Configure Windows NTP Client.



The Configure Windows NTP Client dialog box appears with default information for the NTP server.

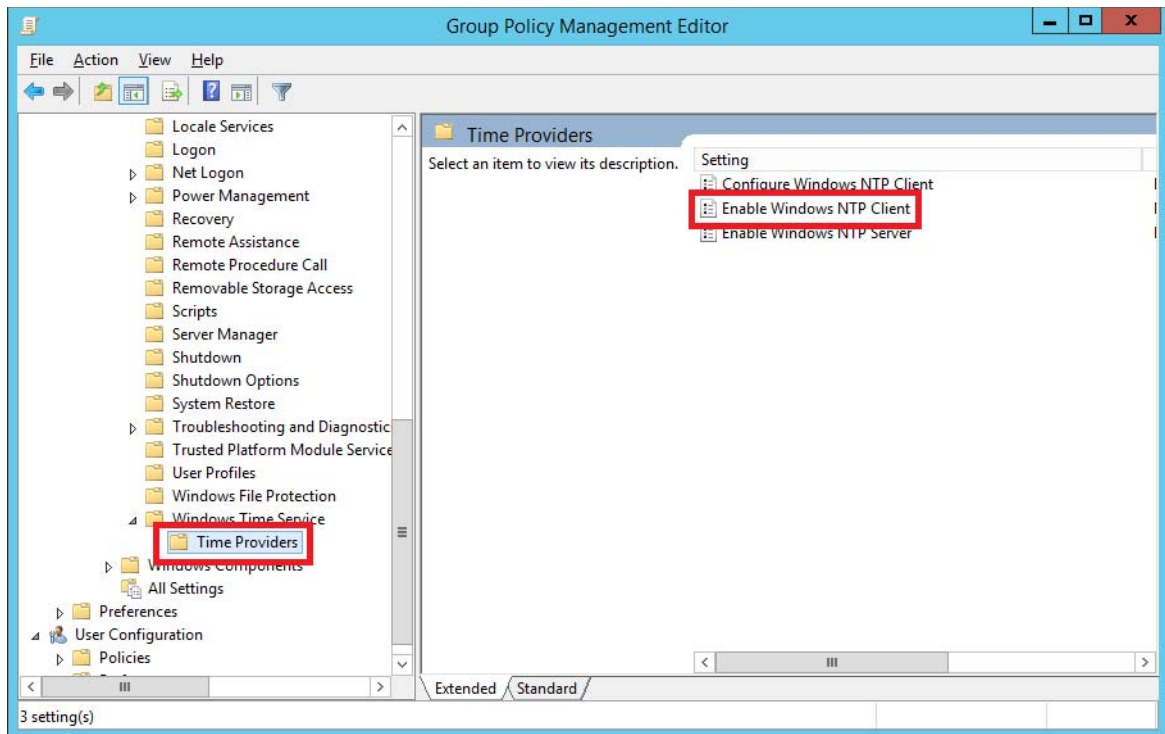
8. Click Enabled and type information as shown in the sample box.

The configuration data propagates the GPS signal through the NTP server to the domain computer.

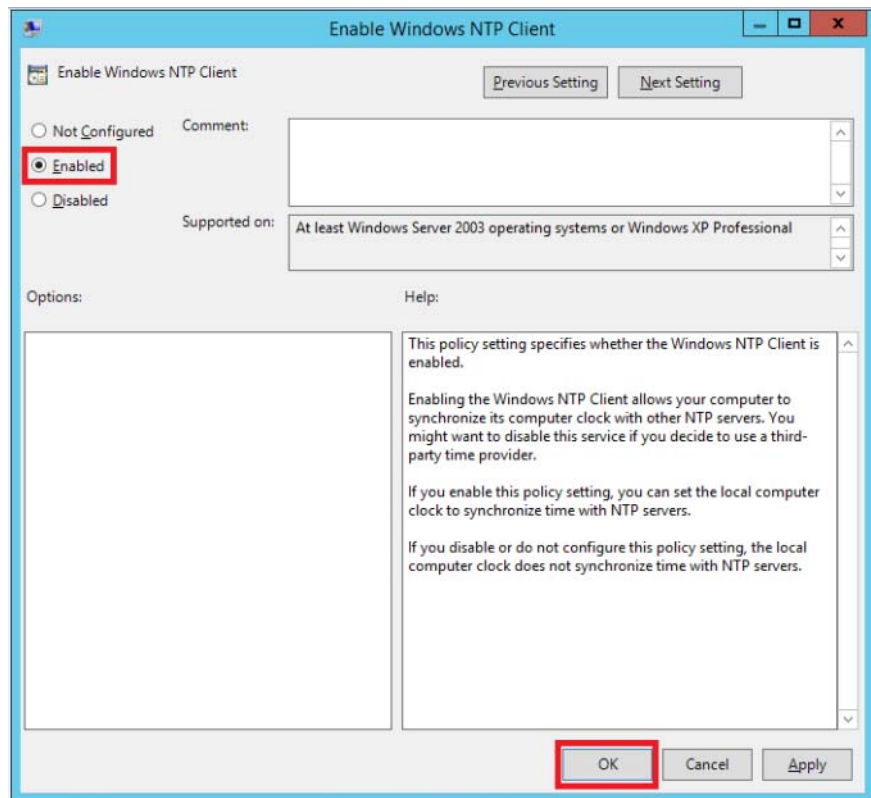


9. Click OK.

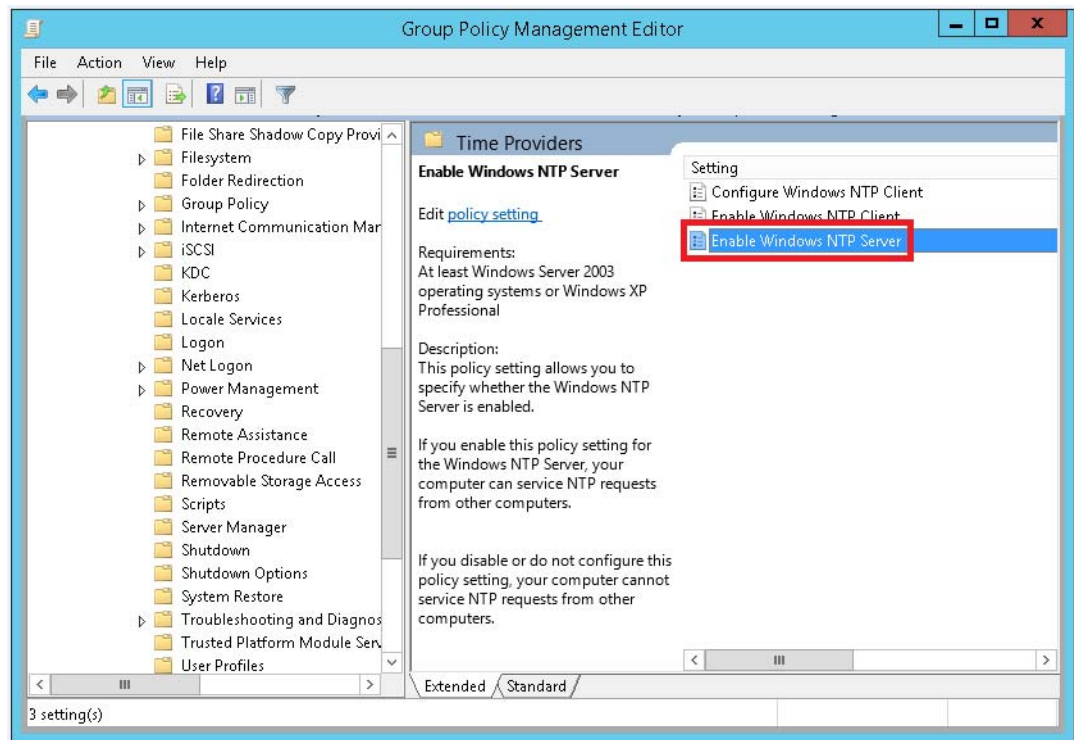
10. In the Time Providers folder, choose Enable Windows NTP Client.



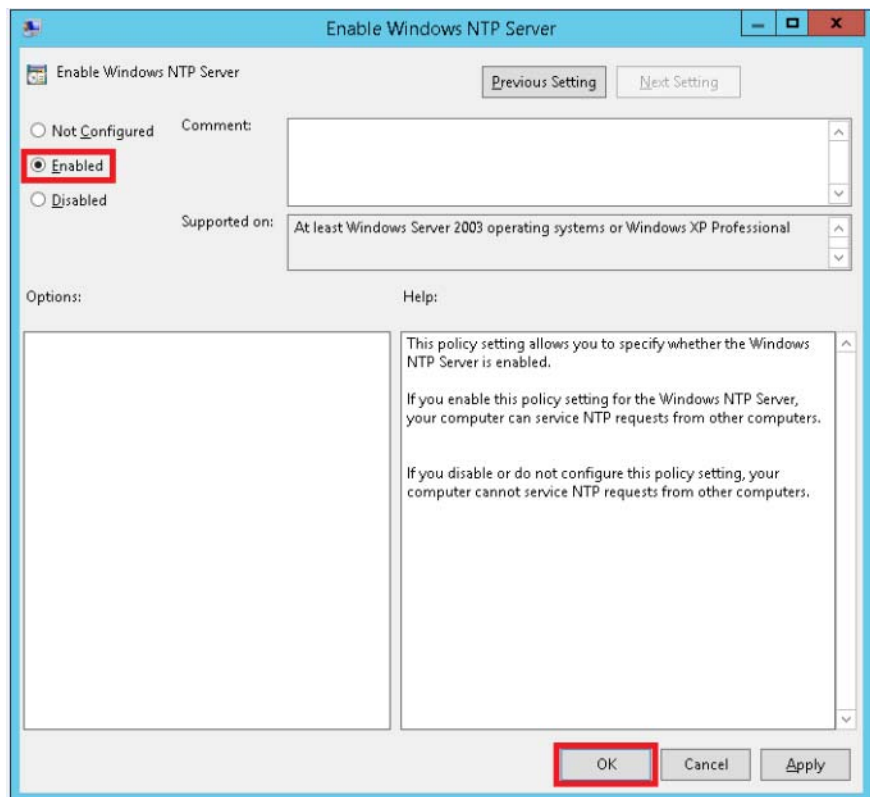
11. Click Enabled and then click OK.



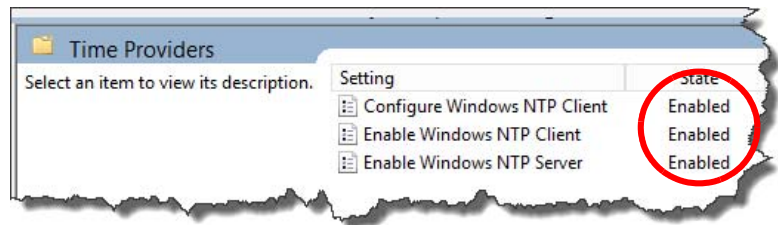
12. Click Enable Windows NTP Server.



13. Click Enabled and then click OK.



The Group Policy Management Editor reappears with the NTP server states 'enabled'



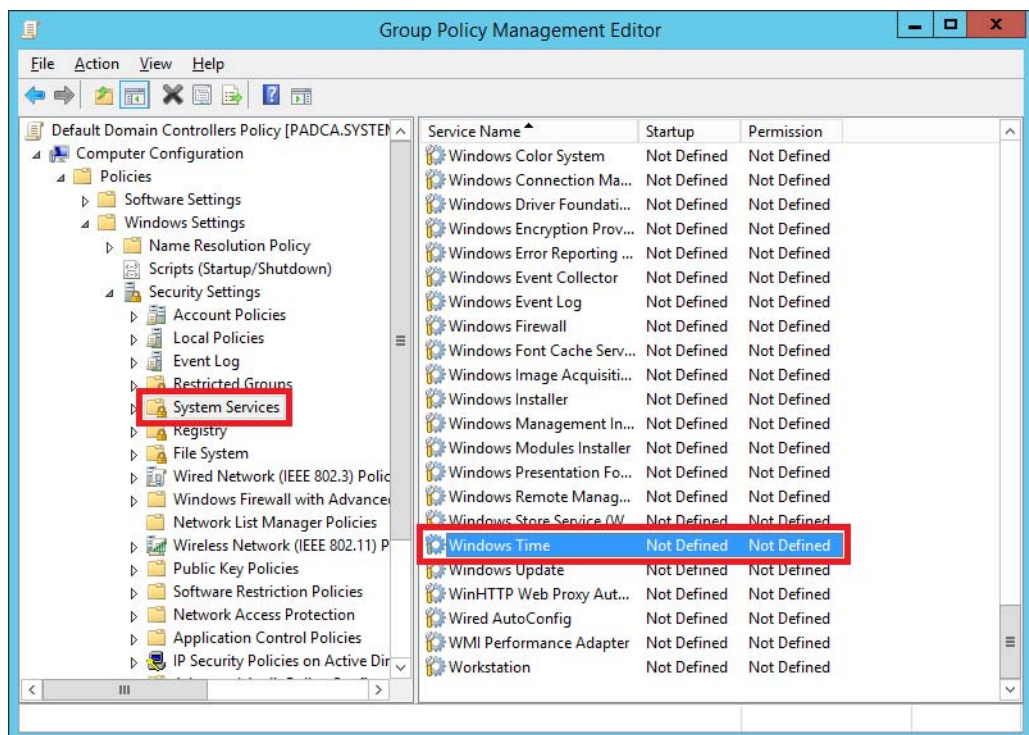
Do **not** close the Group Policy Manager Editor dialog box.

Proceed to [Configuring Windows Time Service](#) to enable the service to automatically commence on start up.

Configuring Windows Time Service

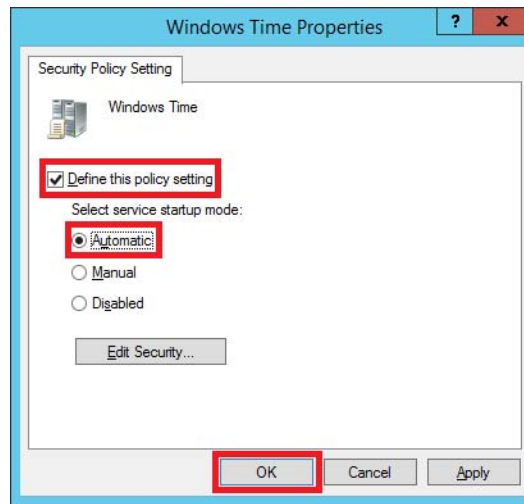
Complete these steps to enable the NTP server policy upon start up.

1. In the tree configuration of the Group Policy Manager Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings.
2. In the System Services folder, click Windows Time.



The Windows Time Properties dialog box appears.

3. Check the 'Define this policy setting' box and select 'Automatic'.



4. Click OK.
5. Close the Group Policy Management Editor dialog box.

Enforcing the Domain Controller Policy

Use a domain controller with these procedures.



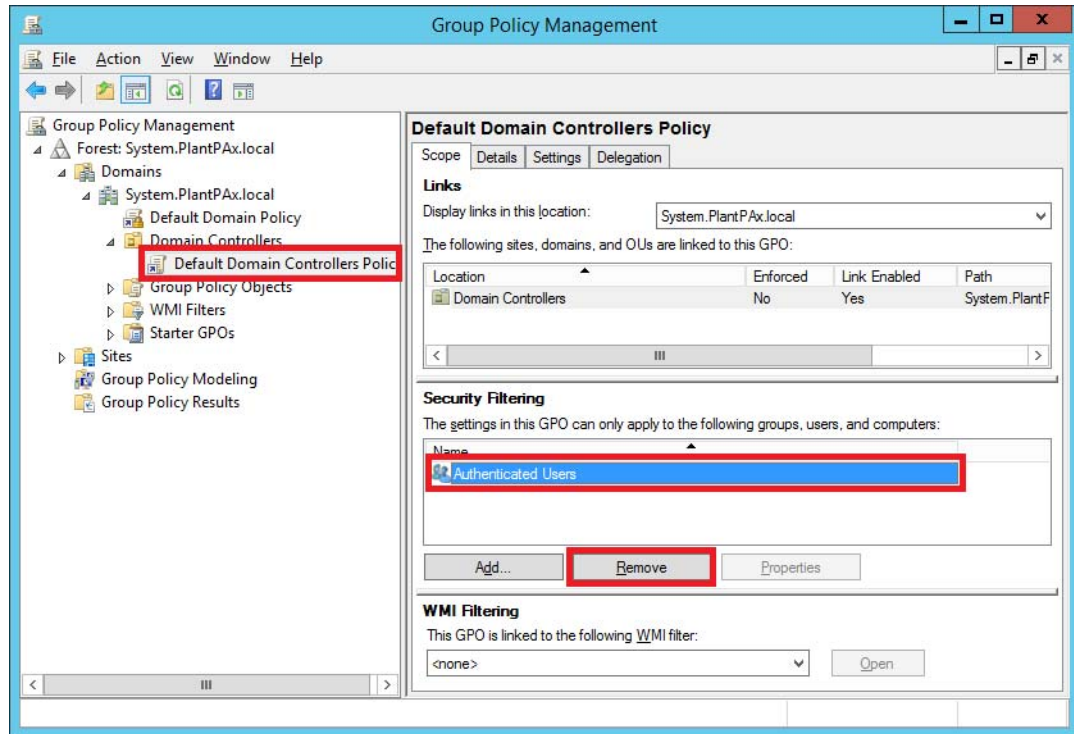
PADCA

This section describes how to enforce the domain computers to use the NTP server settings (see [page 135](#)).

Complete these steps.

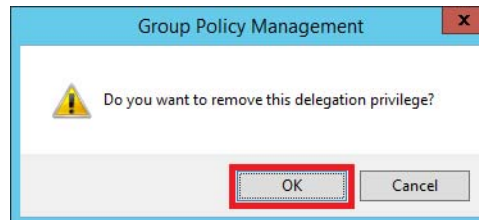
1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.

2. Expand the Domain Controllers folder and click Default Domain Controllers Policy.



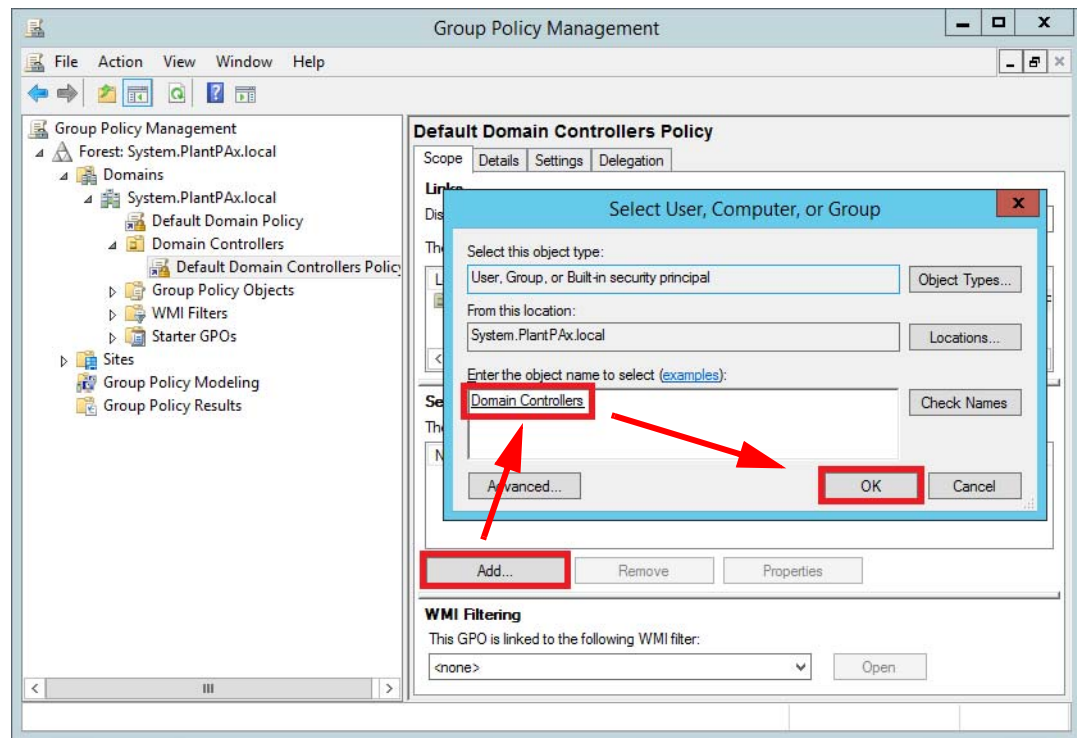
3. Choose Authenticated Users in the Security Filtering box and click Remove.

A warning popup box could appear.

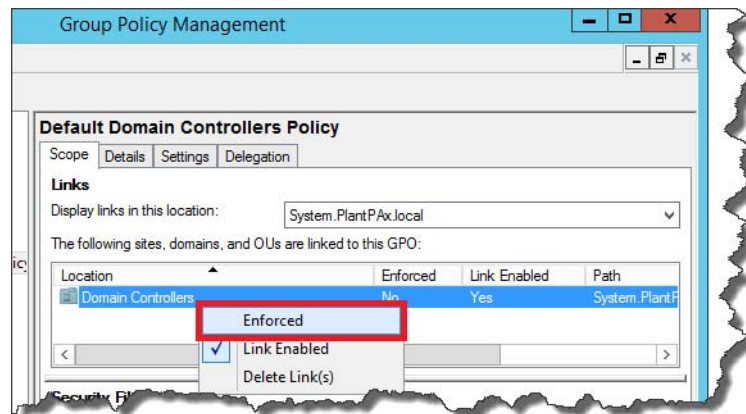


4. Click OK.

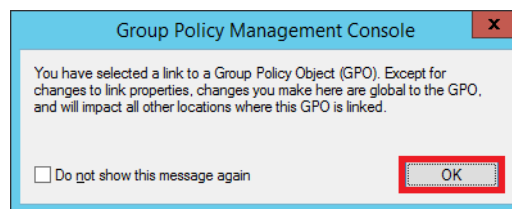
5. Click Add, Domain Controllers, and then OK.



6. Right-click Domain Controllers and choose Enforced.



A popup window appears.



7. Click OK.

Default Domain Policy

This section describes how to configure and enforce all servers and workstations to be connected to the domain controller as an NTP client server. The clock time is synchronized with the domain controller.

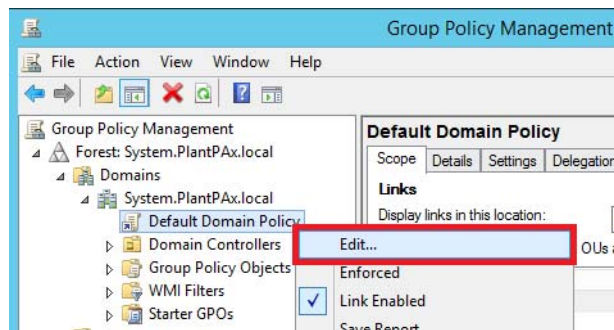
Use a domain controller with these procedures.



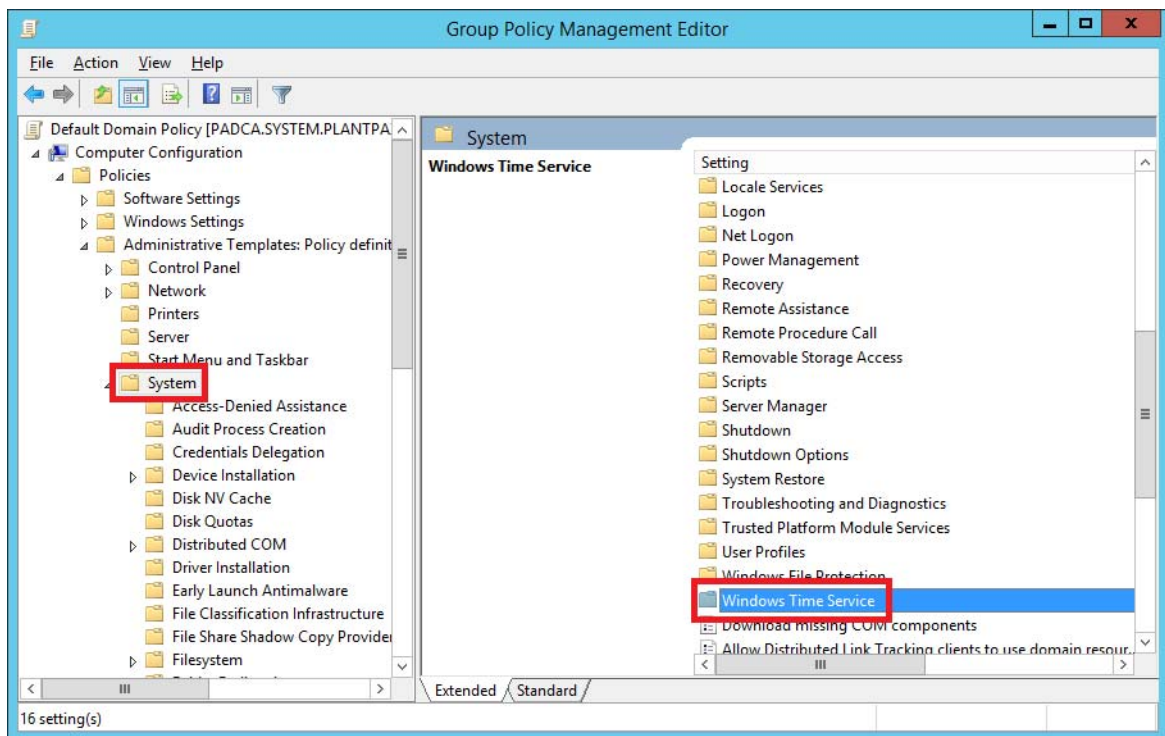
Configuring an NTP Client

Complete these steps to associate the domain controller with the NTP client server.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. Right-click Default Domain Policy and choose Edit.

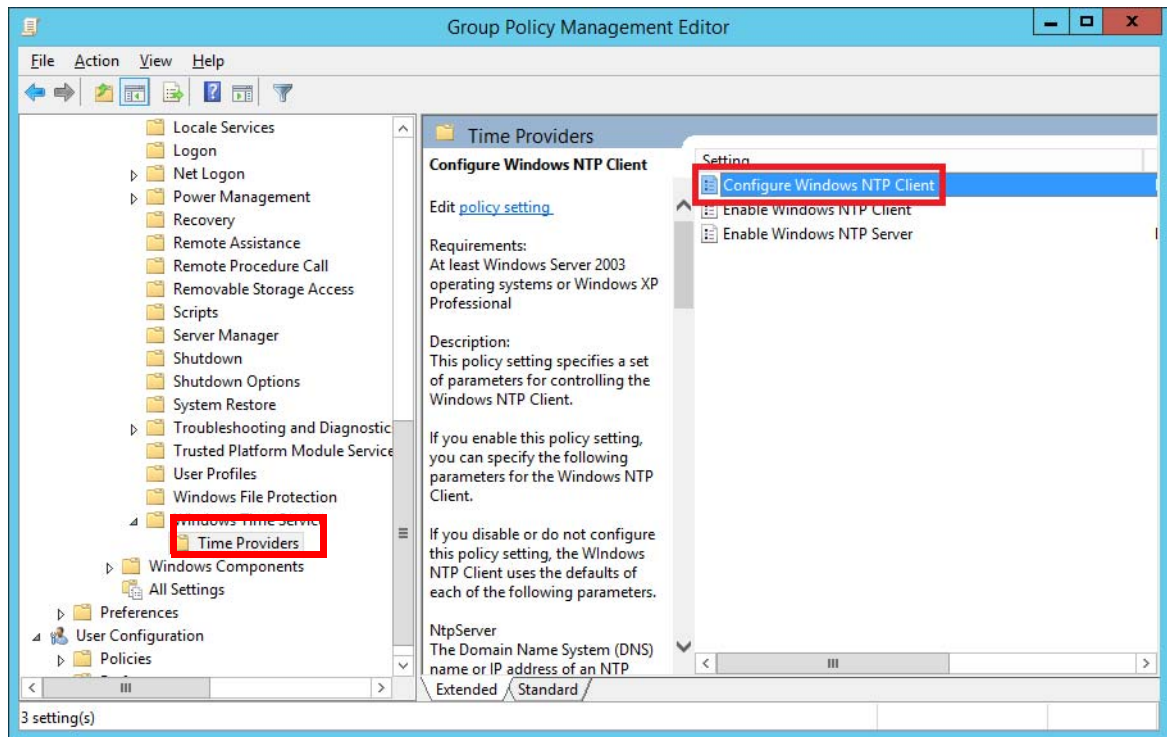


The Group Policy Management Editor dialog box appears.



3. In the tree configuration, click to expand the Computer Configuration folder and choose Policies>Administrative Templates.

4. In the System folder, click Windows Time Service.
5. Click to expand Windows Time Service and click Time Providers.
6. In the Time Providers folder, choose Configure Windows NTP Client.



- Click Enabled and type information as shown in the sample box.

The configuration data associates the domain controllers with the NTP client server.

Configure Windows NTP Client

Configure Windows NTP Client Previous Setting Next Setting

☐ Not Configured Comment:

☒ **Enabled**

☐ Disabled Supported on:

Options:

NtpServer:

Type:

CrossSiteSyncFlags:

ResolvePeerBackoffMinutes:

ResolvePeerBackoffMaxTimes:

SpecialPollInterval:

EventLogFlags:

Help:

This policy setting specifies a set of parameters for controlling the Windows NTP Client.

If you enable this policy setting, you can specify the following parameters for the Windows NTP Client.

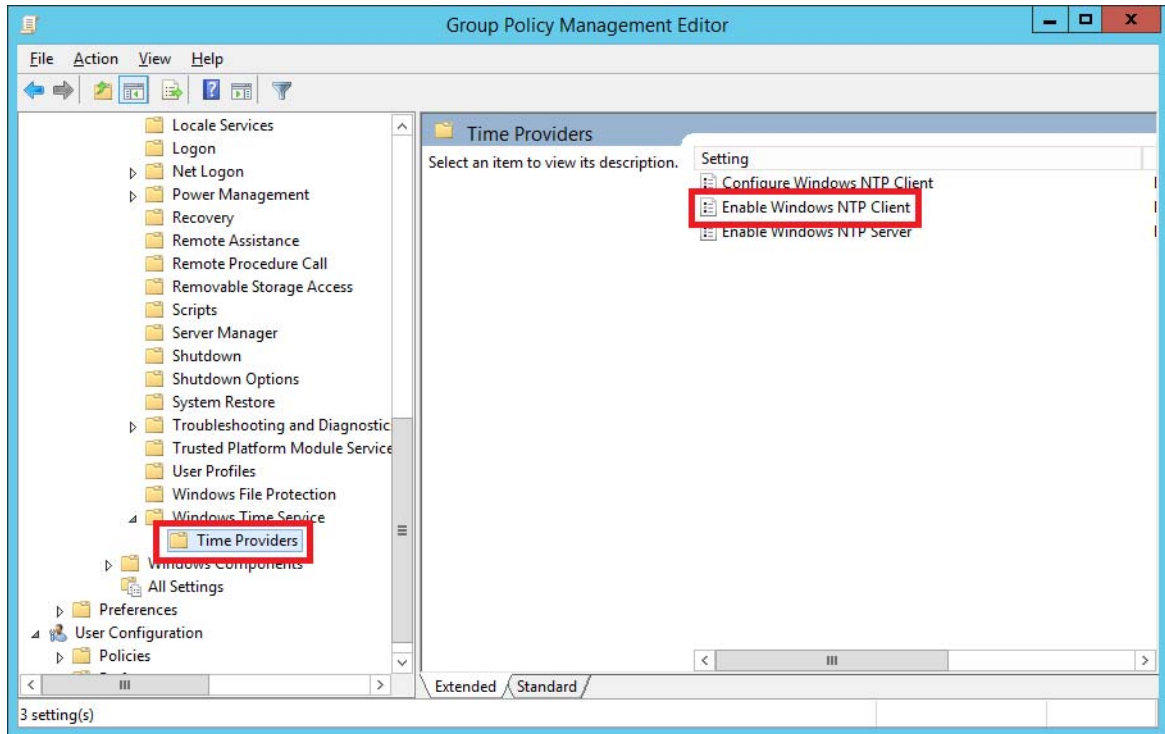
If you disable or do not configure this policy setting, the Windows NTP Client uses the defaults of each of the following parameters.

NtpServer
The Domain Name System (DNS) name or IP address of an NTP time source. This value is in the form of ""dnsName.flags"" where ""flags"" is a hexadecimal bitmask of the flags for that host. For more information, see the NTP Client Group Policy Settings Associated with Windows Time section of the Windows Time Service Group Policy Settings. The default value is ""time.windows.com,0x09"".

Type
This value controls the authentication that W32time uses. The

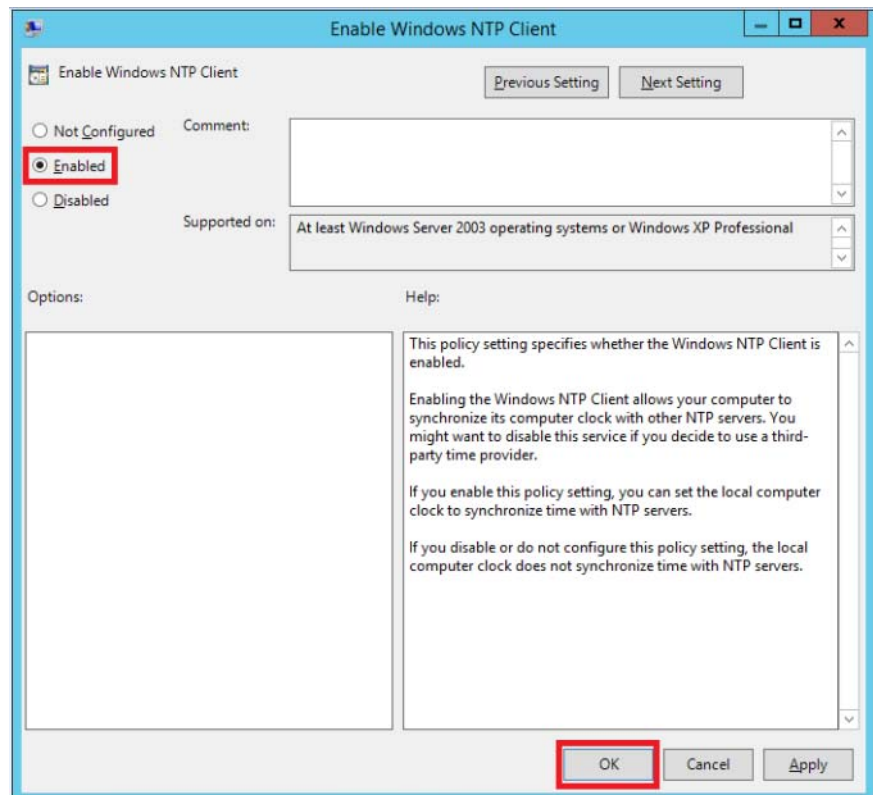
OK Cancel Apply

8. Click Time Providers (in the Windows Time Service folder) and click Enable Windows NTP Client.

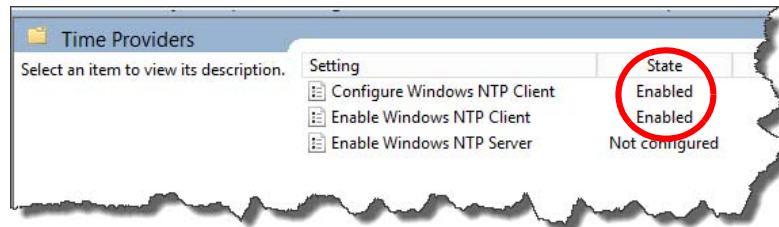


The Enable Windows NTP Client dialog box appears.

9. Click Enabled and then click OK.



The Group Policy Management Editor reappears with the NTP Client-server states 'enabled.'



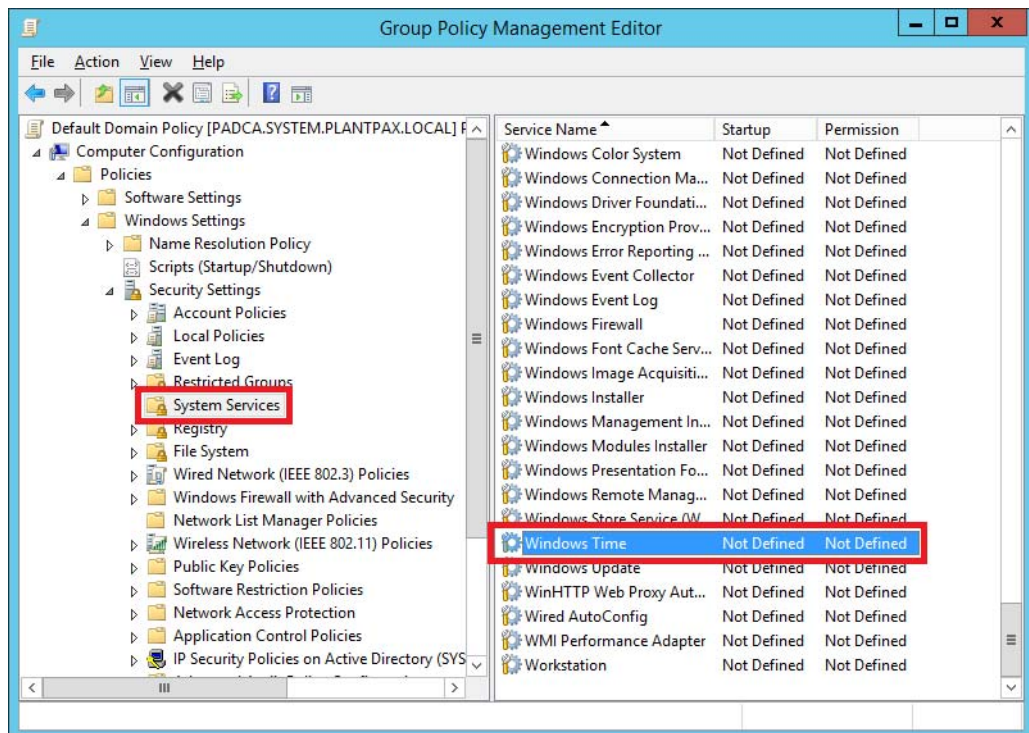
Do **not** close the Group Policy Manager Editor dialog box.

Proceed to [Configuring Windows Time Service](#) to enable the service to automatically commence on start up.

Configuring Windows Time Service

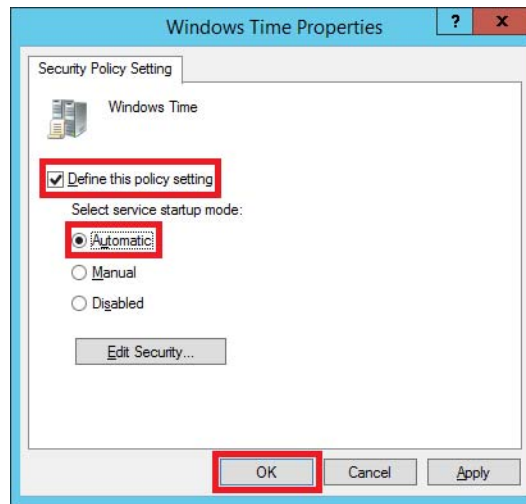
Complete these steps to enable the NTP server policy upon start up.

1. In the tree configuration of the Group Policy Management Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings.
2. In the System Services folder, click Windows Time.



The Windows Time Properties dialog box appears.

3. Check the 'Define this policy setting' box and select 'Automatic'.



4. Click OK.
5. Close the Group Policy Management Editor dialog box.

Configuring Password Strength

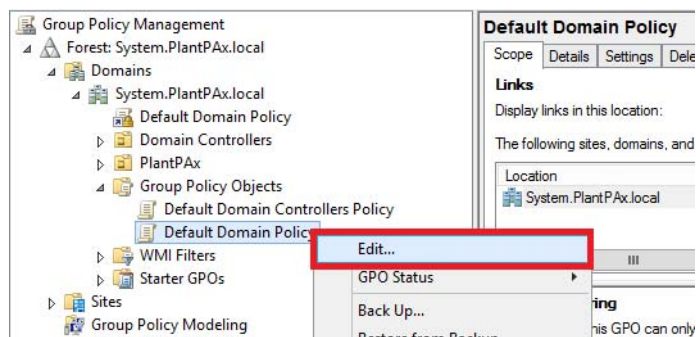
Use a domain controller with these procedures.



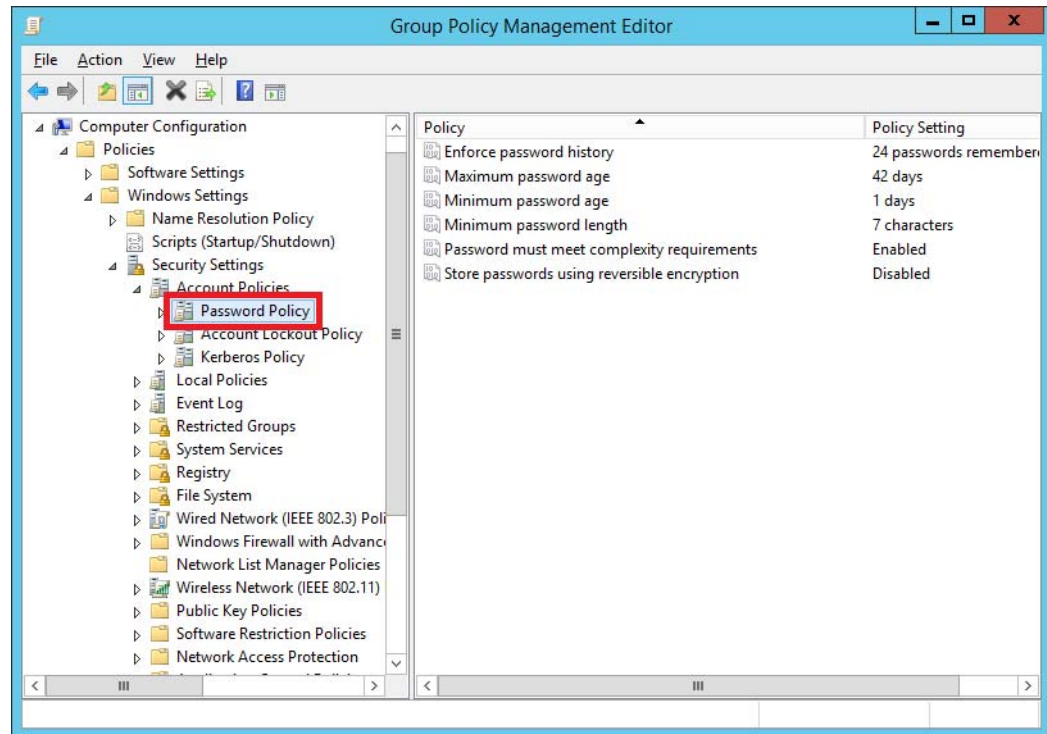
PADCA

The password policy makes sure that security settings are enforced to help protect the system from unauthorized users upon entering the system.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. Right-click Default Domain Policy and choose Edit.



3. In the tree configuration of the Group Policy Management Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings>Account Policies.
4. Click the Password Policy folder and choose one of the policy options that are explained in [Table 19](#).

**Table 19 - Password Policy Description**

Policy	Description
Enforce password history	Complexity requirements are enforced when passwords are changed or created. These requirements include that the password cannot contain the user's account name, parts of the user's full name that exceed two consecutive characters, or a certain length of time that is exceeded before a similar password can be used.
Maximum password age	Security setting that determines the length of time before a password needs to be changed. Best practice is for password to expire 30...90 days to help prevent attacks.
Minimum password age	Minimum password age must be less than the maximum password age. For example, if the maximum password age is 1...999 the minimum password age can be up to 998 days.
Minimum password length	Security setting that determines the least number of characters for a password. Typically, the value of characters is set between 1...14. Zero characters if no password is required.
Password must meet complexity requirements	Security setting determines the minimum requirements to meet complexity requirements. For example, some uppercase or lowercase characters, base 10 digits (0...9), or non-alphabetical characters.
Store passwords using reversible encryption	Reversible encryption is used for password authentication. Microsoft recommends that this protocol be disabled because it's the same as storing plain text versions of the passwords. Microsoft states to use this policy only if 'application requirements outweigh the need to protect password information'.

5. Save your work.

Configuring Account Lockout Policy

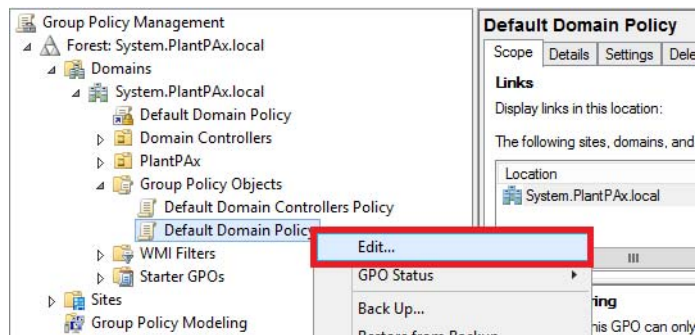
Use a domain controller with these procedures.



PADCA

This policy provides the ability to configure the number of password attempts and how an administrator resolves a user lockout situation.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. Right-click Default Domain Policy and choose Edit.



3. In the tree configuration of the Group Policy Management Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings>Account Policies.
4. Click the Account Lockout Policy folder and choose one of the policy options that are explained in [Table 20](#).

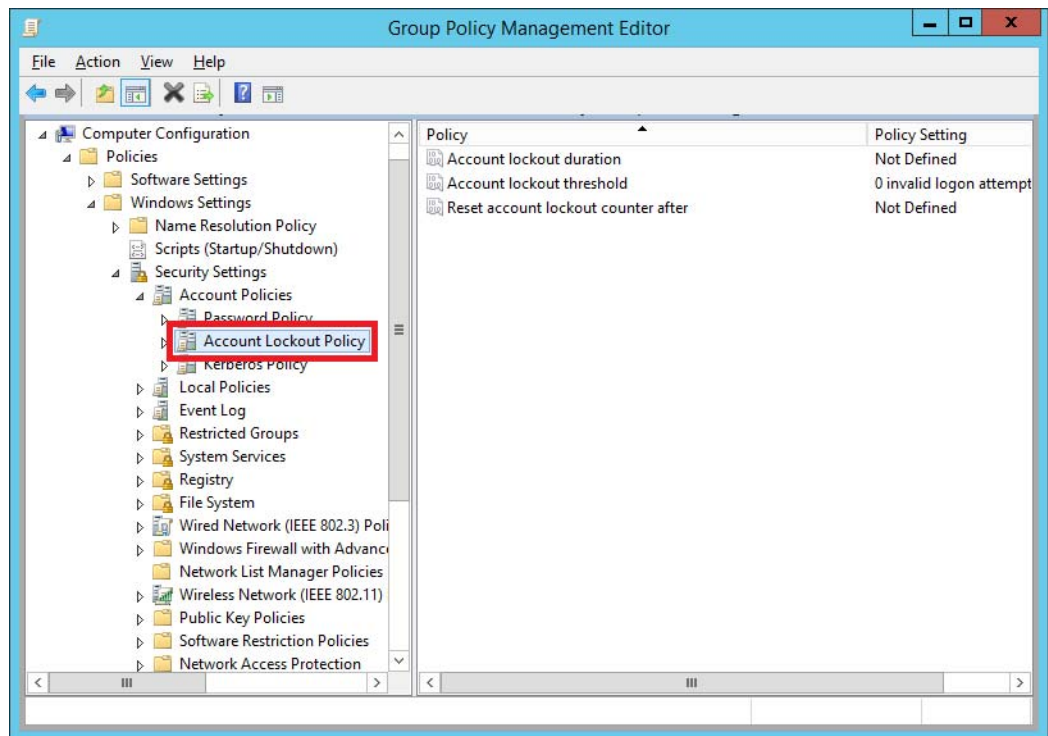
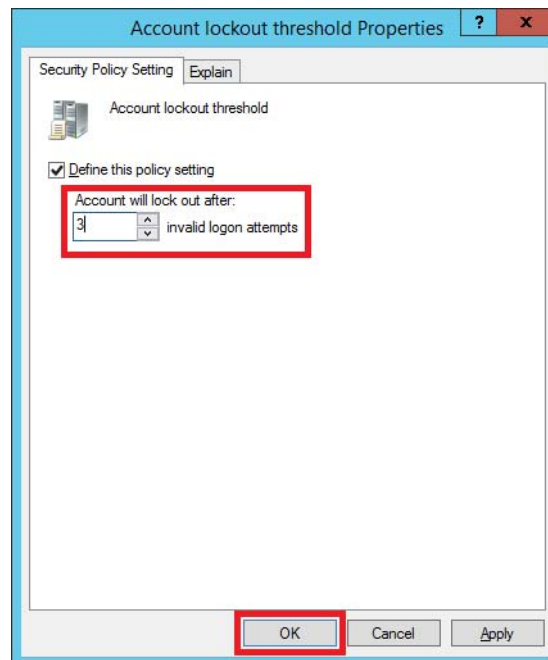


Table 20 - Lockout Policy Descriptions

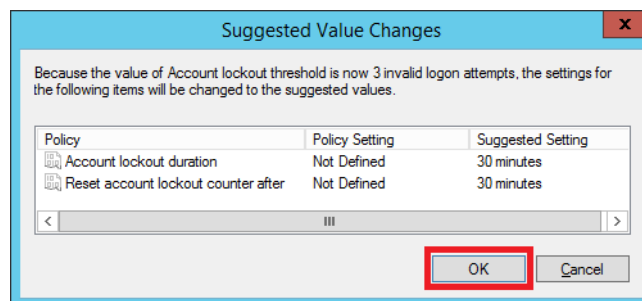
Policy	Description
Account lockout duration	A locked out account cannot be activated until reset by an administrator or the duration period for the lockout has elapsed.
Account lockout threshold	This setting determines the number of failed logon attempts to cause a user account to be locked out. You can set a value between 0...999 failed logon attempts. If you set the value to 0, an account is prevented from being locked out.
Reset account lockout counter after	Setting specifies an amount of time that must expire before a lockout reactivates.

5. To set the number of lockout attempts before a lockout, double-click Account lockout threshold.
6. On the Account lockout threshold Properties dialog box, click the arrows Up or Down to set the number of invalid logon attempts.



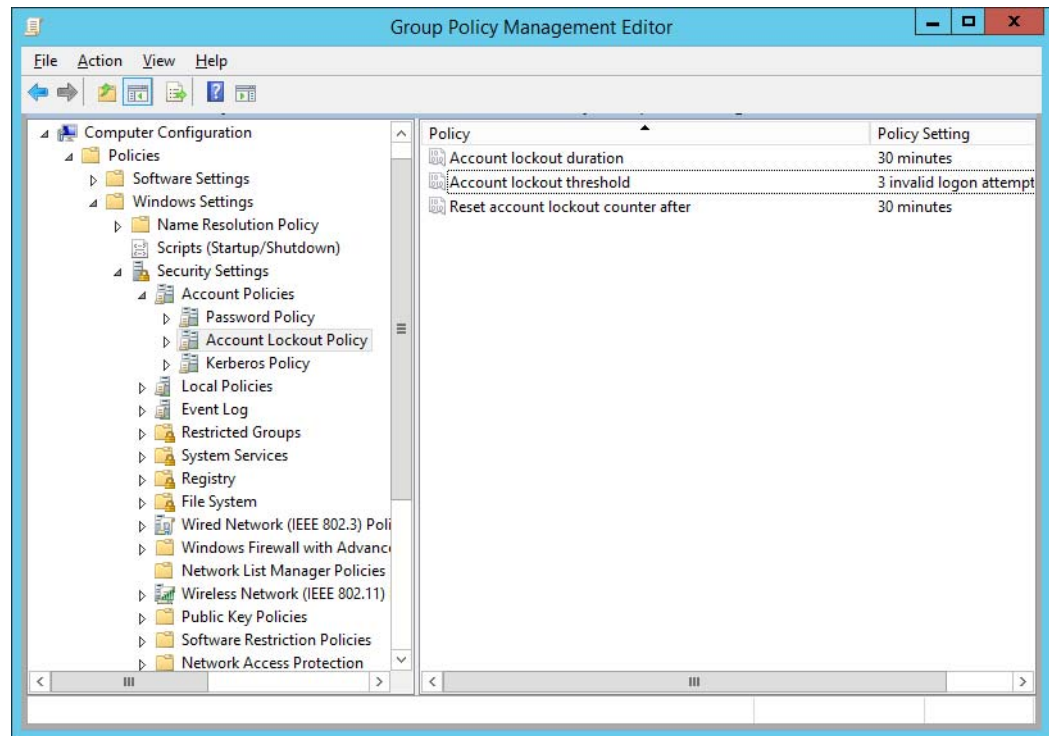
7. Click OK.

The Suggested Value Changes popup window appears with default time settings based on your number of lockout attempts.

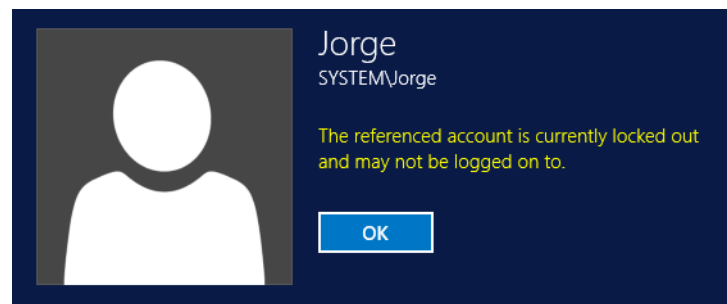


8. Click OK.

The lockout configurations can be monitored on the Group Policy Management Editor dialog box.



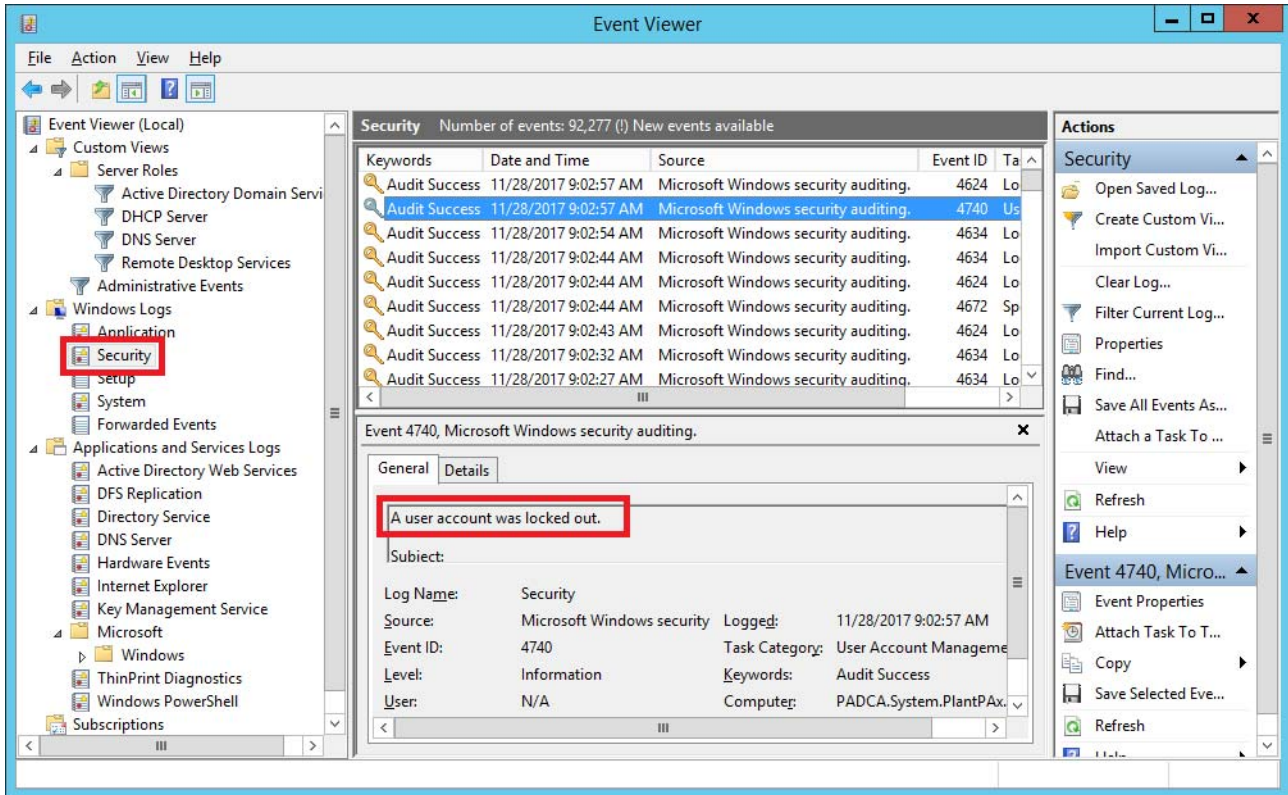
The example shows what a user receives when the configured number of failed logon attempts occurs.



Administrator Security Audit

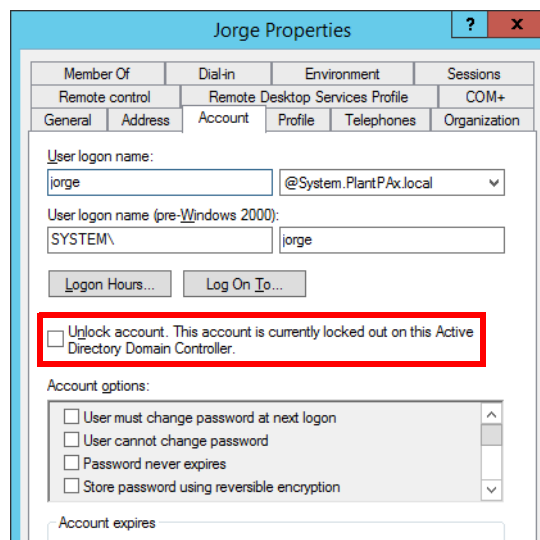
This section describes how administrators can audit logout situations and unlock personnel accounts. Complete these steps.

1. On the Event Viewer dialog box, right-click Security and choose an account.



The user account information appears.

In the Domain controller, the lockout information appears in the Account tab of a user's Properties dialog box.



Configuring Kerberos Policy

Use a domain controller with these procedures.



PADCA

Complete these steps to administer network authentication.

1. In the tree configuration of the Group Policy Management Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings>Account Policies.
2. Click the Kerberos Policy folder and choose one of the policy options that are described in [Table 21](#).

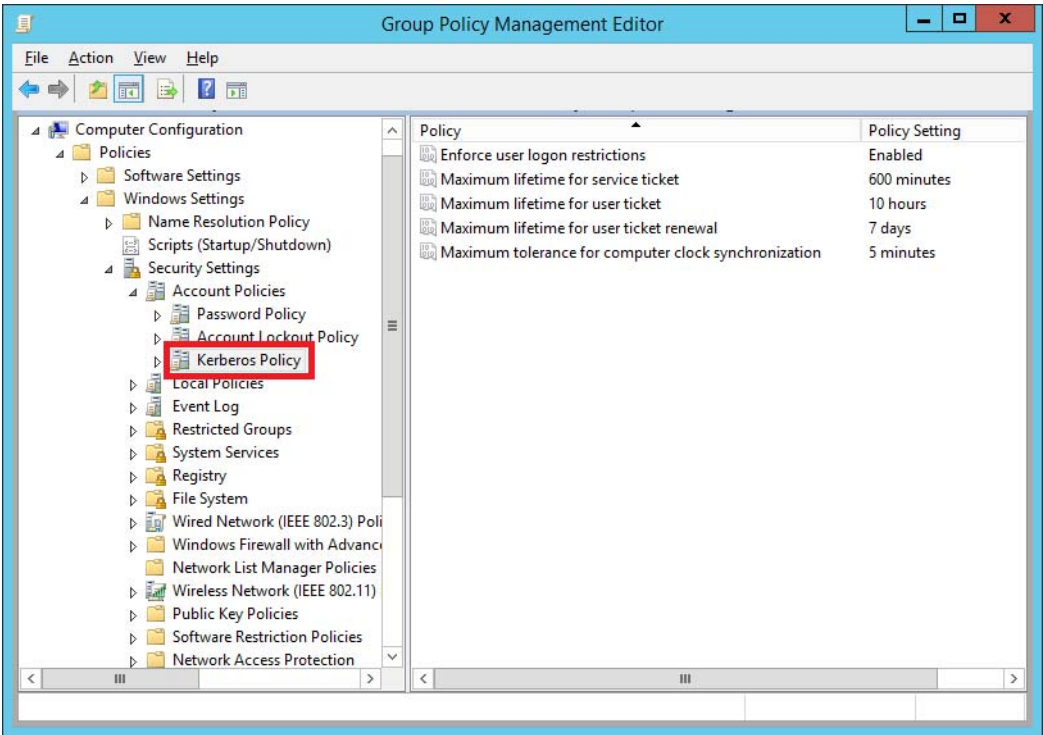


Table 21 - Kerberos Policy Descriptions

Policy	Description
Enforce user logon restrictions	Security setting determines if the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional; the extra step takes time and could slow network access to services. The default is Enabled.
Maximum lifetime for service ticket	Security setting determines the maximum amount of time (in minutes) that a granted session ticket is used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for Maximum lifetime for user ticket. If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message. The client must request a new session ticket from the Kerberos V5 Key Distribution Center (KDC). Once a connection is authenticated, it no longer matters whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket that is used to authenticate the connection expires during the connection. The default amount of time is 600 minutes (10 hours).

Table 21 - Kerberos Policy Descriptions

Policy	Description
Maximum lifetime for user ticket	Security setting determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) can be used. The default amount of time is 10 hours.
Maximum lifetime for user ticket renewal	Security setting determines the time (in days) during which a user's ticket-granting ticket (TGT) can be renewed. The default is 7 days.
Maximum tolerance for computer clock synchronization	Security setting determines the maximum time difference (in minutes) that Kerberos V5 tolerates between the time on the client clock and the time on the domain controller running Windows Server 2003 that provides Kerberos authentication. To prevent 'replay attacks', Kerberos V5 uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client and the domain controller need to be in sync as much as possible. Both computers must be set to the same time and date. Because the clocks of two computers are often out of sync, administrators can use this policy to establish the maximum acceptable difference to Kerberos V5 between a client clock and domain controller clock. If the difference between a client clock and the domain controller clock is less than the maximum time difference that is specified in this policy, any time stamp that is used in a session between the two computers is considered to be authentic. IMPORTANT: This setting is not persistent on pre-Vista platforms. If you configure this setting and then restart the computer, this setting reverts to the default value. The default is 5 minutes.

3. Save your work.

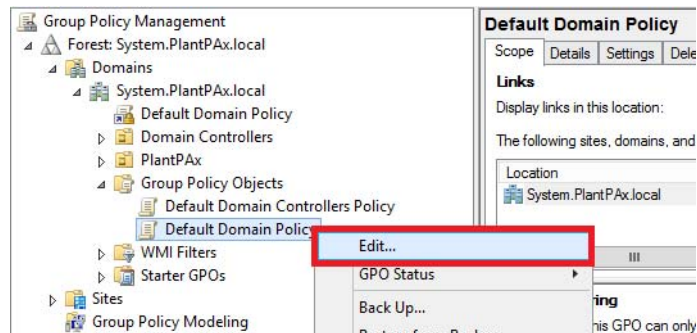
Configuring an Interactive Logon

Use a domain controller with these procedures.

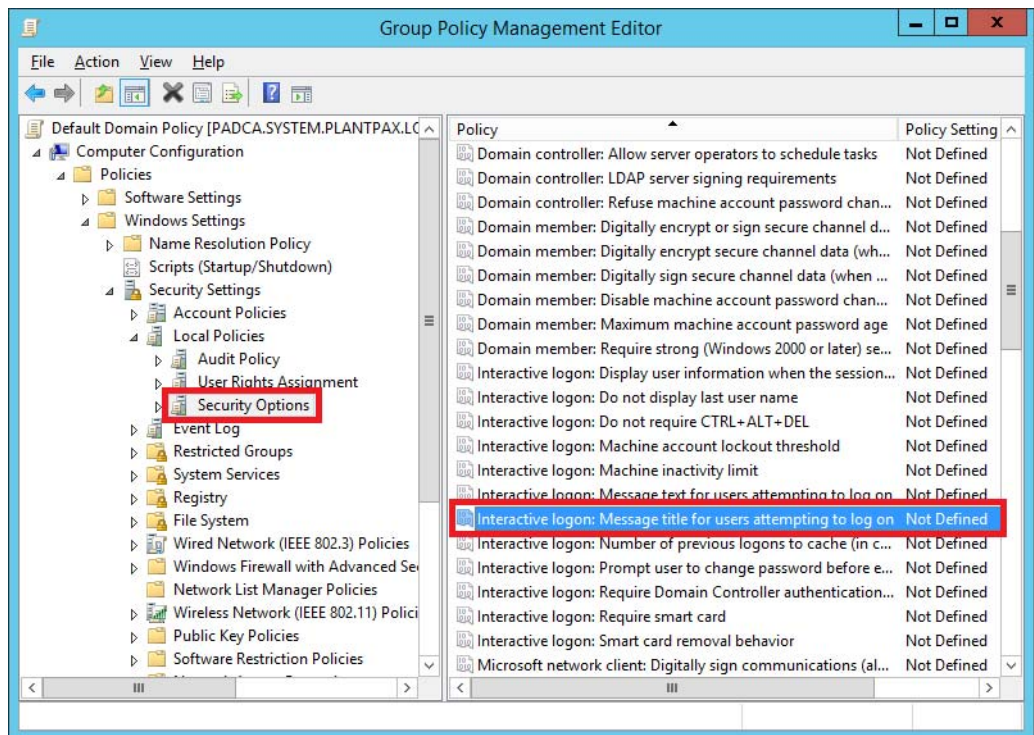


This policy configures a warning message to users of the consequences for misusing company information. The policy is typically used for legal purposes.

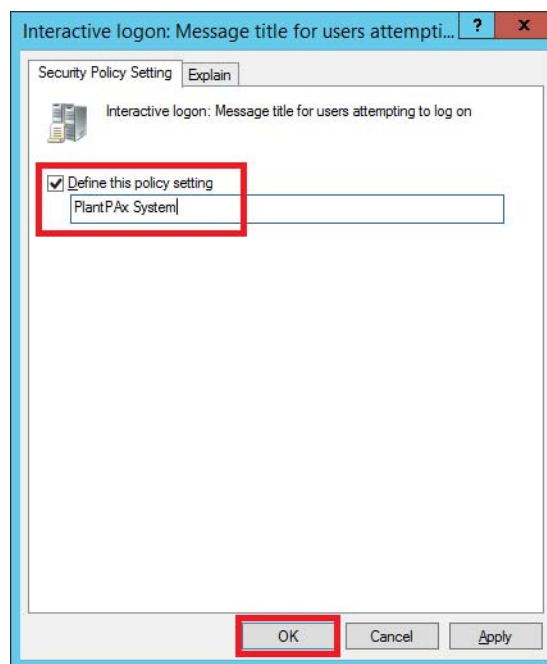
1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. Right-click Default Domain Policy and choose Edit.



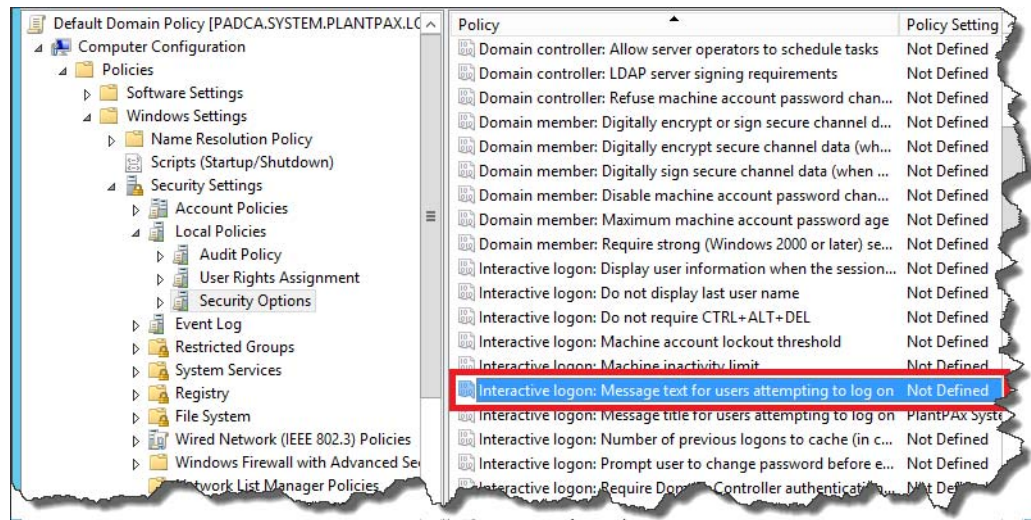
3. In the tree configuration of the Group Policy Management Editor dialog box, click to expand the Computer Configuration folder and choose Policies>Windows Settings>Security Settings>Local Policies.
4. Click the Security Options folder and choose a policy option.



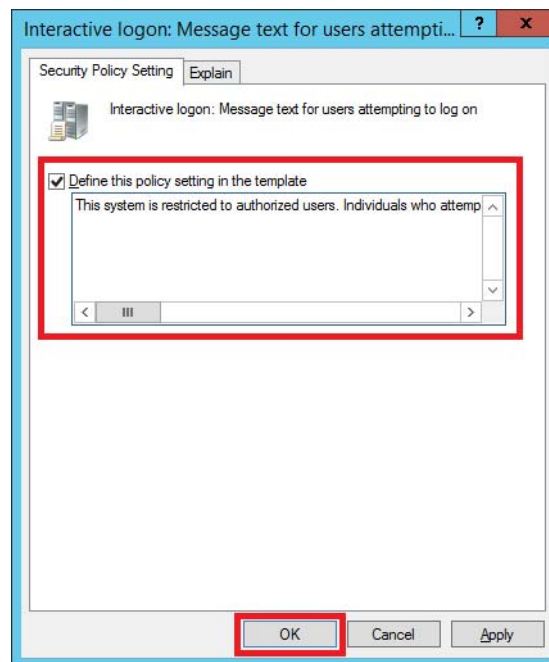
5. Type the name of the group that receives the interactive message and click OK.



6. Double-click the message text.

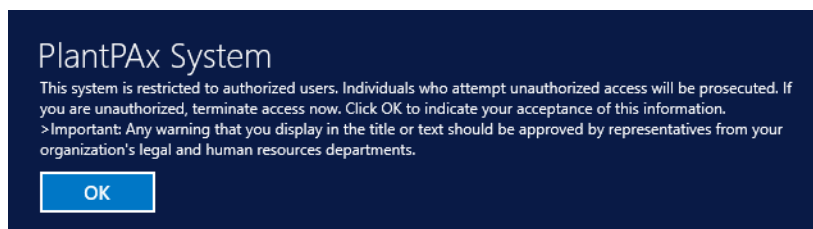


A message text dialog box appears to let you write and edit the template.



7. Click OK.

The example shows the interactive message that appears to users during logon.



Use a domain controller with these procedures.

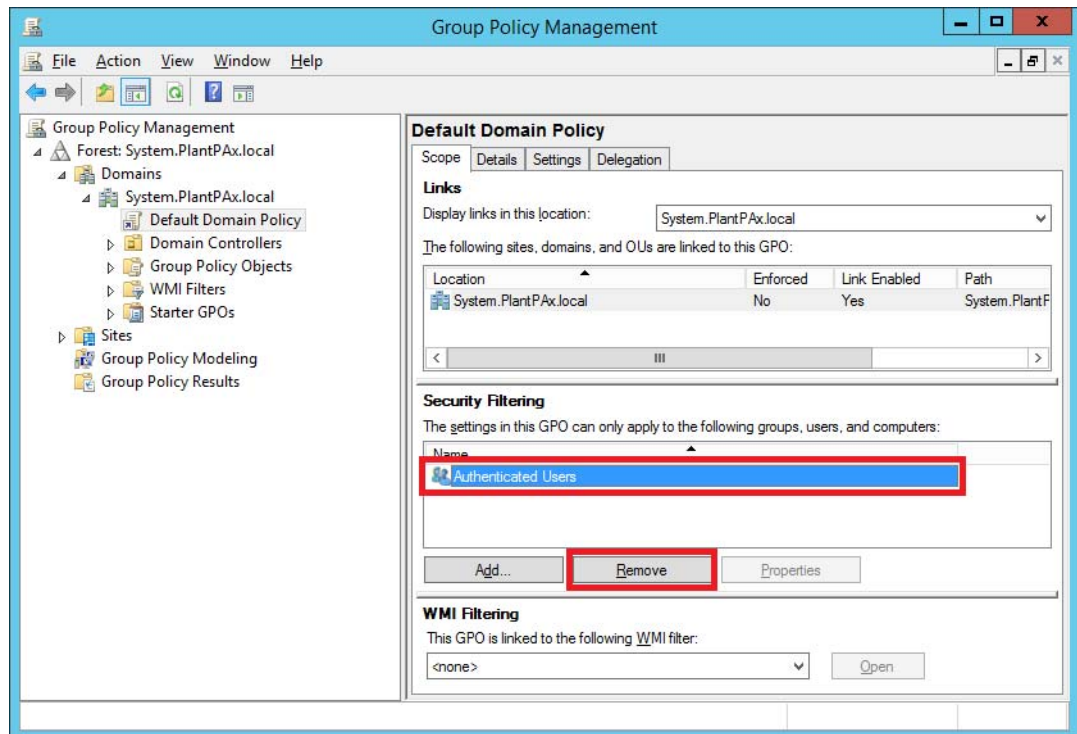


Enforcing the Domain Policy

This section describes how to enforce the servers and workstations that are associated with the domain controller to use the NTP client settings (see [page 145](#)).

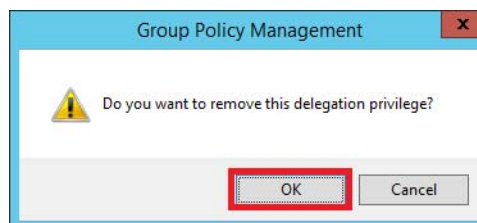
Complete these steps.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. Expand the domain folder and click Default Domain Policy.



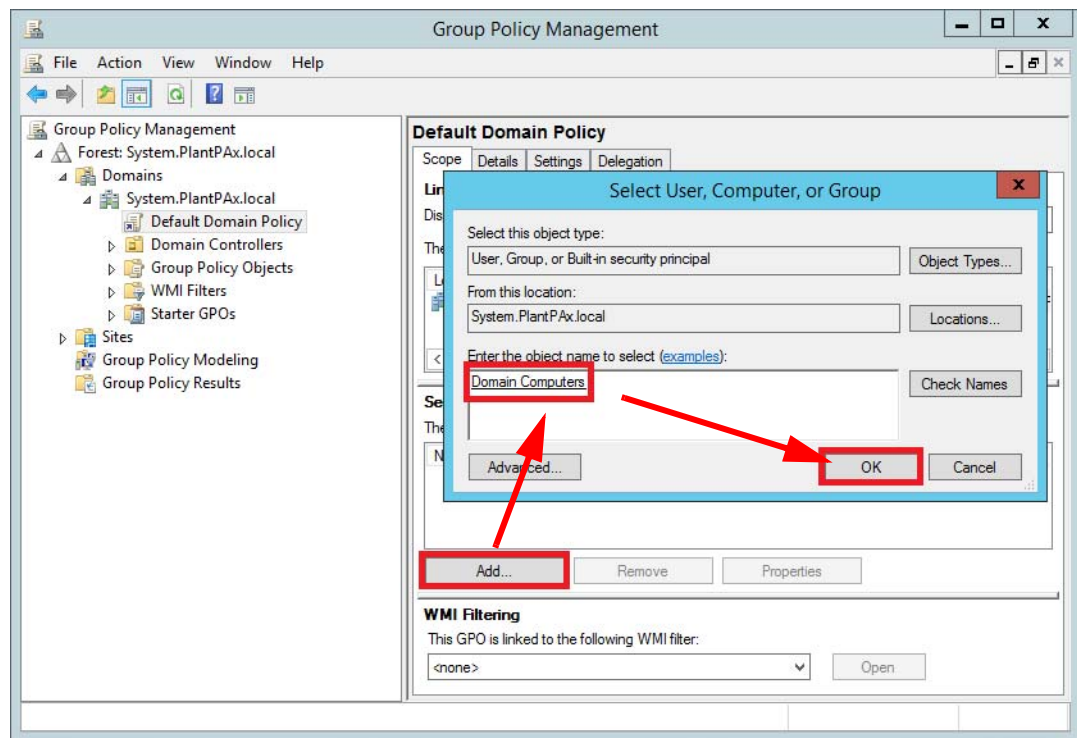
3. Choose Authenticated Users in the Security Filtering box and click Remove.

A warning popup box could appear.

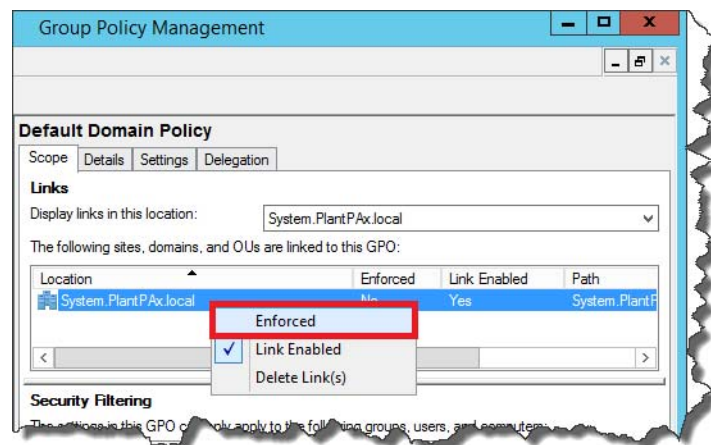


4. Click OK.

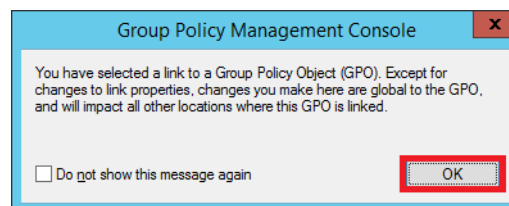
5. Click Add, type an object, and then click OK.



6. Right-click the domain and choose Enforced.



A popup window could appear.



7. Click OK.

PlantPax Users Policy Object

You can create policies for a group of users that restricts privileges and site access. This section describes how to select a group and enforce a policy. For example, a selected group of users cannot use USB drives for system security.

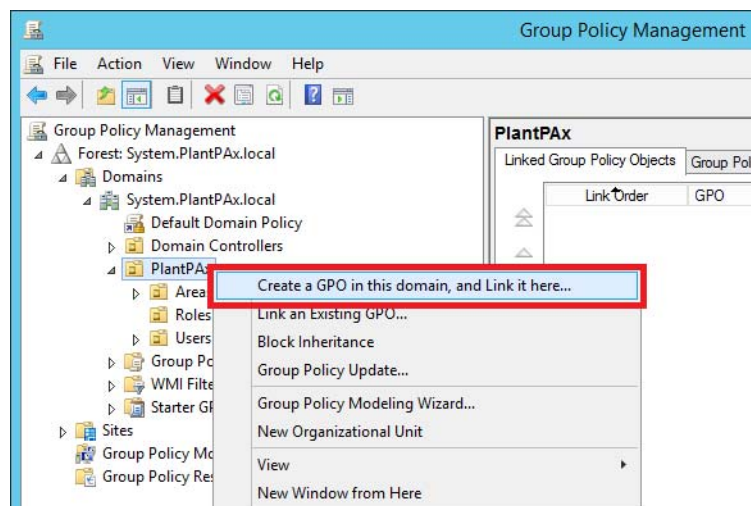
Use a domain controller with these procedures.



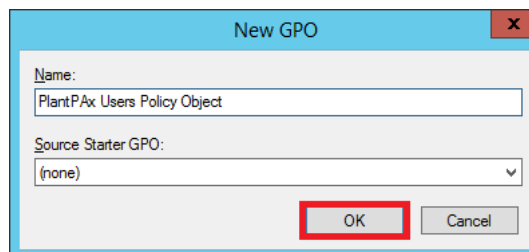
Define Group Access Level

Complete these steps to select a specific group of users to link to a policy.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. In the system domain folder, right-click a domain name and choose Create a GPO in this domain, and Link it here.



3. Type a name for the Group Policy Object.



4. Click OK.

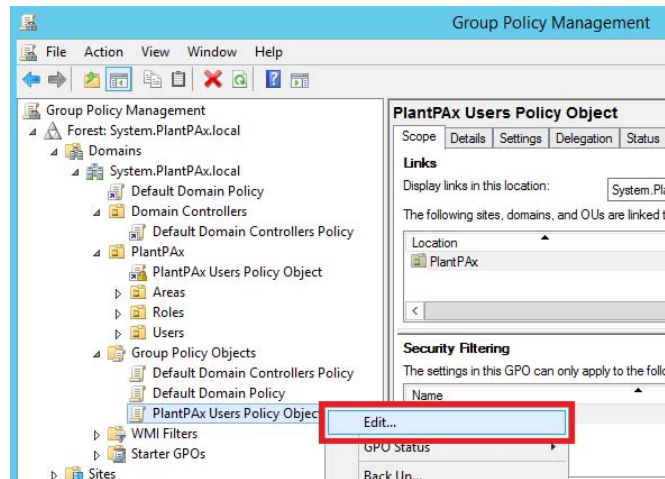
Use a domain controller with these procedures.



USB Drive Protection

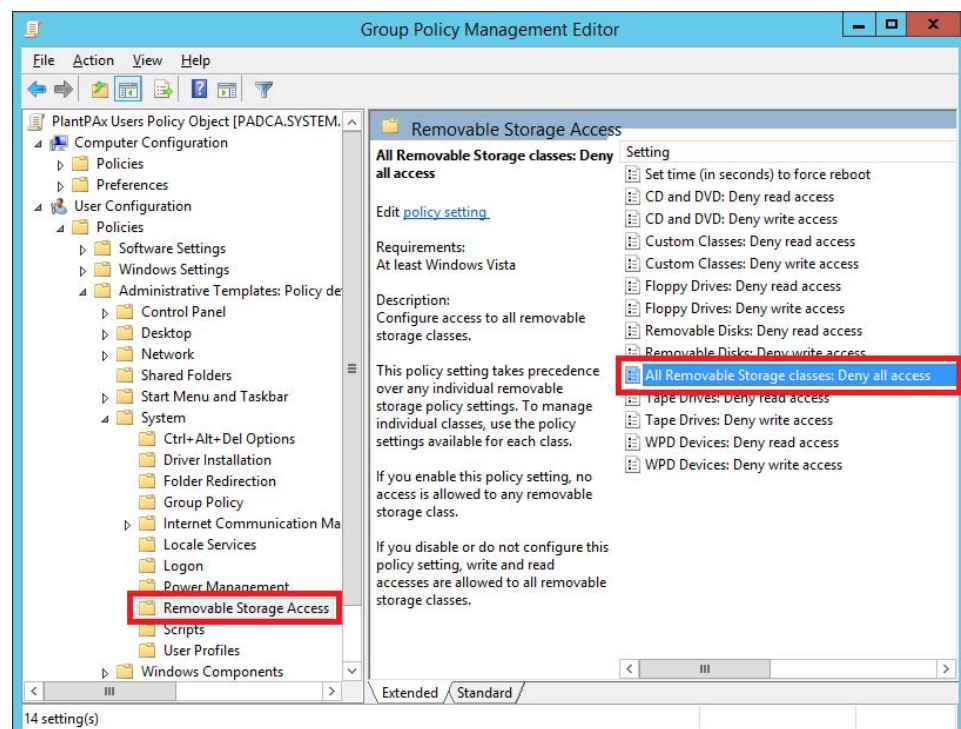
Complete these steps to restrict a group of users from using a USB drive.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. In the system domain folder, click Group Policy Objects, right-click PlantPax Users Policy Objects and choose Edit.

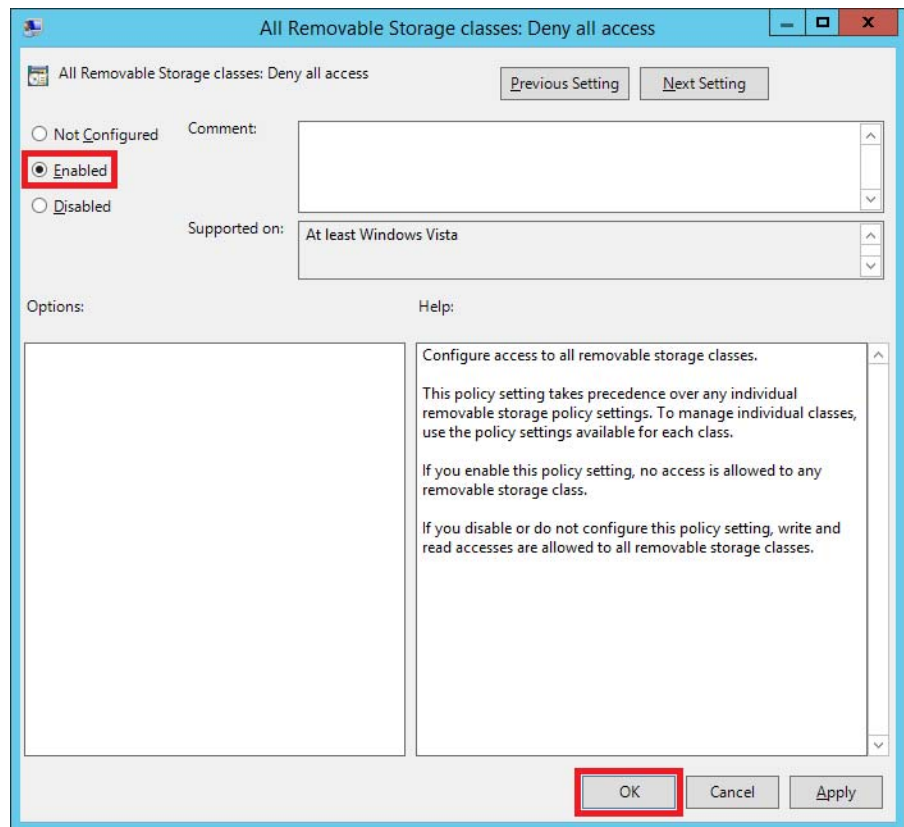


The Group Policy Management Editor dialog box appears.

3. Click to expand the Computer Configuration folder and choose User Configuration>Policies>Administrative Templates>System.
4. Click Removable Storage Access and choose All Removable Storage classes: Deny all access.



5. Click Enabled and OK.



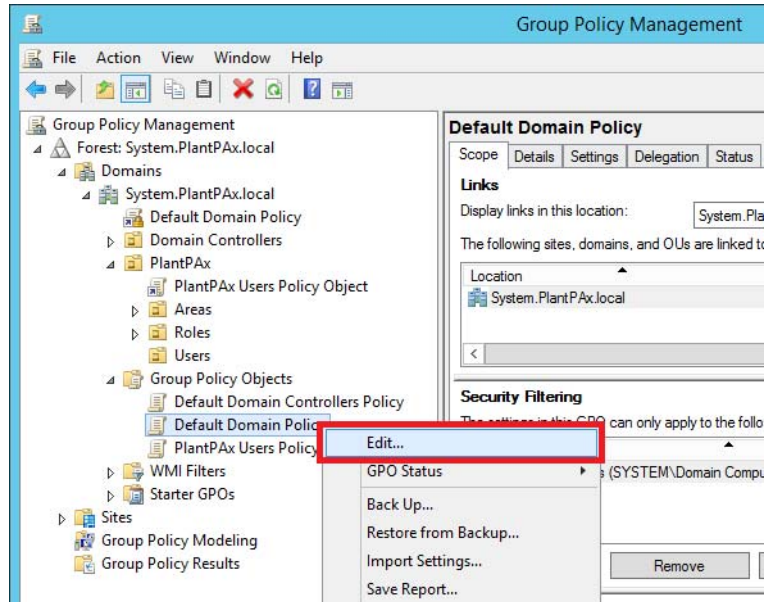
Use a domain controller with these procedures.



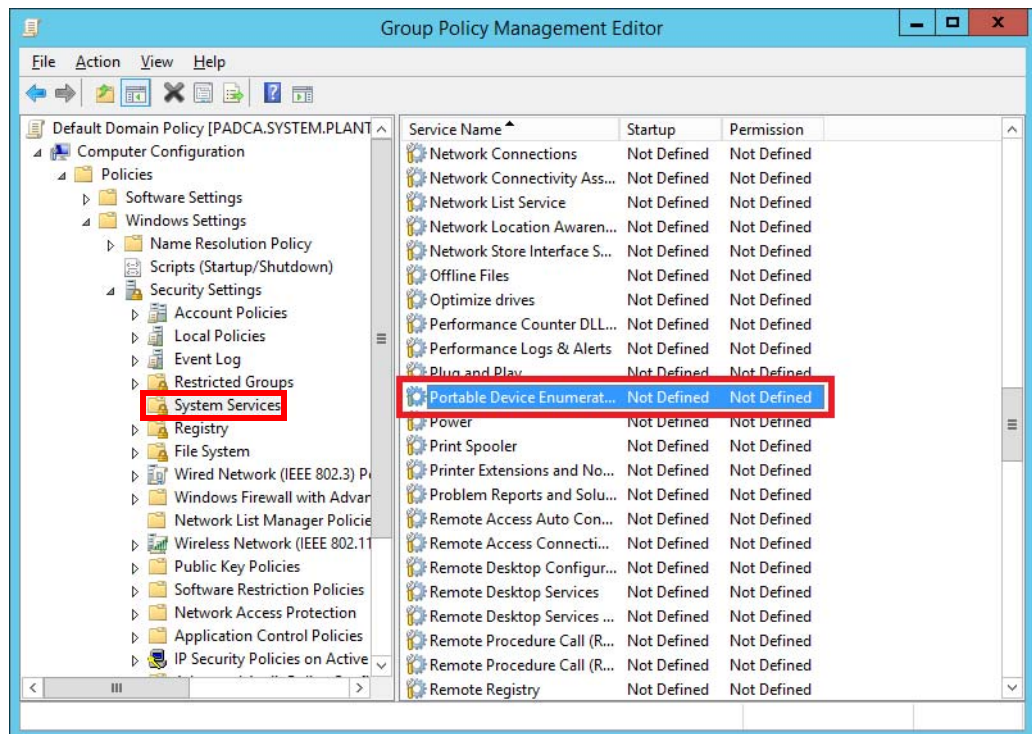
Configure Portable Device Enumerator Service

Complete these steps to enable a service that enforces Group Policy Objects for connected mass storage devices.

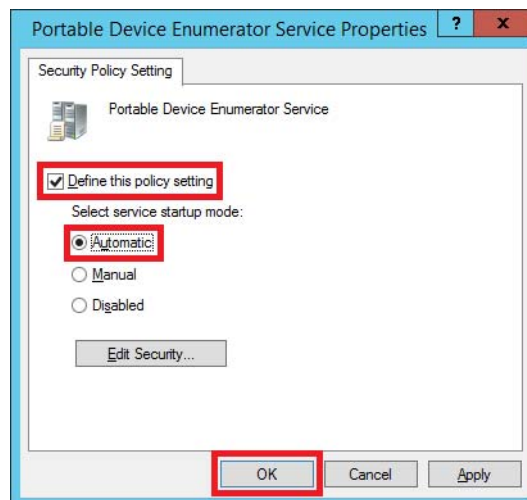
1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. In the system domain folder, click Group Policy Objects, right-click Default Domain Policy and choose Edit.



3. On the Group Policy Management Editor dialog box, open Computer Configuration>Policies>Windows Settings>Security Settings folders.
4. In the System Services folder, click Portable Device Enumerator.



5. Check the 'Define this policy setting' box and select 'Automatic'.

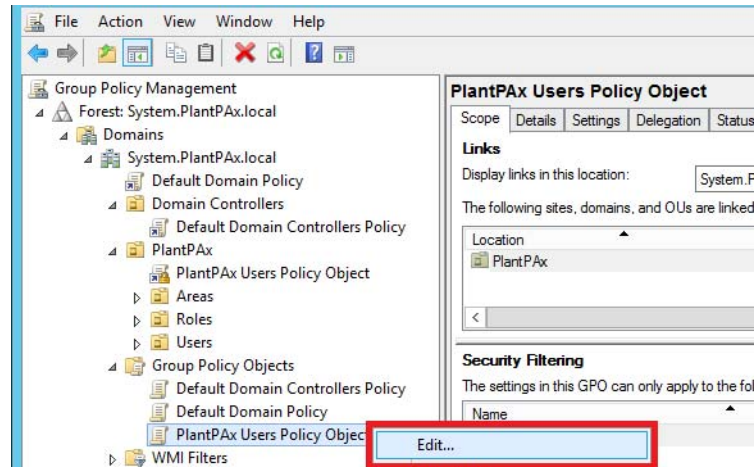


6. Click OK.
7. Close the Group Policy Management Editor dialog box.

Software Access Restriction

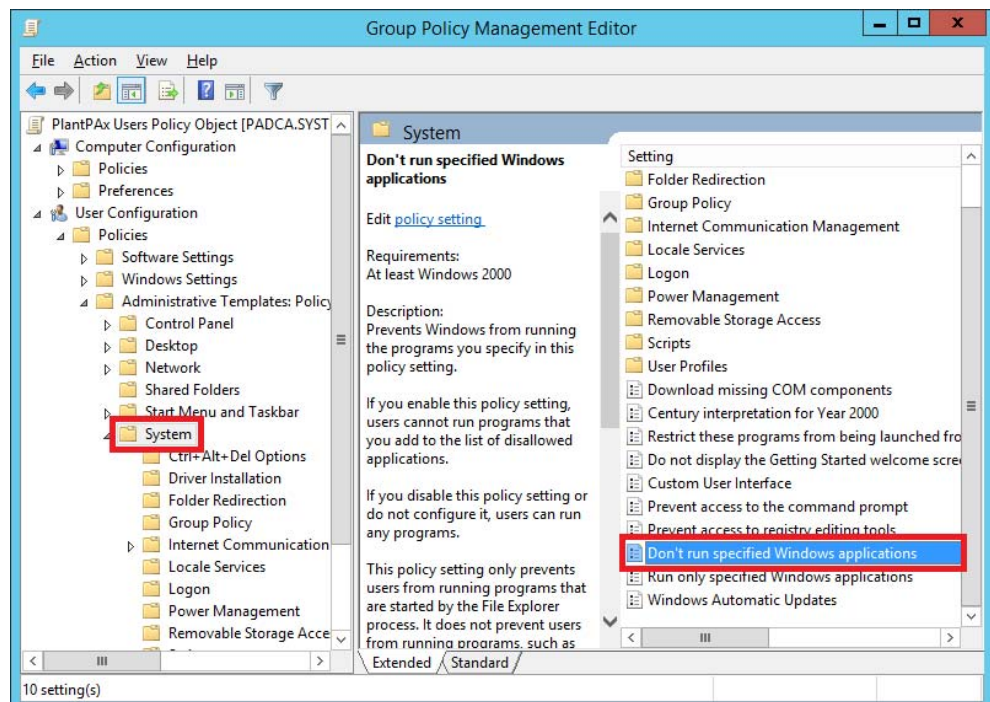
Complete these steps to restrict a group of users from using non-approved software.

1. Repeat [step 1](#) and [step 2](#) on [page 133](#) to access the Group Policy Management dialog box.
2. In the system domain folder, click Group Policy Objects, right-click PlantPax Users Policy Objects and choose Edit.

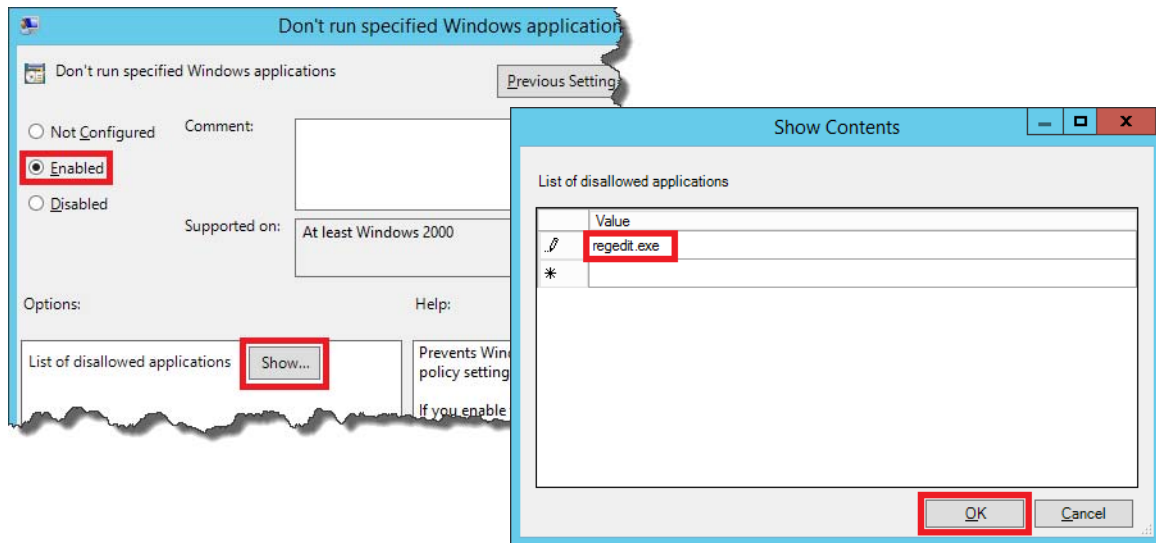


The Group Policy Management Editor dialog box appears.

3. Click to expand the Computer Configuration folder and choose User Configuration>Policies>Administrative Templates.
4. In the System folder, double-click Don't run specified Windows applications.

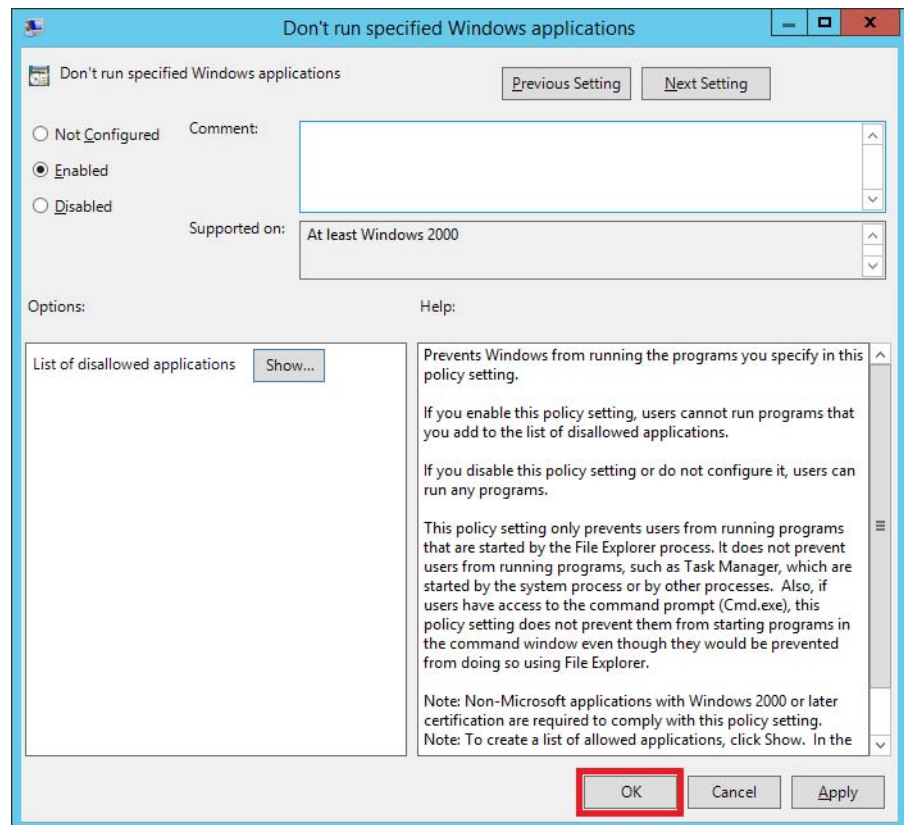


- Click Enabled, Show, and then type any application software to create an access restriction.



- Click OK.

The Don't run specified Windows application dialog box confirms the policy setting.

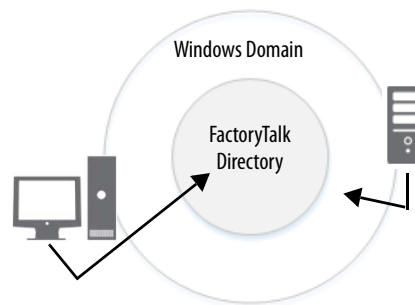


- Click OK.

Configure FactoryTalk Components

In the FactoryTalk® architecture, there are two separate directory types: Local and Network. The Network Directory coordinates the communication between the system elements on multiple clients and servers, such as data servers, HMI servers, and alarm and event servers. If all of your products reside on one computer, you can use the Local Directory.⁽¹⁾

In a PlantPAx® system, the FactoryTalk Directory (FTD) centralizes and shares information across multiple computer systems. The FTD makes this information available through a lookup service to all software products that participate in an application.



IMPORTANT It is required to have a user name and password with administrator privileges to install FactoryTalk software and to specify an FTD location. Use the same user name and password for all FactoryTalk installations on the PlantPAx system.

See [Figure 9 on page 168](#) for the topics that are described in this chapter.

Considerations

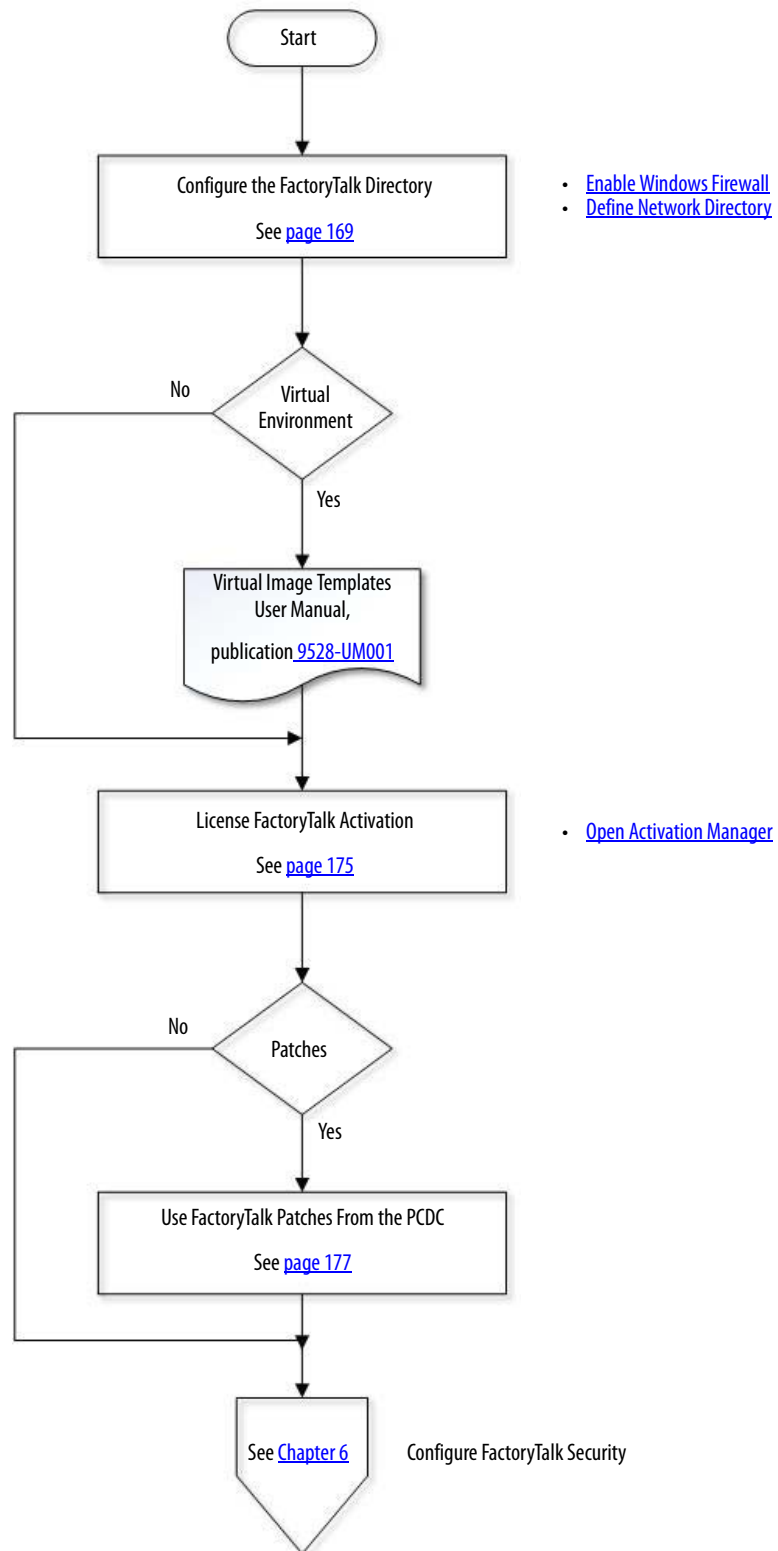
Consider the following suggestions before starting this chapter:

- The FTD server does not require redundancy to maintain availability of the system if the FTD server fails. The FTD information is cached on each computer that is participating in a distributed application as long as the computer had previously accessed the FTD server.
- For compatibility purposes, you must install software components, such as FactoryTalk Services Platform. You also can use the Product Compatibility and Download Center (PCDC) at <http://www.rockwellautomation.com/global/support/pcdc.page>.

(1) Some FactoryTalk products, such as FactoryTalk® VantagePoint®, can address multiple FactoryTalk Directories.

[Figure 9](#) contains the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 9 - FactoryTalk Components Workflow




Configure the FactoryTalk Directory

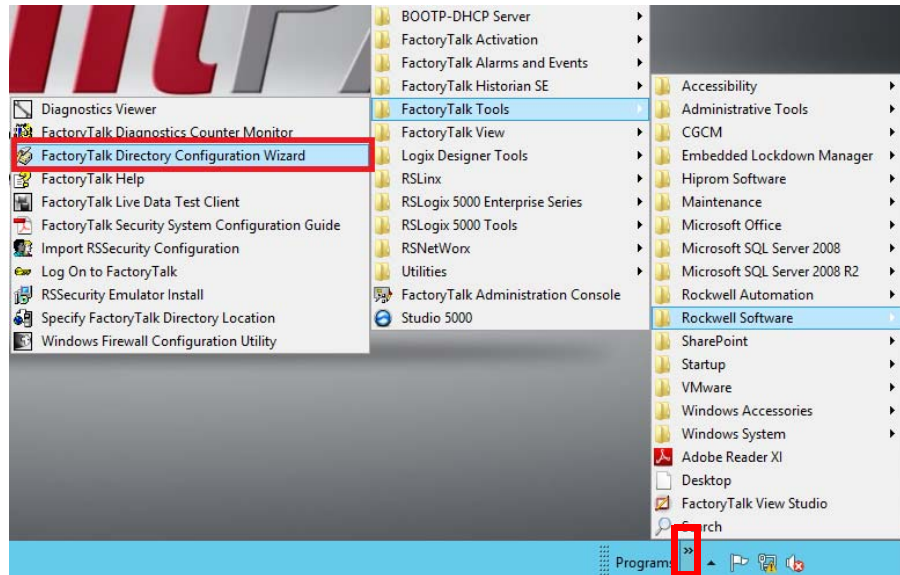
Use servers and workstations with these procedures.



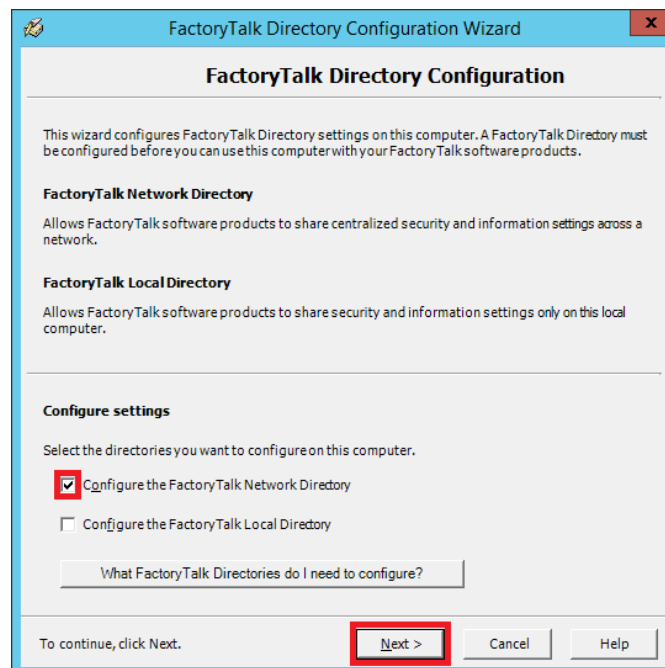
All Servers and Workstations

The PlantPAx system is integrated as a directory to all system computers as defined by the FTD. The following procedures must be completed for **all** computers in the PlantPAx system.

1. Click the Programs  symbol and choose Rockwell Software®>FactoryTalk Tools>FactoryTalk Directory Configuration Wizard.



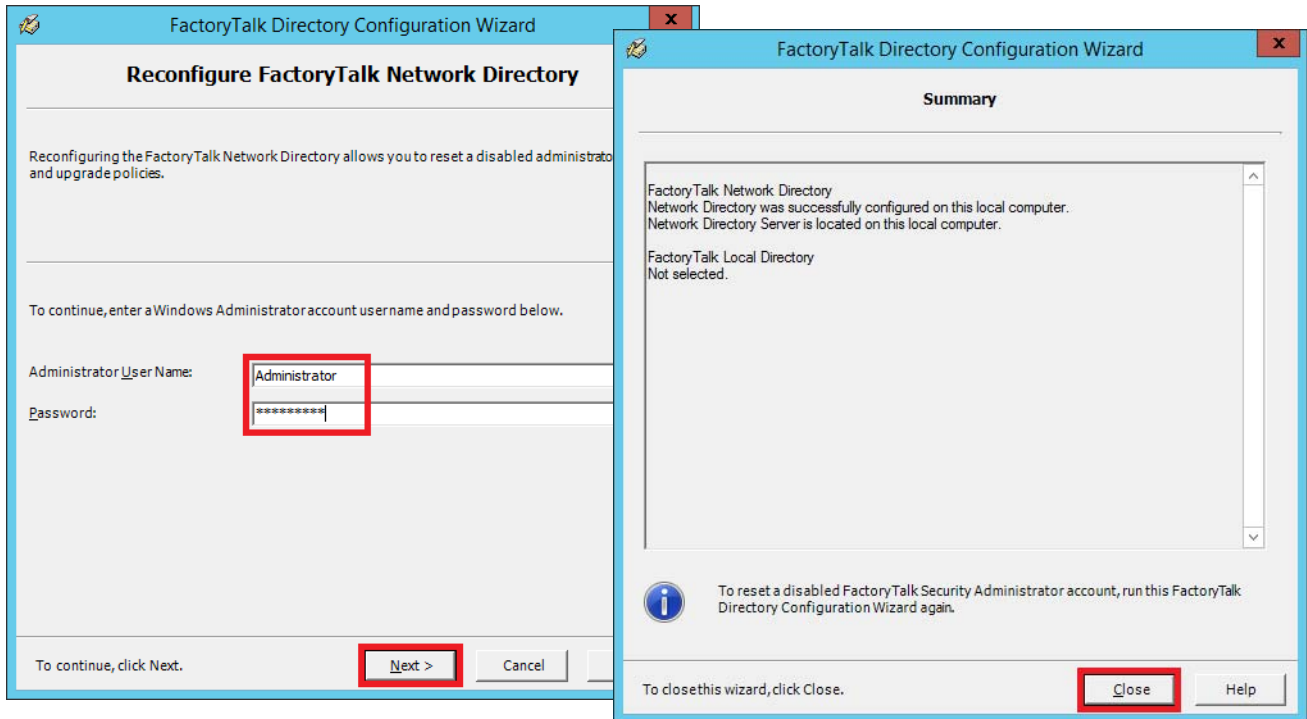
2. Select 'Configure the FactoryTalk Network Directory' and click Next.



IMPORTANT The FactoryTalk Local Directory is optional. But, you must use FactoryTalk View Machine Edition (ME) software with the Local directory.

3. Type any Windows administrator user name and password for the Network Directory, and click Next.


Use the same user name and password for Network and Local directories.

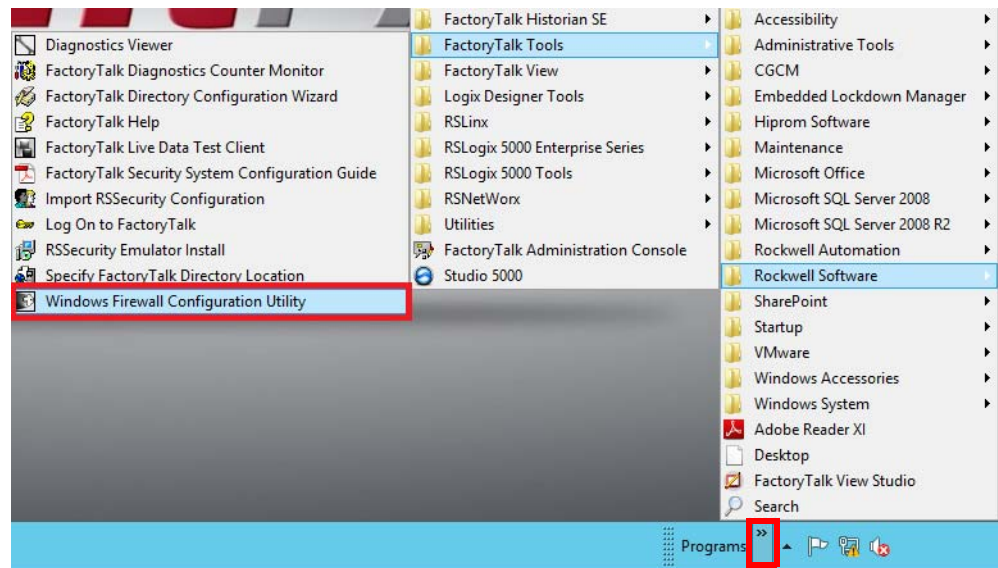


4. Click Close.

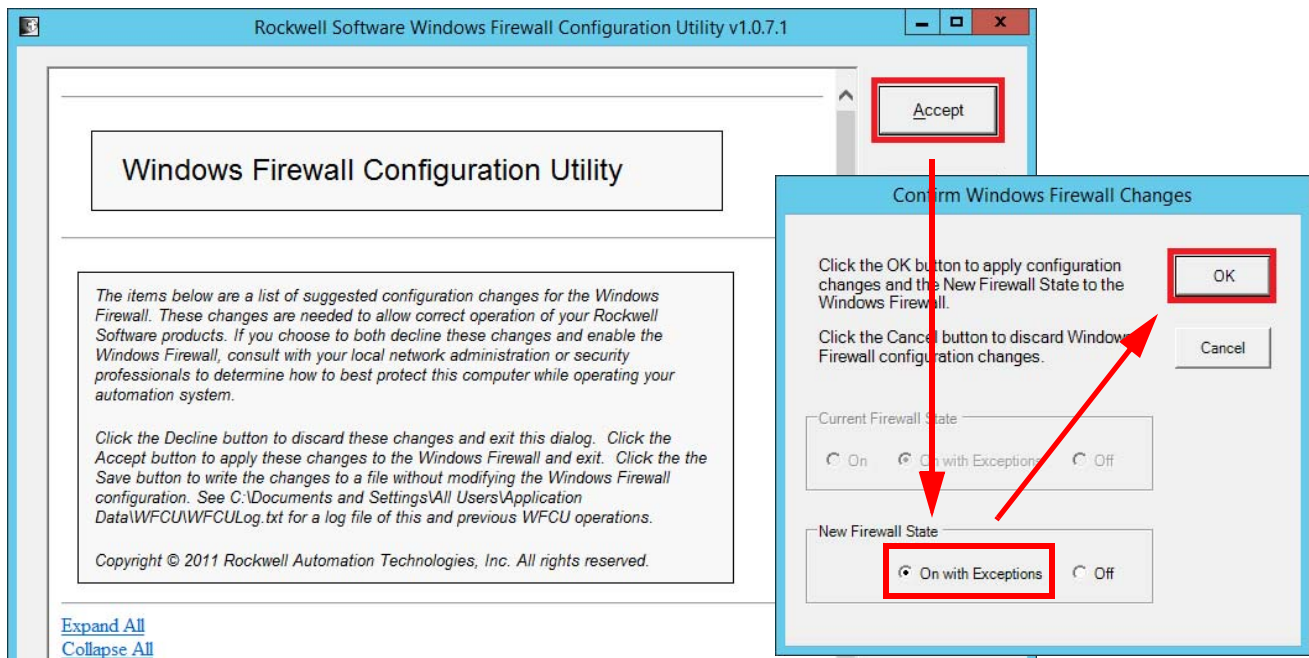
Enable Windows Firewall

Although an option, we suggest that you configure the Windows Firewall utility. This utility creates necessary firewall rules to provide communication between system elements. Complete these steps.

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Tools> Windows Firewall Configuration Utility.




2. Click Accept and select 'On with Exceptions' for the new Firewall state.

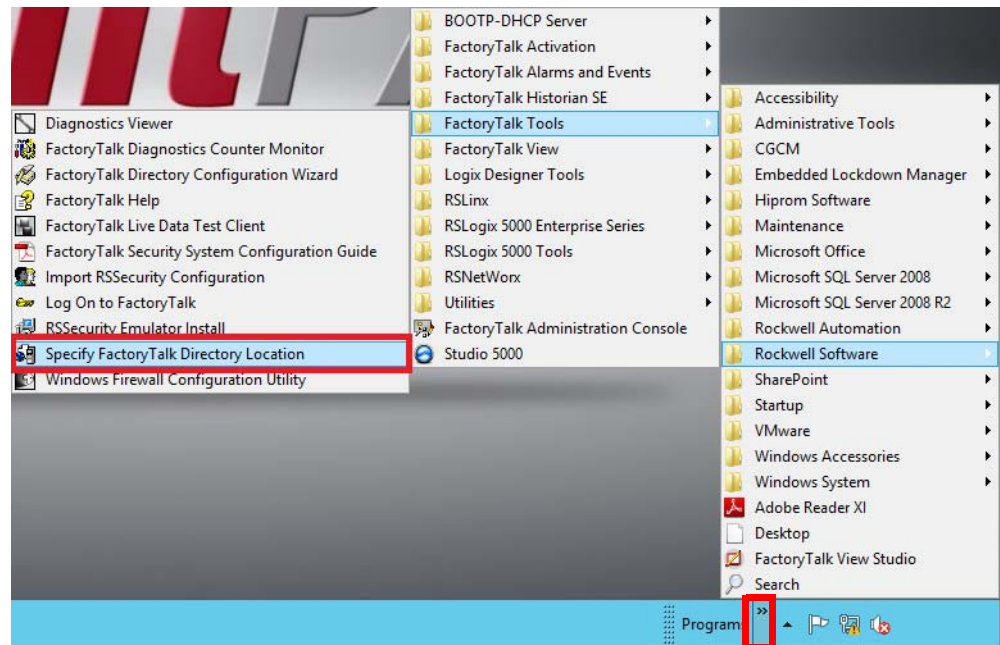


3. Click OK.

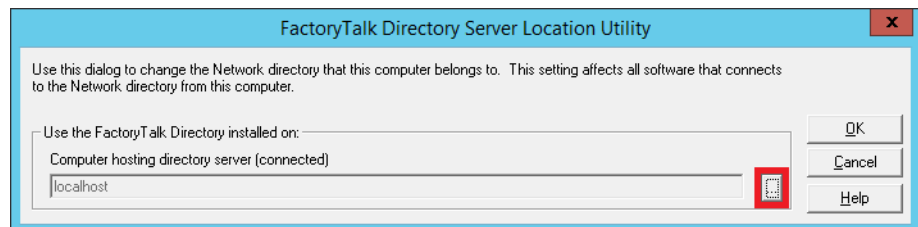
Define Network Directory

The Network Directory **must** be the same for all system computers. Any PASS server can be used as the FTD server.

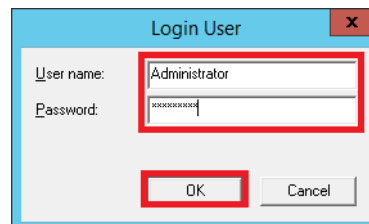
1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Tools>Specify FactoryTalk Directory Location.



2. Click Browse (ellipsis '...') on the FactoryTalk Directory Server Location Utility dialog box.

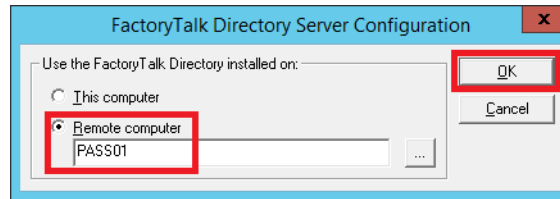


3. Type the same user name and password (with Administrator privileges) that you used to configure the Network and Windows Directory.

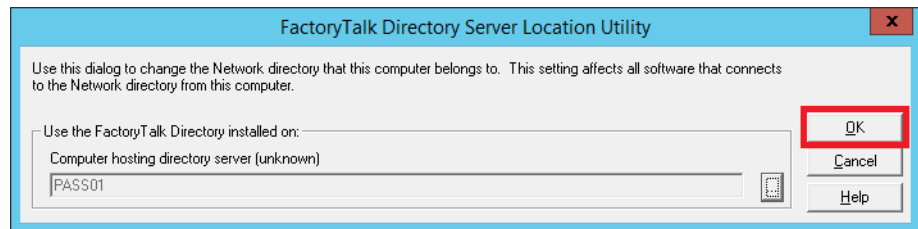


4. Click OK.

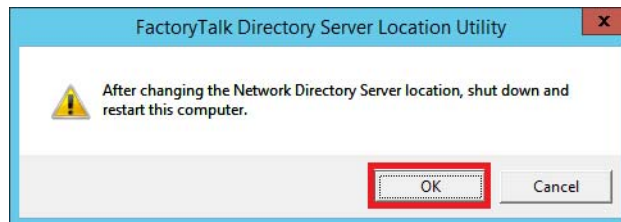
5. Select Remote computer and type the FactoryTalk Directory server.
For example, PASS01. You also can browse for a network name.



6. Verify the desired FactoryTalk server appears in the computer hosting text box, and click OK.

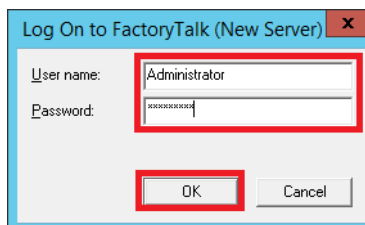


7. Click OK on the message box.



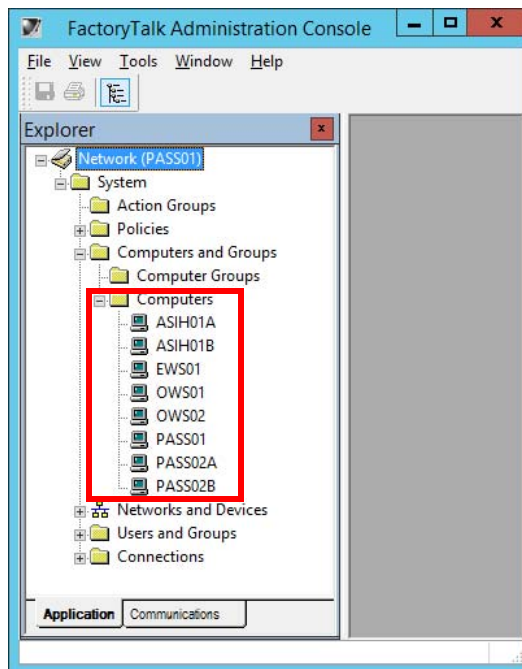
This message is a reminder to restart the computer **after** you finish adding all servers and workstations to the FactoryTalk Directory.

8. Log on by using the server user name and password as shown in [step 3](#).



9. Restart the computer.
10. Repeat [step 5](#) through [step 8](#) for all servers and workstations in the PlantPAx application.
11. Shut down and restart the computer.

When complete, the FTD computers appear in the FactoryTalk Administration Console.



Proceed to [page 175](#) to activate software licenses.

Use FactoryTalk Activation to Apply Licenses

Use the PASS with these procedures.




PASS01

FactoryTalk Activation software provides a secure, software-based system to apply Rockwell Automation® licenses for continuous use of FactoryTalk software and other Rockwell Automation software products.

With FactoryTalk Activation software, there is no need for a physical master disk or any physical media. Instead, activation files are generated and distributed electronically.

Open Activation Manager

On the selected Activation Manager computer, start the activation process by opening the FactoryTalk Activation Manager.

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Activation>FactoryTalk Activation Manager.

The FactoryTalk Activation Manager window appears.



2. Click Help to use the instructions to complete the activations.

For additional instructions and information on activation types, host IDs, and how to use a plug and play dongle, see Activate Rockwell Software Products, publication [FTA-QS002](#).

You also can use the website at <https://activate.rockwellautomation.com>.

[Table 22](#) provides some guidelines after you activate the software.

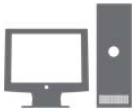
Table 22 - Activation Considerations

Consideration	Details
Software that is not activated	If the components you have installed cannot be activated, for example, because the activation server is unavailable, then the software continues to run for up to 7 days. The seven-day grace period provides time to correct the problem with acquiring activations, without disrupting critical applications. If activation is restored within 7 days, normal operations resume. If activation is not restored, the grace period expires. After the grace period expires, if you restart the components and activation remains unavailable, the software runs for 2 hours in Demo mode.
Location of activation server	The PASS is the primary choice for activation management and is recommended to be the location of the activation server. In the instance that the PASS is not an acceptable location, for example, when you use a redundant PASS solution, the EWS is the secondary choice. In this instance, the EWS can be a dedicated station with a permanent Ethernet connection to the system. The FactoryTalk Activation software can be configured to run as both a server and client utility.
Options for adding activation files to the PASS	To make concurrent floating activations available to activation clients, first you must download the activation files to the activation server computer, from the Rockwell Automation® Activation window. If the PASS has internet access, see Open Activation Manager on page 175 . If the PASS does not have internet access, the activations can be downloaded on another computer with internet connectivity and then transferred to the PASS.
Protect activation files	Activation files are simple text files that must have a .lic extension. As long as the .lic extension is retained, you can copy or rename an activation file without harming it. However, tampering with text inside the activation file can disable your Rockwell Software® products. If an activation file is damaged or deleted, contact Rockwell Automation Technical Support. For safekeeping, keep an original set of your activation files on back-up media. Use descriptive names for the files, so that you can identify them later, and copy them back to the appropriate computers. Activation files are locked to the Host IDs of the computers (or dongles) that need them. Activation fails for Rockwell Software products on a computer where the specified Host ID is not recognized by the activation file.

Proceed to [page 177](#) to learn how to access and configure software patches.

Use FactoryTalk Patches From the PCDC

Use a workstation with these procedures.



All Computers

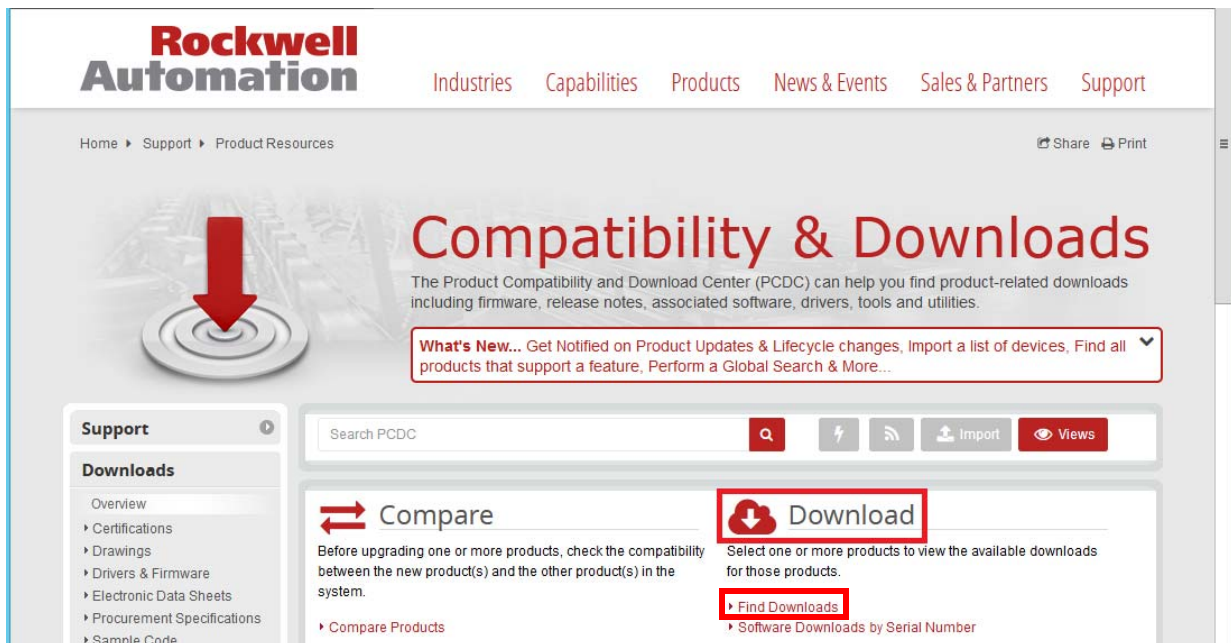
We recommend that you periodically review and update the available software patches and firmware updates for the Rockwell Automation components on your PlantPAx system. Before implementing Rockwell Automation updates, we recommend that you verify them on a non-production system, or when the facility is non-active. Verification helps to make sure that there are no unexpected results or side effects.

You must restart a computer after installing each patch.

IMPORTANT If you are installing a new PlantPAx system, we recommend that you use the specifications in the PlantPAx Selection Guide, publication [PROCES-SG001](#).

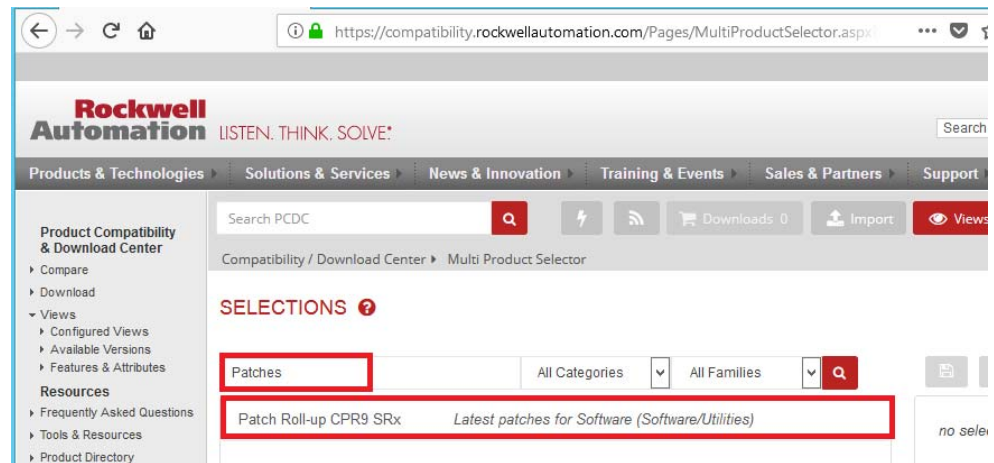
1. Click <http://www.rockwellautomation.com/rockwellautomation/support/downloads.page> to open the Product Compatibility and Download Center (PCDC).

You also can access the PCDC link from the [ab.com](#) website.



2. Under Download, click Find Downloads.

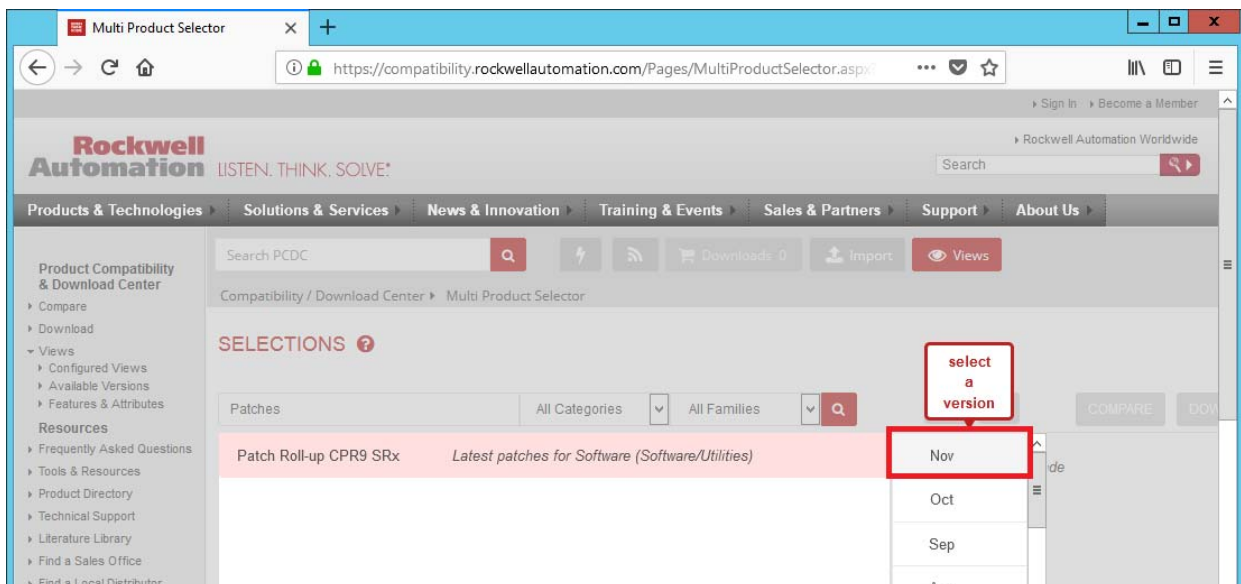
3. In the Product Search text box, type Patches.



The search results appear under the Search text boxes.

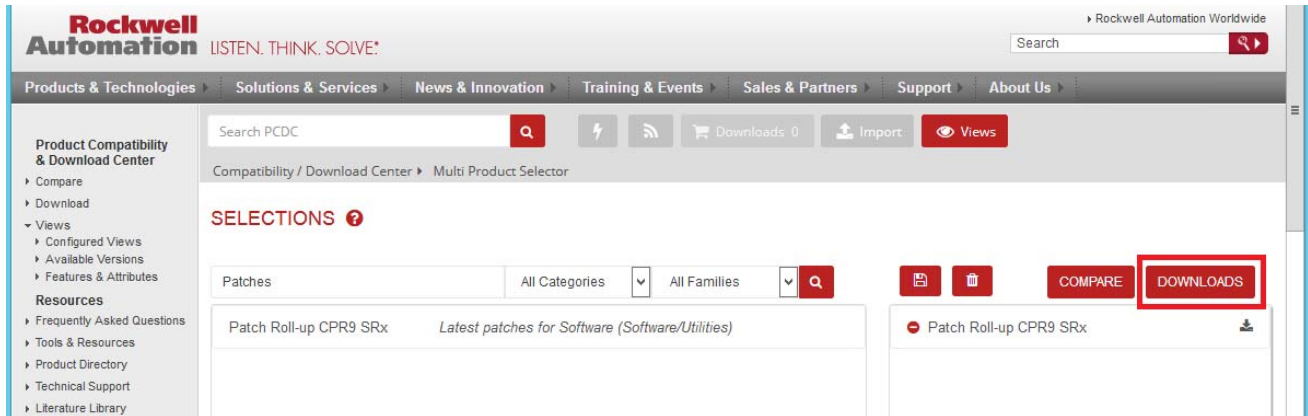
4. Double-click the search results.

Our example is Patch Roll-up CPR9 SRx.

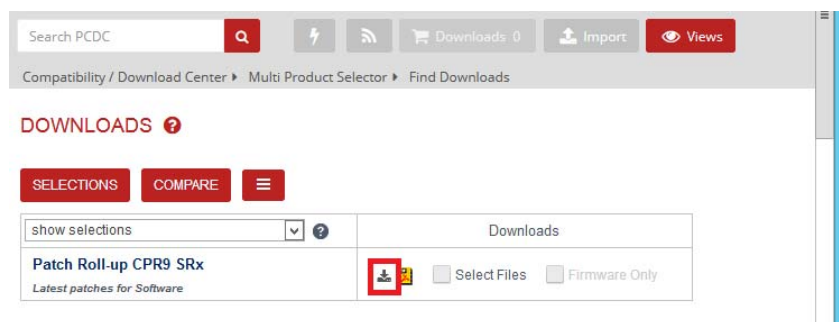


5. Do one of the following items:

- To select a version, click the search results to access a list. Select a desired category and click Downloads.
- To use the current version, click Downloads.



6. Click the Show Downloads button.

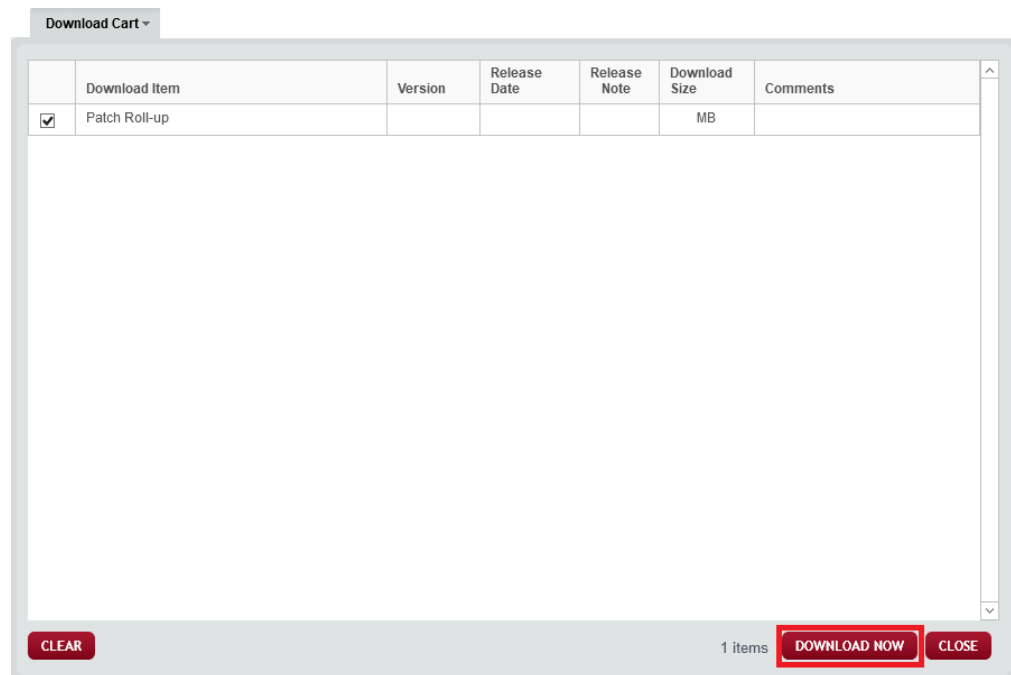


7. In the Downloads list, click each box to add the item to the Download Cart.

The number of items in the cart increase proportionally to the number of boxes that you click. To remove an item from the cart, click a box to remove a check mark.



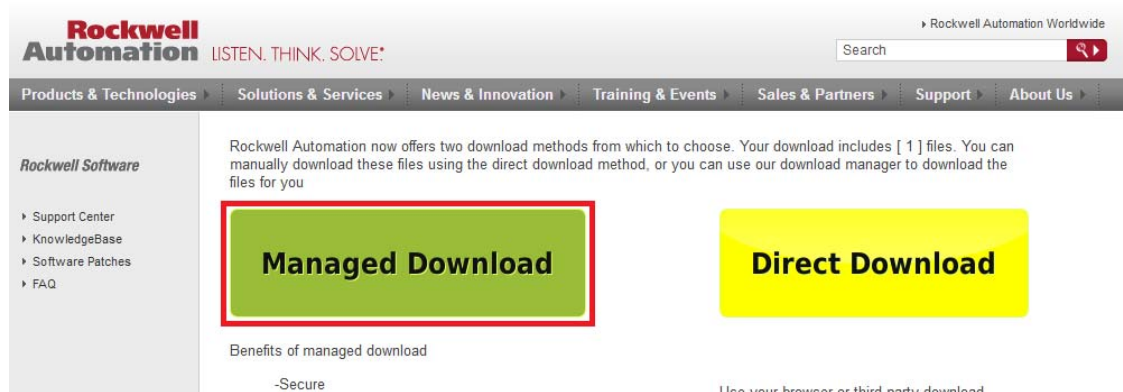
8. Click the Download Cart and then click Download Now.



You need a user name and password to download files.

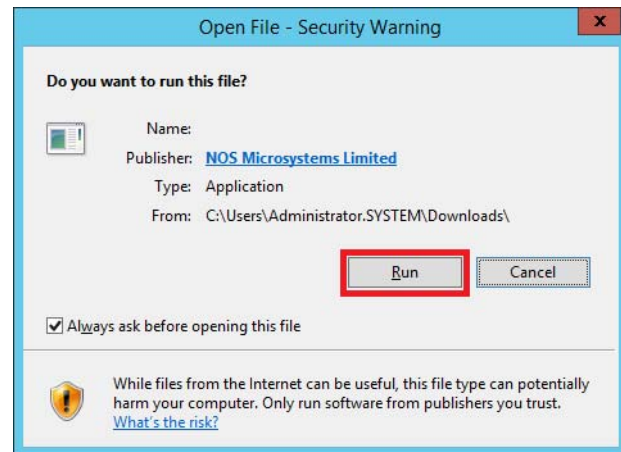
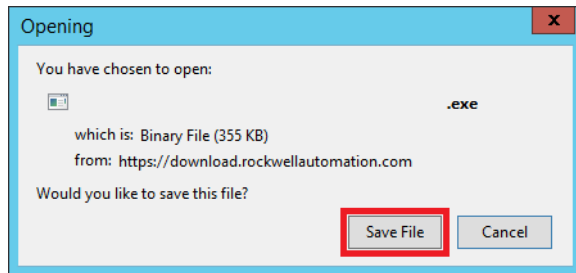
9. Read the software license agreement and click Accept.

There are two ways to download the patches: managed or direct (browser).



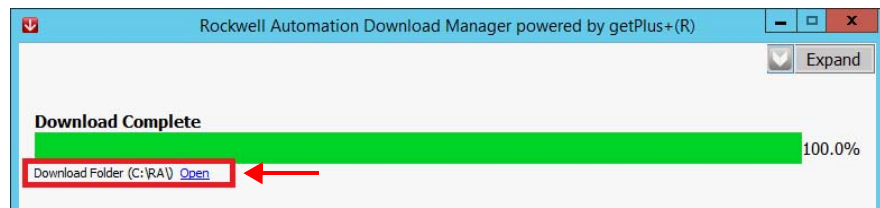
10. We recommend that you click Managed Download.

11. Click Save File and then click Run.



The Download Manager opens.

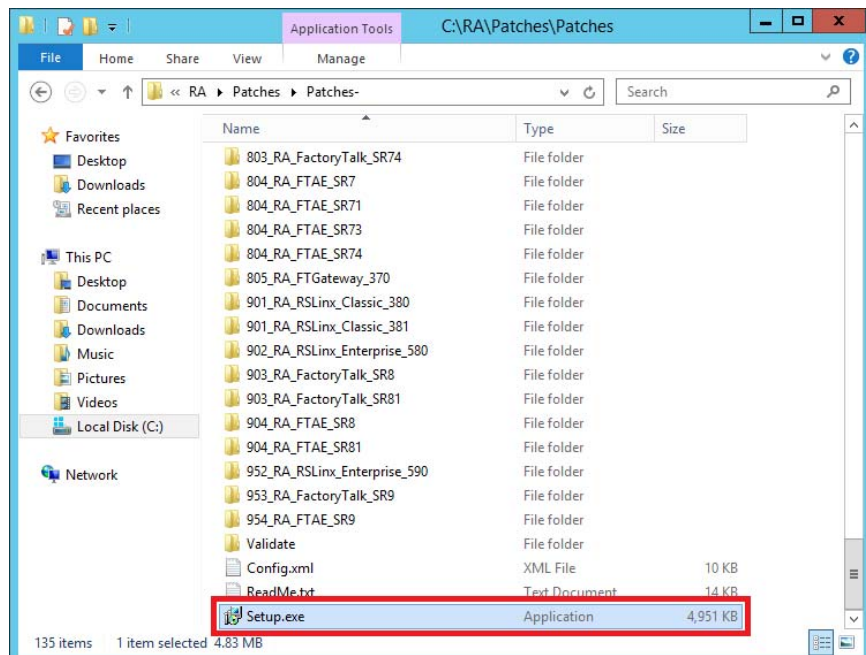
A progress bar shows the installer path to the download folder.



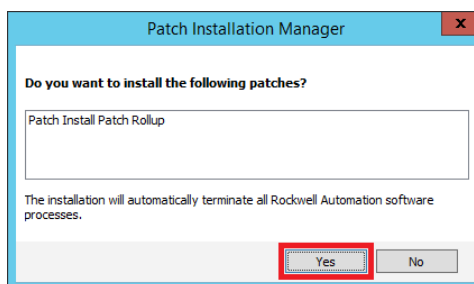
12. Click Open underneath the progress bar (next to the download folder path).

Copy the downloaded patch folder to all PlantPAx servers and workstations for which the patch applies.

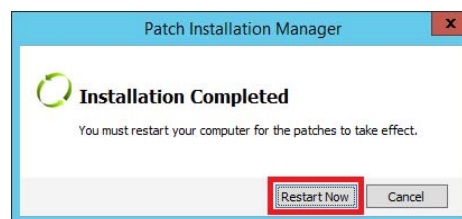
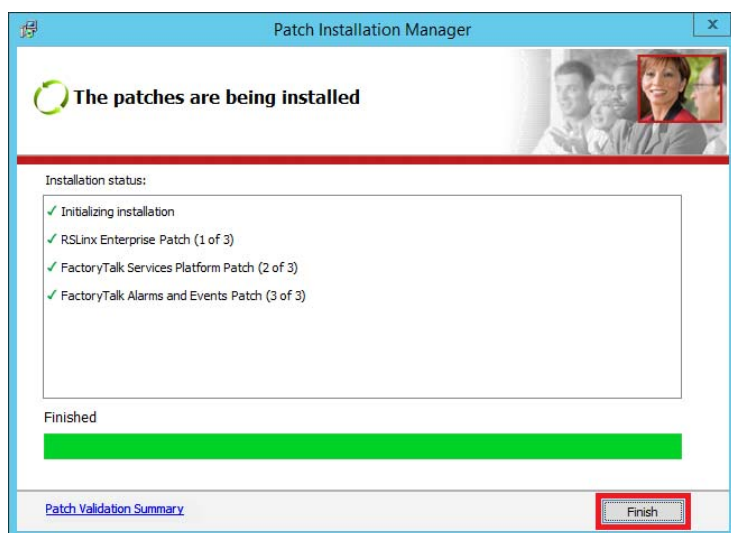
13. Click Local Disk (C:) and choose Setup.exe.



14. Click Yes to install the patches.



15. Click Finish and Restart Now.



Configure FactoryTalk Security

FactoryTalk® Security provides access restriction to only those individuals who legitimately need access to specific automation assets. FactoryTalk Services Platform (FTSP) includes the FactoryTalk Administration Console that provides the interface for configuring your system.

This chapter describes how to administer privileges to users and groups to define who can access hardware devices and software products. Permissions authenticate an identity and authorize that person to access that resource and perform only allowed actions. The centralized security system with a modern DCS, such as the PlantPAx® system, helps to make sure the data that is being received and processed is from a trusted source.

The Users and Groups in the FactoryTalk View console let you control who accesses the FactoryTalk system and from which computer. Access can be restricted to a single user or group of users to help simplify the administration of permissions.

When setting up security, create groups first and grant the appropriate permissions to the group. With groups, you create a security structure without needing to know exactly the users that comprise the groups. When users are added to the group, they inherit the permissions that are granted to the group.

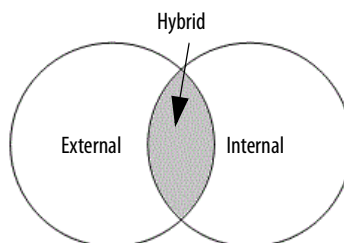
Considerations

As shown in [Figure 10](#), there are groups that require separate configuration:

- External – Involves Windows-linked user groups in a domain controller
- Internal – Includes users not in a domain but grouped in the FactoryTalk Directory (FTD).

The overlap between these two groups creates a hybrid group.

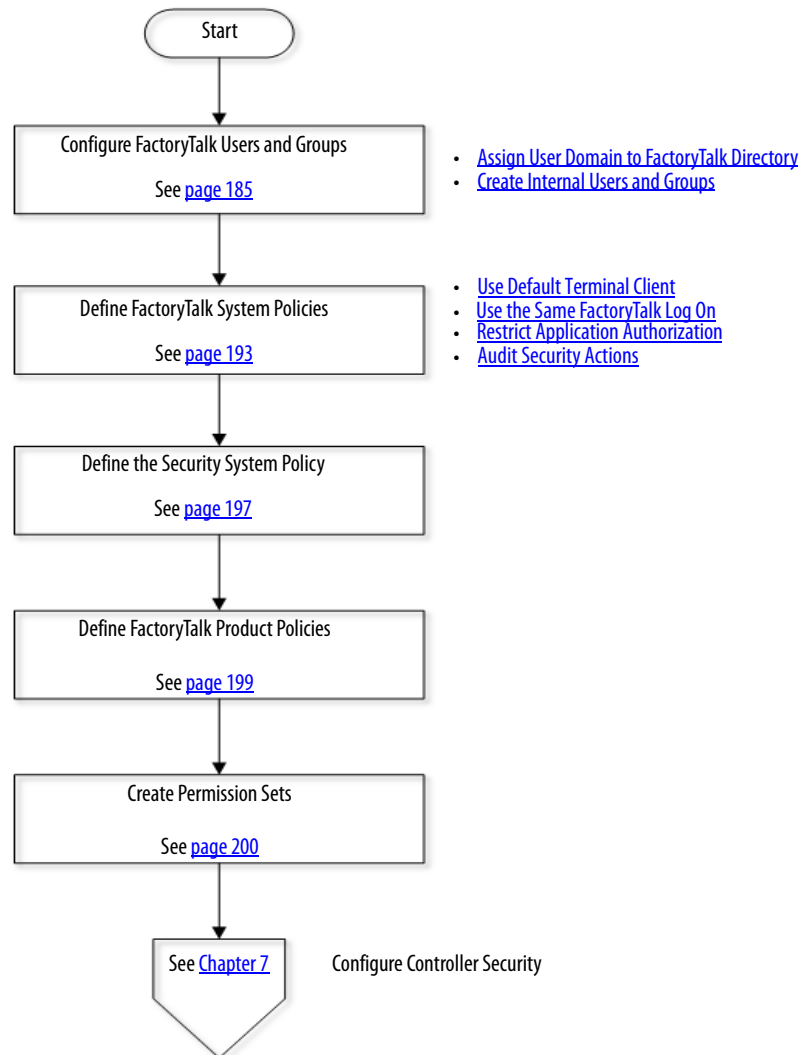
Figure 10 - Users and Groups Example



IMPORTANT Even if your application has a domain, we highly recommend that you configure a hybrid group. The internal connections, via the hybrid, permit operations to continue if there is loss of a domain connection.

[Figure 11](#) contains the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 11 - FactoryTalk Security Workflow



Configure FactoryTalk Users and Groups

Use an Engineering Workstation with these procedures.




The FTD stores information about which users have access to the parts of a control system. During the logon, FactoryTalk security uses this information to verify an identity and then permissions that are assigned to the user. Authorized users can then access secured parts of the application.

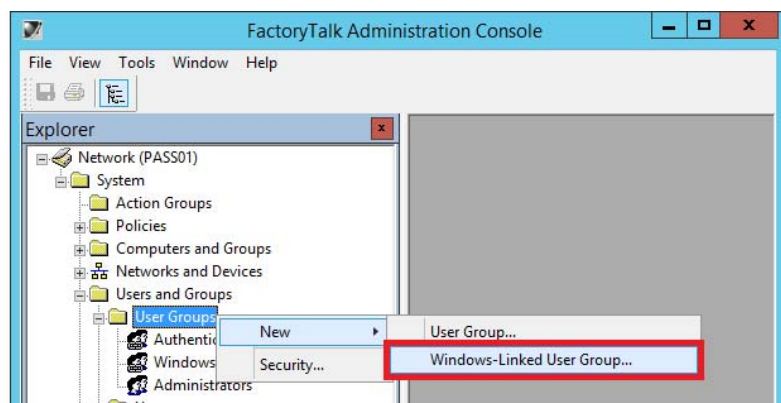
Assign User Domain to FactoryTalk Directory

The following subsections walk you through how to link user accounts in a Windows domain into FactoryTalk security. These procedures, including assigning groups, roles, and areas, **must** be completed for domain credentials to be recognized in the FTD.

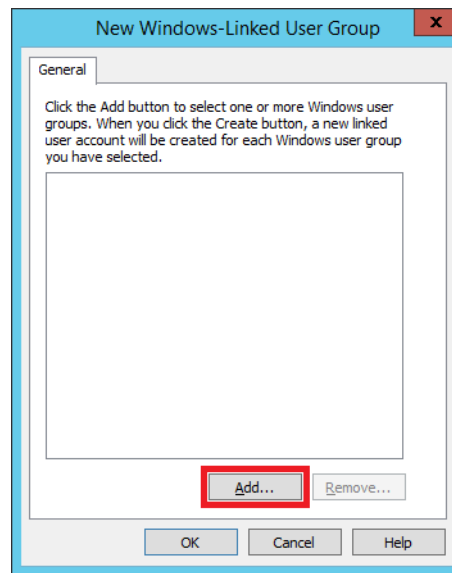
Linking External Users and Groups

Windows-linked user accounts must be assigned access rights to validate that the users are authorized for the work that is approved for the group. (Domains are explained in [Chapter 3](#).)

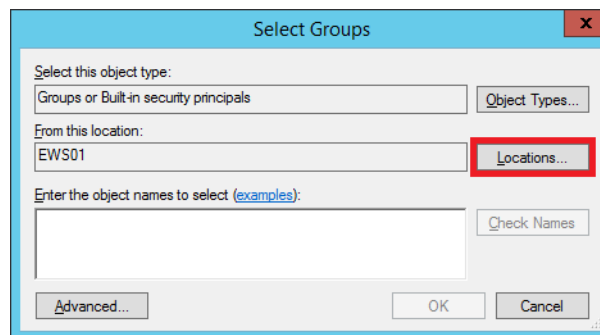
1. Click the Programs  symbol and choose Rockwell Software® > FactoryTalk Administration Console.
2. Select the network directory and click OK.
3. Under the Network Directory, click System and then Users and Groups to expand both folders.
4. Right-click User Groups and choose New > Windows-Linked User Group.



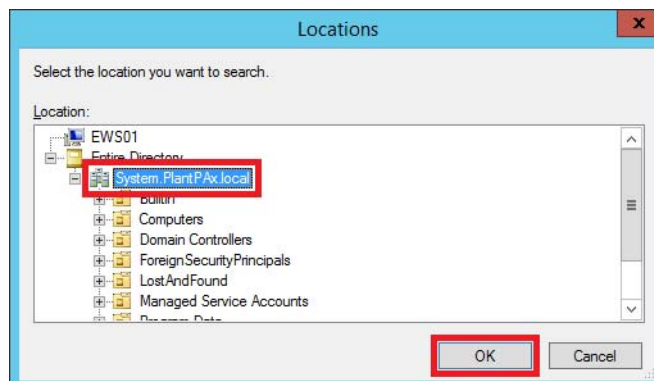
5. Click Add.



6. On the Select Groups dialog box, click Locations.



7. To search for the PlantPAX groups in the domain, open Entire Directory and select a domain name (System.PlantPAX.local is an example).



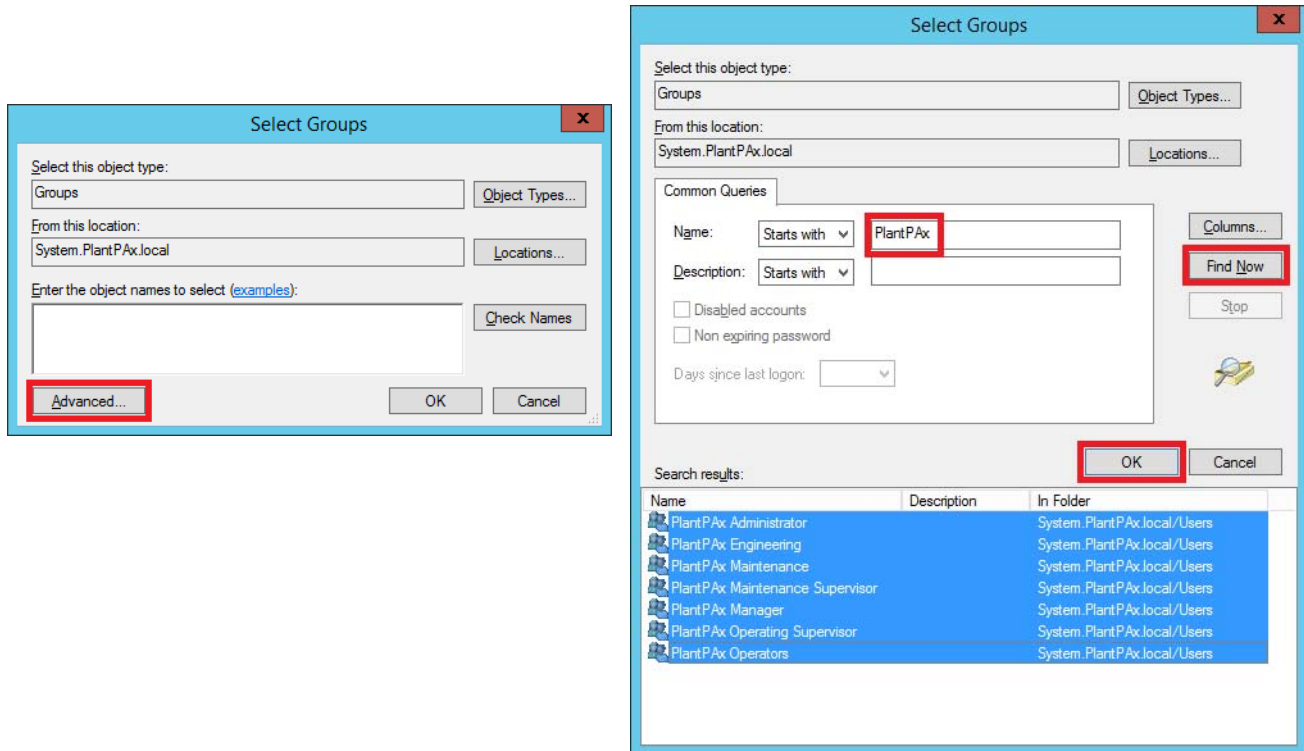
8. Click OK.

Importing Active Directory Roles

Complete these steps to import specific roles, such as supervisor, operator, maintenance, into groups.

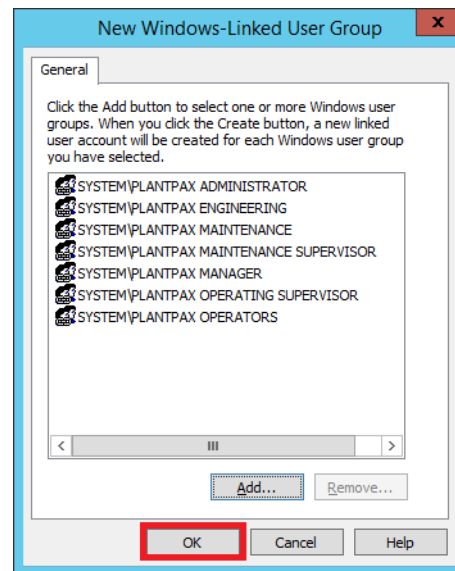
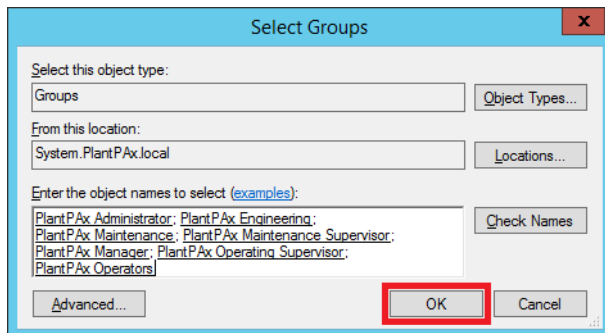
1. On the Select Groups dialog box, click Advanced.

To access this dialog box, repeat [step 1](#) through [step 5](#) on pages [185-186](#).

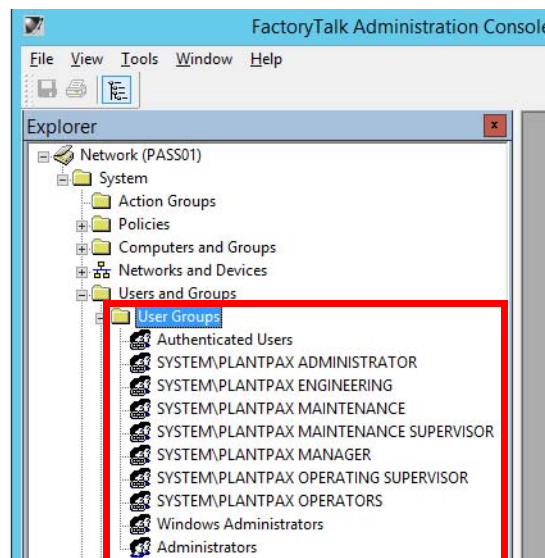


2. Type PlantPAx.
3. Click Find Now to display a list of roles that you grouped in [Chapter 3](#).
4. Select all desired windows-linked groups and click OK.

5. To accept the selections, click OK on the following dialog boxes.



All of the domain groups and roles are listed under the FTD User Groups.



Importing Active Directory Areas

Complete these steps to assign groups with engineering or non-engineering access rights. Engineering access allows modifications to Library faceplates.

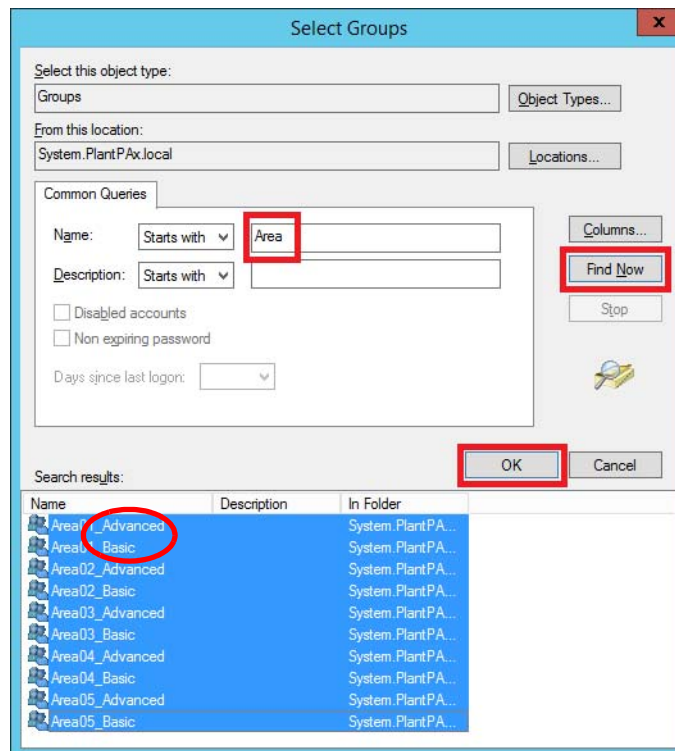
1. From the New Windows-Linked User Group dialog box, click Add.

To access this dialog box, repeat [step 1](#) through [step 4](#) on [page 185](#).

2. From the Select Groups dialog box, type an object name.

For example, Area.

3. Click Find Now.

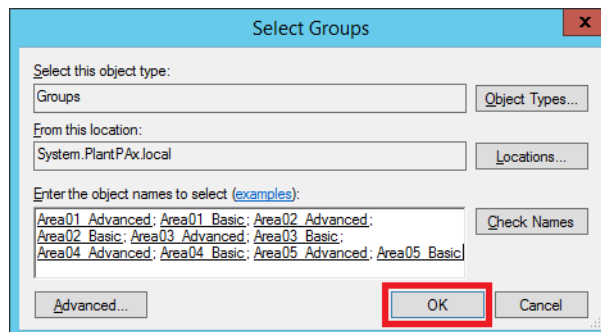


Observe with area descriptions the terms 'Advanced' and 'Basic'.

- Advanced provides access to engineering modifications on Process Library faceplates.
- Basic allows access to non-engineer functions, such as Maintenance, Operator, on Process Library faceplates.

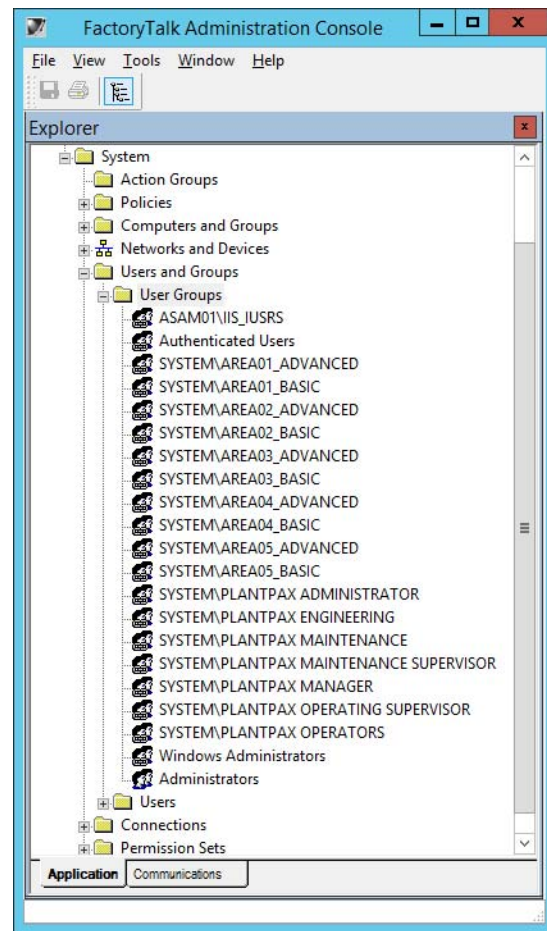
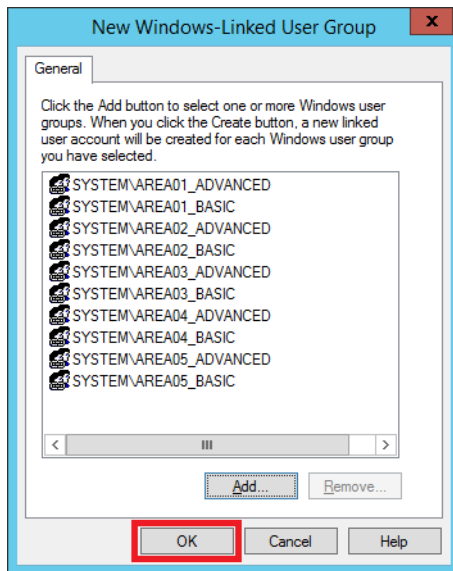
See [Area Groups on page 121](#) to configure security for different areas of your application.

4. Select an object from the list and click OK.
5. The object groups appear in the text box of the Selection Groups dialog box.



6. Click OK.

7. Click OK again, and the assigned areas appear in the Network Directory under User Groups.



Create Internal Users and Groups

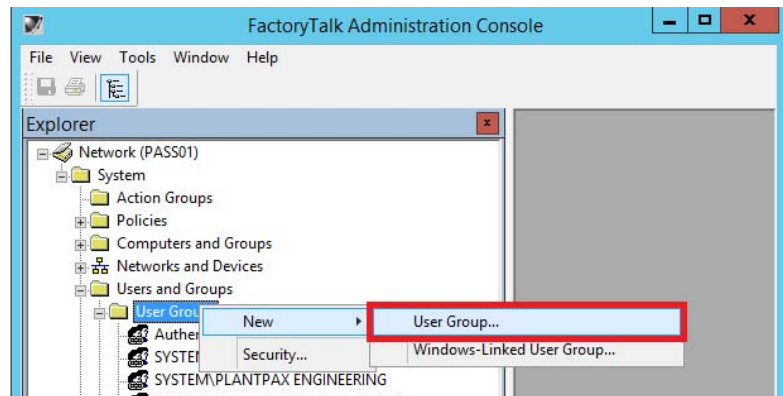
Use an Engineering workstation with these procedures.



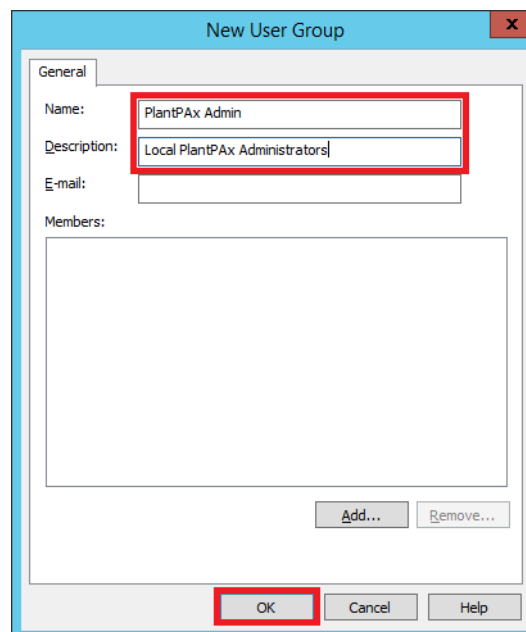
This section describes how to create an internal and a hybrid users group for smaller systems that don't have a domain infrastructure. A hybrid group, which is composed of external (domain) and internal (FTD) users, is recommended for continued operation if the domain connection is lost.

Complete these steps.

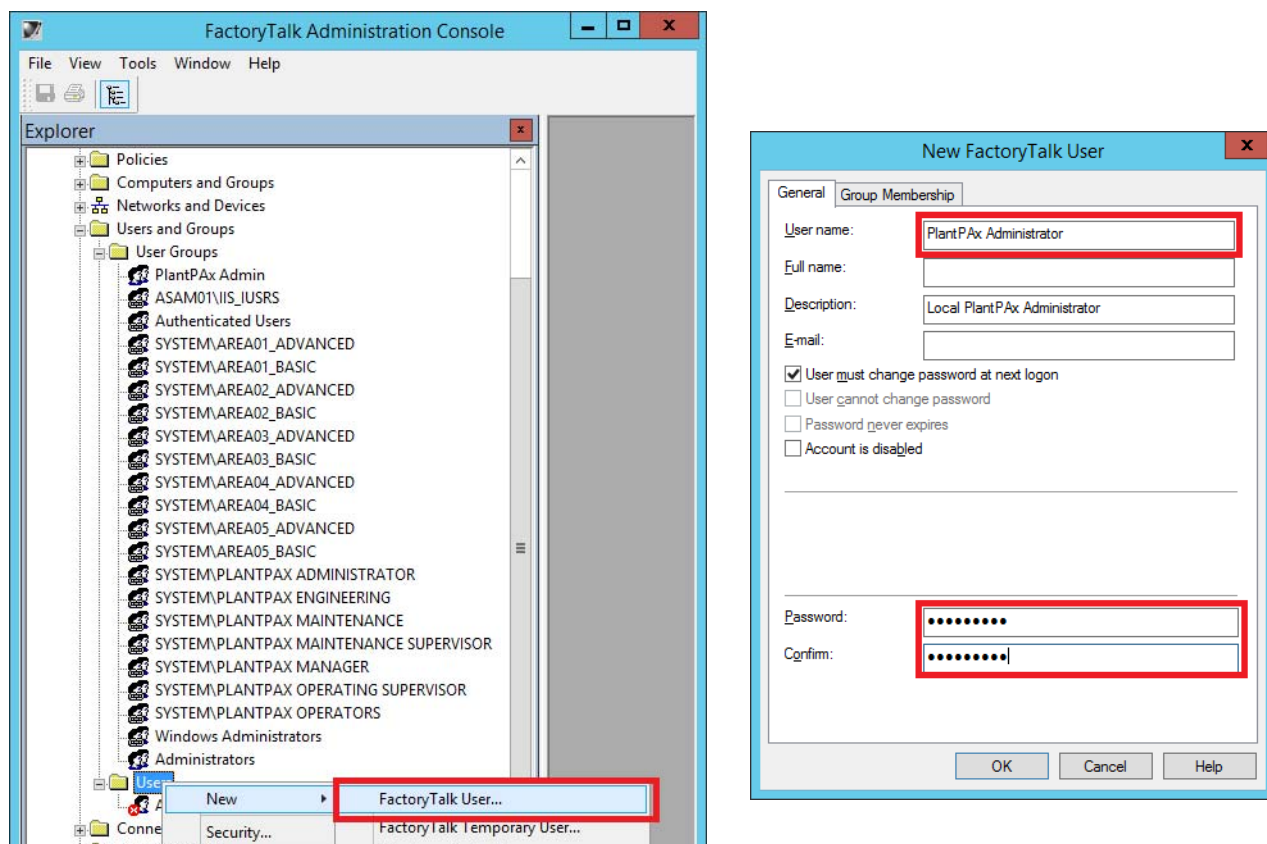
1. Click the Programs >> symbol and choose Rockwell Software® > FactoryTalk Administration Console.
2. Select the network directory and click OK.
3. Under the Network Directory, click System and then Users and Groups to expand both folders.
4. Right-click User Groups and choose New>User Group.



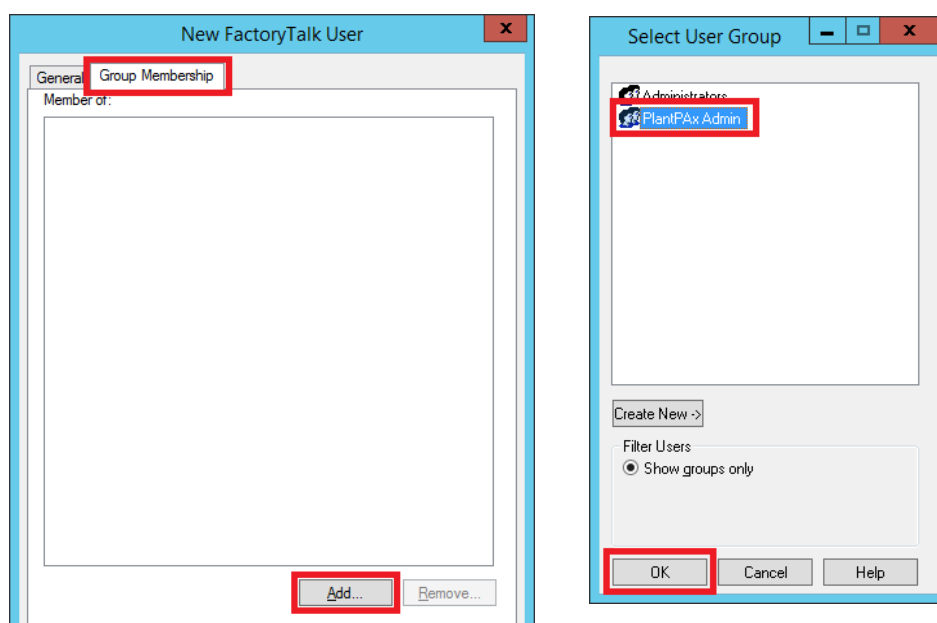
5. Type a new user group name and click OK.



6. Right-click the Users folder, and choose New>FactoryTalk User.
7. Type a user name and description.
8. Enter a password and then type the same password as confirmation.



9. In the Group Membership tab, choose Add, and then select a group to be linked to the new user.



10. Click OK.

- Repeat [step 4](#) through [step 10](#) to add a new local group and users to the system.

TIP You can also create guest users with known passwords to control this type of access in the system.

For a list of HMI security codes, see the Rockwell Automation Library of Process Objects, publication [PROCES-RM002](#).

Define FactoryTalk System Policies

This optional section describes how to use Remote Desktop Services (RDS) to access FactoryTalk applications, such as thin clients.

Use Default Terminal Client

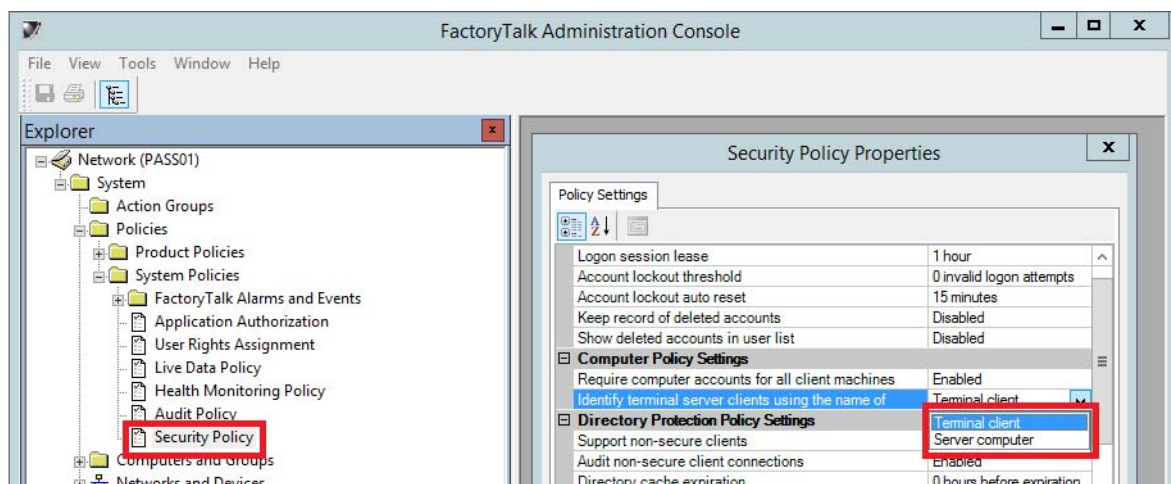
Use an Engineering Workstation with these procedures.



You have two server options: terminal client or server computer; terminal being the default.

- On the network directory (see steps 1...2 on [page 191](#)) under System > Policies > System Policies, double-click Security Policy.
- On the Policy Settings dialog box under Computer Policy Settings, leave terminal client as the default for remote desktop services to be available.

TIP Select Server computer from the pull-down menu and click OK if you want external client computers to be able to log in to the FTD without any pre-configuration. This option, however, does not let you track specific actions from the terminal client.



- Click OK.

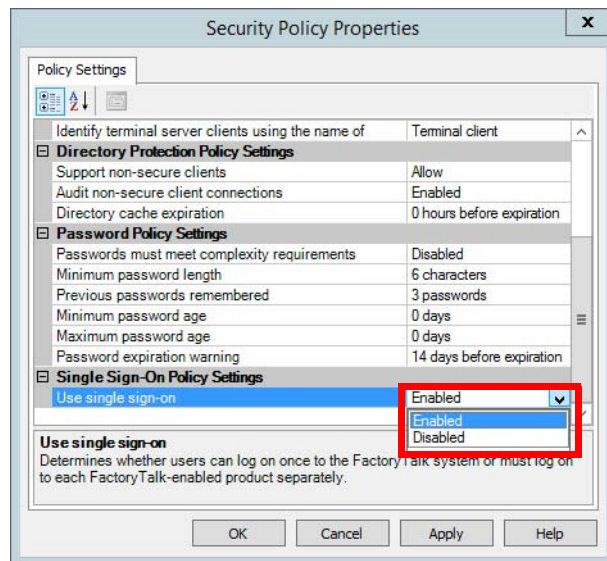
Use the Same FactoryTalk Log On

You have options to enable/disable access to multiple FactoryTalk products with the same FTD logon.

1. On the network directory (see steps 1...2 on [page 191](#)) under System>Policies>System Policies, double-click Security Policy.
2. Scroll down to Single Sign-On Policy Settings and leave Enabled as the default.

This setting lets you use the same FactoryTalk log in for multiple products.

TIP Select Disabled from the pull-down menu if you want separate logins to be used for each FactoryTalk product.

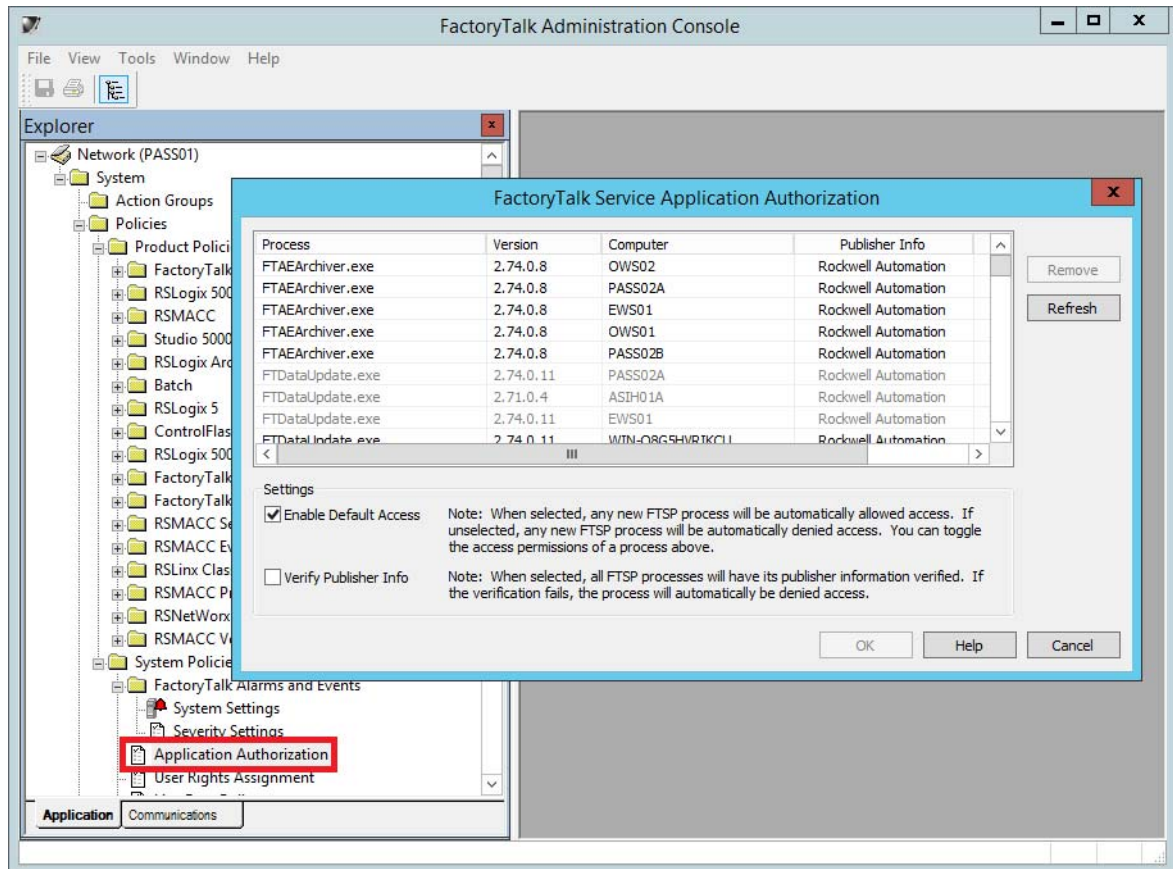


3. Click OK.

Restrict Application Authorization

You can verify and configure FactoryTalk Services application authorization.

1. On the network directory (see steps 1...2 on [page 191](#)) under System>Policies>System Policies, double-click Application Authorization.



2. In the (lower) Settings section of the dialog box, use the 'Enable Default Access' default.

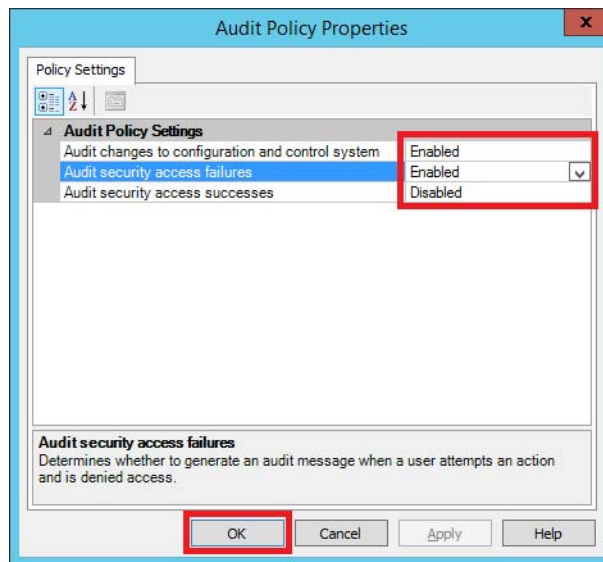
This setting automatically authorizes application access.

3. If you want to require application verification, click 'Verify Publisher Info' and click OK.

Audit Security Actions

You can enable an audit to track configurations and security.

1. On the network directory (see steps 1...2 on [page 191](#)) under System>Policies>System Policies, double-click Audit Policy.
2. Under Audit Policy Settings, select Enabled from the Audit security access failures pull-down menu.



3. Click OK.

Proceed to [page 197](#) to determine security permissions for groups and users.

Define the Security System Policy

Use an Engineering Workstation with these procedures.

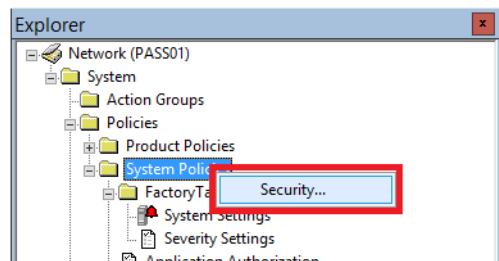


EWS

This section describes how to configure permissions for groups and users to perform actions that are based on their security levels. The access level can be based in the domain or local groups, however, the user needs to be a member of only one single group. For example, if you are a member of the Administrators and the Operators groups and you are denied access, you lose Administrator permissions. You have the lowest security access in both groups.

Complete these steps.

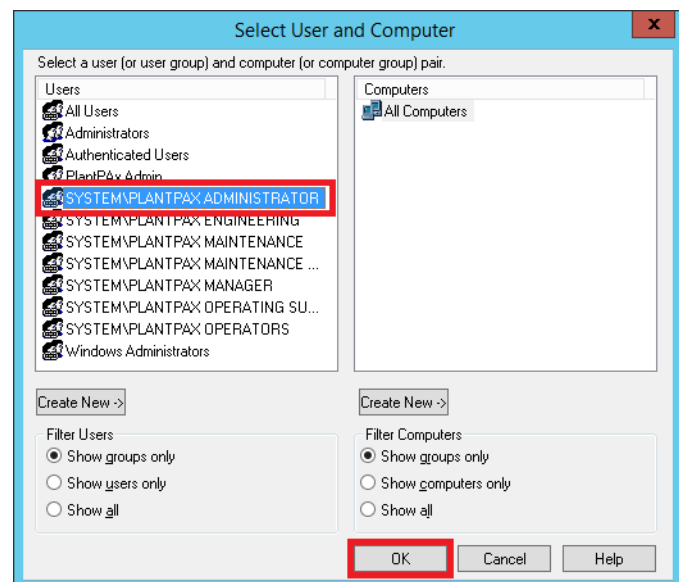
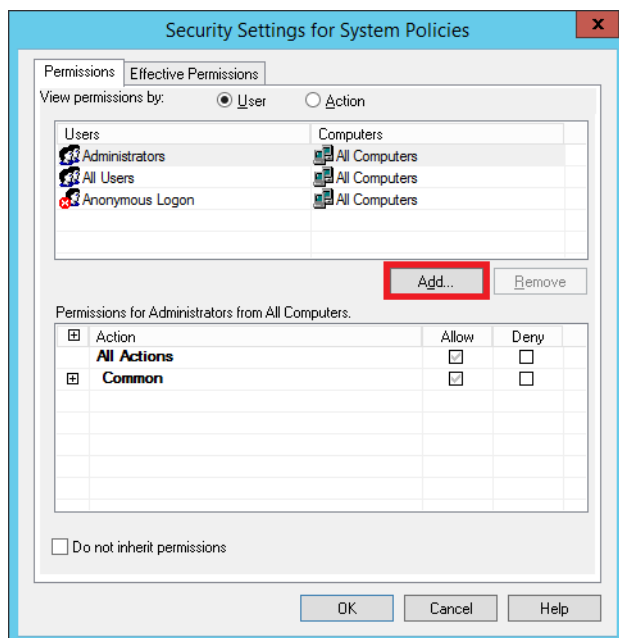
1. On the network directory (see steps 1...2 on [page 191](#)) under System>Policies, right-click System Policies and choose Security.



2. On the Permissions tab of the Security Settings for Systems Policies dialog box, click Add.

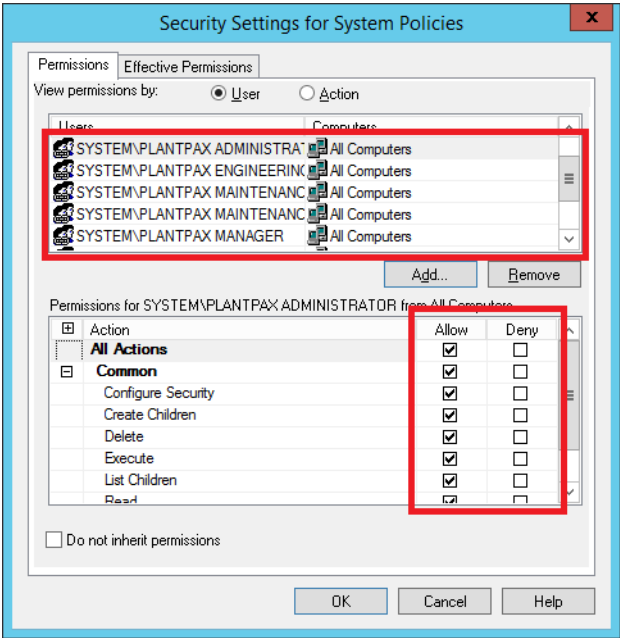
The Select User and Computer dialog box appears.

3. Select a PlantPAx group and click OK.



4. Repeat [step 3](#) to add each group.
5. When all groups are added, select one group at a time in the top half of the Security Settings for System Policies dialog box.

6. In the lower half of the dialog box, do one of the following actions:
- Click the ‘Allow’ or ‘Deny’ box for a bold-faced category to select all boxes.
 - Click ‘+’ in front of a bold-faced category to display a list of subcategories. Click each ‘Allow or ‘Deny’ box.



If Deny is selected, a warning message appears.

7. Click ‘Yes’ to verify a permission that is being denied, if applicable.
8. Click OK when finished.

[Table 23](#) is an example of security permissions per group classification.

Table 23 - Group Security Levels

System Policies	Operator	Operator Supervisor	Maintenance	Maintenance Supervisor	Manger	Engineer	Administrator
Configure Security	Deny	Deny	Deny	Deny	Deny	Allow	Allow
Create Children							
Delete							
Execute							
List Children							
Read							
Write							

See [Appendix A](#) for how to access an attachment that has suggested security permissions on a Microsoft Excel spreadsheet. The tabs include permissions for System Policies, Product Policies, Computer and Groups, Network and Devices, Users and Groups and Connections.

Define FactoryTalk Product Policies

Use an Engineering Workstation with these procedures.

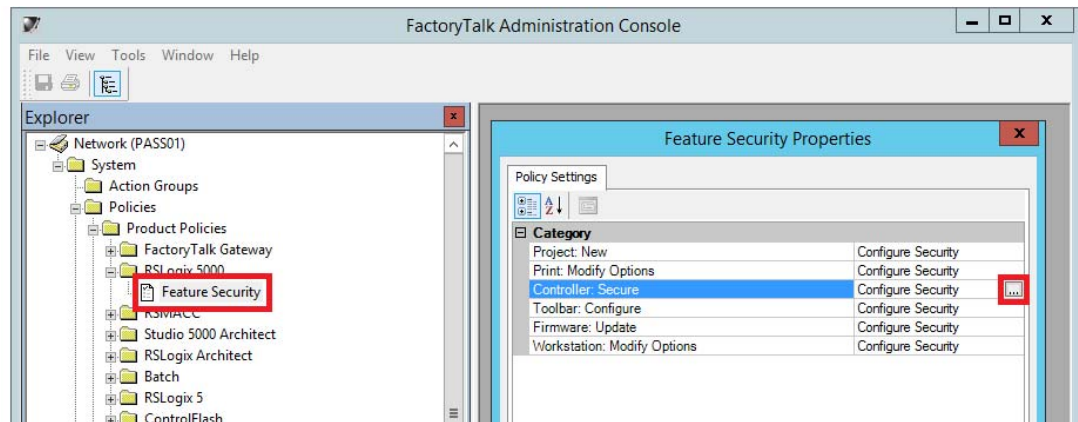


This section describes how to define users and groups with controller security in FactoryTalk software. Complete these steps.

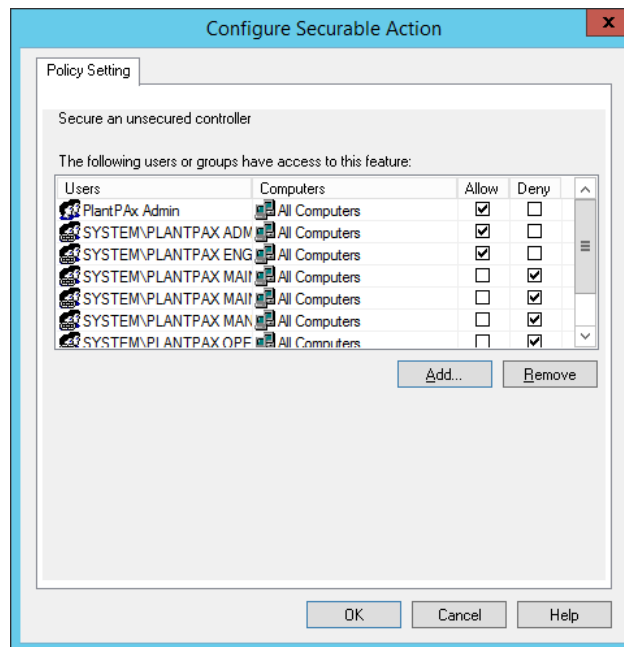
1. On the network directory, click System>Policies>Product Policies>RSLogix 5000®>Feature Security.

You also can configure feature security by clicking System>Policies, right-click Product Policies and choose Feature Security.

2. On the Policy Settings tabs, click Controller Secure.



3. Click Browse (...).
4. Click Add, select a PlantPAx group, and then click OK.



5. Repeat [step 4](#) to add all desired groups.
6. Click the 'Allow' or 'Deny' box.
7. Click OK.

Create Permission Sets

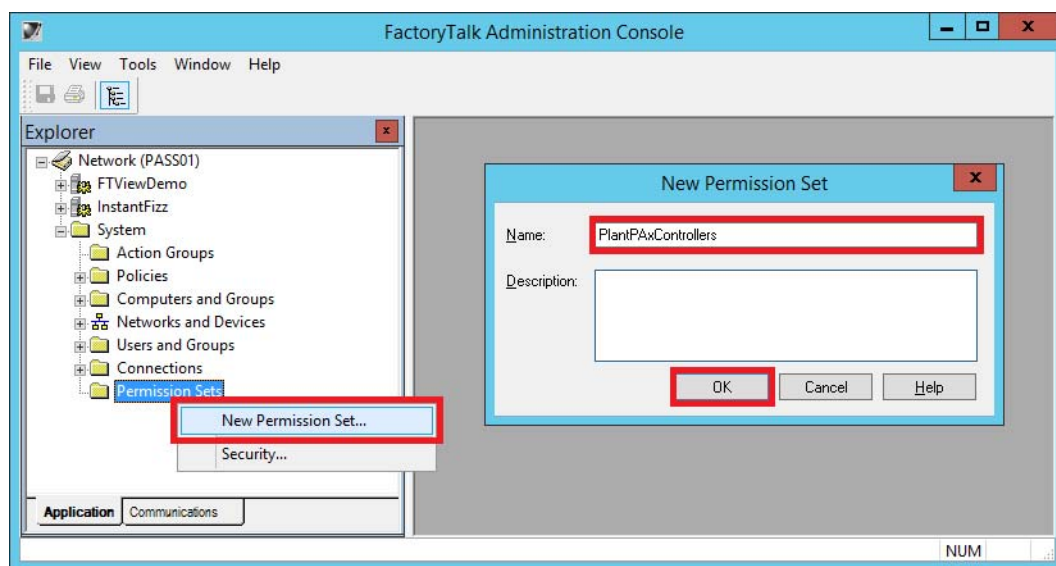
Permission sets are an option to identify a set of actions that are allowed or denied for one or more user groups or computer groups in a FactoryTalk network directory. The permissions are used with the controller security settings, and the same permissions can be used with multiple controllers.

When a user opens a project that has been secured with a permission set, the Logix Designer application verifies that the ID of the FactoryTalk Directory matches the ID stored in the project. Guest Users also can be assigned permissions.

For more information, see the FactoryTalk Security System Configuration Guide, publication [FTSEC-QS001](#).

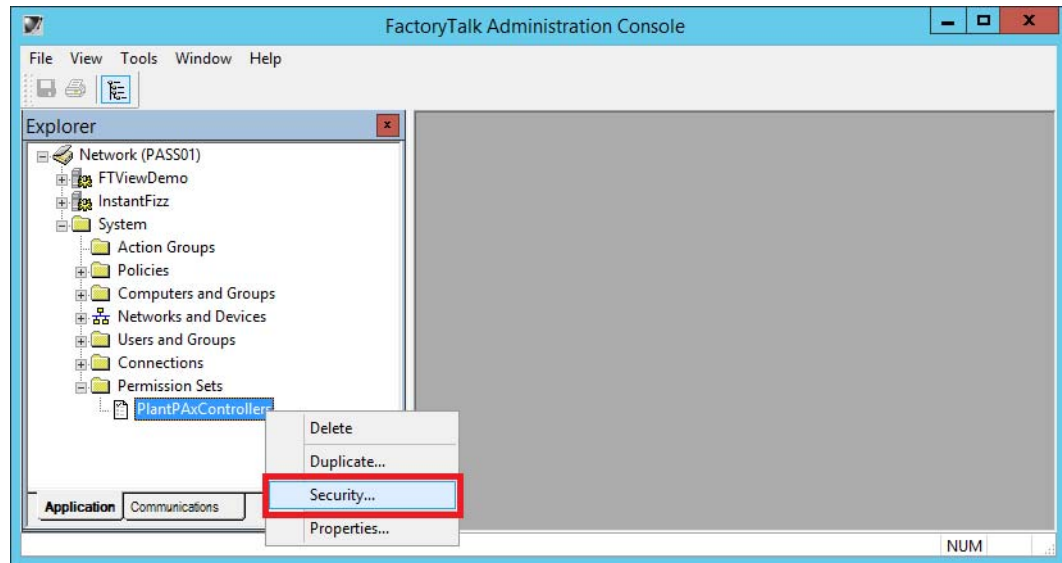
Complete these steps.

1. On the FactoryTalk Administration Console, right-click Permission Sets and choose New Permission Set.

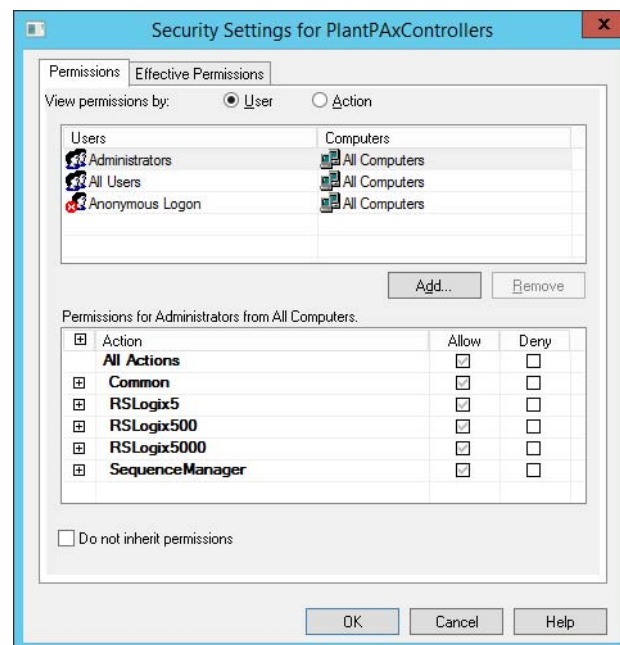


2. Type a name for the permission set and click OK.

3. In the left column under Permission Sets, right-click the permission set name and choose Security.



The Security Settings for PlantPAx Controllers appears.



4. Set the allowable actions by clicking the respective Allow or Deny checkboxes.

Notes:

Configure the Controller

This chapter describes how to enable system communication and security enhancements for PlantPAx® system controllers. We assume that you have a basic understanding of the operation of Rockwell Automation® controllers. We do recommend that you review the sizing guidelines in the PlantPAx Distributed Control System Selection Guide, publication [PROCES-SG001](#), to use the controller that fits your system requirements.

To help mitigate the risk of data intrusion, controllers have enhanced protection with the Studio 5000 Logix Designer® application. The layer of device protection is independent of FactoryTalk® software security.

The security enhancements include the following (with the last three being independent of FactoryTalk):

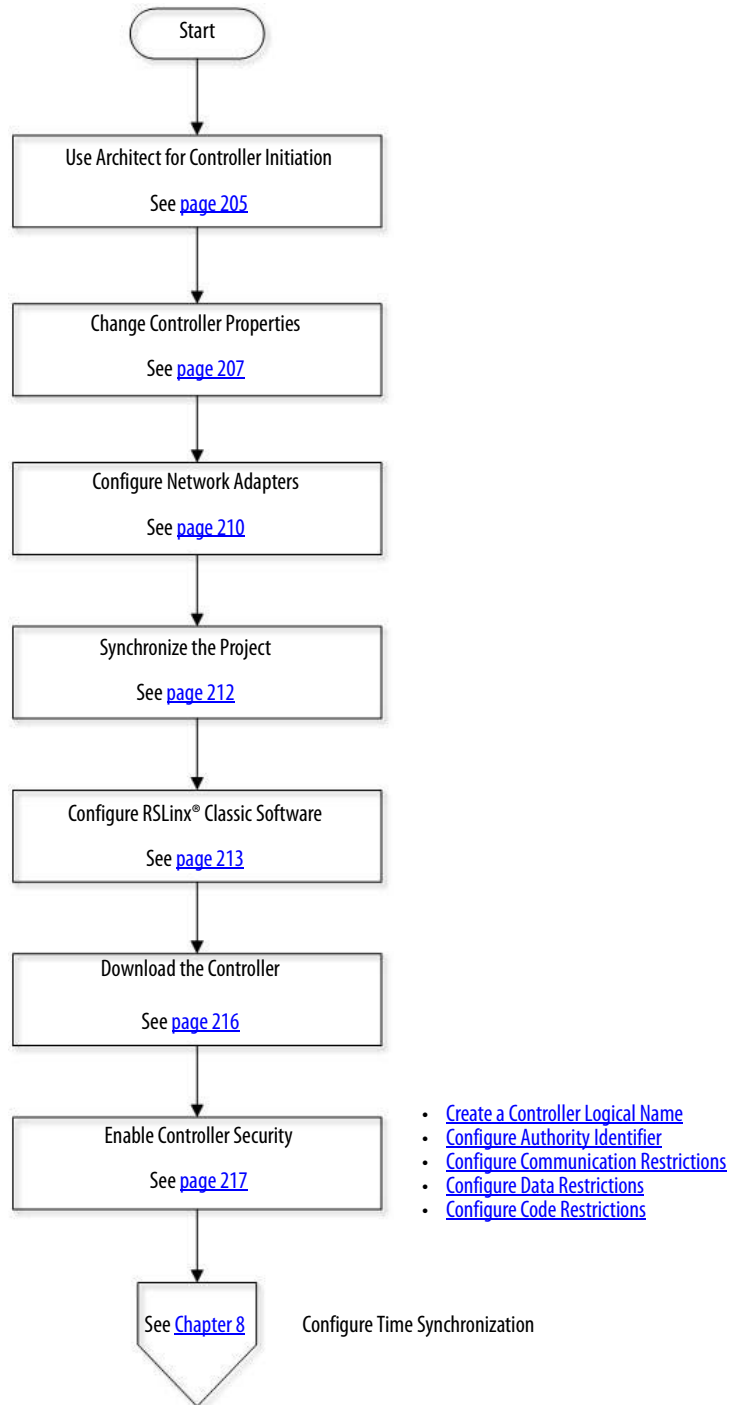
- **Security Server Validation**—To access a secured controller or project file, the application verifies via the FactoryTalk Directory that you are authorized for such use.
- **Restricted Communication**—ControlLogix® controllers accept communication only through selected slots.
- **Restricted External Data Access**—External Access and Constant tag attributes control access to tags and safeguard against changes to their values.
- **Source Protection**—A source key can be applied to routines and Add-On Instructions to guard against code from being edited inside the Logix Designer environment.

Consideration

Before starting this chapter, prioritize your system security level to match the authorized users in FactoryTalk Security.

[Figure 12](#) shows the topics that are described in this section. Click or see the page number for quick access to a section.

Figure 12 - Controller Security Workflow



Use Architect for Controller Initiation

Use an Engineering Workstation with these procedures.




The Studio 5000 Architect™ application provides a controller with pre-defined functionality that is based on the selected system template. Once you select a template and create a project, you must configure RSLinx software to communicate the software data to the controller.

There are three templates available depending on the size and scope of your project:

- **Distributed Architecture– Multiple Process Servers:** Contains two PASS servers; multiple Operator Workstations (OWSs), and an Engineering Workstation (EWS).
- **Distributed Architecture – Single Process Server:** Contains one PASS server; multiple Operator Workstations (OWSs), and an Engineering Workstation (EWS).
- **Process Skid with Logix Batch Sequence Manager:** Skid-based equipment that includes three CompactLogix™ controllers and one PanelView™ terminal to be integrated into overall system.

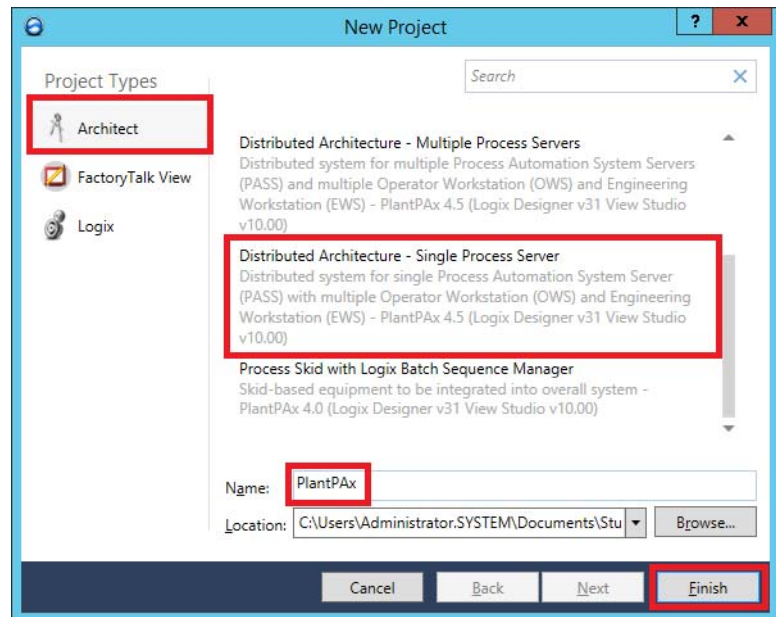
Complete these steps to select a template.

1. Click the Programs  symbol and choose Rockwell Software® > Studio 5000®.

The Studio 5000 Common Launcher appears.



The New Project dialog box appears.

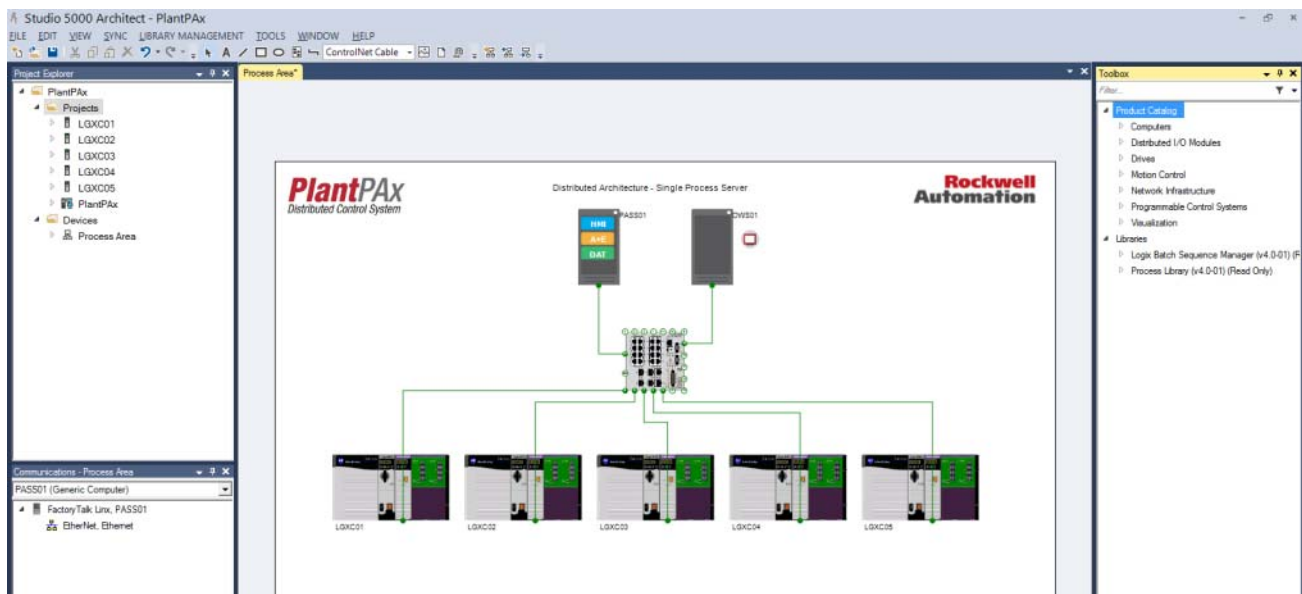


2. Under Project Types, click to select Architect and then click the second template (Distributed Architect - Single Process Server) for this example.

TIP The Common Launcher dialog box is used for all products in Studio 5000 environments. The product types that appear in the left pane depend on the products that are installed for your workstation.

3. Type a program name and click Finish.

The Architect canvas can take a couple minutes to open. The canvas appears with a layout of the architecture and a pre-defined controller for the selected template.



For a detailed description of the Architect application, see the PlantPAx Distributed Control System Application User Manual, publication [PROCES-UM003](#).

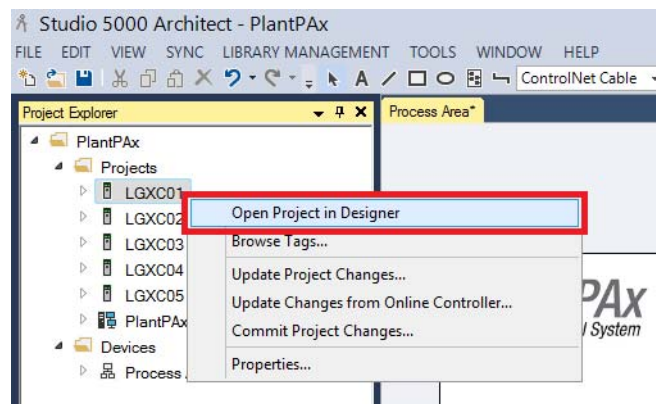
Change Controller Properties

Use an Engineering Workstation with these procedures.

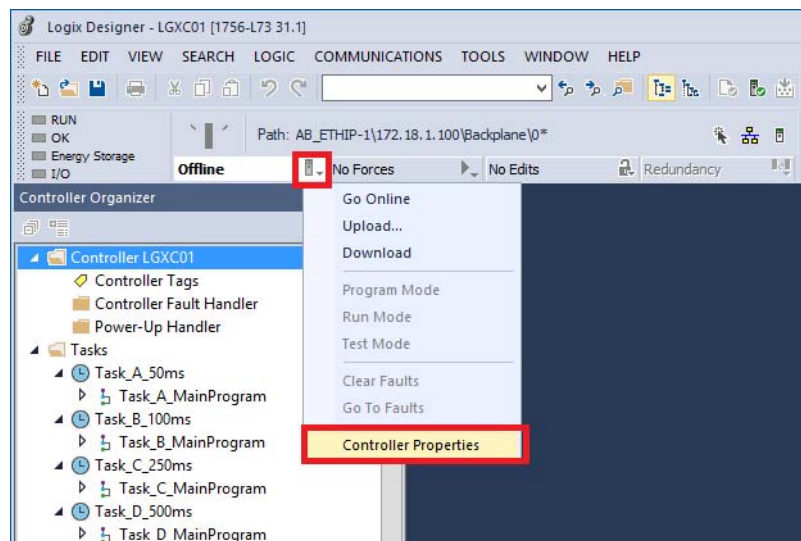


This section shows how to use the Studio 5000 Logix Designer application inside the Architect project to modify a controller. Changes include how to select another controller type, assign a name, and to enable redundancy, if applicable. Complete the following steps.

1. In the top, left pane of the Architect project, right-click a controller (LGXC01 in our example) and choose Open Project in Designer.

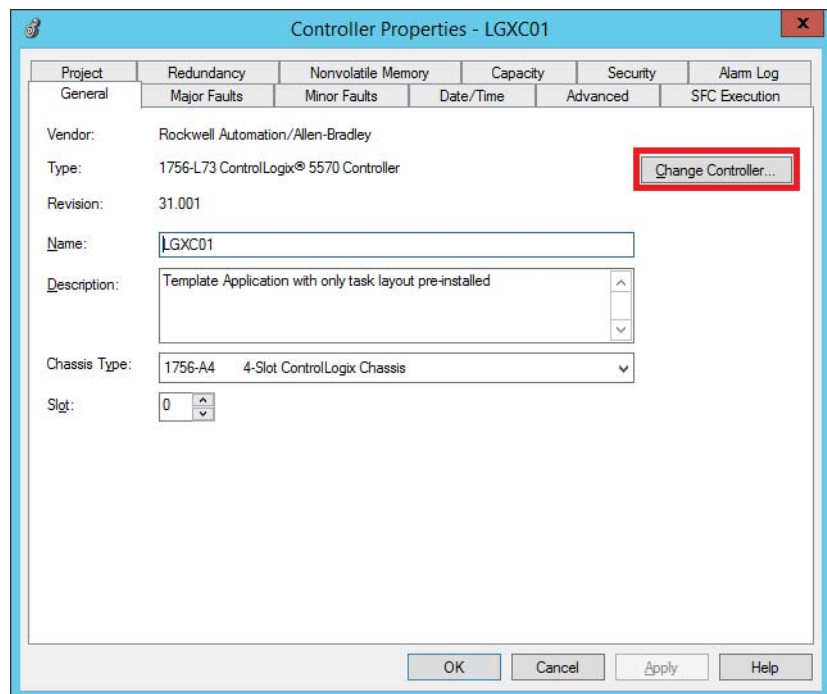


Wait a short time while the Logix Designer application opens.



2. Right-click the controller icon  and choose Controller Properties.

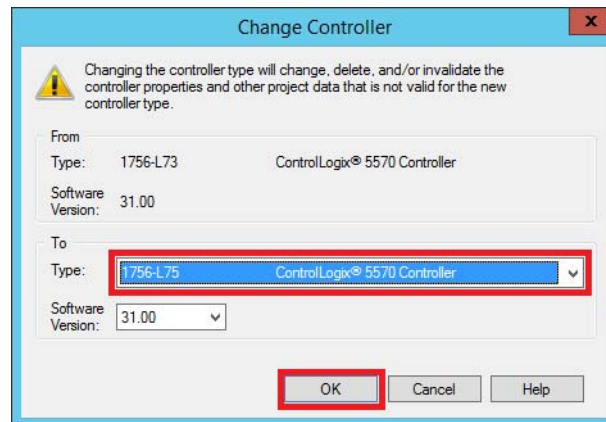
The Controller Properties dialog box appears.



You can modify the controller name in the Name field. The template default is 'LGXC01'.

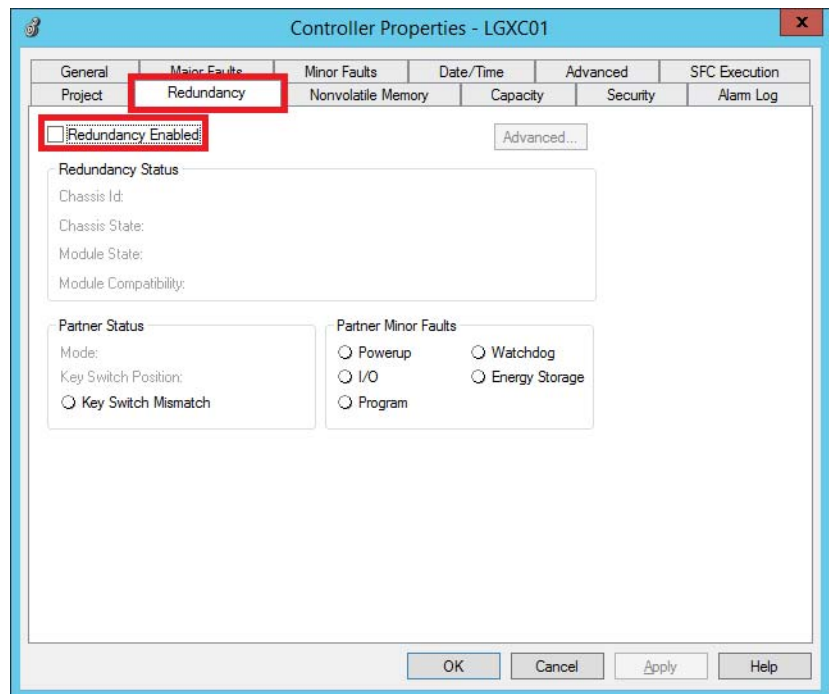
If you change the name to a specific area, for example 'Boiler', that is the controller name after the application is synchronized.


3. To select another controller type, click Change Controller.



4. Click the pull-down menu, select another controller from the list, and click OK.

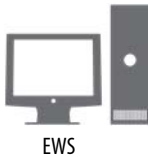
5. If you are using a redundant controller, click the Redundancy tab.



6. Check the Redundancy Enabled box (**only** if you are configuring this controller for redundancy) and click OK.
7. Click the Save icon  at the top of the Logix Designer window.

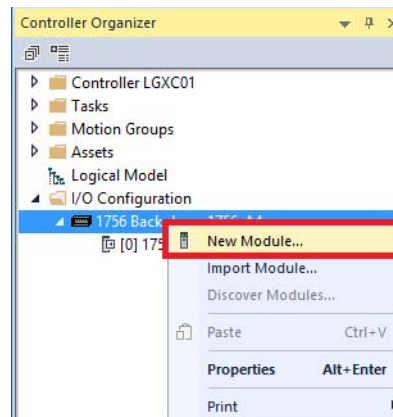
Configure Network Adapters

Use an Engineering Workstation with these procedures.

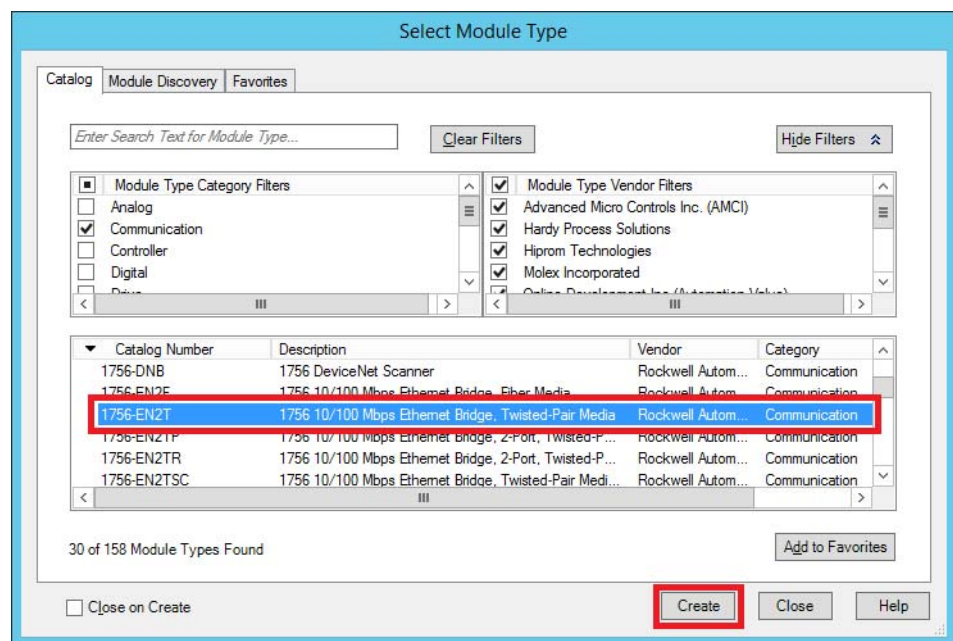


A local communication adapter added to a Logix controller provides for communicate with PASS servers and workstations at the Supervisory level. Complete these steps.

1. Open a Logix Designer project.
2. In the Controller Organizer, right-click the controller backplane and choose New Module.

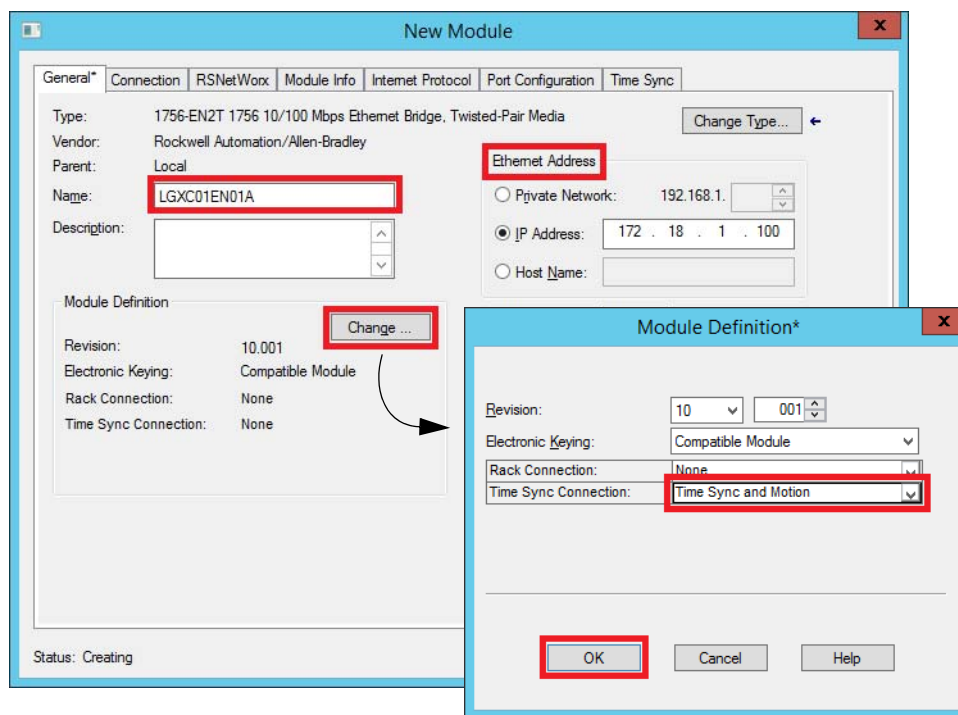


The Select Module Type dialog box appears.



3. Select a communication adapter for your application (Ethernet module in our example) and click Create.

The New Module dialog box appears.



4. Type an adapter name and IP address.
See [Table 24](#) for details.
5. Click Change.
6. On the Module Definition dialog box, select Time Sync and Motion from the Time Sync Connection pull-down.
7. Click OK.
8. Repeat [step 2](#) through [step 7](#) for each slot in the local chassis of the target controller.

IMPORTANT You must synchronize your project to update the changes with the existing controller information. This option sends the modified project from Logix Designer back to the Architect application. See [page 212](#).

Table 24 - Network Adapter Information

Name	IP Address	Architecture	Cat. No.
LGXC01EN01A	172.18.1.100	Star	1756-EN2T
LGXC01EN01B	172.18.1.101	Star	1756-EN2T
LGXC01EN02	172.18.2.10	Device Level Ring/Star	1756-EN2TR

Synchronize the Project

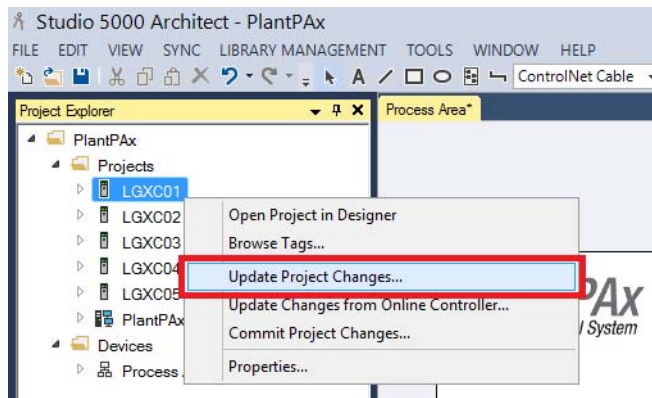
Use an Engineering Workstation with these procedures.



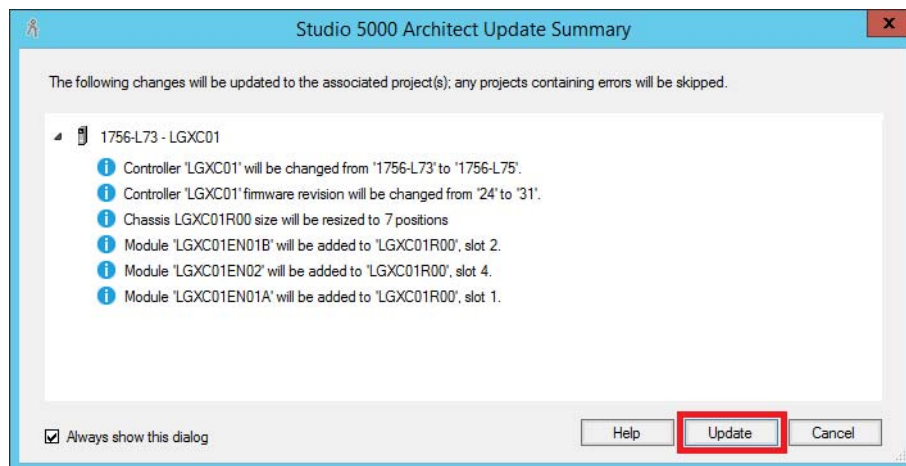
EWS

Complete these steps to update controller information in the Architect application.

1. In the Architect application, right-click the controller and choose Update Project Changes.



The Update Summary dialog box appears.



2. To see a preview of the synchronized changes, click ▸ to expand the project.

The changes appear in the Message box.

3. Click Update.

The Ethernet Configuration dialog box appears.

4. Leave the devices and their port configuration as is, and click OK.


A wait message appears while the project is being synchronized.

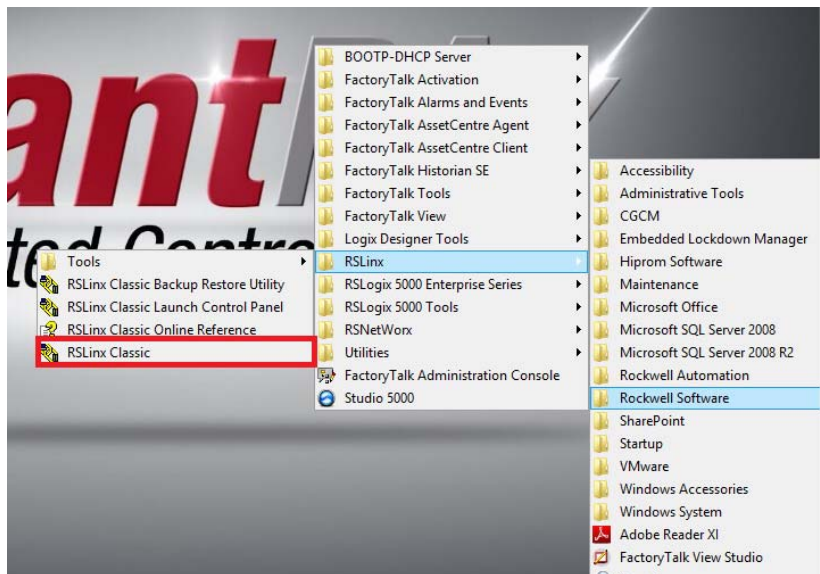
Configure RSLinx Classic Software

Use an Engineering Workstation with these procedures.



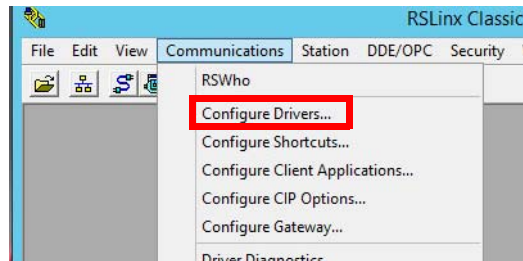
Complete these steps to configure RSLinx Classic software, which is a communication interface between the controller and FactoryTalk View software products. Examples show how to configure two drivers: EtherNet/IP and Ethernet.

1. Click the Programs  symbol and choose Rockwell Software>RSLinx>RSLinx Classic.



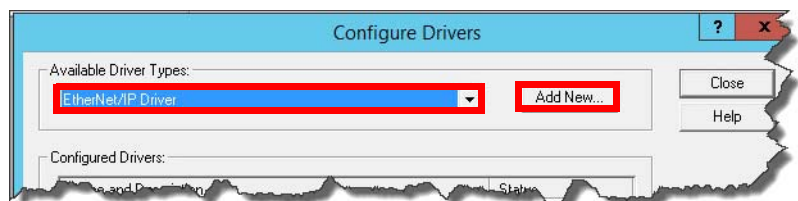
The RSLinx Classic dialog box appears.

2. Click the Communications tab and choose Configure Drivers.

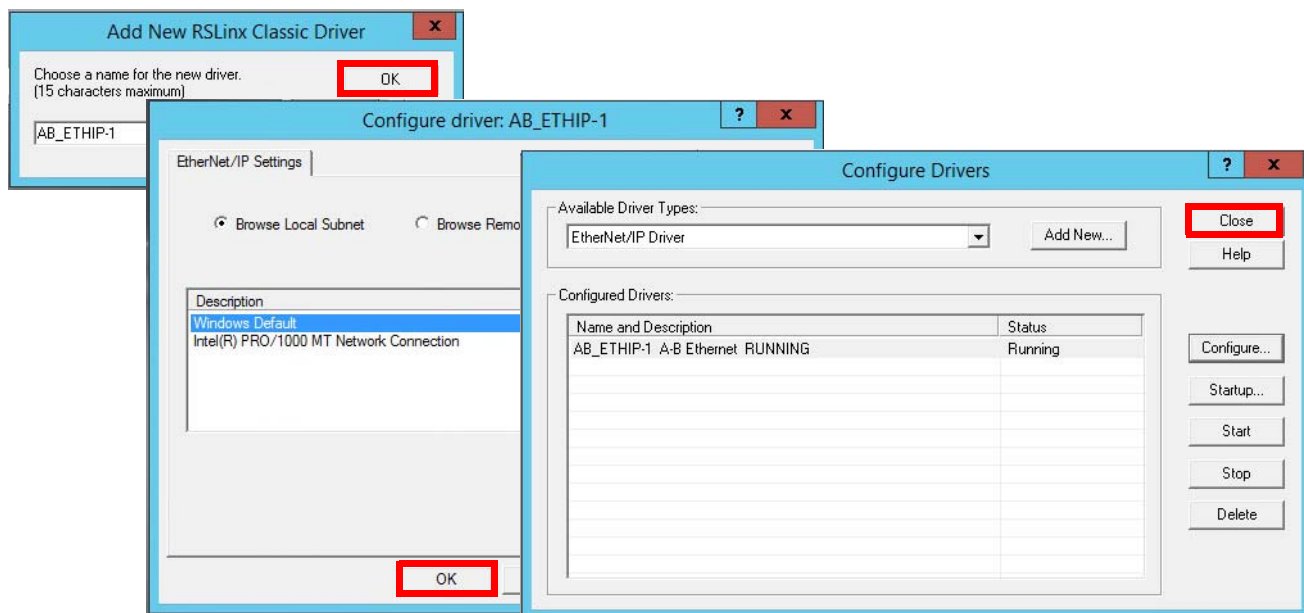


The Configure Drivers dialog box appears.

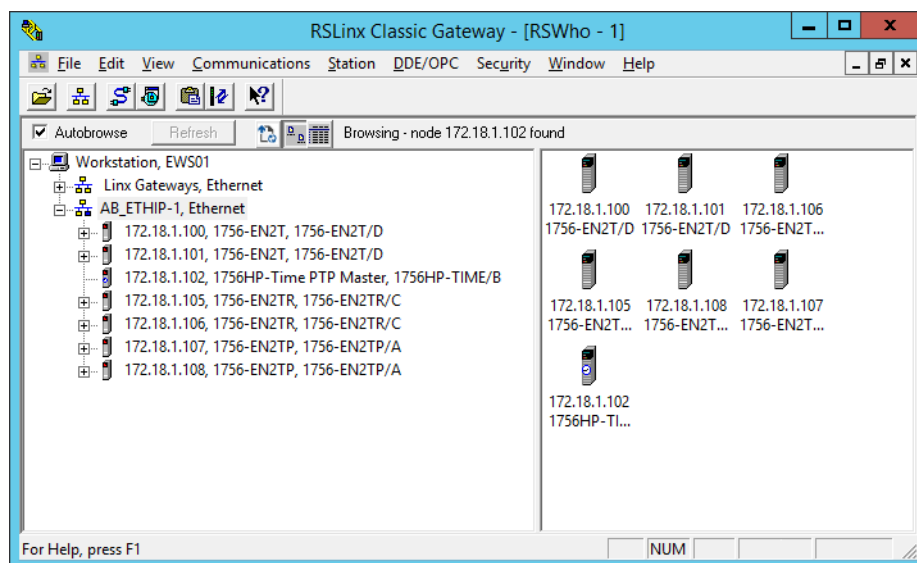
3. From the Available Driver Types pull-down menu, select the EtherNet/IP Driver and click Add New.



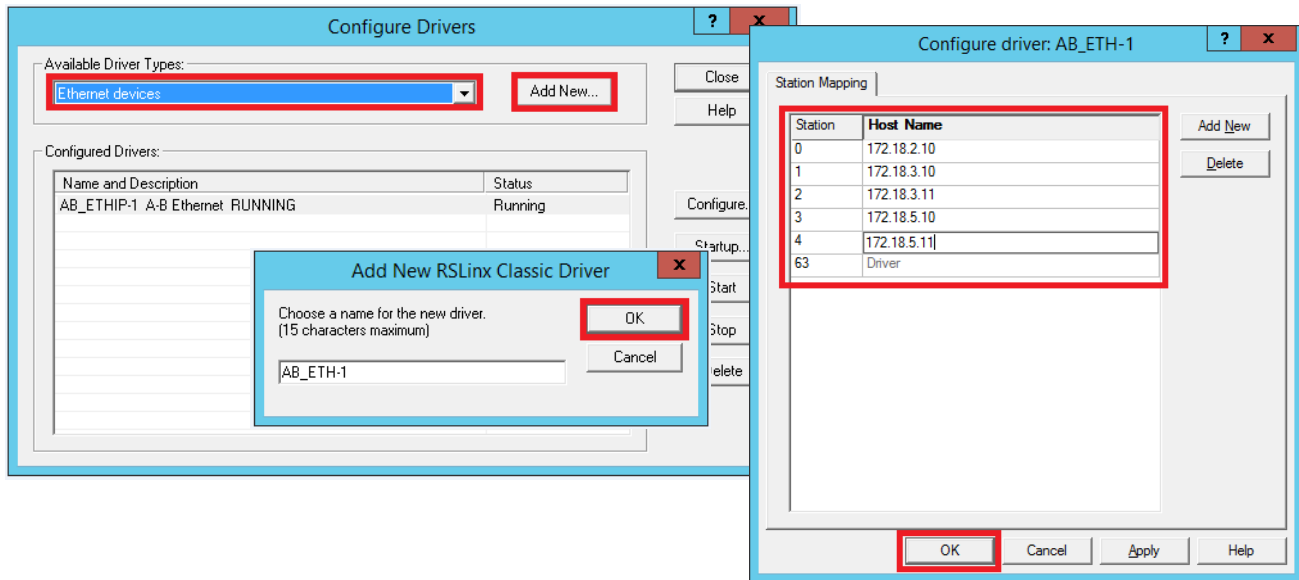
4. To complete the driver selection, click OK and then Close on the following dialog boxes.



The EtherNet/IP devices in the network appear under the network communication driver.

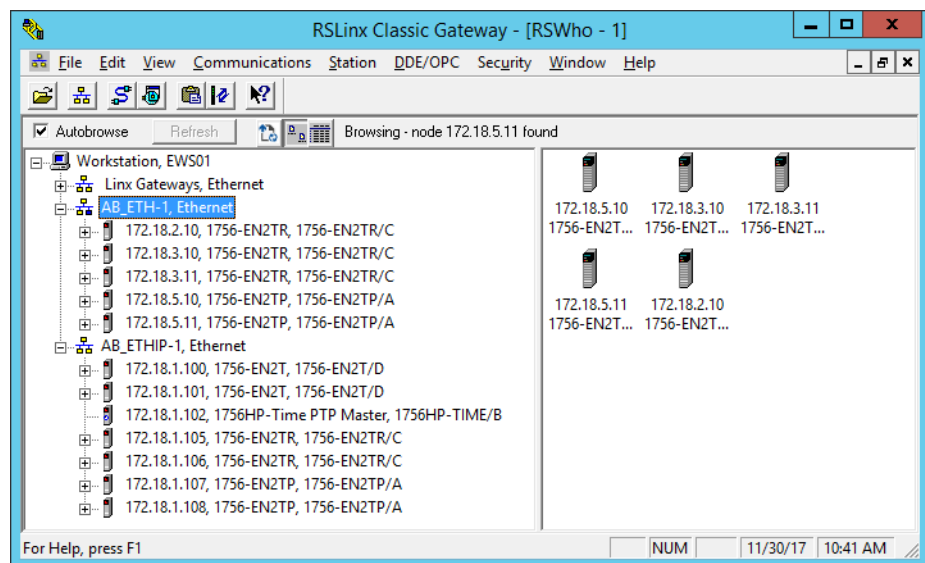


5. To add an Ethernet driver for routing in another network, repeat [step 1](#) and [step 2](#).
6. Select Ethernet devices and click Add New.



7. Click OK and type IP addresses.
8. Click OK.

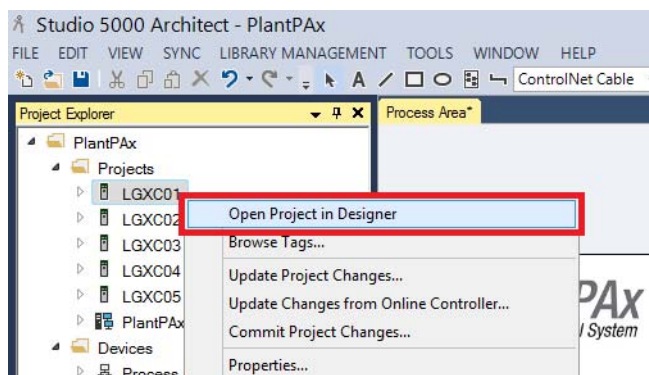
The Ethernet devices in the network appear under the network communication driver.



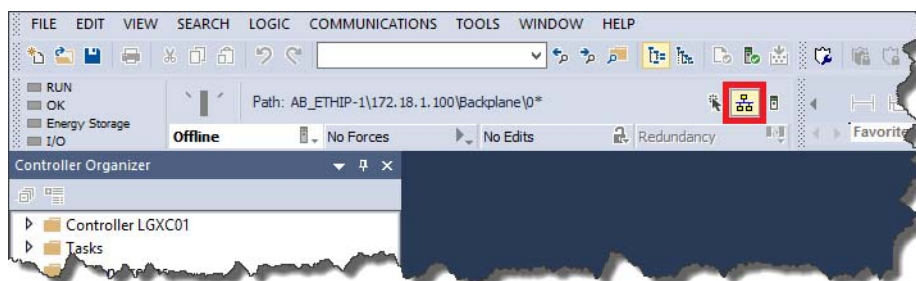
Download the Controller

Complete these steps to download the controller.

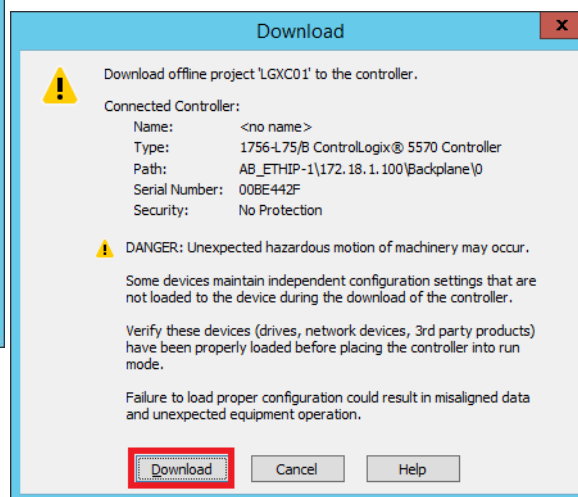
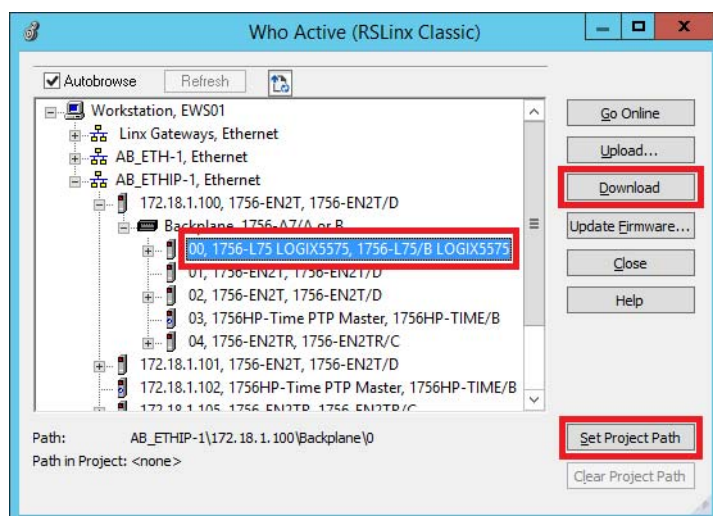
1. In the Architect project, right-click a controller (LGXC01 in our example) and choose Open Project in Designer.



2. Click the Who Active button.




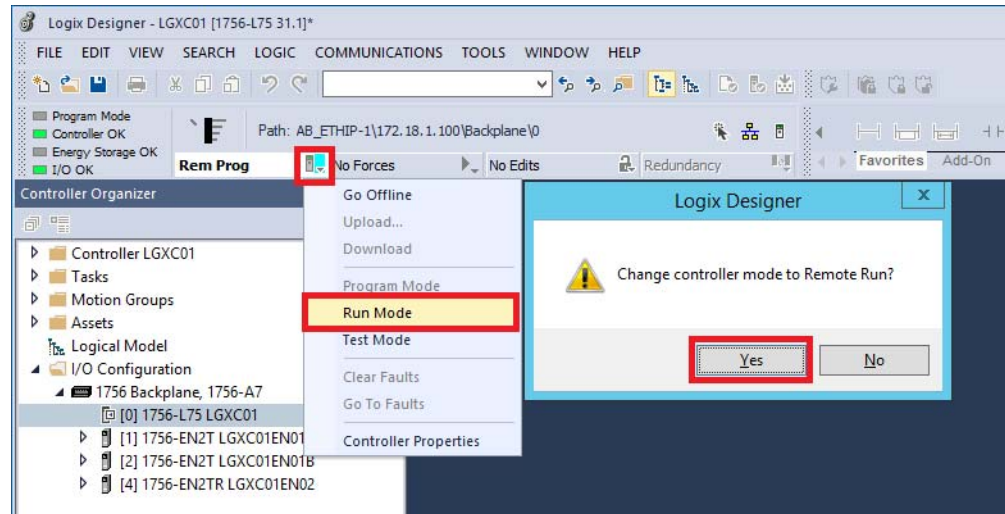
3. Browse the controller through the communication path (this action updates the path).
4. Click the controller path, Download, and then Set Project Path.



5. Click Download again.

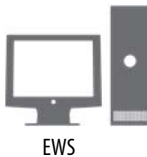
The Download Project Documentation and Extended Properties box enables multiple parties to share information.

6. Click the controller  symbol and select Run mode.
7. Click Yes.



Enable Controller Security

Use an Engineering Workstation with these procedures.

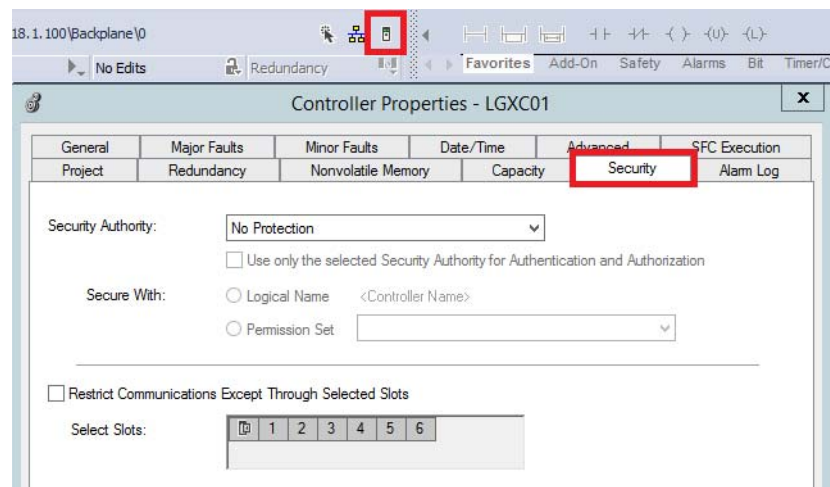


You must be an authorized user to administer controller security.

IMPORTANT This procedure requires that you have defined FactoryTalk product policies. See [page 199](#).

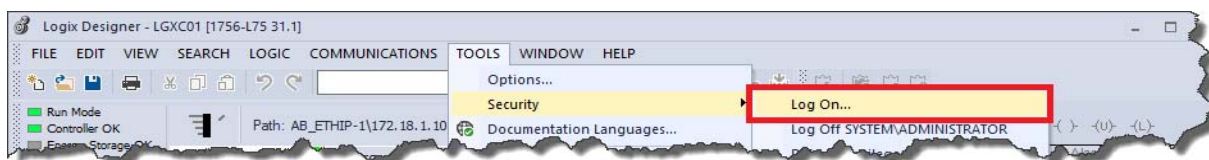
Complete these steps.

1. In the Controller Organizer of the Logix Designer application, double-click the controller icon to open the properties.

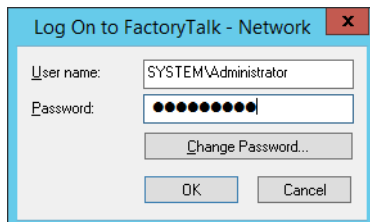


2. Click the Security tab.

- From the Tools menu, right-click Security and choose Log On.

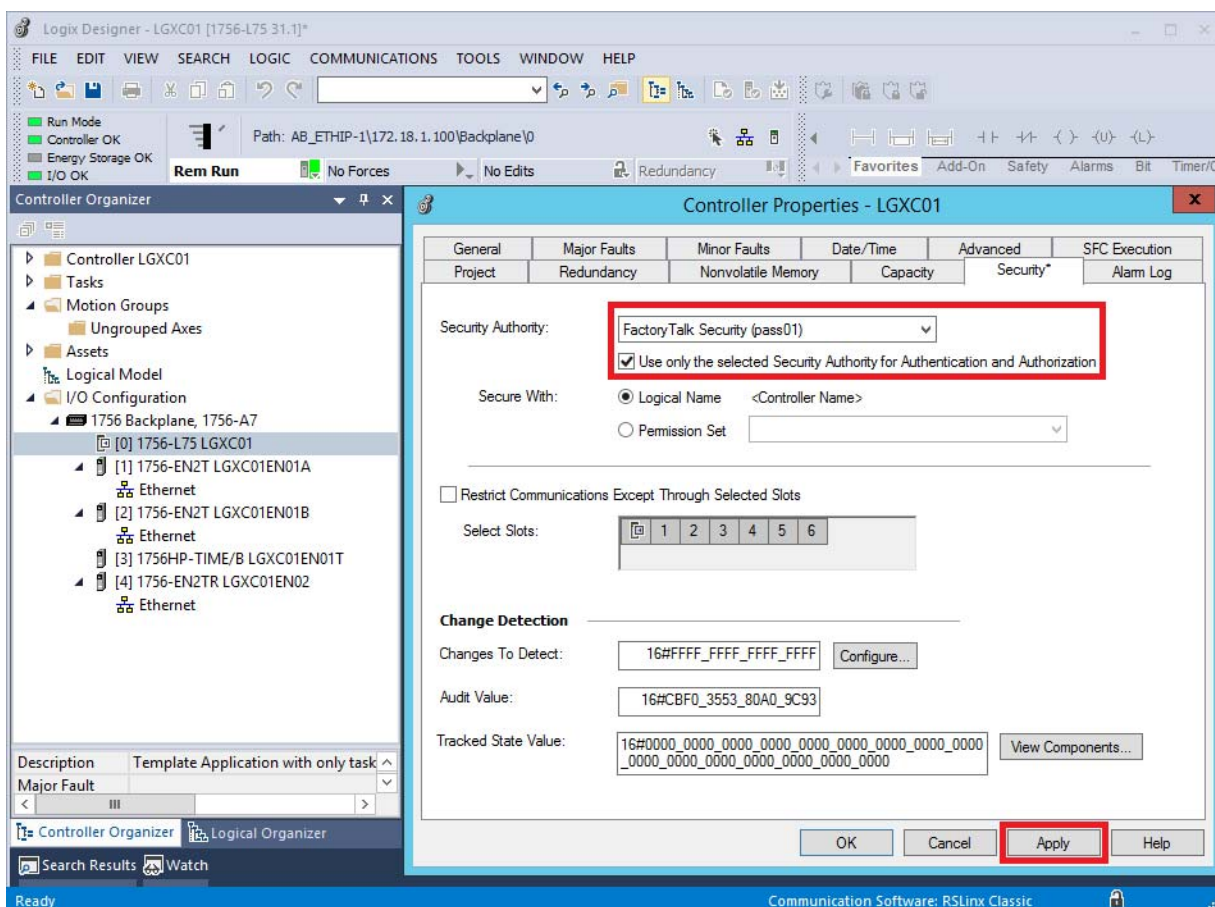


- Type an authorized user name and password and click OK.



See [page 217](#) to configure users with controller security.

- Click Yes on successive dialog boxes to confirm the project.
- In the Controller Organizer, double-click the controller to open the properties dialog box; click the Security tab.



- Select FactoryTalk Security Directory from the Security Authority pull-down menu.

- Click Use only the selected Security Authority for Authentication and Authorization and click Apply.

A warning message appears.

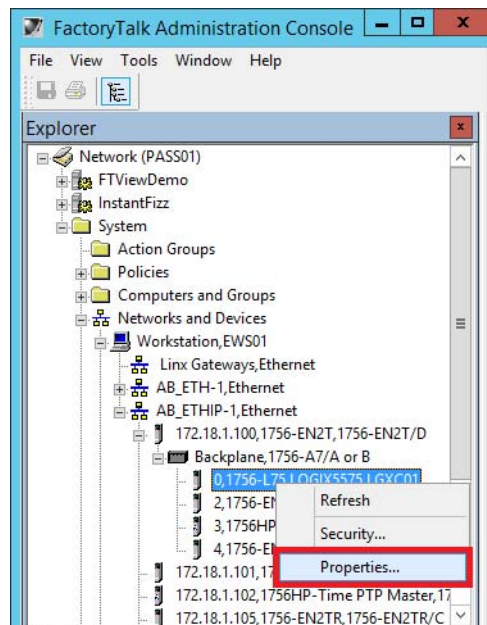


- Click Yes.

Create a Controller Logical Name

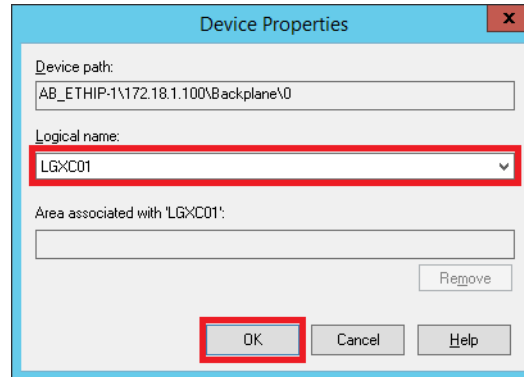
Complete these steps to create a name for the controller in the FactoryTalk Directory.

- Click the Programs >> symbol and choose Rockwell Software>FactoryTalk Administration Console.
- Browse to the controller and then browse to the communication driver.
- Right-click the communication driver and choose Properties.



- On the Device Properties dialog box, click the pull-down and select the controller name.

TIP If the name does not appear in the Networks and Devices tree, open RSLinx Classic and go to the controller resource with RSWho. When you navigate to the resource in RSLinx Classic the controller path information updates in RSLinx Classic.




- Click OK.

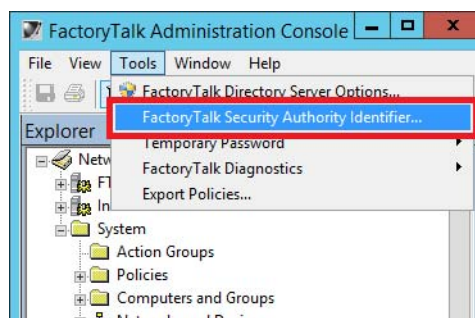
Configure Authority Identifier

This optional procedure is necessary only if you want to access a controller project from outside the system and still use FactoryTalk security. Projects that are secured to a specific Security Authority cannot be recovered if the identifier of the FTD that is used to secure the project no longer exists.

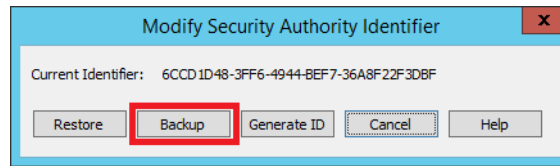
IMPORTANT We recommend that you back up the FTD and save unsecured versions of the project file to a secure location.

Complete these steps.

- Click the Programs  symbol and choose Rockwell Software>FactoryTalk Administration Console.
- Click the Tools menu and choose FactoryTalk Security Authority Identifier.

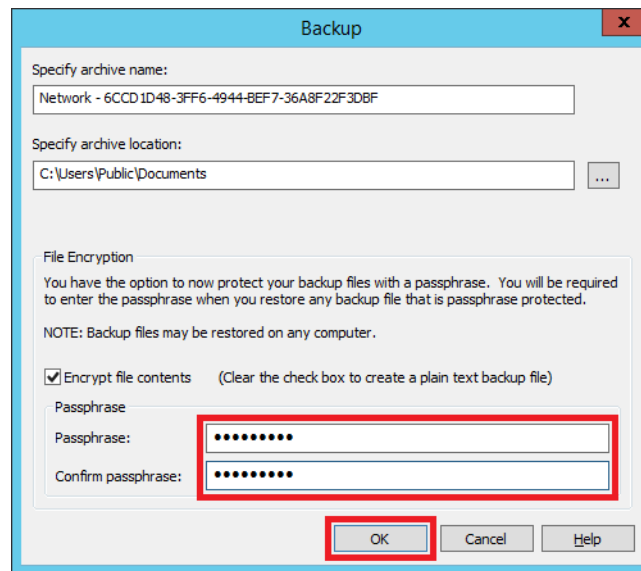


- Click Backup on the message window.



We recommend that you encrypt the file and enter a passphrase that you use during the restore process.

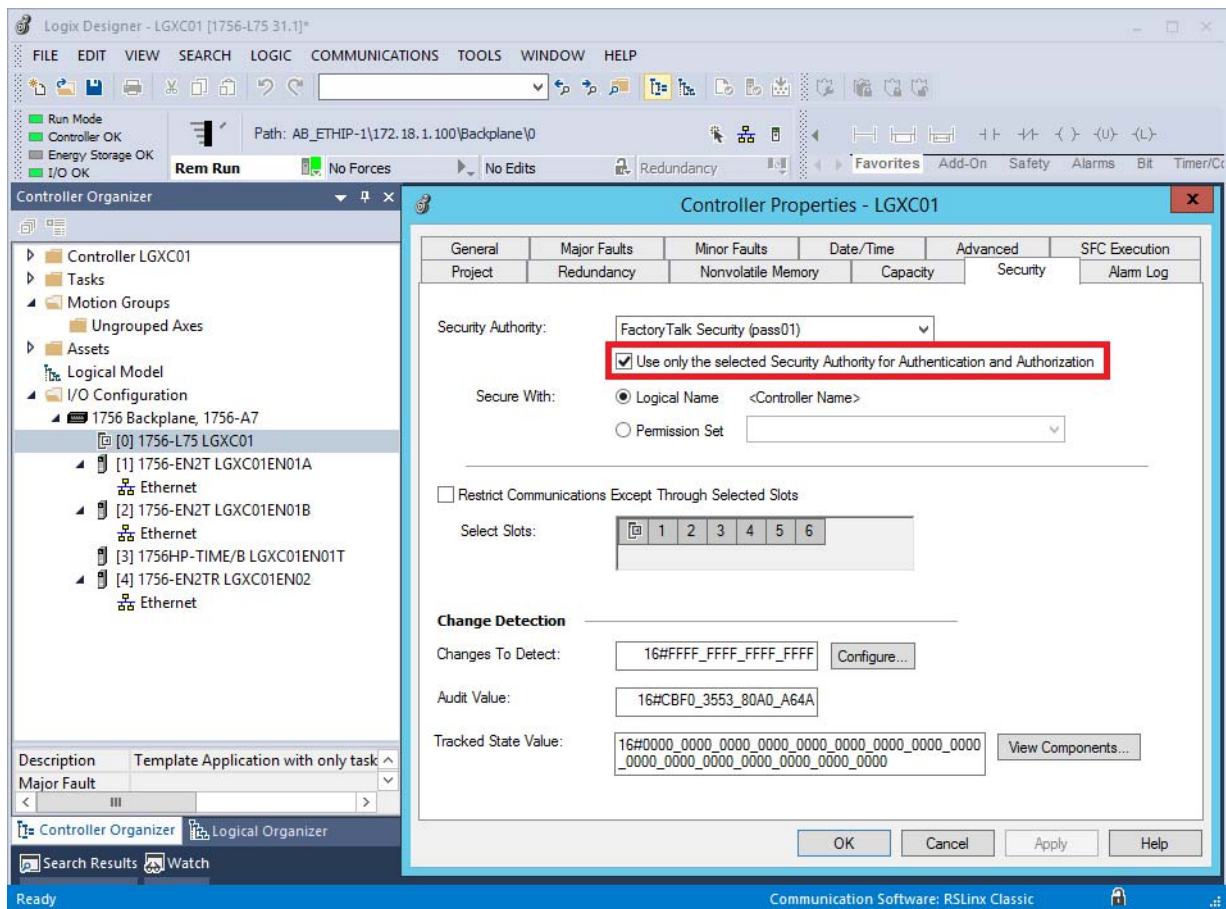
- On the Backup dialog box, click 'Encrypt file contents' and type a passphrase; click OK.



Complete these steps to restore a project on another computer.

- Repeat [step 1](#) and [step 2](#) on [page 220](#).
- Click Restore on the message window.
- Select a file and click Next.
- Type the Restore passphrase and click OK.
- Select 'Restore Security Authority in Identifier Only'.
- Click Finish.

The Logix Designer application can be opened now in another system directory. Observe the check in the box for 'Use only the selected Security Authority for Authentication and Authorization.'



The following steps are required if the file is returned and the authority identifier does not work.



1. Click the Programs » symbol and choose Rockwell Software>FactoryTalk Administrative Console.
2. Click the Tools menu and choose FactoryTalk Security Authority Identifier
3. Click Generate ID.
4. Click Close.

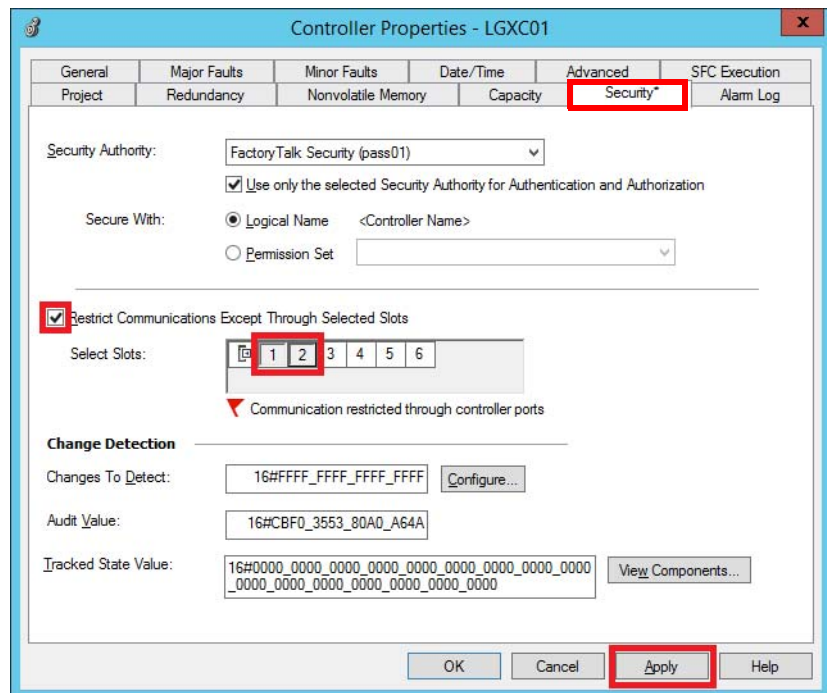
Configure Communication Restrictions

This section describes how to restrict non-authorized communication modules from being added to a ControlLogix backplane.

1. In an Architect project, right-click a controller and choose Open Project in Designer.
2. Under the I/O Configuration folder in the Controller Organizer, double-click the controller.

The Controller Properties dialog box appears.

3. Click the Security tab.



4. Click the Restrict Communications Except Through Selected Slots box.
5. Select each number that represents an authorized communication module slot in the controller.

Slot positions appear dimmed when selected.

6. Click Apply.

New data communication modules must have authorized access to be installed in the selected slots.

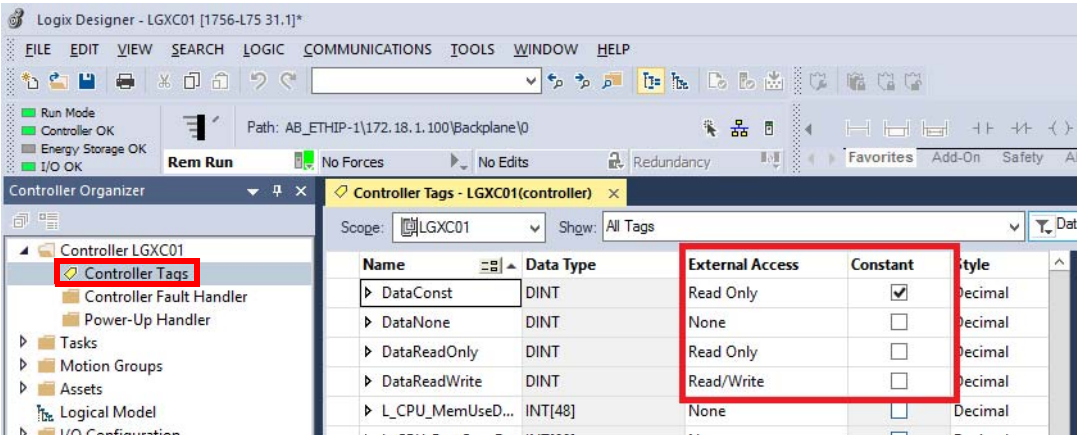
Configure Data Restrictions

This section describes how to program Logix data tags to control external application access, such as HMI applications. The three external access tags are the following:

- Read/Write
- Read Only
- None


1. In an Architect project, right-click a controller and choose Open Project in Designer.
2. Double-click Controller Tags.

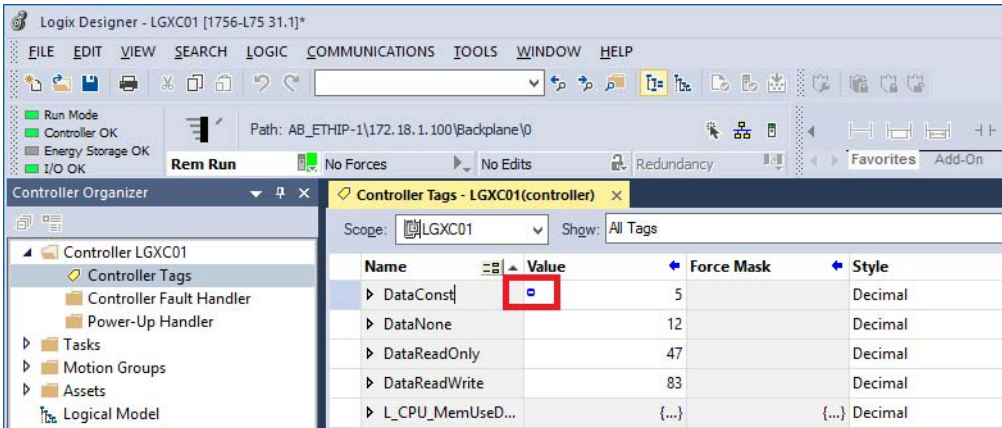
The tags appear in the right pane of the project.



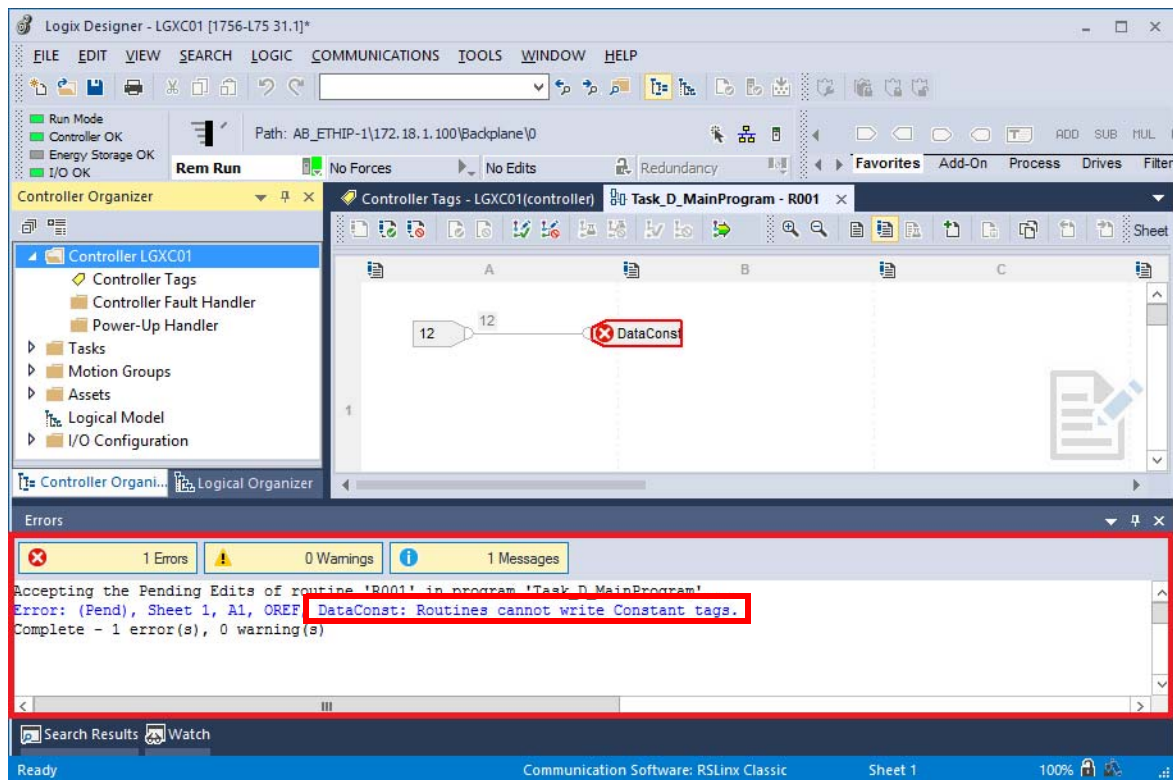
3. To create a write restriction, click Constant to create a Read Only tag.

A Constant tag cannot have its values changed programmatically.

A Constant tag symbol  appears in the Value column for the selected tag



The Logix Designer compiler helps prevent write data in the reserved data.

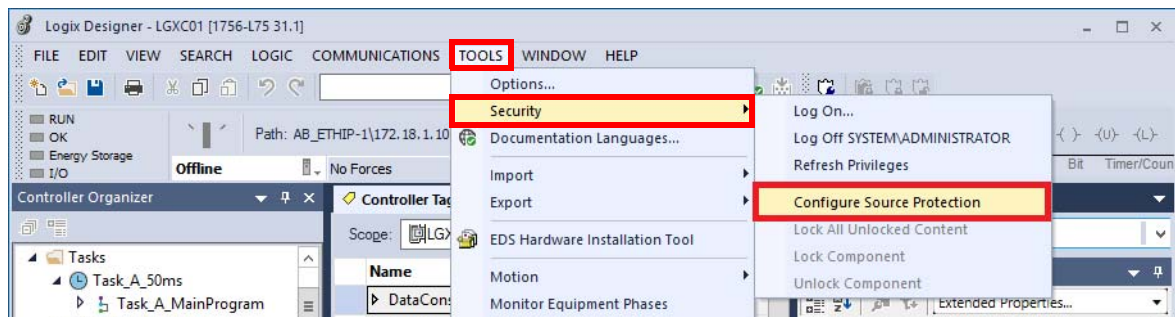


Configure Code Restrictions

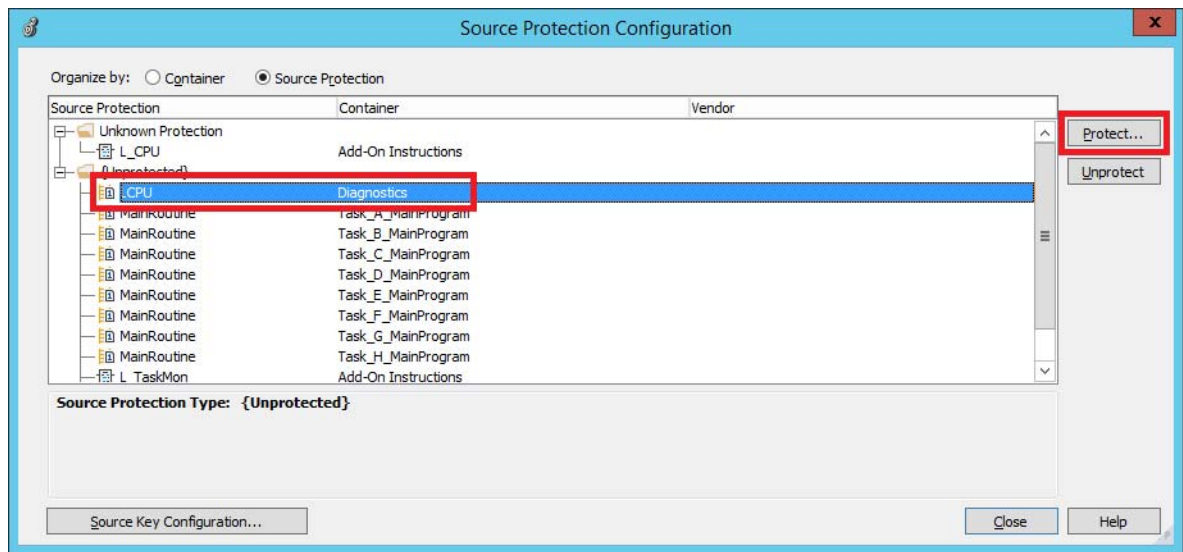
Source Protection is applied to routines and Add-On Instructions to help prevent third-party access to components. This section shows how to apply Source keys, which are user-generated, case-sensitive passwords.

Complete these steps in **Offline mode** to enable a source key.

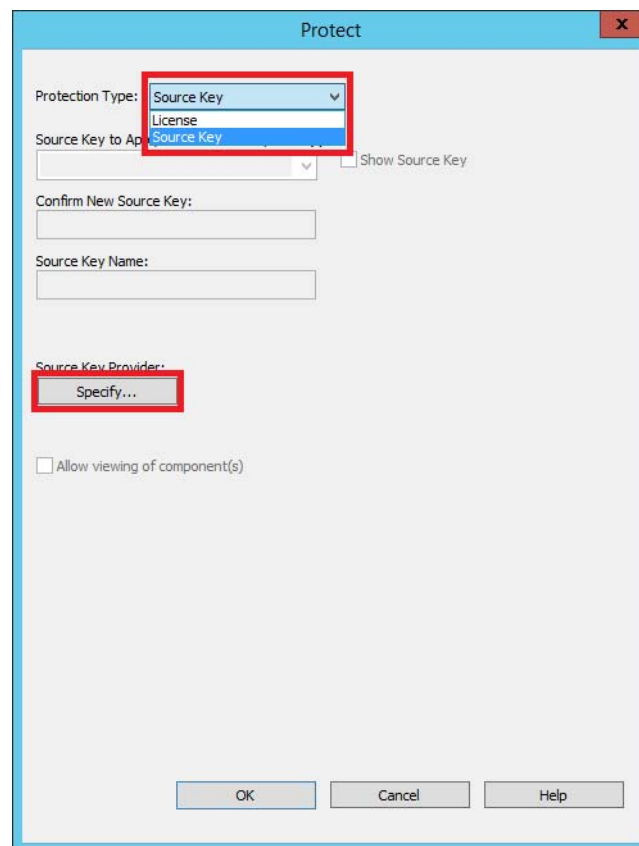
1. In an Architect project, right-click a controller and choose Open Project in Designer.
2. Click the Tools menu and choose Security>Configure Source Protection.



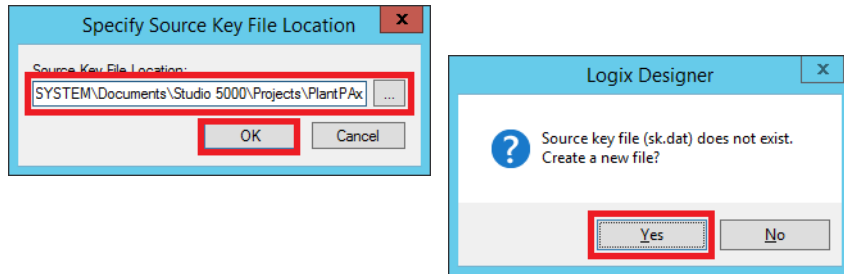
3. Select any desired routine or Add-On Instruction to be protected, and then click Protect.



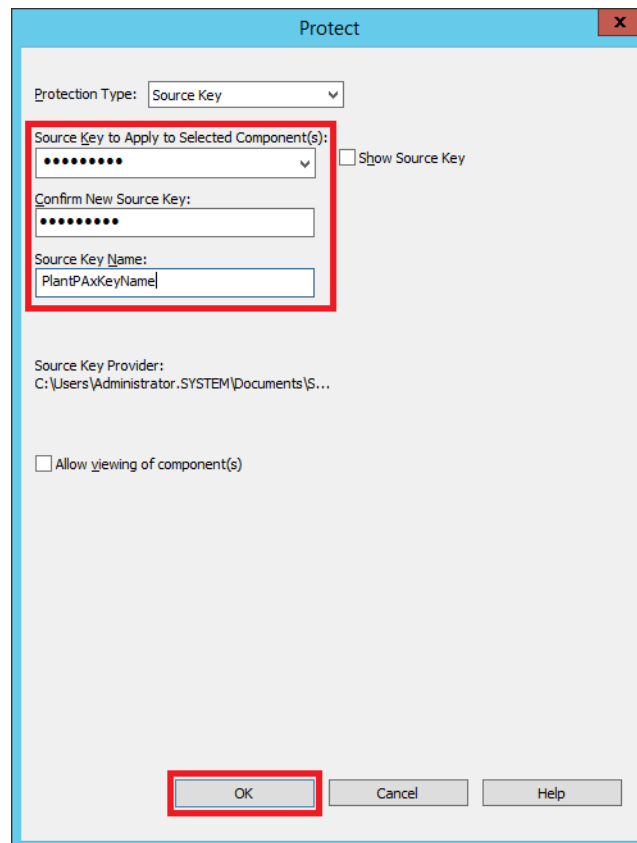
4. Choose Source Key from the Protection Type pull-down menu and click Specify.



5. To specify a source key location, click Browse (ellipsis '...') to the path and click OK.

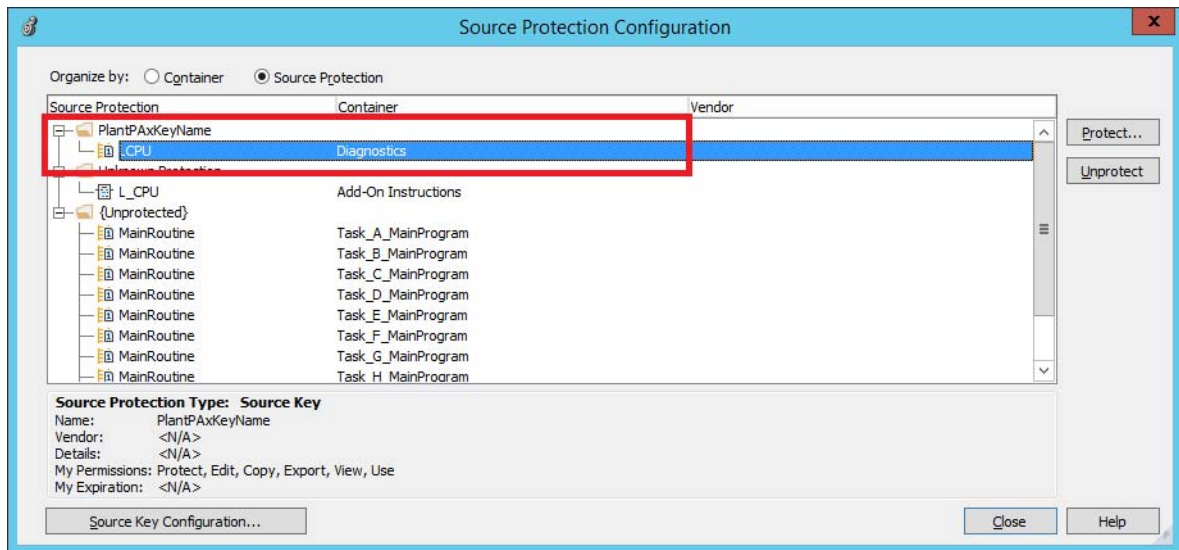


6. Click Yes to confirm the source key file creation (sk.dat).
7. Type a source key (and jot down) to be applied and then type the name as shown in the example graphic, 'PlantPAxKeyName.'

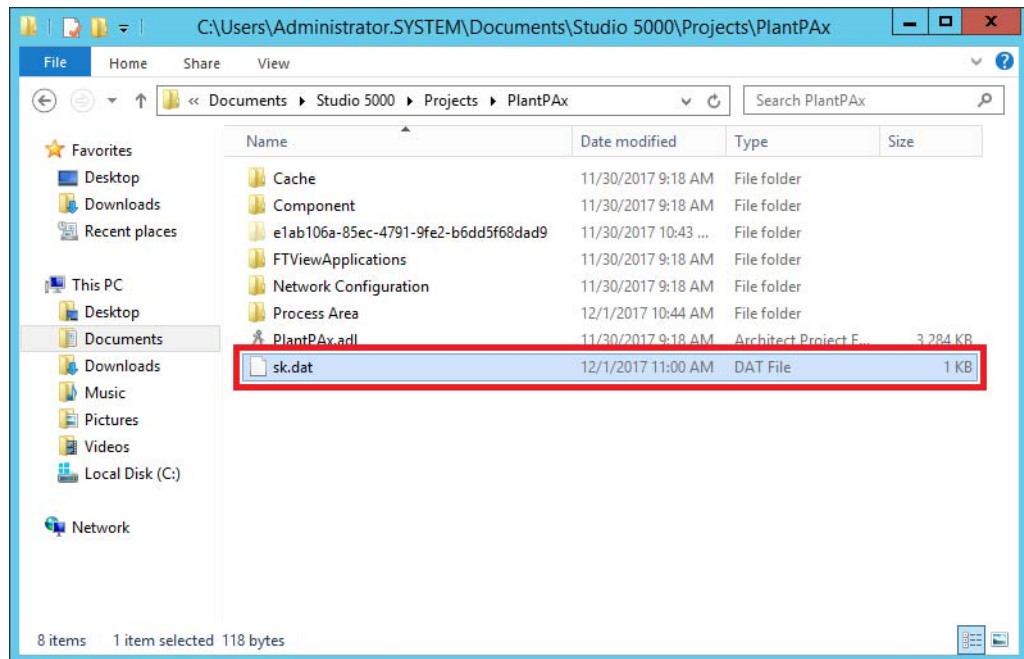


8. Click OK.

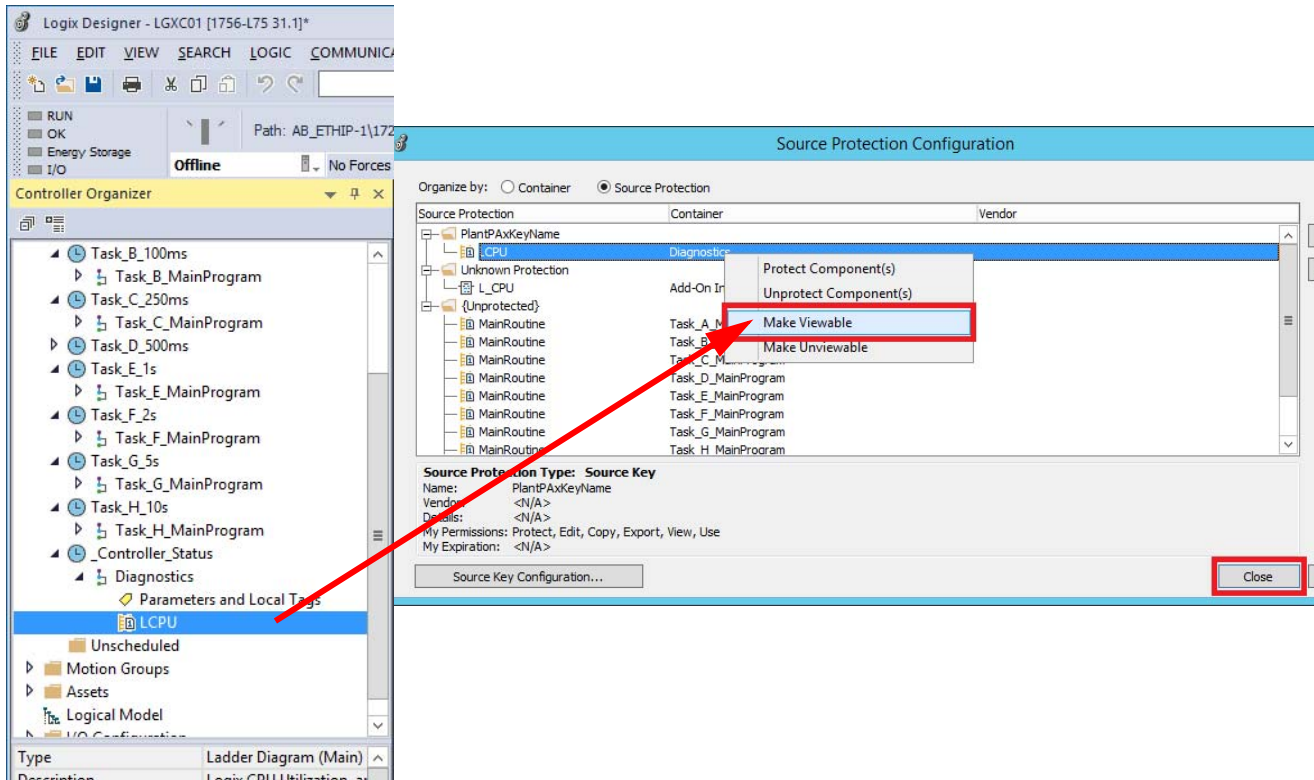
The source key name appears in the Source Protection column.



The source key file (sk.dat) is recorded in the path that you designated in [step 3](#).



If the source key file is moved from the designated file location, the component cannot be viewed.



9. To view the component, right-click the source key and choose Make Viewable.
10. Click Close.

Notes:

Configure Time Synchronization

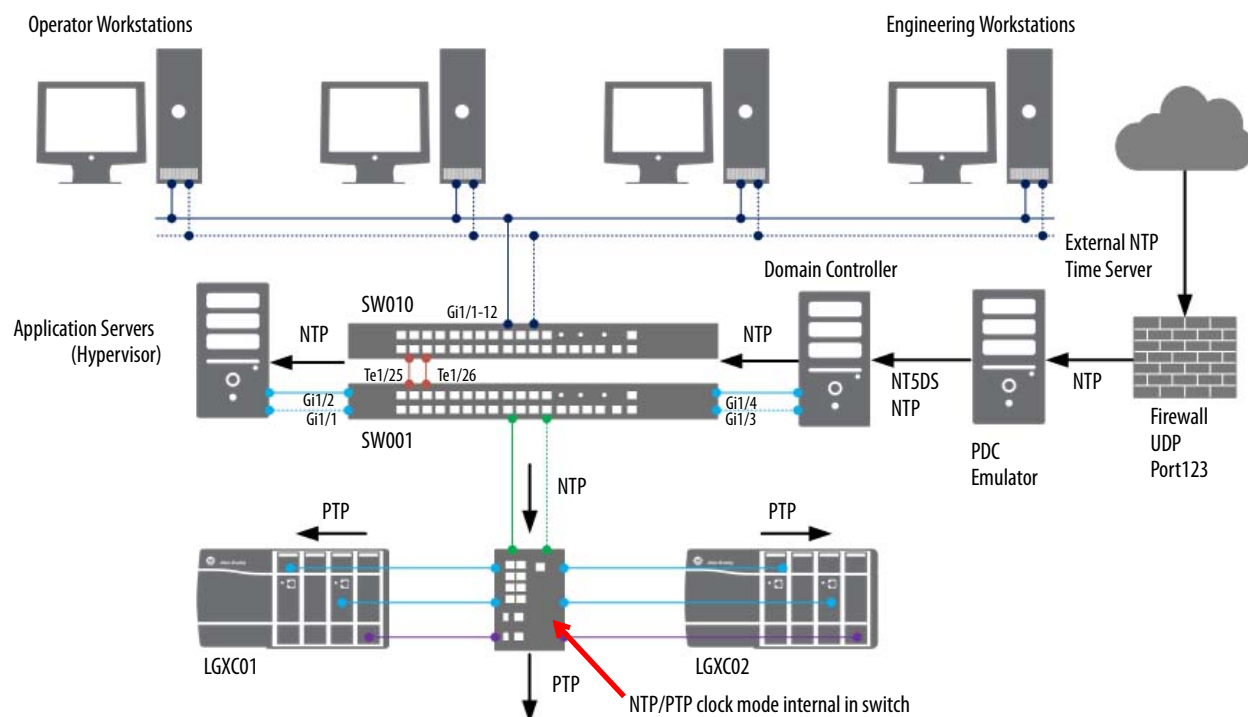
In a PlantPAx® system, time synchronization is essential for controllers, workstations, and servers to reference the same time for any event or alarm that occurs. To provide accuracy for sequence of events and historical data, several protocols are available to control and monitor the clocks. The internal clock deemed the reference is called the Grandmaster clock.

This chapter describes procedures for configuring time-sync applications by using two common protocols:

- Network Time Protocol (NTP)
- Precision Time Protocol (PTP)

NTP synchronizes time over the plant floor on an Ethernet network as shown in [Figure 13](#) and [Figure 14](#). NTP sources Coordinated Universal Time (UTC) as the universal standard for current time. Typically for Windows, a domain controller sources UTC time and becomes the Reliable Time Server for the domain.

Figure 13 - System Time Synchronization Example Using an External NTP Server



Two methods are described to use UTC time in your domain:

- Via your local network (intranet) or the Internet ([Figure 13](#))
- Via GPS ([Figure 14](#))

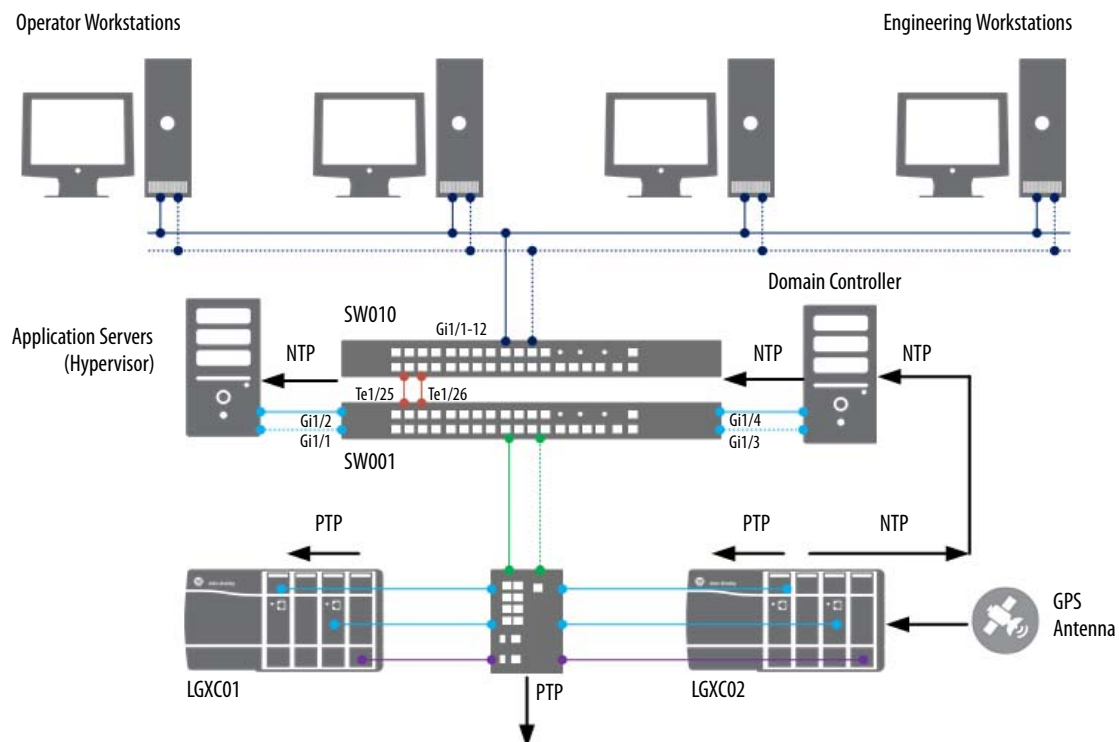
The Internet can introduce more propagation delays than GPS that can cause inaccuracies in your system. Although the NTP system affords algorithms to calculate accurate time for either method, the GPS method provides better accuracy.

The Stratix switch is responsible for converting network time protocol (NTP) to precision time protocol (PTP). This functionality is available only in the Stratix 54x0 family.

GPS uses a global positioning system for high precision time accuracy. All components, as shown in [Figure 14](#), with real-time clocks follow the same reference. However, a 1756HP-TIME module propagates directly to computers, controllers, and other devices via Ethernet switches.

For more information on time synchronization and CIP Sync, see the Integrated Architecture® and CIP Sync Configuration manual, publication [IA-AT003](#).

Figure 14 - 1756 Time Example (GPS Reference)



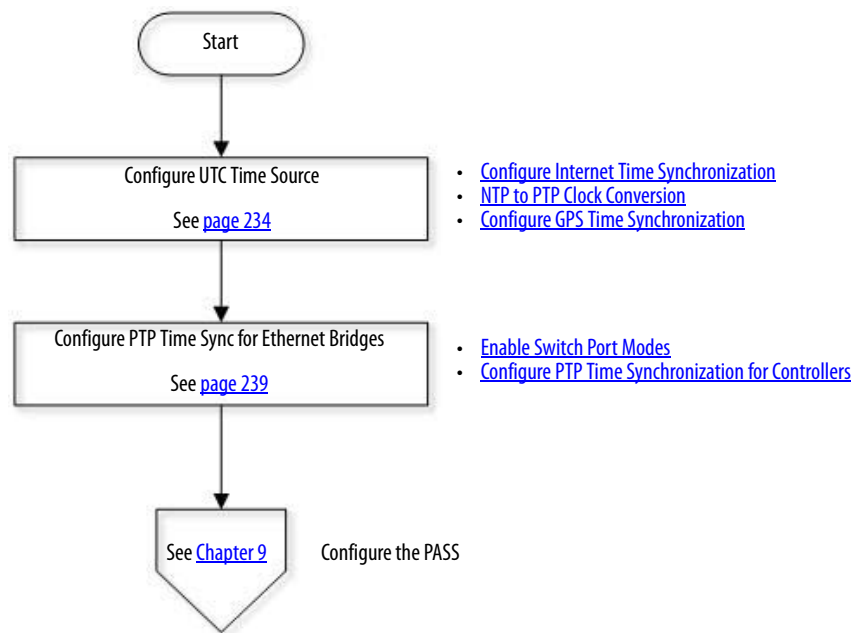
Considerations

Consider the following suggestions before starting this chapter:

- Decide which network time source — external NTP or GPS reference — that you are going to use. For additional information, see [Chapter 1](#) and [Chapter 3](#) for switch address configuration and domain controller connections with an NTP server, respectively.
- To enable CIP Sync functionality in a ControlLogix® controller, select Time Synchronization in Ethernet adapters by using Studio 5000® Logix Designer software.

[Figure 15](#) contains the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 15 - Time Synchronization Workflow



Configure UTC Time Source

UTC is independent of time zones and enables NTP to be used anywhere in the world regardless of time zone settings.

Use a domain controller with these procedures.



Configure Internet Time Synchronization

This section describes how to configure the Windows Time Service (w32Time) to use the Internet as a medium for sourcing a UTC time. Use the Windows time utility from an elevated command prompt.

Complete these steps by using the domain controller that is hosting the PDC emulator role (PADCA).

1. Open an elevated Command session and click the Windows Key.
The Start Menu appears.
2. Choose Command Prompt (admin).
3. From within this Command session, type the following while substituting for the <pool> argument per your requirements:
w32tm /Config /ManualPeerList:<pool> /SyncFromFlags:Manual /Reliable:yes /Update

IMPORTANT <pool> is a place holder for the URL or URLs of multiple time servers (for example, atomic clocks). If you cannot access the Internet, those URLs could be of your parent domain controller. You can research UTC sources for your proximity, but [Table 25](#) has examples that work for the U.S.

Table 25 - Internet <pool> Examples

Example	Purpose
us.pool.ntp.org,0x8	URL specifies a single server
0.us.pool.ntp.org,0x8 1.us.pool.ntp.org,0x8 1.us.pool.ntp.org,0x8 2.us.pool.ntp.org,0x8	URLs specify the use of 4 unique servers

There are (at least) four server pools of pool.ntp.org. But, the preferred assignment for <pool> is the first one (us.pool.ntp.org,0x8). Windows Event Viewer can log errors for URLs that do not respond.

The 0x8 qualifier specifies Client Mode packets for server communication. For more information, Microsoft Knowledgebase 875424.

You can specify a list of URLs that are <space> separated and enclosed in quotes. Make sure to append a type identifier for the URLs identifier as shown in [Table 25](#). For example, 0x8 (client mode).

The illustration shows an example that sources the U.S. pool.

```
Administrator: Cmd
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>w32tm /Config /ManualPeerList:us.pool.ntp.org,0x8 /SyncFromFlags:Manual /Reliable:yes /Update
```

If your system cannot access the Internet, <pool> can be a single target such as your parent or local Domain controller. Your domain time might not be within tolerable differences of other domains in your enterprise.

Table 26 - Local (non-internet) <pool> Example

Example	Purpose
.	Uses the current computer (PADCA) as the time source
PADCA	Specifies a network time server on your local network

- After you have commanded the w32tm utility by using the new configuration in [step 3](#), use the Net utility to stop and then start the Windows Time Service from the same command session.

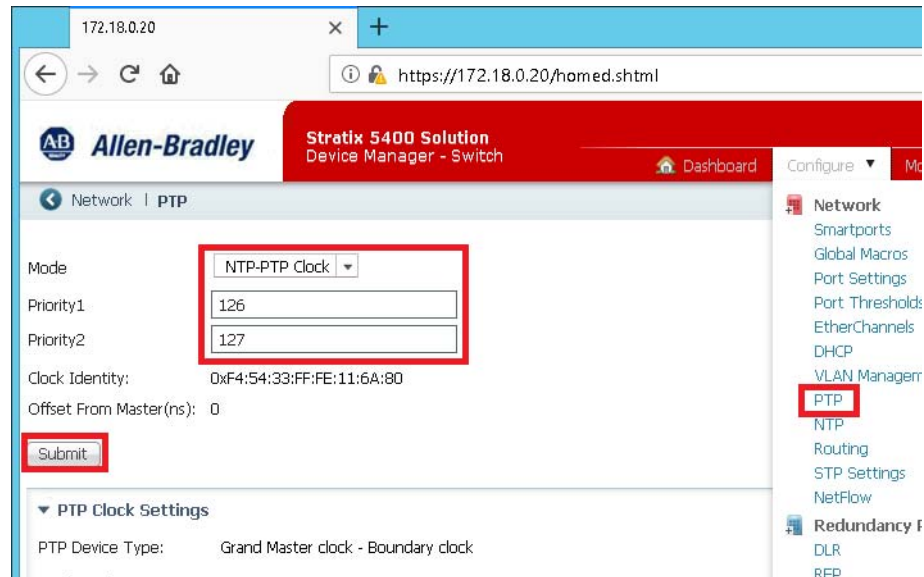
```
C:\Windows\system32>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

C:\Windows\system32>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.
```

NTP to PTP Clock Conversion

This section illustrates how to configure a Stratix 5400 to convert Network Time Protocol (NTP) to Precision Time Protocol (PTP),

1. From the Device Manager of the switch, click Configure and choose PTP.
2. From the Mode pull-down, select NTP-PTP Clock.
3. Type a priority value for Priority1 and Priority2.



4. Click Submit.

Configure GPS Time Synchronization

If you do not implement an Internet or intranet-based time source, this section helps you configure a Global Positioning System (GPS) time source.

The 1756HP-TIME Module is used in the examples for this section. The module receives the GPS time reference and propagates the time to the computers by using NTP to the automation devices through PTP (CIP Sync).

The 1756HP-TIME module obtains time from various sources and provides time synchronization on other devices, thus acts as a gateway between different time synchronization methods.

1. Using the Logix Designer application, add the 1756HP-TIME module to your project.
2. Right-click the module to access the Module Properties dialog box.

Use an Engineering Workstation with these procedures



EWS

3. Click the Configuration tab.

Module Properties: Local:3 (1756HP-TIME 3.002)

General | **Configuration** | Advanced | Time Sync | Internet Protocol | Port Configuration | Network | Vendor

Source Settings
Source: Internal GPS (Receiver) ▼

Time Output
☒ CIP Sync (PTP)
☒ Network Time Protocol - NTP
☐ IRIG - B
☐ Post Lock-Lost Transmission

External Source Address: 0 . 0 . 0 . 0
 NTP Update Interval: 1 hour ▼

Coordinate System Time
☐ Enable CST Mastership

Universal Time Reference
☐ Pre V16 Logix Controller Support (-2 years)

Webserver
☐ Enable Webserver

Advanced CIP Sync Settings
 Priority 1: 128 (Master Override)
 Priority 2: 128 (Tie Breaker)
 Time To Live: 1 ▼
 Sync Interval (s): 1 ▼

Description Settings
 User Name: 1756-TIME
 User Location:

Status: Running

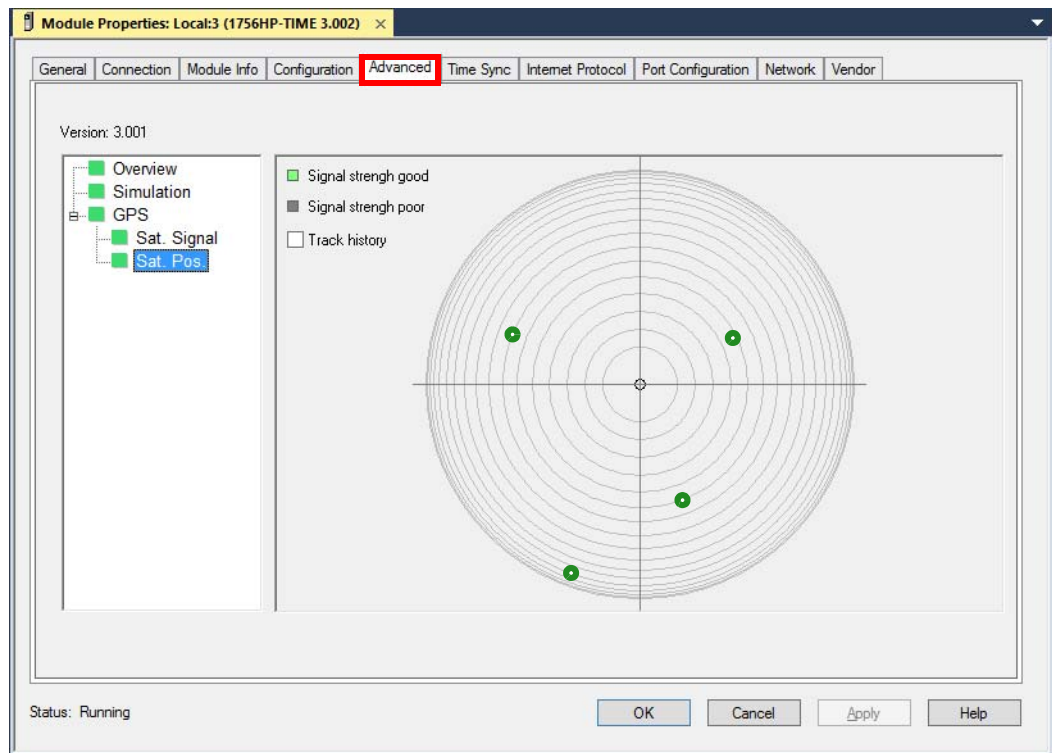
OK Cancel Apply Help

4. From the Source pull-down menu, select Internal GPS (Receiver).

5. In the Time Output area, select the desired Time Sync method.

The CIP Sync priority can be changed for the desired Time Sync method.

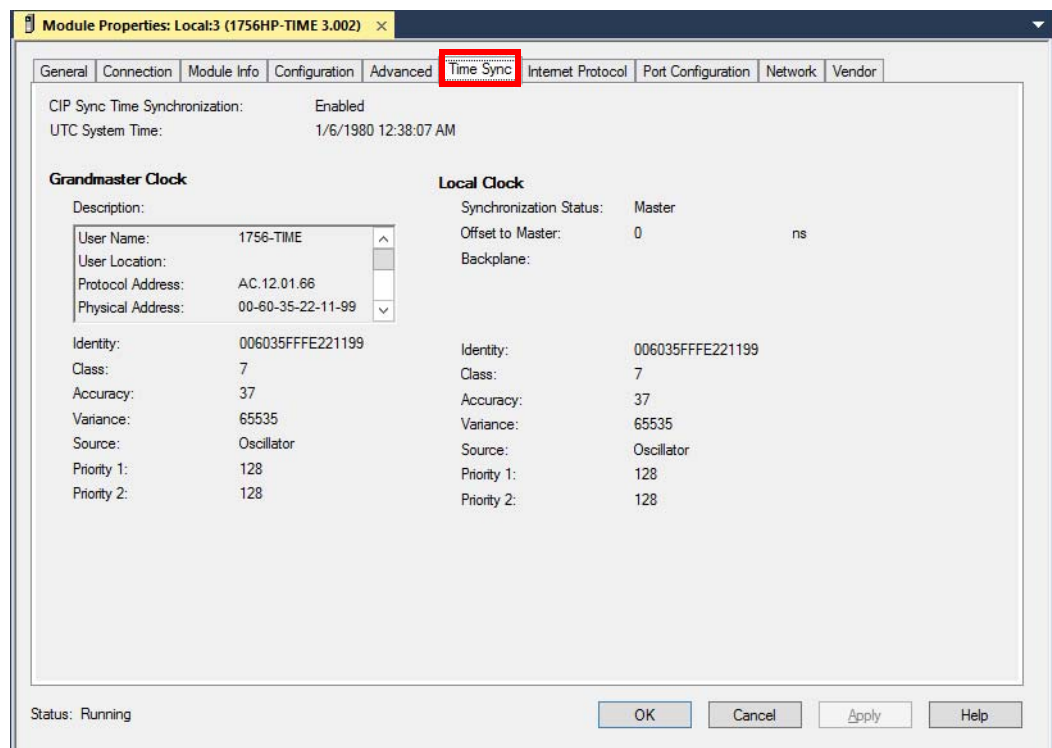
6. Click the Advanced tab.



You can follow the Master status in the Advanced tab.

7. Click the Time Sync tab.

This tab lets you confirm the Grandmaster Clock and the actual time status.



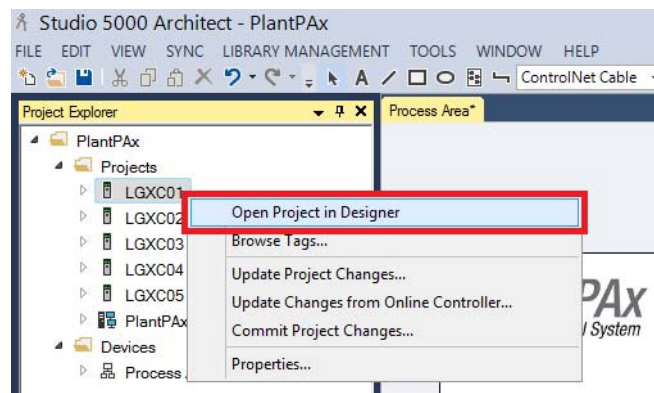
Configure PTP Time Synchronization for Ethernet Bridges

Use an Engineering Workstation with these procedures.



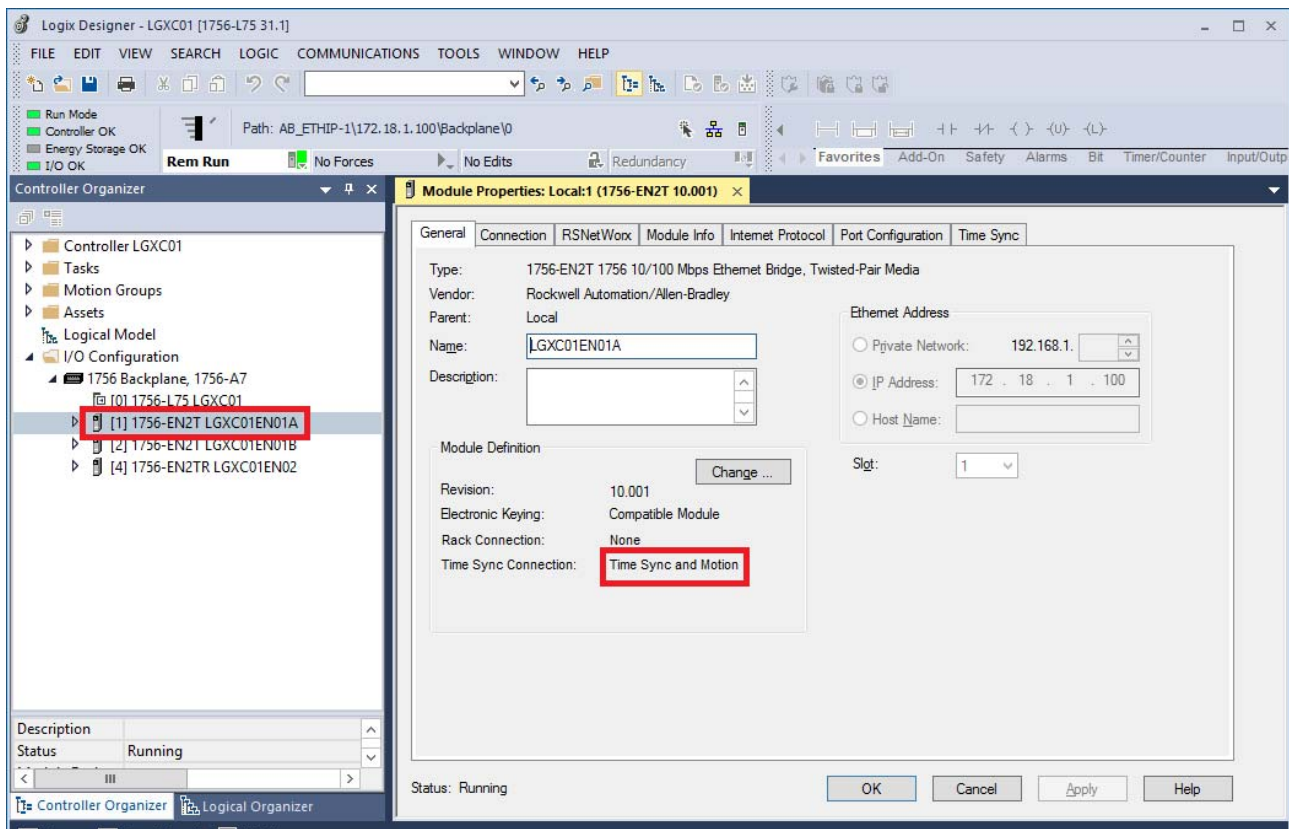
Precision Time Protocol (PTP) enables precise synchronization of clocks in measurement and control systems. PTP generates a Master-Slave relationship among the clocks in the system. Clocks, which are synchronized over the EtherNet/IP network, derive their time from a clock that is selected as the Grandmaster clock. The Time Sync and Motion option **must** be enabled for Ethernet bridge modules to propagate time through the network via switches.

1. In the Architect application, right-click a controller and choose Open Project in Designer.



2. On the General tab of the Module Properties dialog box, make sure that 'Time Sync and Motion' is selected for the connection.

See [page 211](#) for procedures on how to change a Module Definition.



3. If online, click the Time Sync tab to confirm Grandmaster clock settings.

Enable Switch Port Modes

By default, PTP is disabled on all Fast Ethernet and Gigabit Ethernet ports. The switch supports the following Synchronization Clock modes:

- End-to-End Transparent — In this mode, all switch ports are enabled by default. The switch transparently synchronizes all slave clocks with the master clock connected to the switch. This mode causes less jitter and error accumulation than Boundary mode.
- Boundary — Use this mode for networks with fewer than four layers of cascaded devices to avoid jitters and errors. The switch becomes the parent clock to which the other devices that are connected to the switch synchronize their internal clocks.
- Forward (default) — Traffic is forwarded through the switch (while being prioritized by QoS) but is not acted on by the switch.

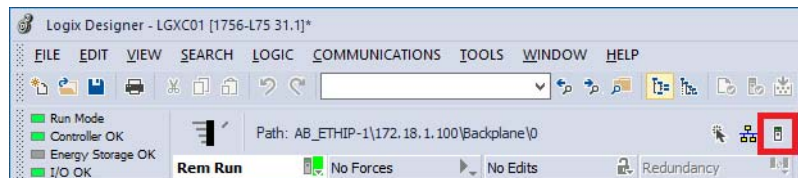
CIP Sync time synchronization supports Boundary and End-to-End Transparent modes. End-to-End Transparent mode synchronizes all switch ports with the Grandmaster clock by using the IEEE 1588V 2 End-to-End Transparent clock mechanism, and is the preferred mode.

For more information, see the Stratix® Managed Switches User Manual, publication [1783-UM007](#).

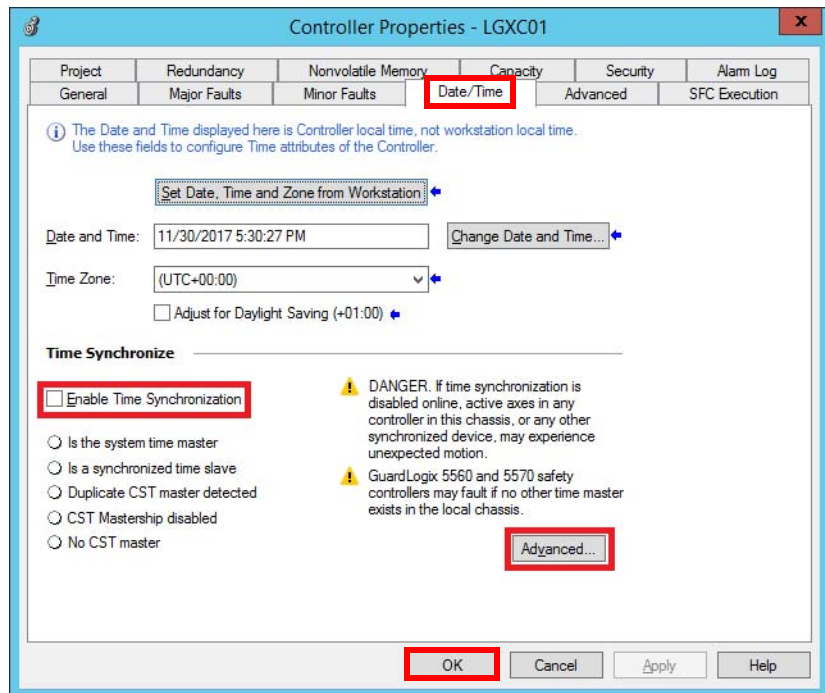
Configure PTP Time Synchronization for Controllers

A Logix controller that is CIP Sync enabled and designated the Grandmaster clock is the real-time source for the control system. The controller synchronizes with the PTP between the controllers and networks. Complete these steps.

1. Using the Logix Designer application, click the Open Controller™ Properties symbol.



The Controller Properties dialog box appears.

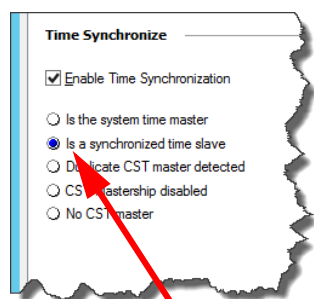


2. On the Date/Time tab, click Enable Time Synchronization.

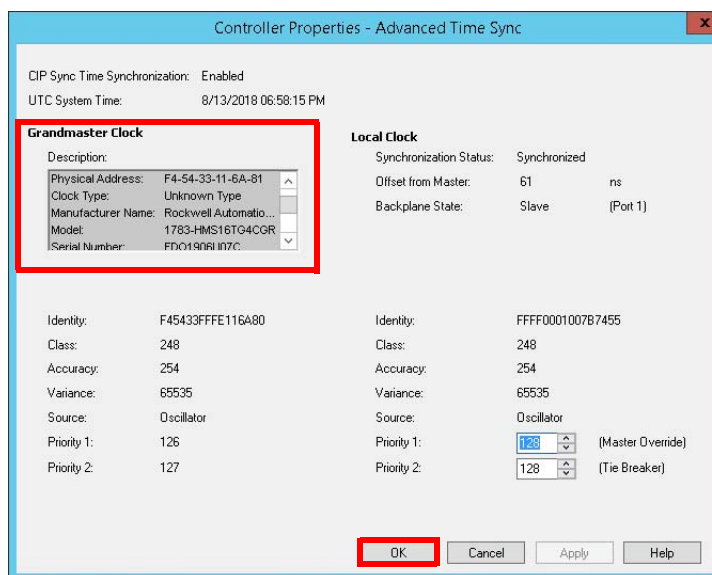
IMPORTANT Use your local time to configure the Time Zone and Adjust for Daylight Saving.

3. Click Advanced.

4. Click OK on the Controller Properties dialog box.



The status 'Is a synchronized slave' appears when the controller is synchronized.



The Grandmaster clock reference can be confirmed.

Configure the Process Automation System Server (PASS)

The Process Automation System Server (PASS) is a required system element for the PlantPax® system. The PASS hosts essential software components that run the system, including the FactoryTalk® Directory (FTD).

This chapter describes how to configure these components that comprise the PASS:

- HMI server – Stores HMI project components, such as graphic displays, and provides these components to Operator Workstations (OWS) upon request
- Data server – Accesses information from the process controllers and provides information to servers and workstations in the PlantPax system
- Alarm and Event server – Provides alarm information from the controllers and servers to the OWSs upon request.

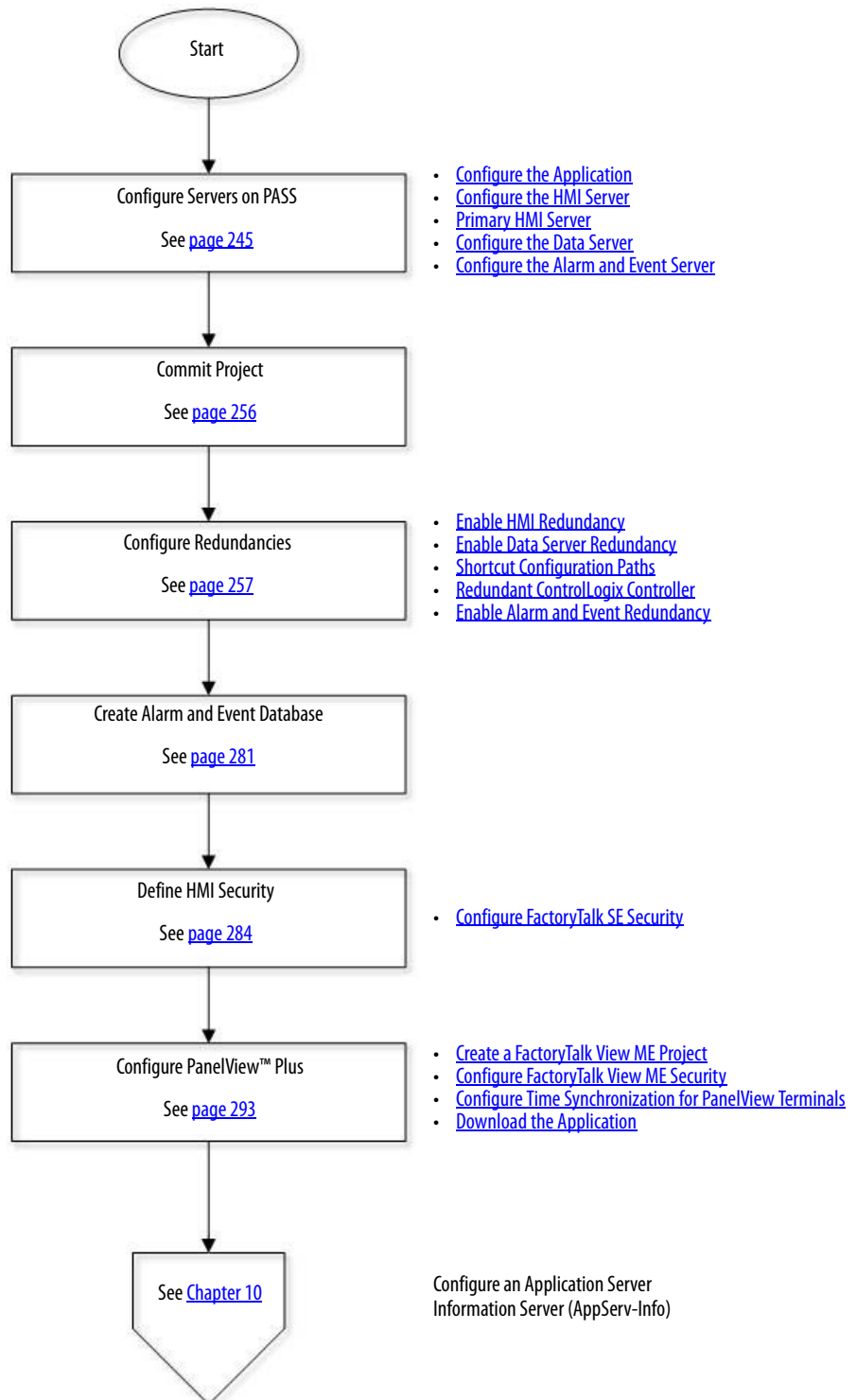
Considerations

Consider the following suggestions before starting this chapter:

- The PASS server or servers must be deployed before doing the procedures in this section.
 - For templates based on your system requirements, see the PlantPax Virtualization User Manual, publication [9528-UM001](#).
- Determine how many PASS servers are required for your architecture.
 - See ‘Determining the Number of PASS Servers’, in the PlantPax Distributed Control System Selection Guide, publication [PROCES-SG001](#).
- PASS servers can be configured as redundant for HMI servers, data servers, and/or alarm servers.

[Figure 16](#) shows the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 16 - PASS Workflow



Configure Servers on PASS

In this section, you configure the human machine interface (HMI) server, data server, and the Alarms and Events server.


Use an Engineering Workstation with these procedures

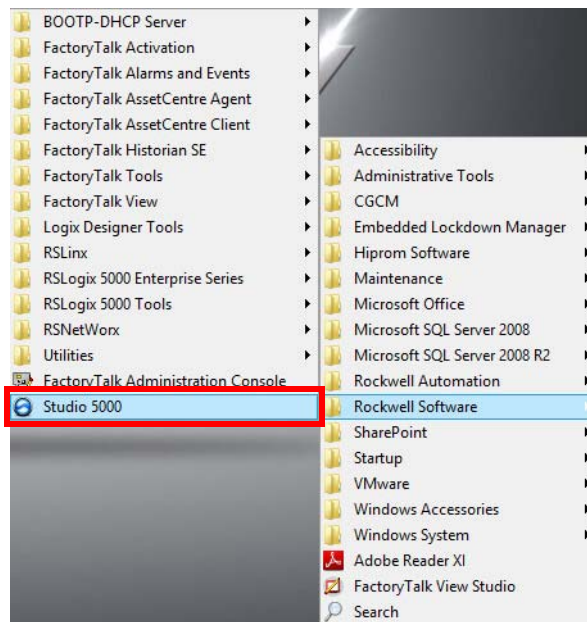


Configure the Application

In this section, you configure the application on an engineering workstation (EWS).

Complete the following steps:

1. Click the Programs  symbol and choose Rockwell Software®> Studio 5000®.



The Studio 5000 splash screen appears.

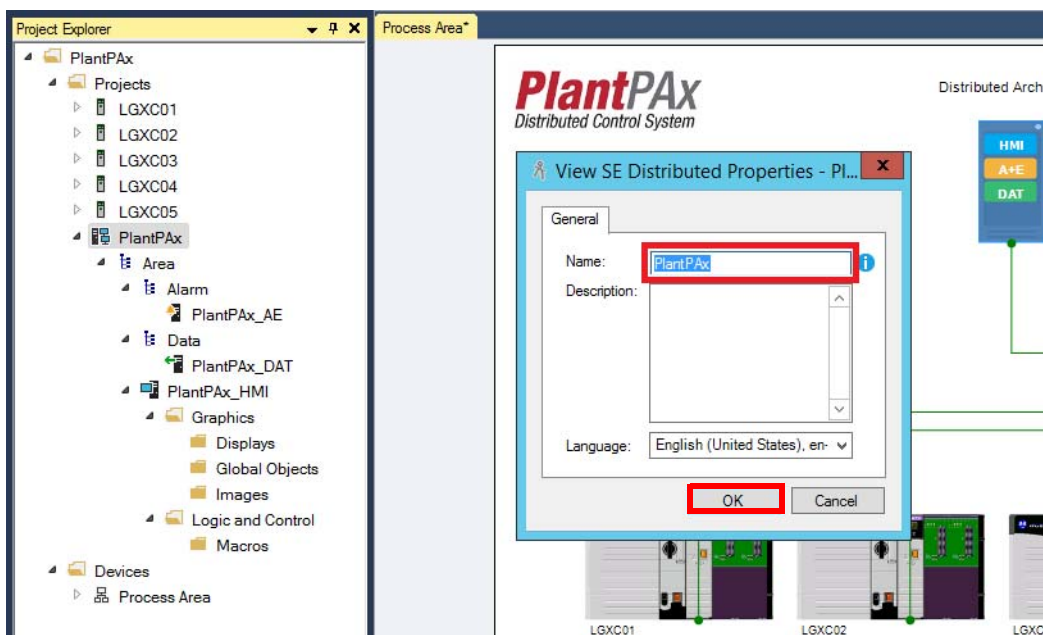
2. Select an existing project (PlantPAx in the example).



IMPORTANT If you want to change the application and/or area name, complete [step 3](#) through [step 6](#). If you want to keep 'PlantPax' as the application name and 'Area' as the area name, continue to [Configure the HMI Server on page 247](#).

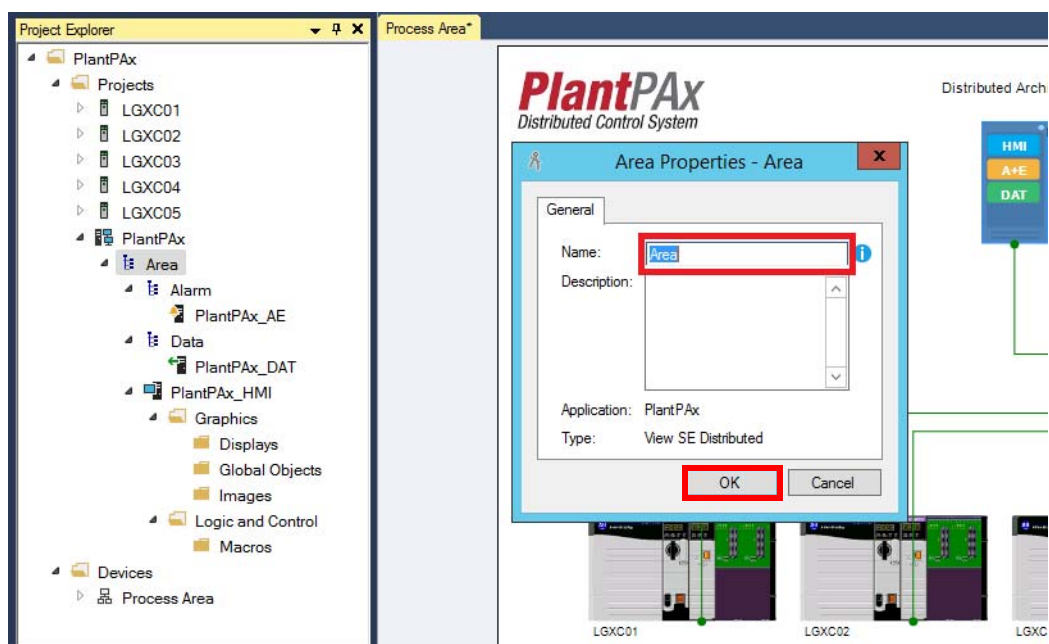
3. In the Logix tree, double-click PlantPax>Projects>PlantPax.

4. Click OK to accept the default application name 'PlantPax'.



5. In the Logix tree, double-click PlantPax>Projects>PlantPax>Area.

6. If desired, change the Area name and click OK; otherwise click OK to accept the default Area name 'Area'.



Configure the HMI Server

The HMI server is configured within your Studio 5000 Architect® and FactoryTalk View Site Edition (SE) application. The HMI server stores HMI project components, such as graphic displays, and serves these components to OWSs upon request. The HMI server can also manage tag databases and log historical data. Multiple HMI servers can exist on the PlantPAx system.

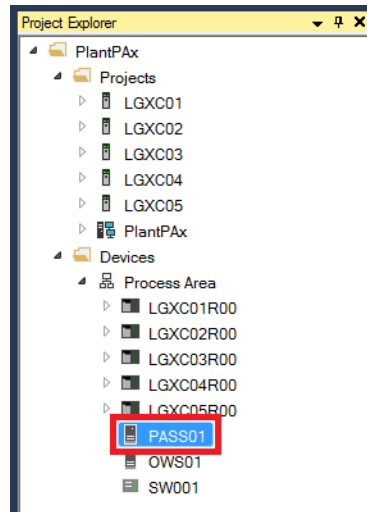
Use an Engineering Workstation with these procedures



Primary HMI Server

Complete the following steps.

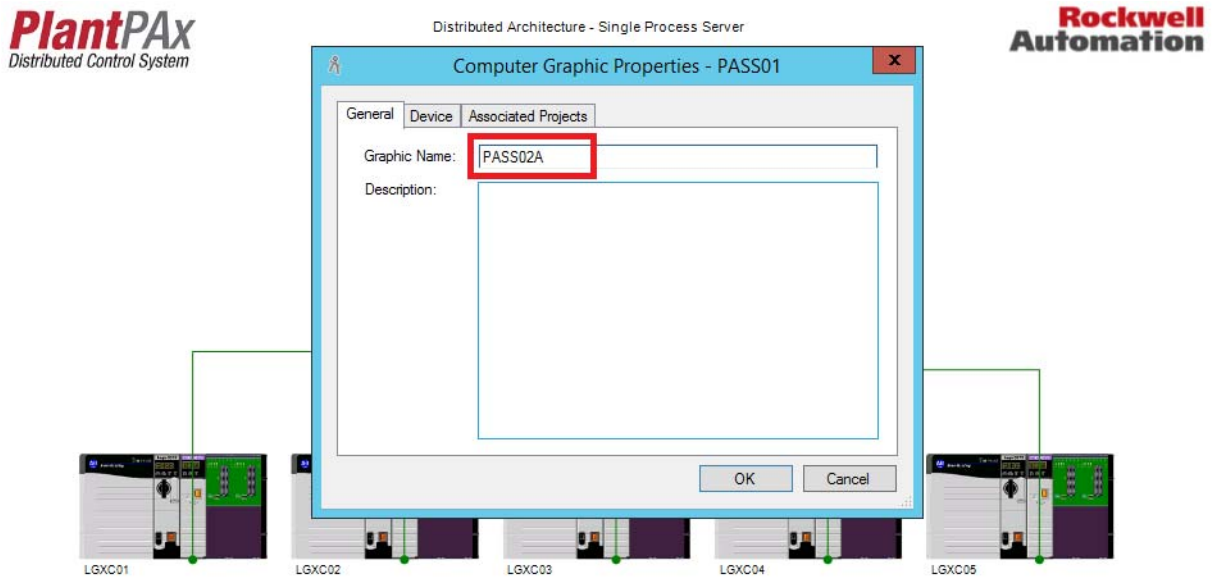
1. Open the Architect application and a project.
2. In the Project Explorer area, click PlantPAx>Projects>Devices>Process Area and choose PASS01.



The Computer Graphics Properties dialog box appears in the Process Area layout page of an Architect project.

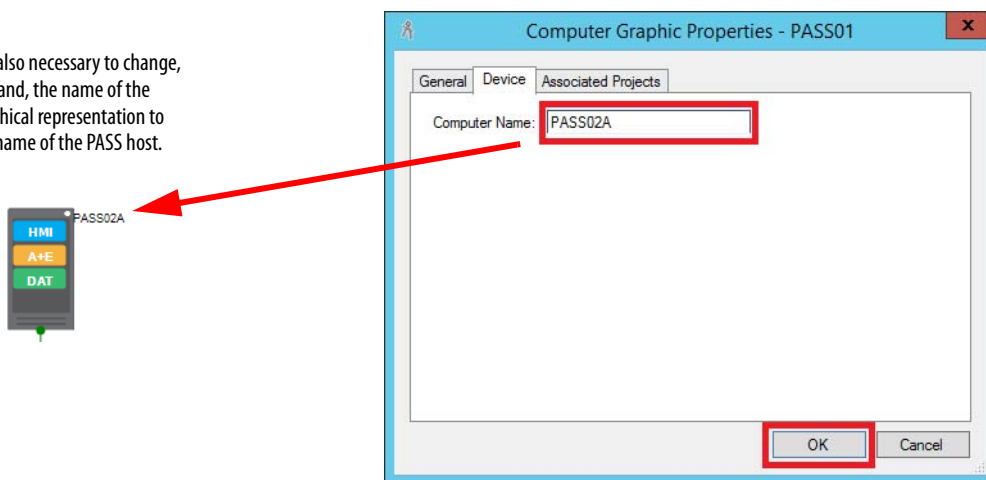
TIP The following step does not change the name of the actual server, just the name of the graphical representation of the server.

3. In the General tab, change the server name to the project name.



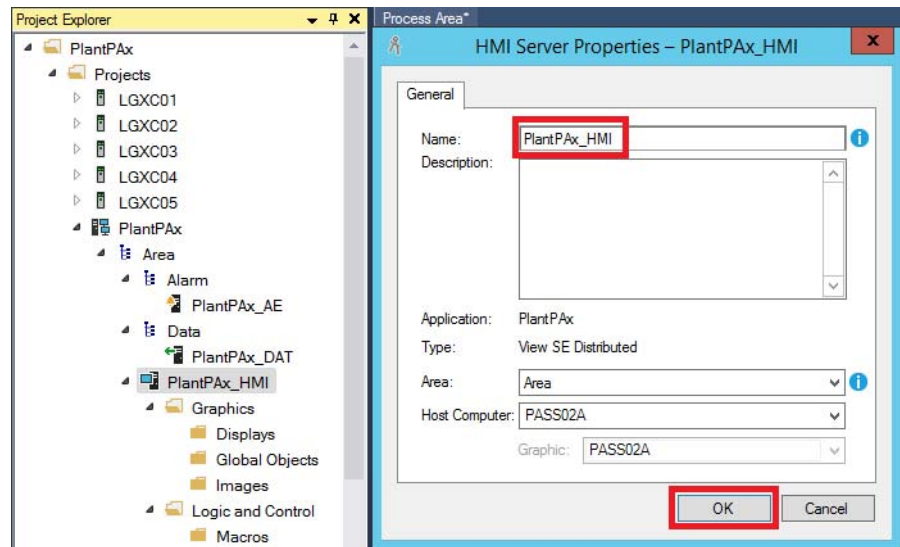
4. In the Device tab, type the computer name that hosts the PASS.
For example, PASS02

It is also necessary to change, by hand, the name of the graphical representation to the name of the PASS host.



5. Click OK.

6. If you need to change the name of the HMI server, click Projects>PlantPAx>Area and choose PlantPAx_HMI.
7. Type the new name and click OK.



Configure the Data Server

Use an Engineering Workstation with these procedures



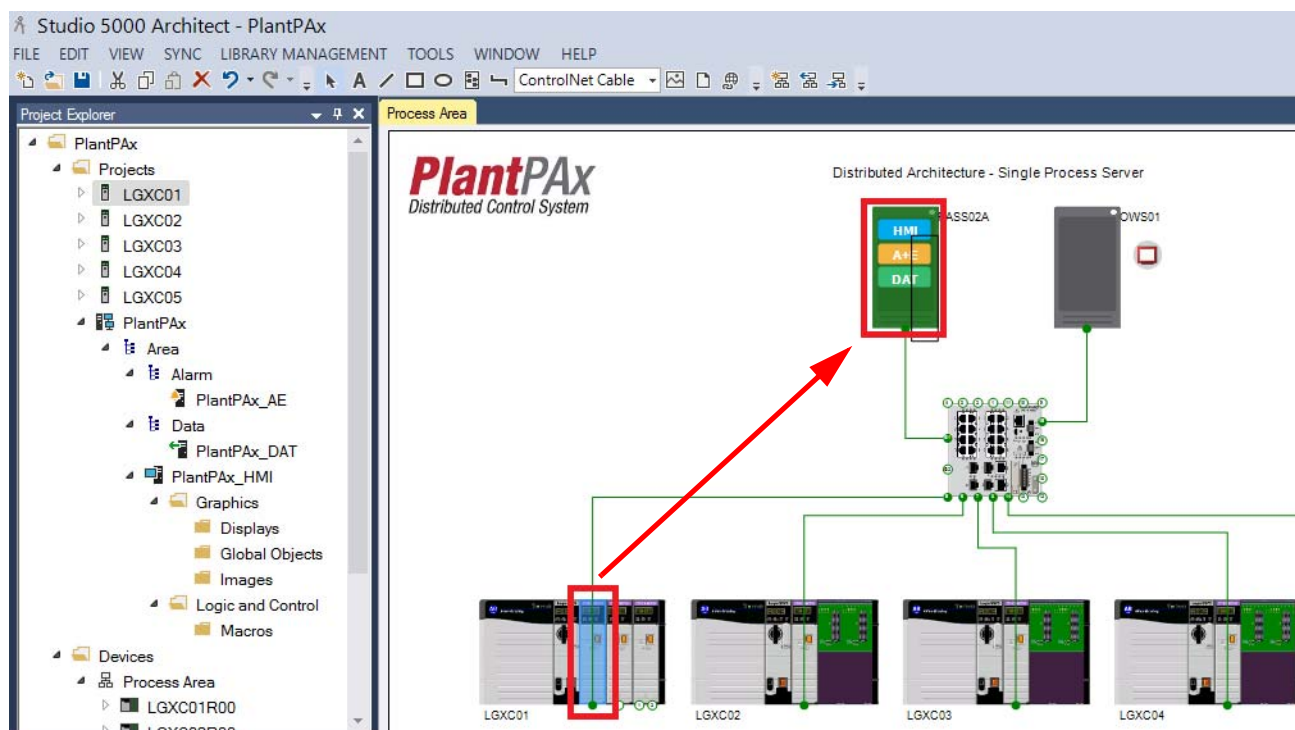
In this section, we create shortcuts on data servers (FactoryTalk Linx) to connect controllers. The communication path to network devices is automatically updated in a Studio 5000 Architect or FactoryTalk View project.

Complete the following steps.

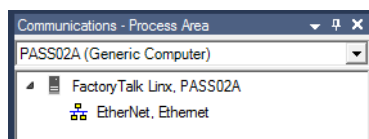
1. If you need to change some configuration, right-click PlantPAx_DAT in the Project Explorer and choose Properties to specify the server in the graphical process display. Otherwise, continue with the next step.

Observe in the Communication pane (bottom example) that there is no connection.

2. Drag the communication module from the LGXC01 chassis and drop it onto the PASS02A computer.

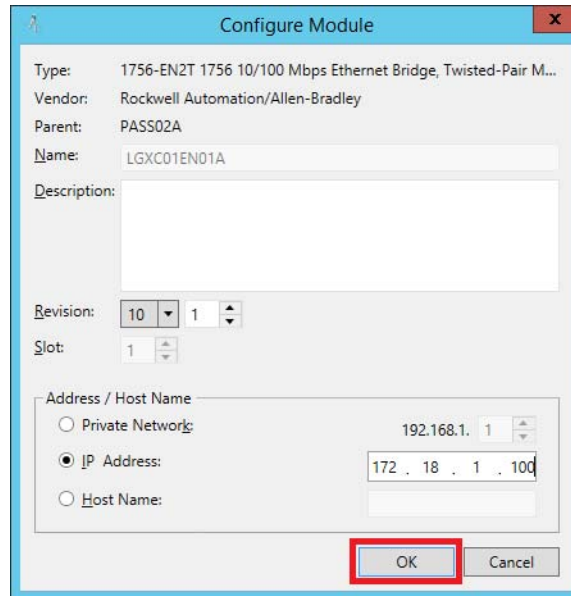


Communication Pane

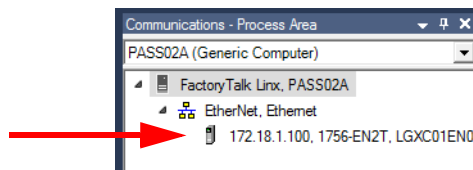


When the communication module is dropped onto the PASS server, the Configure Module dialog box appears.

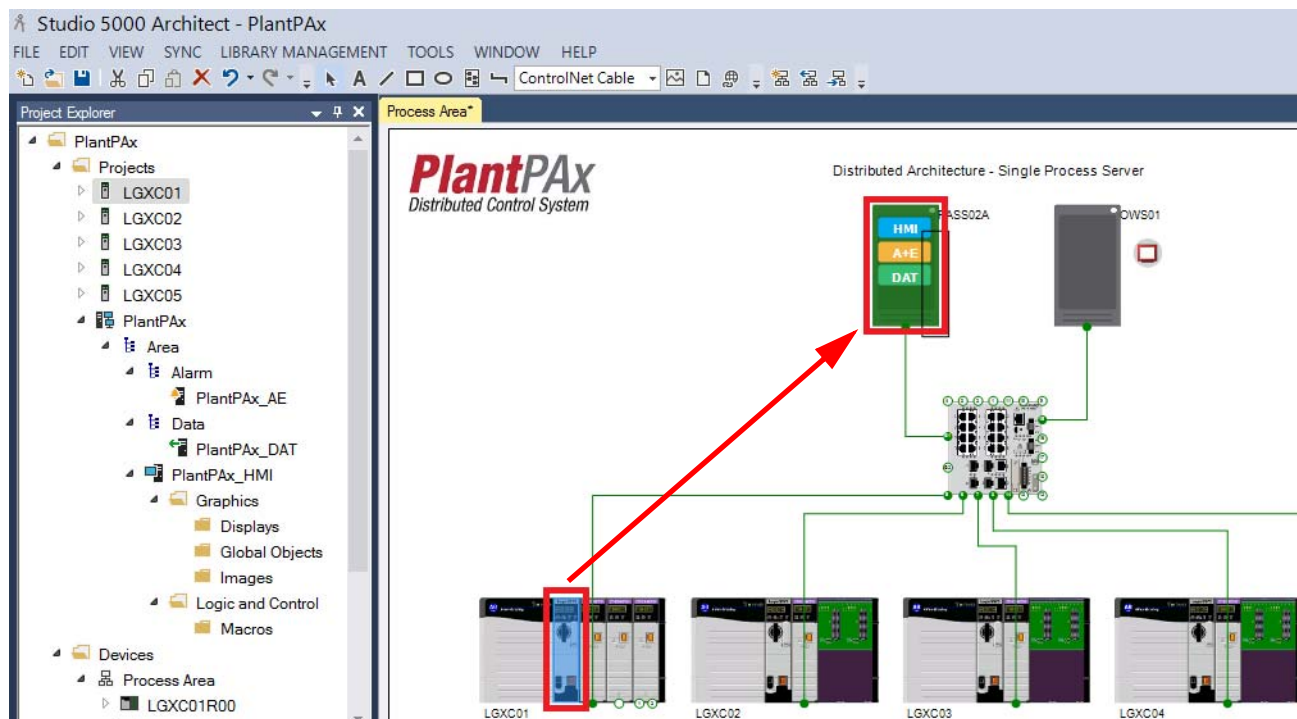
3. (Optional) Type a Description.
4. Accept the rest of the defaults and click OK.



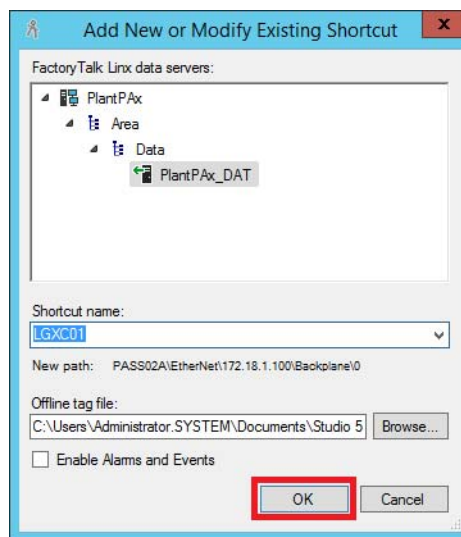
The communication shortcut is updated with the adapter name.



5. Drag the controller from the LGXC01 chassis and drop it into the PASS02A computer.



The Add New or Modify Existing Shortcut dialog box appears.

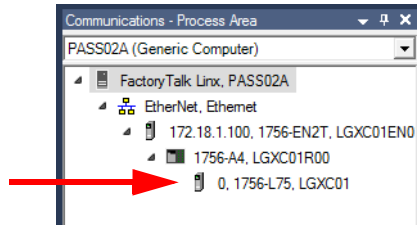


An Architect project uses the template controller name by default. Our example is LGXC01.

We do **not** recommend that you change the shortcut name.

6. Accept the defaults and click OK.

The shortcut is created for the controller.



7. Save your work.

Use an Engineering Workstation with these procedures



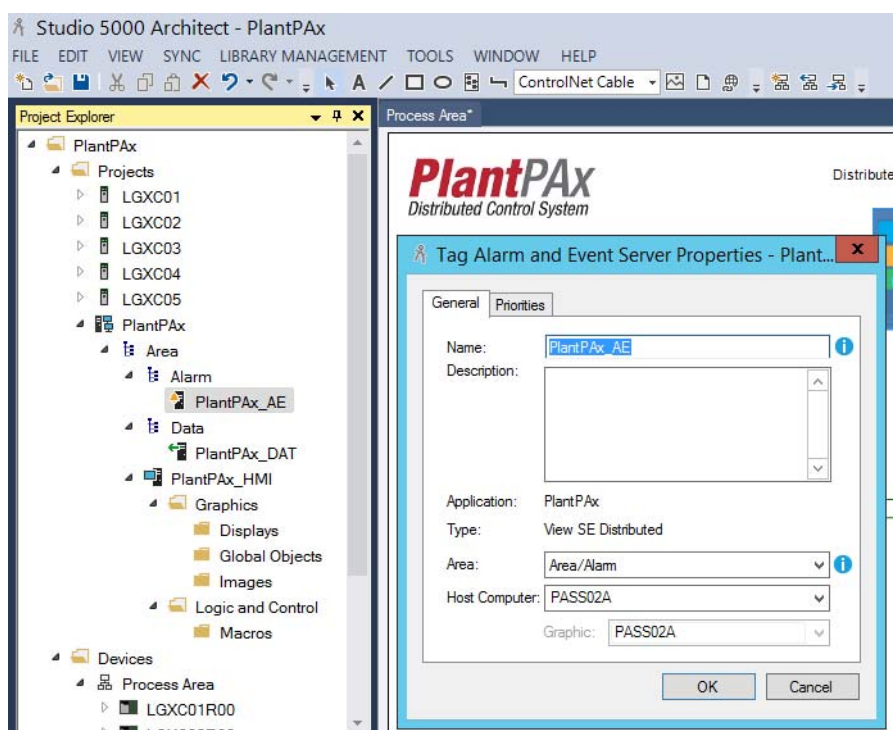
Configure the Alarm and Event Server

The Alarms and Events server is configured within the Studio 5000 Architect and FactoryTalk View SE application. This server publishes information from controllers and servers available to all subscribing OWSs.

In this section, we describe how to configure alarm and event servers for tag-based alarms. We also show how to set the alarm severity.

1. If you want to change some Alarm and event configuration, right-click Projects>PlantPAx>Area>Alarm>PlantPAx_AE in the Project Explorer.

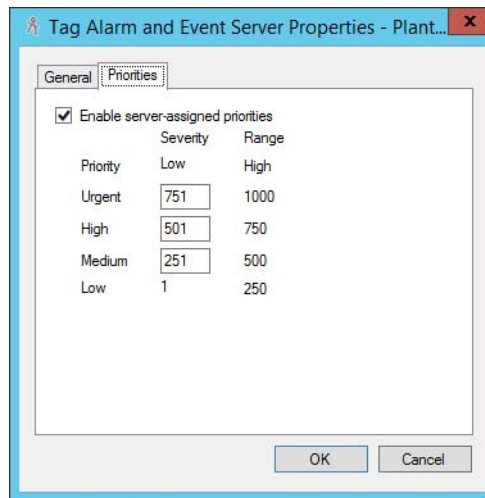
The Tag Alarm and Event Server Properties dialog box appears.



An Architect project defaults the alarm name and host computer.

2. (Optional) In the General tab, type a description and click OK.

3. In the Priorities tab, accept the defaults and click OK.



For more information on alarm severity, see Appendix B in the Rockwell Automation® Library of Process Objects Reference Manual, publication [PROCES-RM002](#).

4. Save your project.

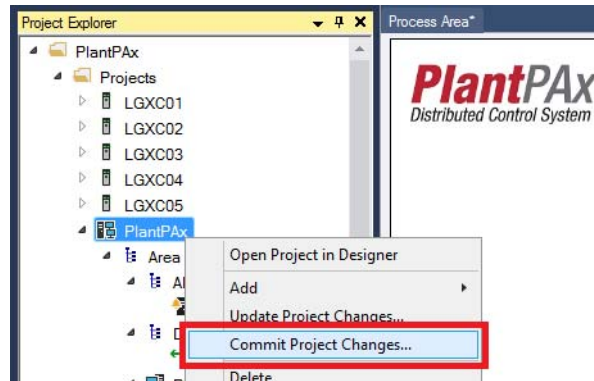
Proceed to [page 256](#) to commit your project.

Commit Project

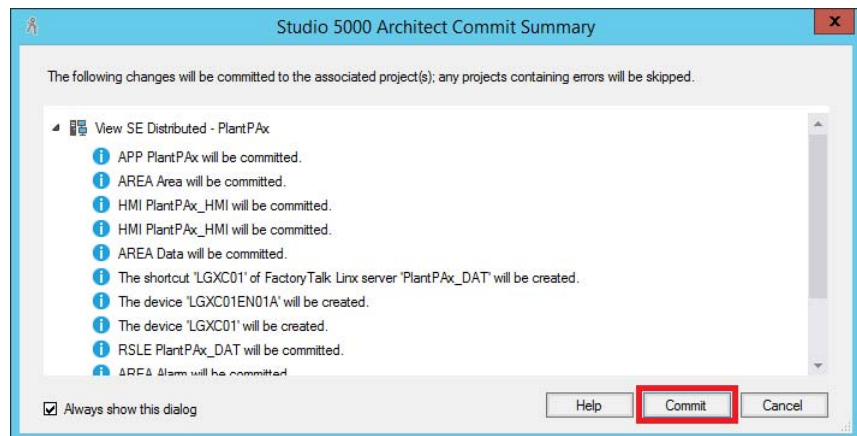
When you commit a project, all data is sent from the Architect project to the FactoryTalk View application. The data is updated in the server for the respective servers: HMI, Data, and Alarms and Events.

Complete the following steps:

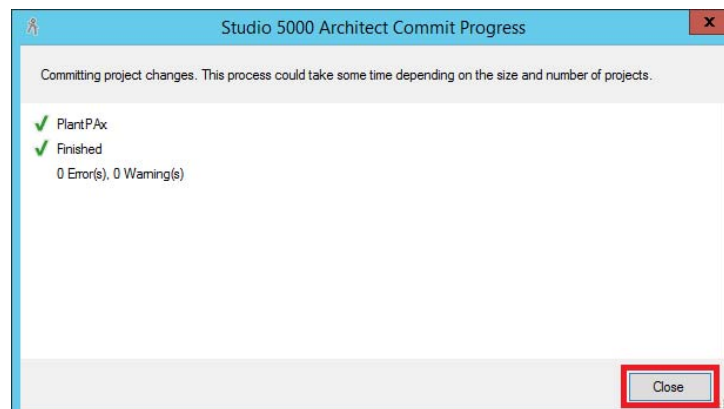
1. In the Project Explorer, right-click PlantPAx>Projects>PlantPAx and choose Commit Project Changes.



2. In the Commit Summary dialog box, click Commit to perform the commit process.



3. Once a check mark appears next to your project in the Committing Projects dialog box, the configuration of the servers is complete.
4. To close the Committing Projects dialog box, click Close.



Configure Redundancies

This section describes for to configure redundancies for the HMI, Data, and Alarm and Event servers.

Enable HMI Redundancy

This section describes how to copy the primary HMI server application folder to the secondary HMI server. This procedure is performed only the first time the primary HMI server is copied.


Copy the Primary HMI Server to the Secondary Server

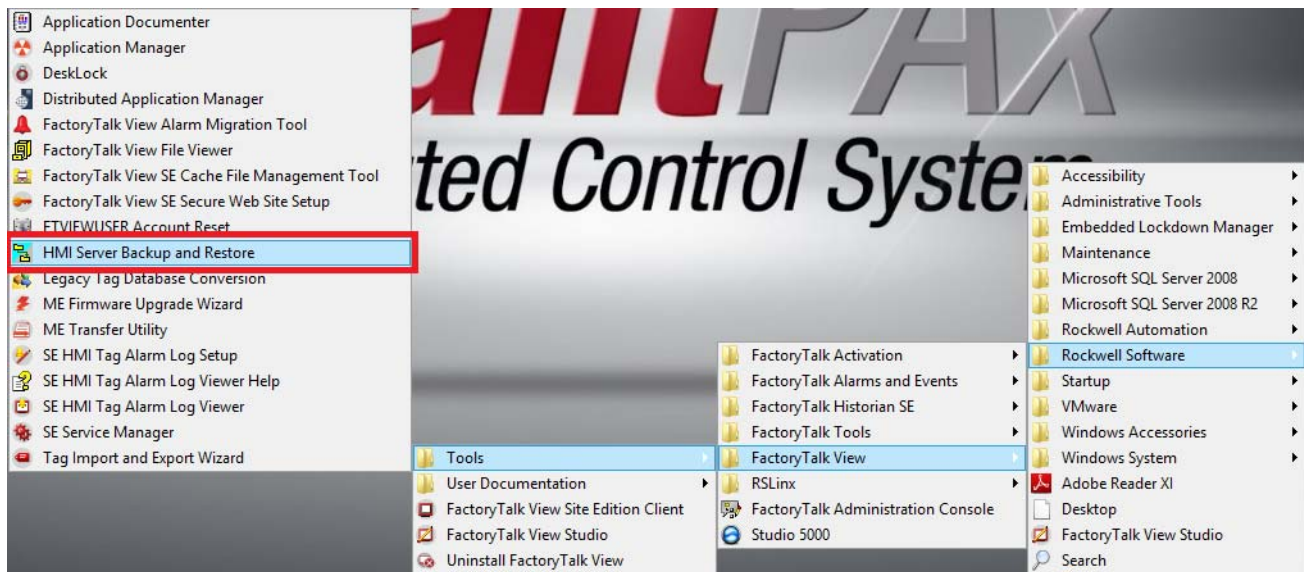
To copy the primary HMI server to a location on the secondary server, complete these steps.

Use a PASS with these procedures.



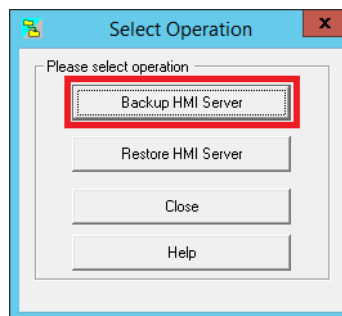
PASS02A

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk View>Tools>HMI Server backup and Restore.



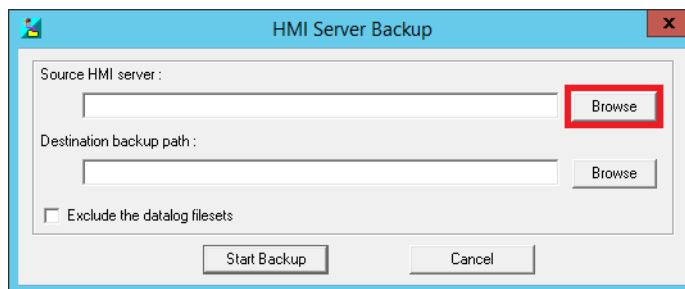
The Select Operation dialog box appears.

2. Click 'Backup HMI Server'.

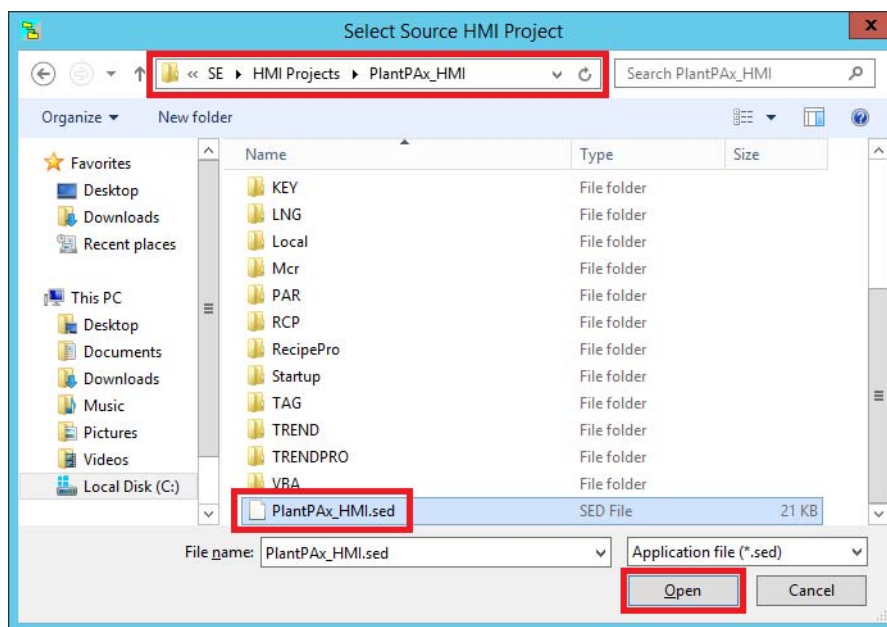


The HMI server backup dialog box appears.

3. Click Browse for the Source HMI server.

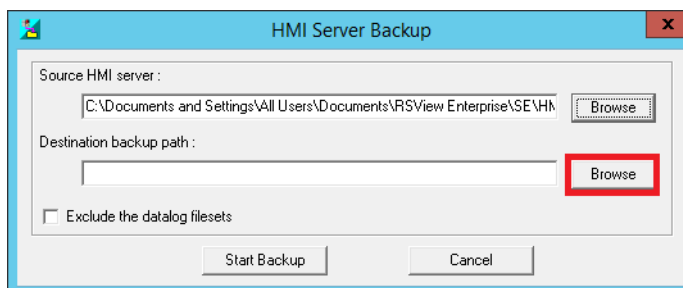


4. Navigate to the primary HMI server that was created earlier and choose the .sed file.



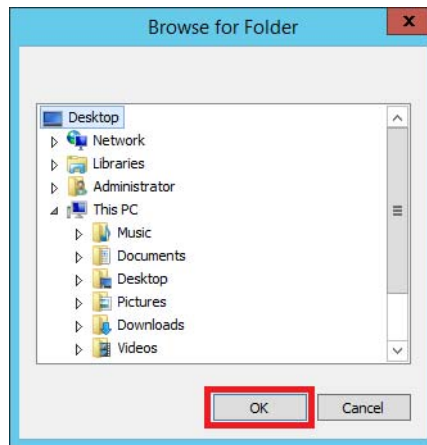
5. Click Open.
6. Click Browse for the Destination backup path.

The destination is on the same physical machine as the Source HMI Server. 'Desktop' is a good choice because it's convenient and easy to access.

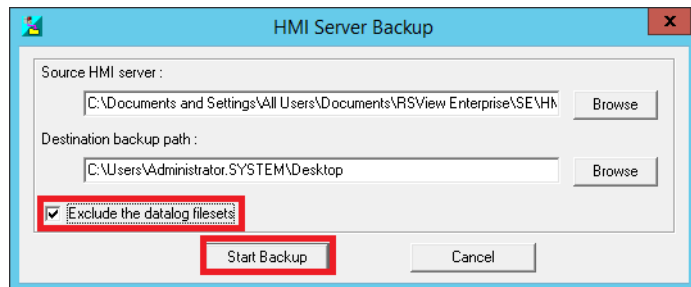


7. Choose any destination path and click OK.

'Desktop' is our example.



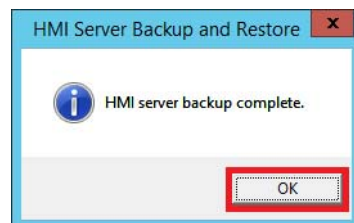
8. Check 'Exclude the dialog filesets'.



9. Click Start Backup.

When the backup is complete, the 'HMI server backup complete' dialog box appears.

10. Click OK.



The Select Operation dialog box reappears.

11. Click Close.

Copy Primary Folder to Secondary Server

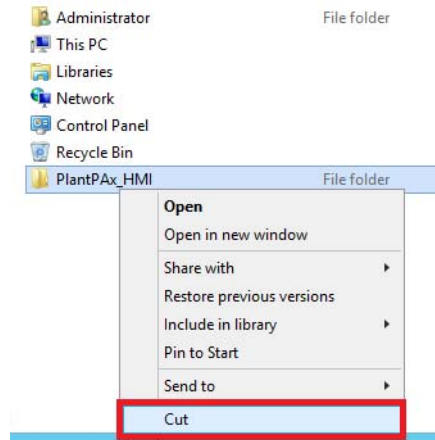
The destination folder has to be cut from the primary physical machine and pasted on the secondary HMI server physical machine.

Use a PASS with these procedures.

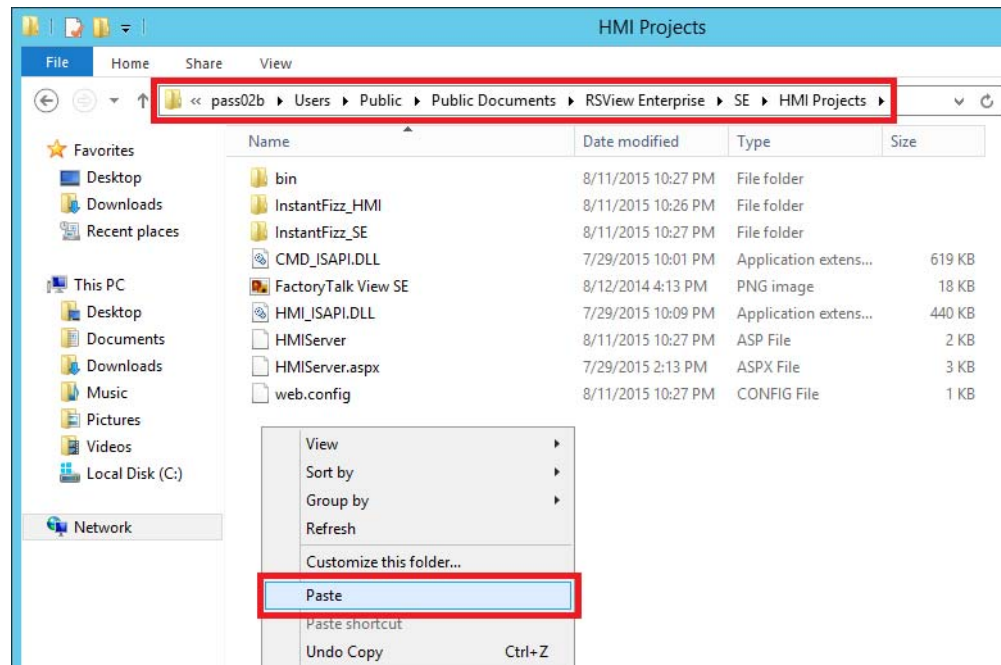


PASS02A

1. In Windows Explorer, navigate to the destination folder you created (Desktop in our example), right-click the folder name, and choose Cut.



2. Paste the HMI server folder into the secondary server folder (Site Edition (SE) HMI Projects folder).



The default path is:


C:\Users\Public\Public Documents\RSVIEW Enterprise\SE\HMI projects.

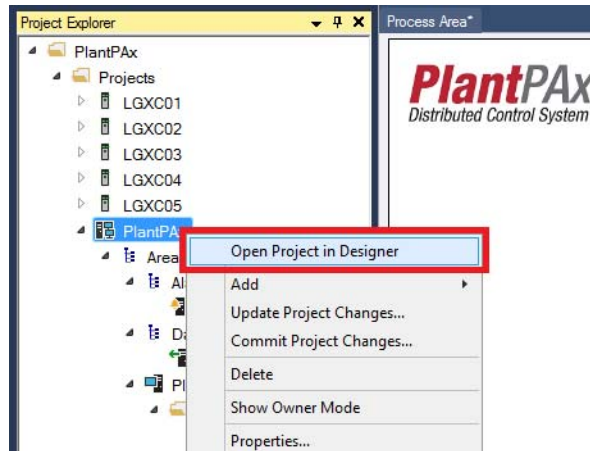
Set Up HMI Redundancy

Use an Engineering Workstation with these procedures

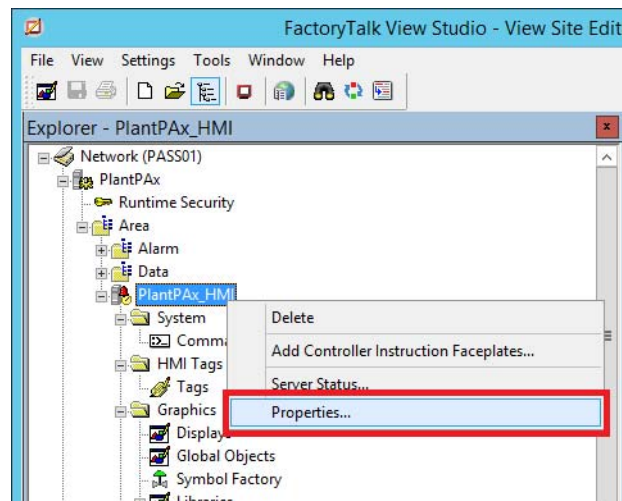


This section describes how to use HMI Properties to enable redundancy. Complete these steps.

1. Click the Programs  symbol and choose Rockwell Software> Studio 5000.
2. From the Studio 5000 splash screen, select an existing project (PlantPAX in the example).
3. In the Project Explorer, right-click PlantPAX>Projects>PlantPAX and choose Open Project in Designer.

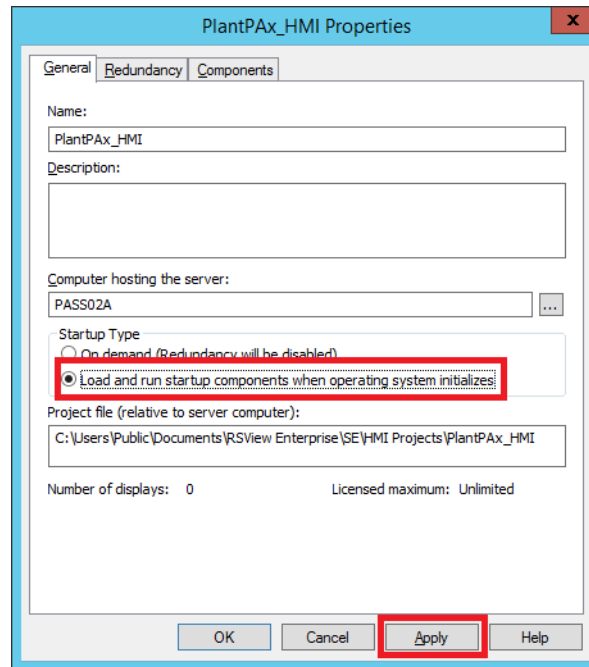


4. In FactoryTalk View Studio, right-click the HMI server name and choose Properties.

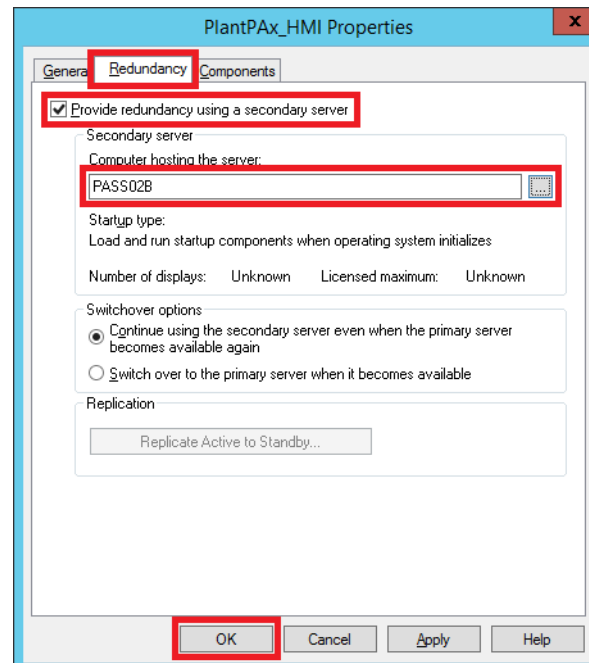


The HMI Server Properties dialog box appears.

5. On the General tab, click 'Load and run startup components when operating system initializes'.

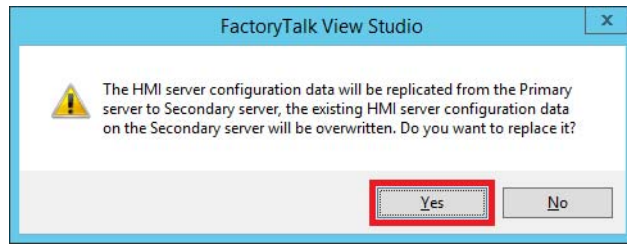


6. Click Apply.
7. Click the Redundancy tab.



8. Check 'Provide redundancy using a secondary server'.
9. Click Browse (ellipses '...') and select the Secondary server.
10. Click OK.

A message window appears.

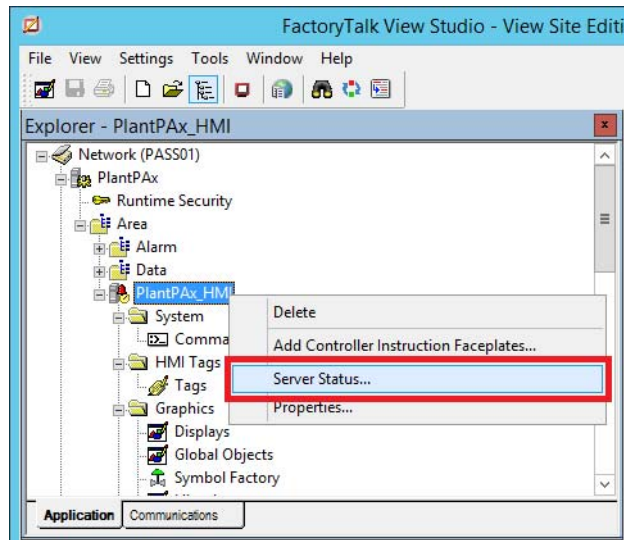


11. Click Yes.

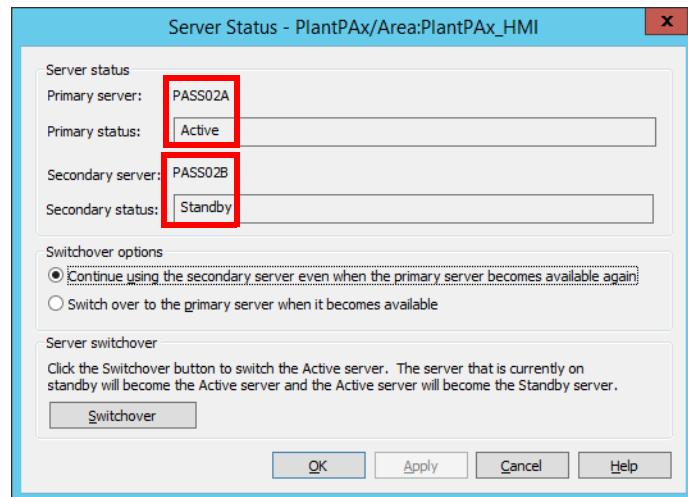
Server Status

In this section, you verify the status of the Active (Primary) and Standby (Secondary) servers.

1. In FactoryTalk View Studio, right-click the HMI server name and choose Server Status



2. In the Server Status dialog Box, verify the following:
 - The Primary server (for example, PASS02A) is correct and 'Active'
 - The Secondary server (for example, PASS02B) is correct and 'Standby'.



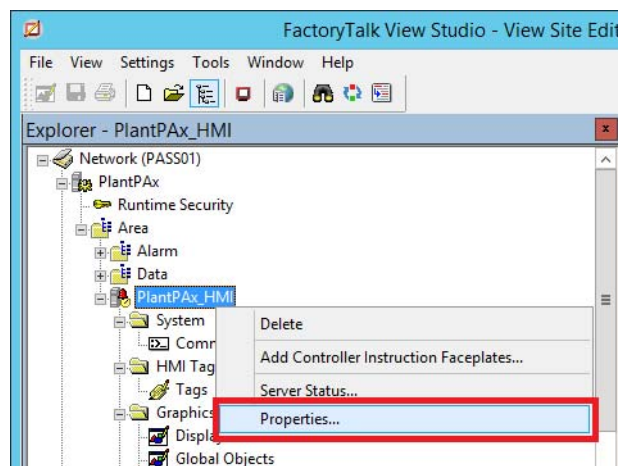
3. Click OK.

Replicate Active to Standby

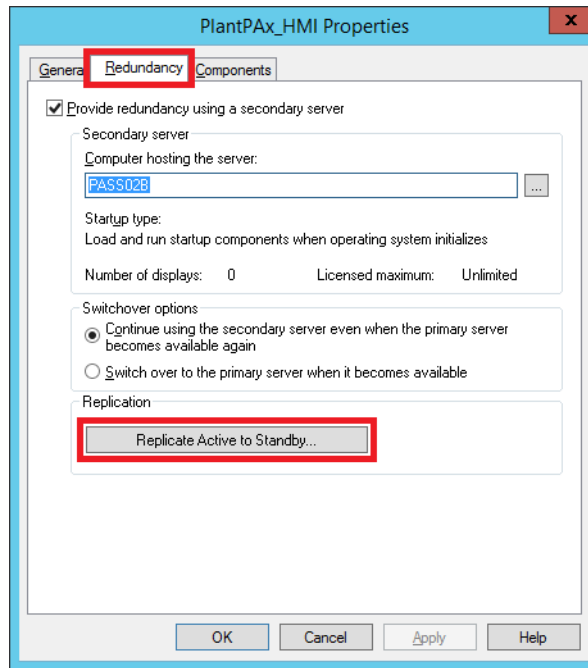
In this section, you replicate the Primary properties from the Primary server to the Secondary server.

IMPORTANT Every change that is made in the Primary server must be replicated. The replication process is always from the Active to the Standby.

1. In FactoryTalk View Studio window, right-click the HMI server name and choose Properties.



The HMI server properties dialog box appears.



2. On the Redundancy tab, click 'Replicate Active to Standby'.

A replication warning appears.

3. Click Yes.

A progress bar shows the status of the copy process.

TIP The Secondary server no longer automatically restarts when the copy process completes.

4. Click Close.

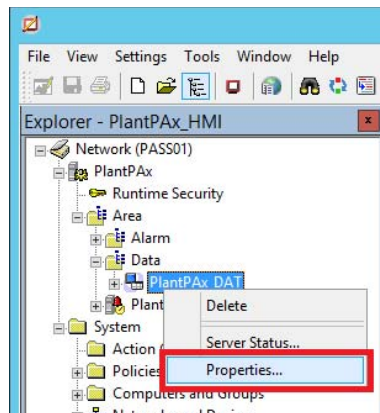
Enable Data Server Redundancy

This section describes how to configure a Secondary server and edit redundant controller paths.

Set Up Data Redundancy

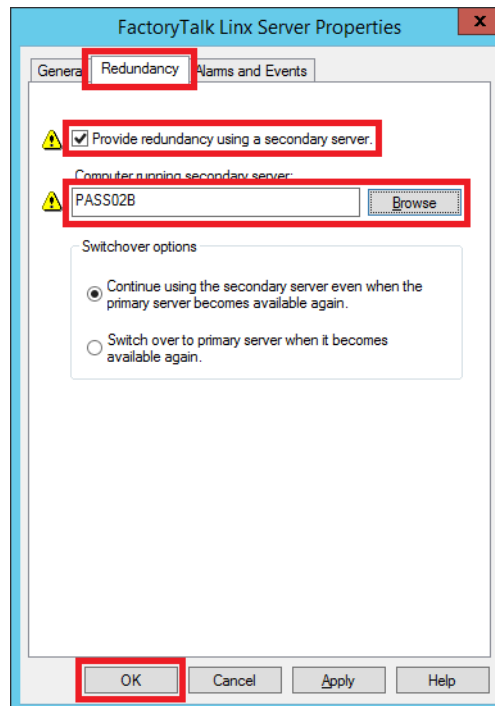
Complete the following steps.

1. Open your project (PlantPax in the example). See [step 1](#) through [step 3](#) for more information.
2. In the Explorer, right-click PlantPax>Area>Data>PlantPax_DAT and choose Properties.



The FactoryTalk Linx Server Properties dialog box appears.

3. In the Redundancy tab, check 'Provide redundancy using a secondary server' box.

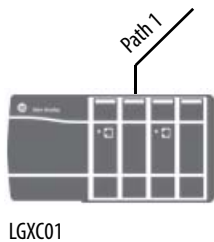


4. Click Browse and select the secondary server.
5. Click OK.

Shortcut Configuration Paths

The PlantPAx system provides several methods for enabling communication with controllers via shortcuts:

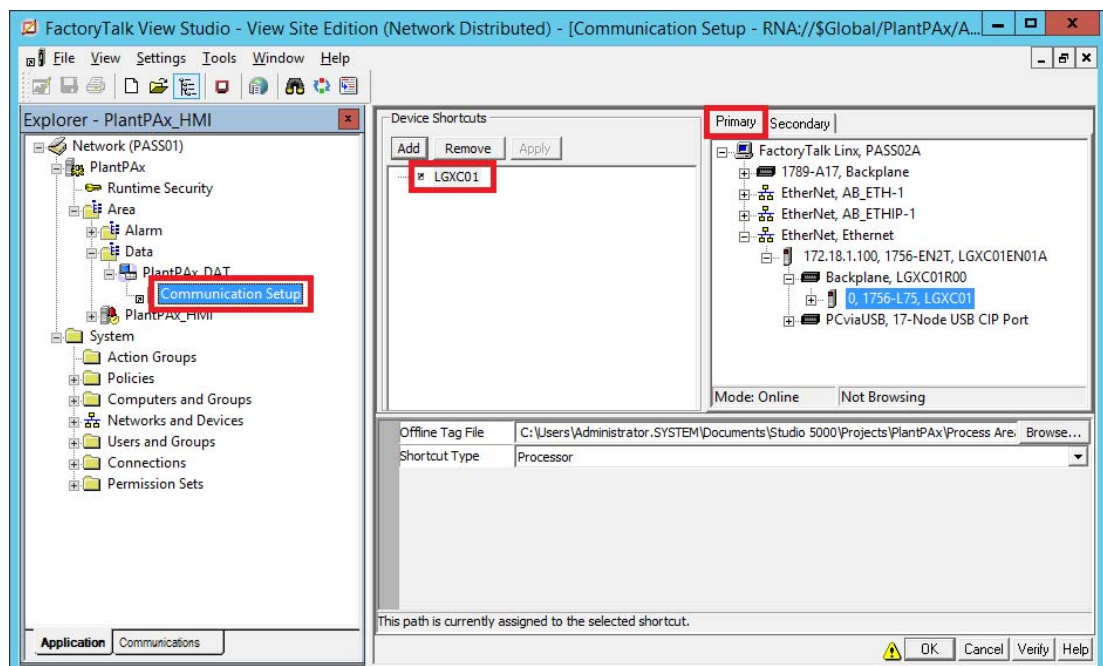
- Single Redundant Path (processor) — This ‘traditional’ redundant path has a single IP address with a Simplex controller or redundant set of controllers.
- Dual Redundant Path — Each of two adapter modules in a controller chassis have their own IP address. If one adapter has a break in communication, the other adapter is available as a redundant backup.
- Redundant ControlLogix® controller — This method also requires fixed IP addresses at the controller level. There is a primary IP address and a secondary IP address configured for a redundant pair of Ethernet adapters. A switchover from the primary controller uses the IP address of the adapter in the secondary controller.



Configure a Single Redundant Path

This section describes how to configure an IP address for a Simplex controller.

1. If necessary, expand the primary Data server (PlantPAx_DAT in the example).



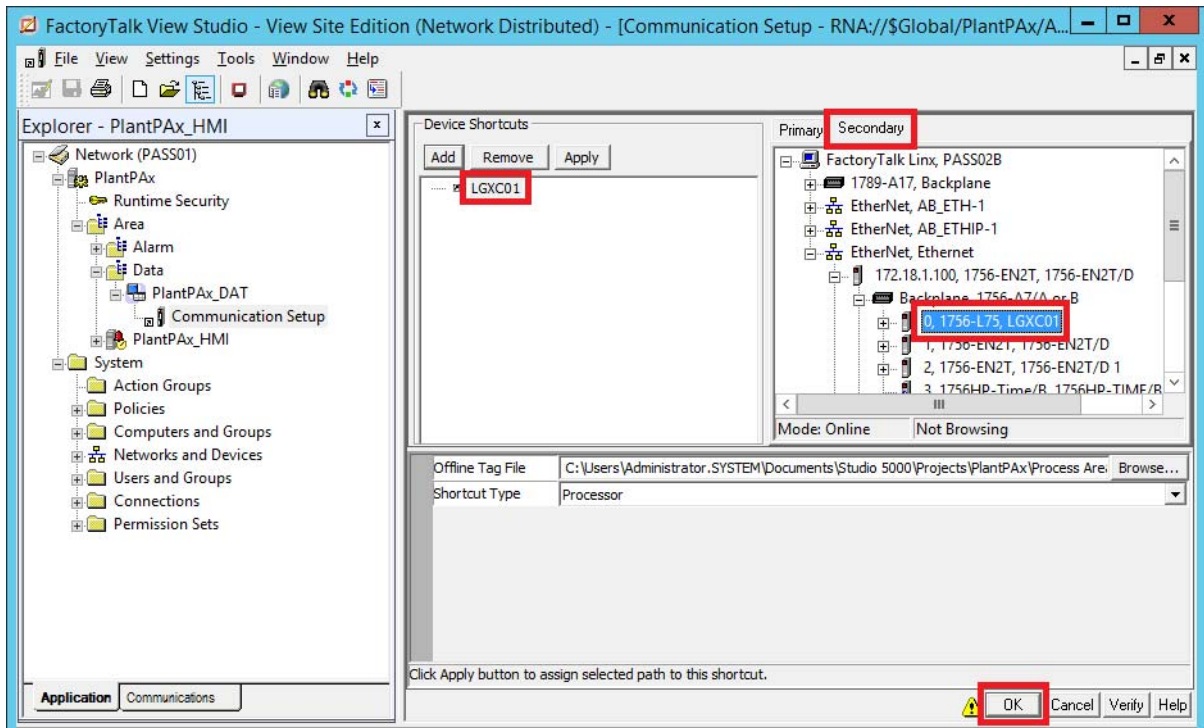
2. Double-click Communication Setup.

The Communication Setup window appears.

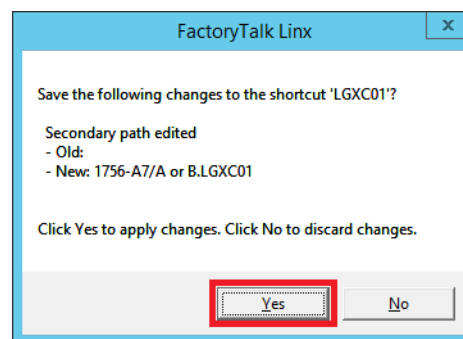
3. Click the shortcut (LGXC01 in the example).
4. Click the Primary tab and select the path to the controller (1756-L75, LGXC01 in the example).

If you are using data server redundancy, you must configure a patch from the secondary data server to the controller.

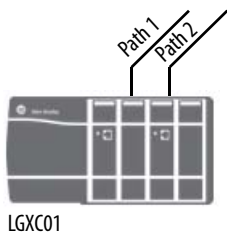
5. On the Communication Setup window, click the Secondary tab.



6. Click Verify (third button to the left of OK).
7. Click OK to close the verification dialog box.
8. Navigate to and select a path to the controller.
9. Click OK.



10. Review the summary of changes and click Yes to apply.
11. Right-click the data server name (PlantPax_DAT in the example) in the Explorer tree and choose Server Status.



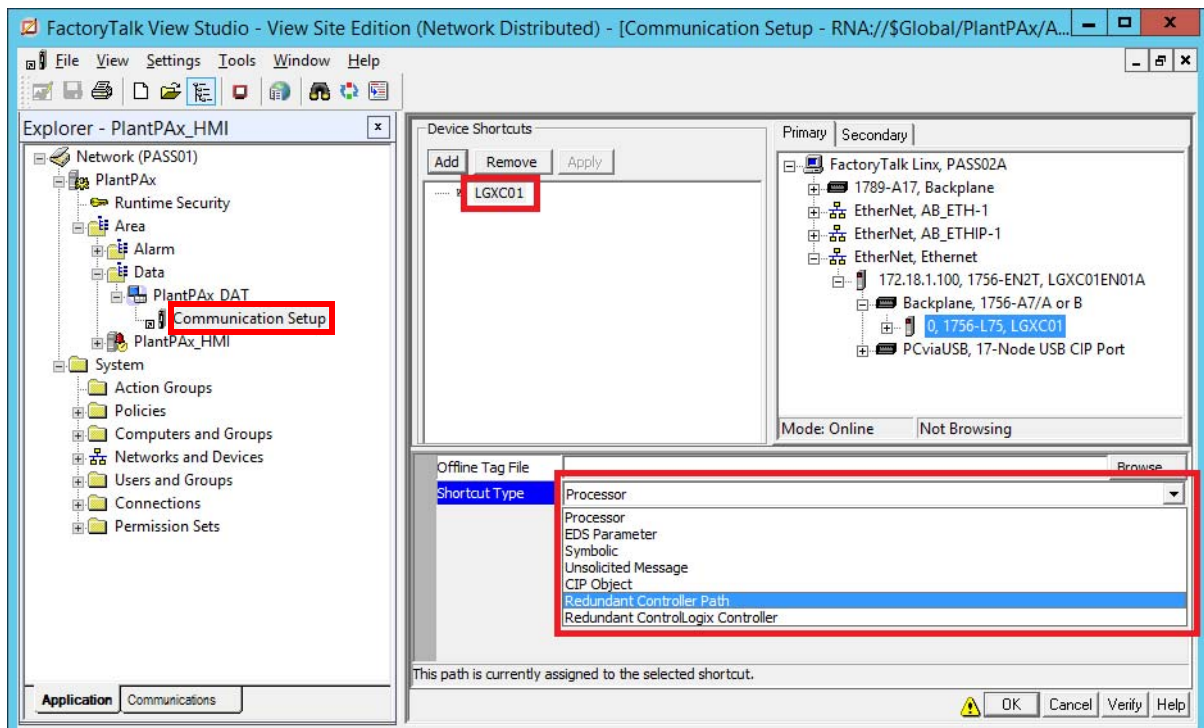
The Server Status dialog box appears.

12. Click OK.

Configure a Dual Path for a Simplex Controller

Complete these steps to configure dual IP address paths for separate adapters in the same controller chassis.

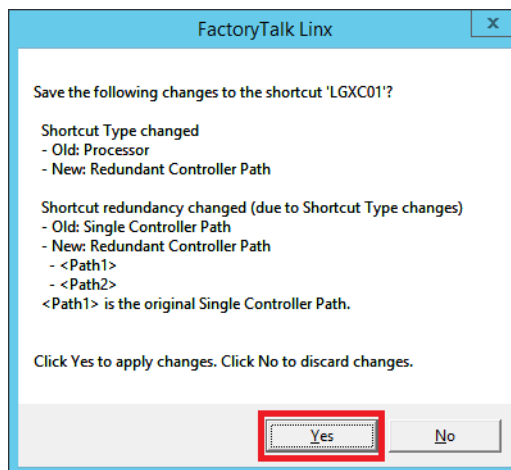
1. Expand the primary Data server (PlantPax_DAT in the example).
2. Double-click Communication Setup.



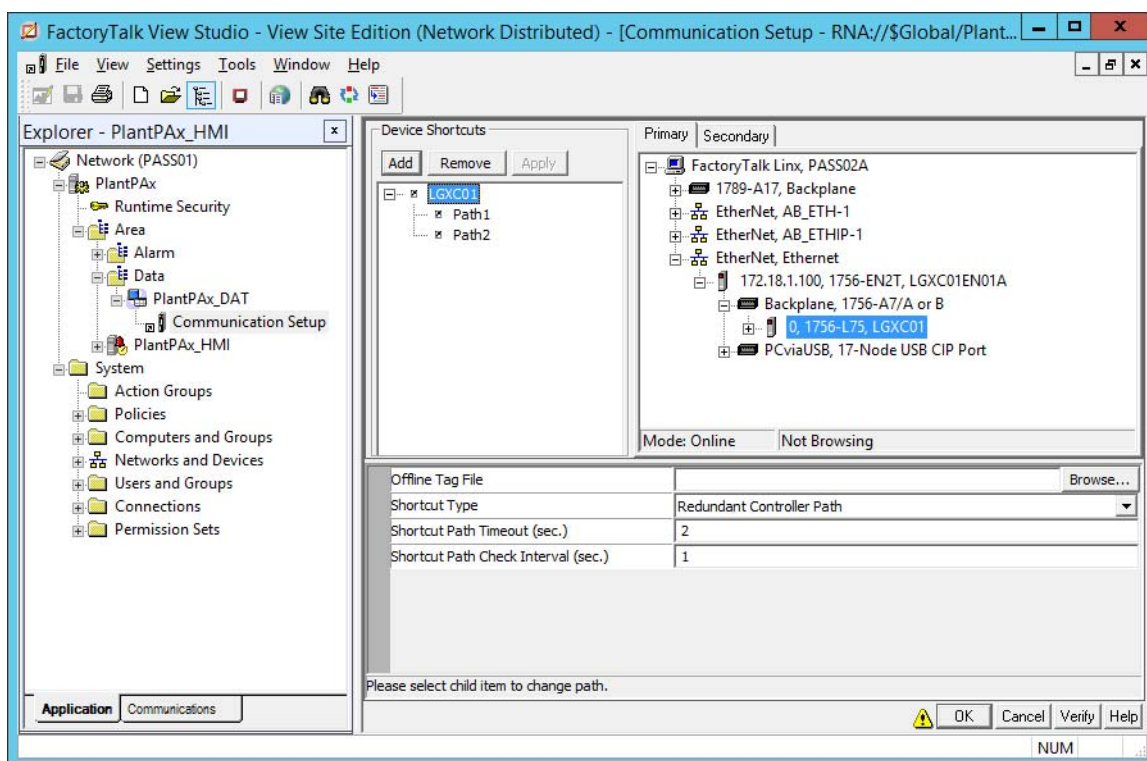
The Communication Setup window appears.

3. Click the shortcut (LGXC01 in the example).

4. Click Shortcut Type and choose Redundant Controller Path from the Processor pull-down.



5. Click Yes.
6. Click the shortcut (LGXC01 in the example).
7. Click the Secondary Tab and select (1756-L75, LGXC01 in the example).

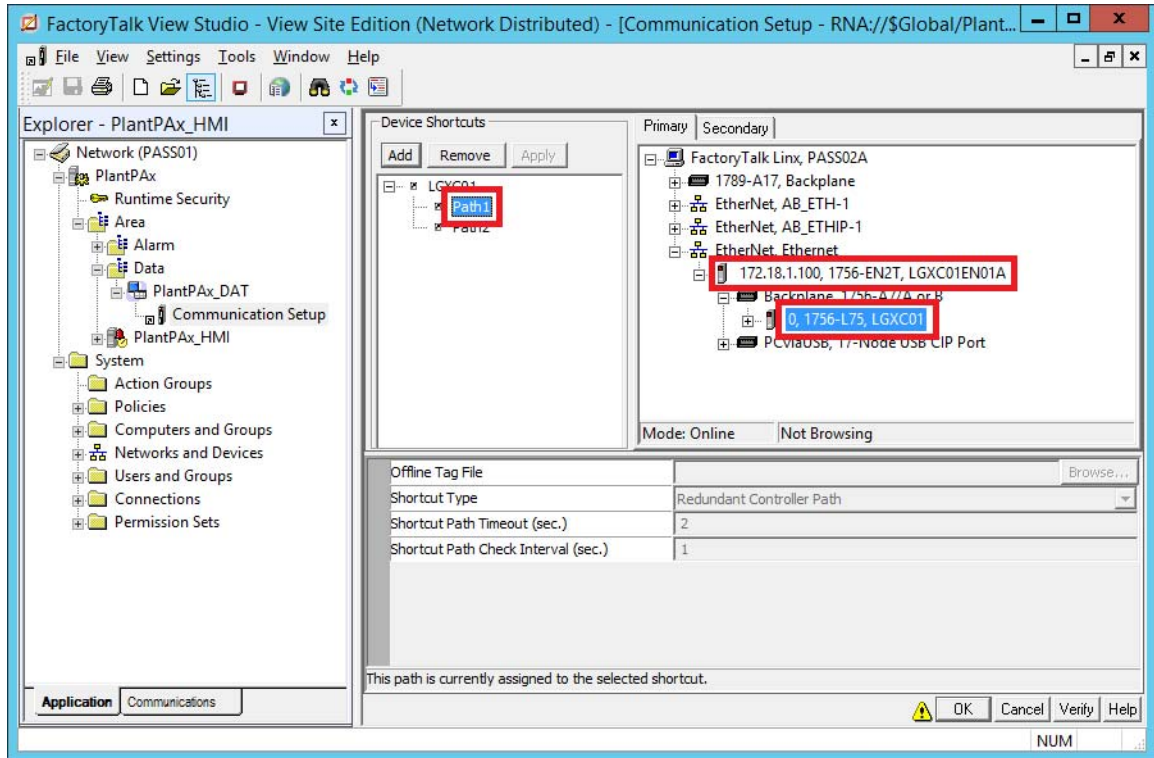


8. Do **not** click OK. Remain on the Communication Setup window to finish configuring the adapter paths, starting on [page 271](#).

Select Path 1 for the Primary Data Server

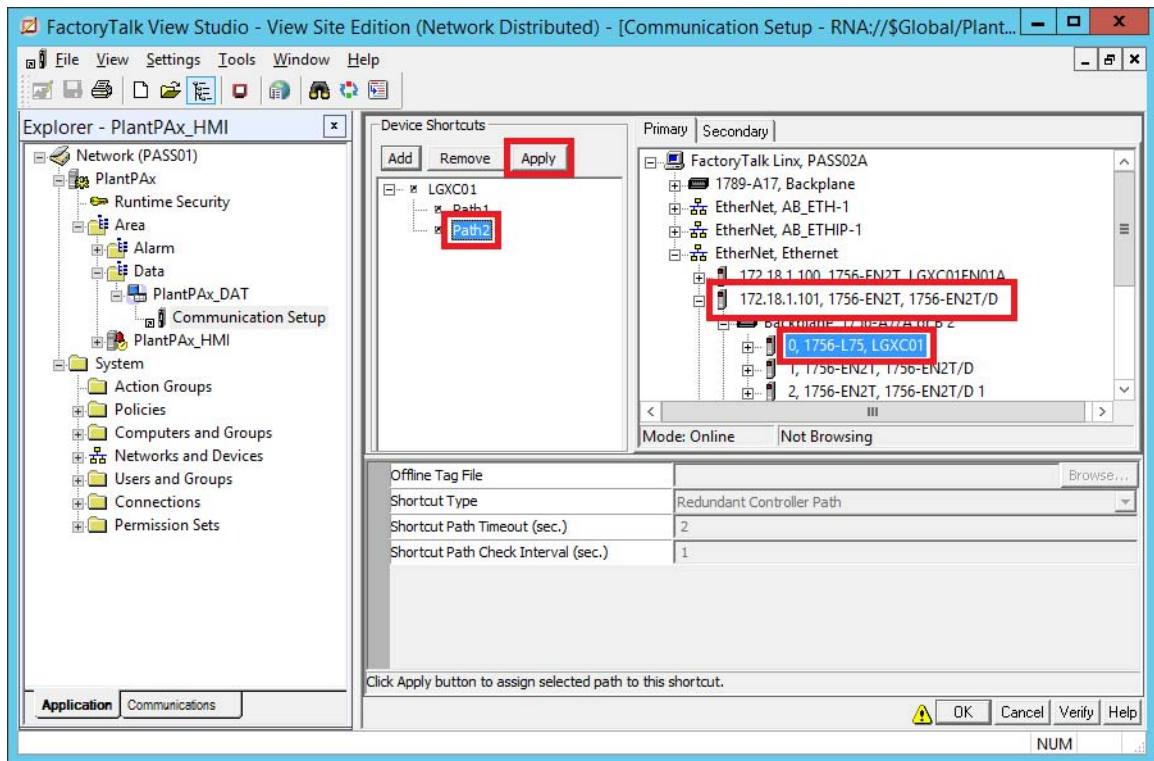
Complete these steps to select the IP address for the path 1 adapter.

1. Select Path 1 for the shortcut.



2. From the Primary tab, select the IP address for the path 1 adapter and the controller.

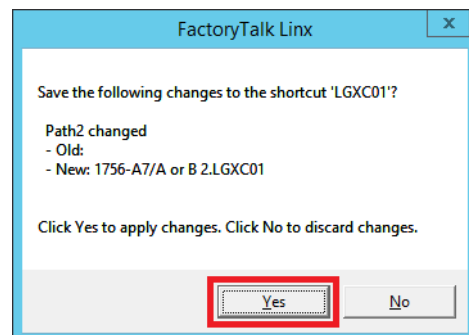
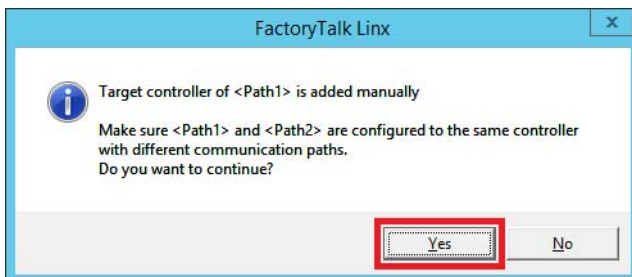
3. Click Apply.



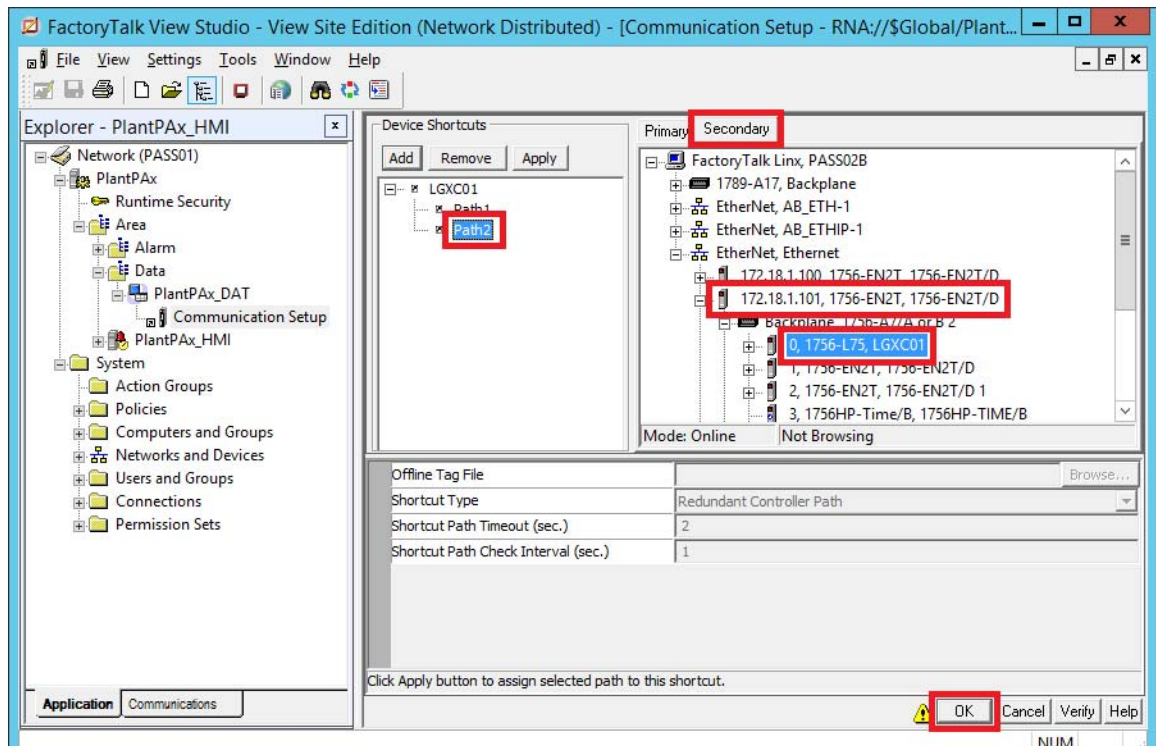
Select Path 2 for the Primary Data Server

Complete these steps to select a different IP address for a second adapter for path 2.

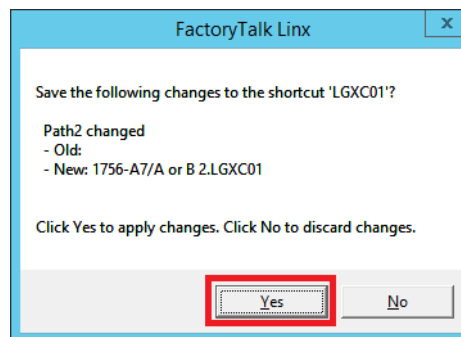
1. Select Path 2 for the shortcut.
2. From the Primary tab, select the IP address for path 2 and the controller.
3. Click Apply.
4. Click Yes twice to assign both paths to the Primary server.

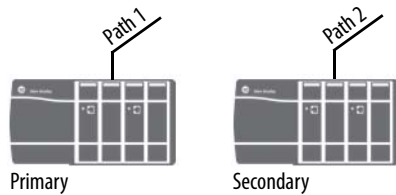


5. Click the Secondary tab and select Path 1.
6. Select the IP address for the path 2 adapter and the controller.
7. Click Apply.



8. Click OK.
9. Click Yes on the message window.

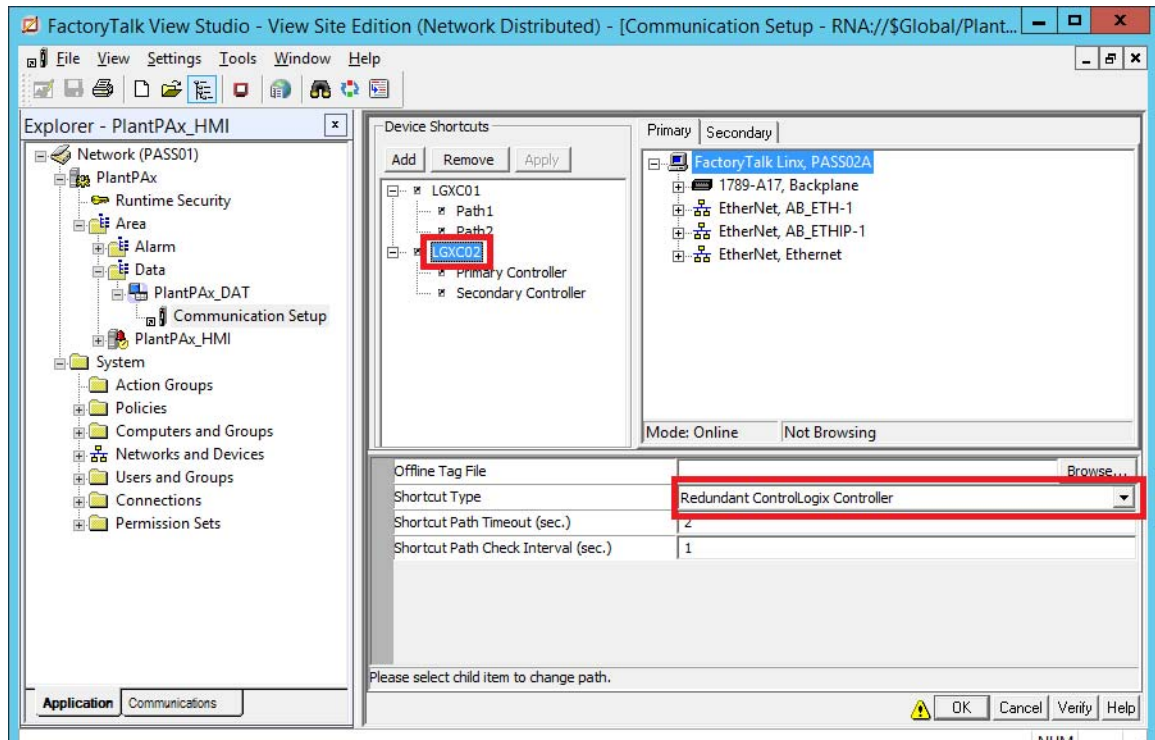




Redundant ControlLogix Controller

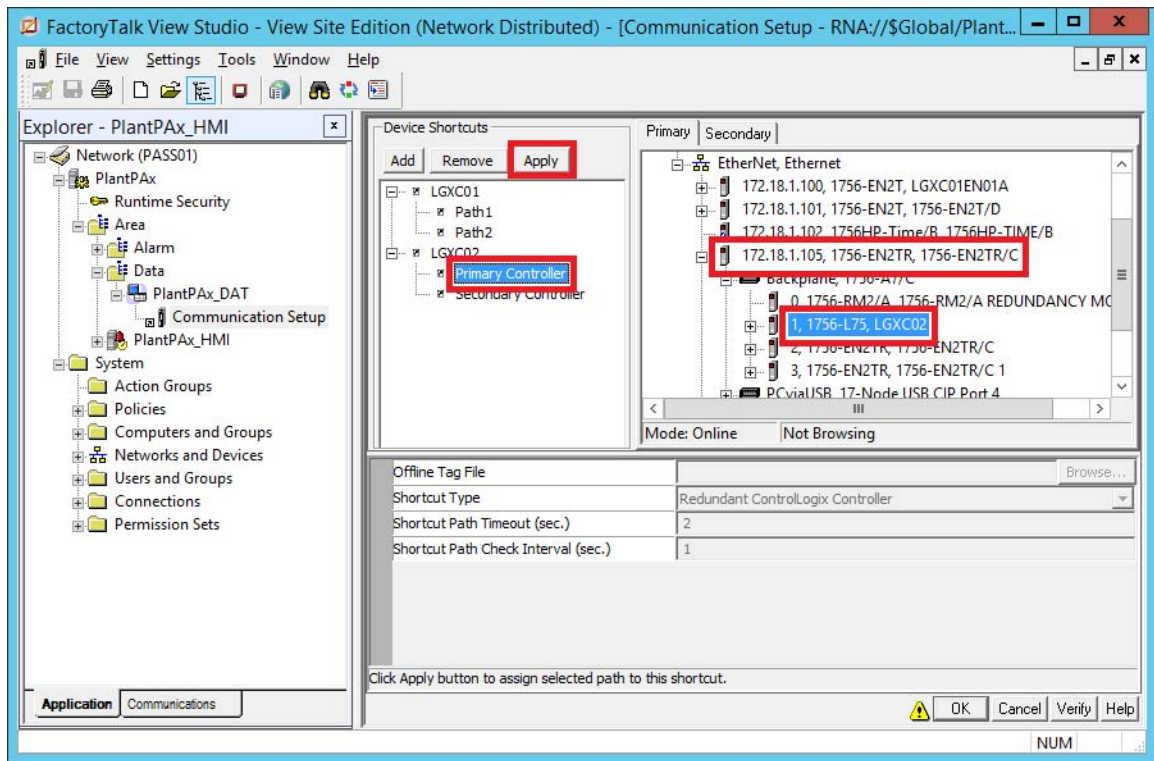
Complete these steps to assign a fixed IP address to a redundant pair of ControlLogix controllers.

1. From the Communication Setup window, click the second shortcut (LGXC02 in the example).



2. Select Redundant ControlLogix Controller from the Shortcut Type pull-down menu.

3. Click Apply.



4. Click the Primary Controller shortcut.

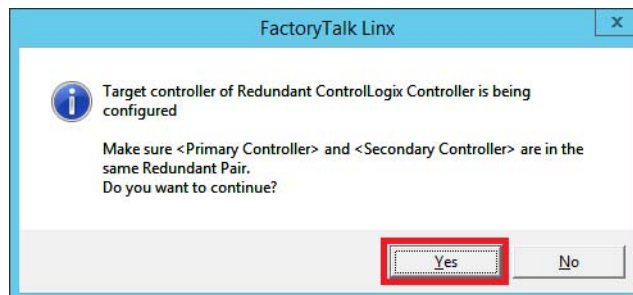
5. From the Primary tab, select the IP address of the adapter and the primary controller.

Observe that our example shows the IP address of 172.18.1.105.

IMPORTANT Make sure the HMI communication card is configured to disallow an IP address swap. Configure a different IP address than the first HMI communication card.

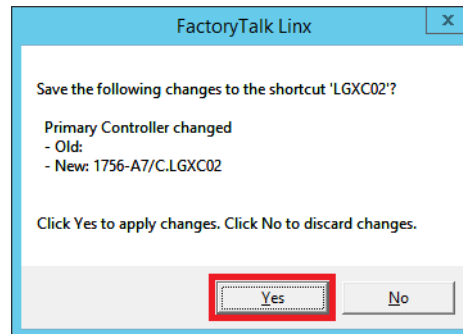
6. Click Apply.

A FactoryTalk Linx popup window appears with the message the target controller is being configured.

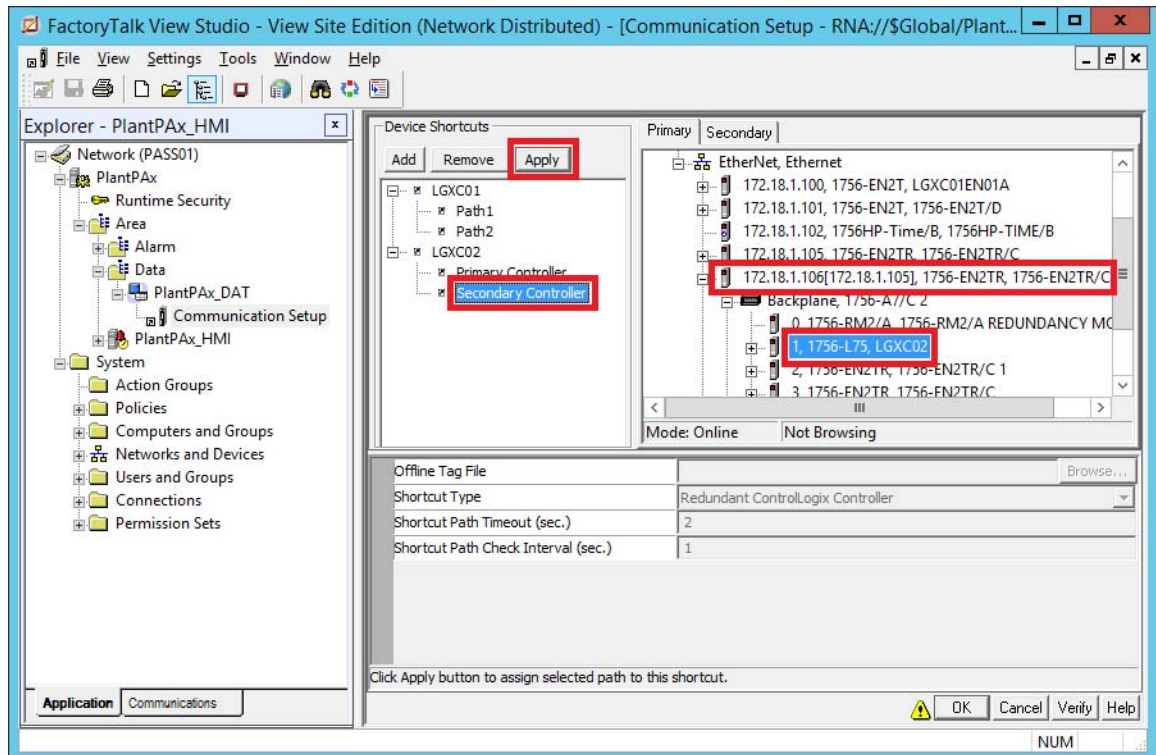


7. Click Yes.

Another FactoryTalk Linx popup window appears with a message that changes are being made to the controller shortcut (LGXC02 for our example).

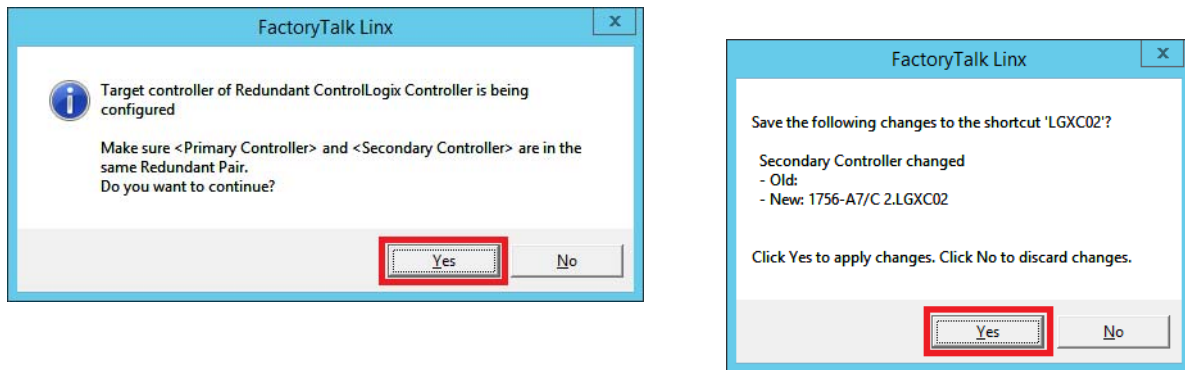


8. Click Yes.
9. From the Communication Setup dialog box, click the Secondary Controller.

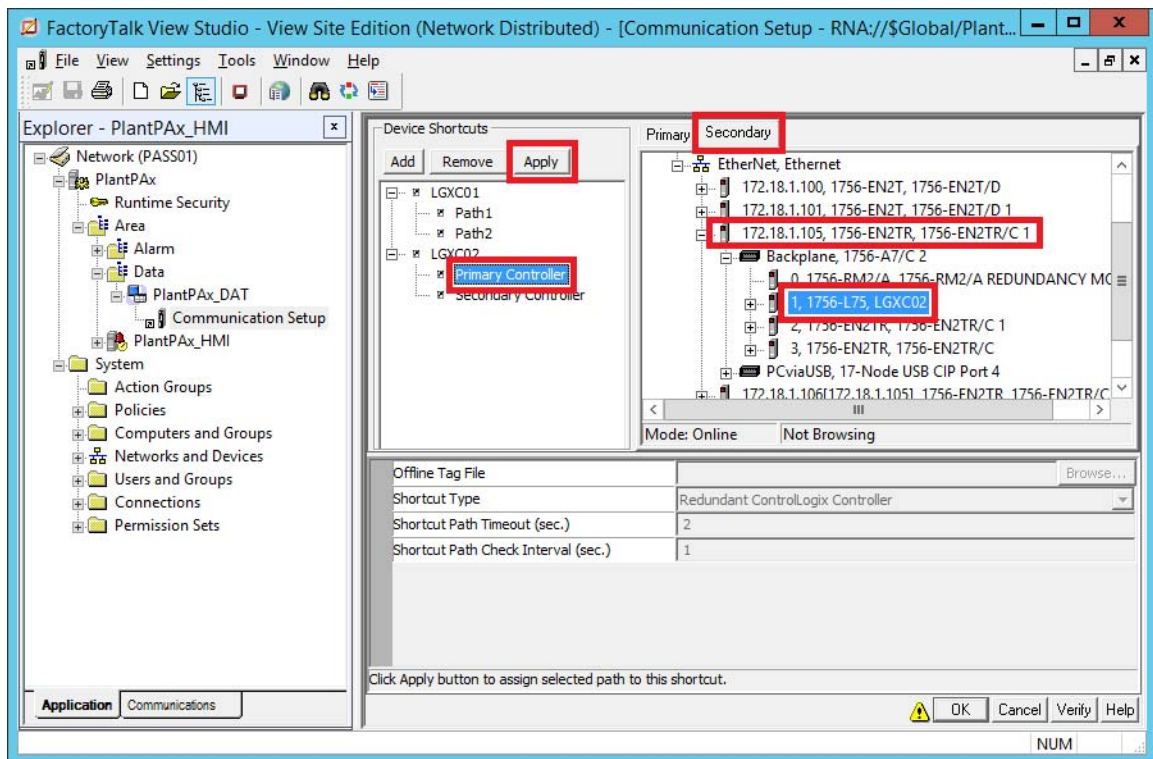


10. From the Primary tab, select a different IP address for the adapter and the primary controller.
Observe that our example shows the IP address of 172.18.1.106.
11. Click Apply.

FactoryTalk Linx popup windows appear.

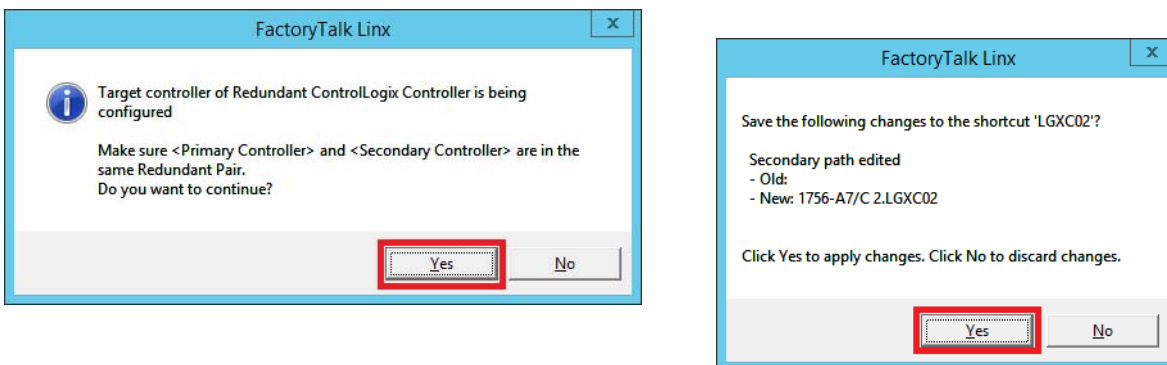


12. Click Yes for each message.
13. Click the Secondary tab, and then click Primary Controller shortcut.

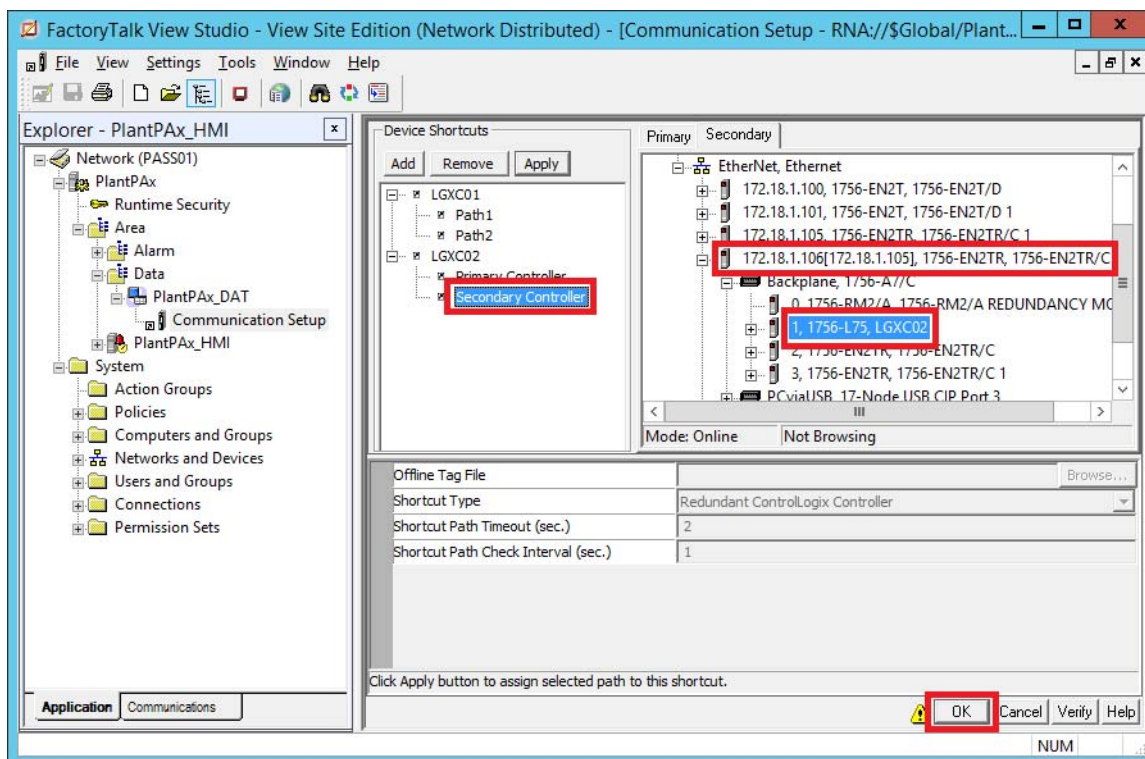


14. Select the same IP address of the adapter and the controller that you did for the data server for the primary controller in [step 5 on page 275](#).
Observe that our example shows the IP address of 172.18.1.105.
15. Click Apply.

FactoryTalk Linx popup windows appear.

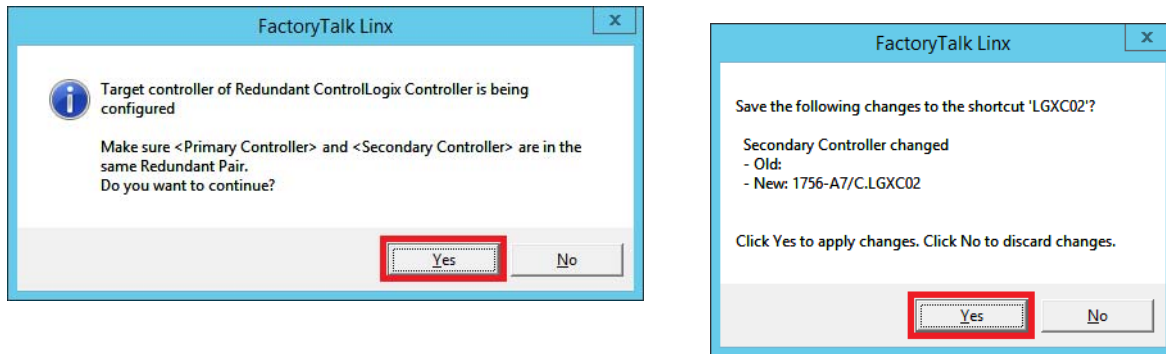


16. Click Yes for each message.
17. Click Secondary Controller.



18. Select the same IP address of the adapter and the controller that you did for the data server for the secondary controller in [step 10 on page 276](#).
Observe that our example shows the IP address of 172.18.1.106.
19. Click OK.

FactoryTalk Linx popup windows appear.

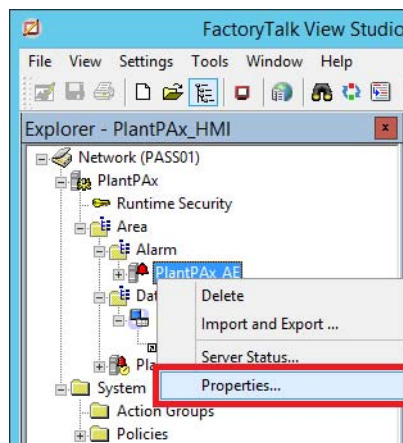


20. Click Yes for each message.

Enable Alarm and Event Redundancy

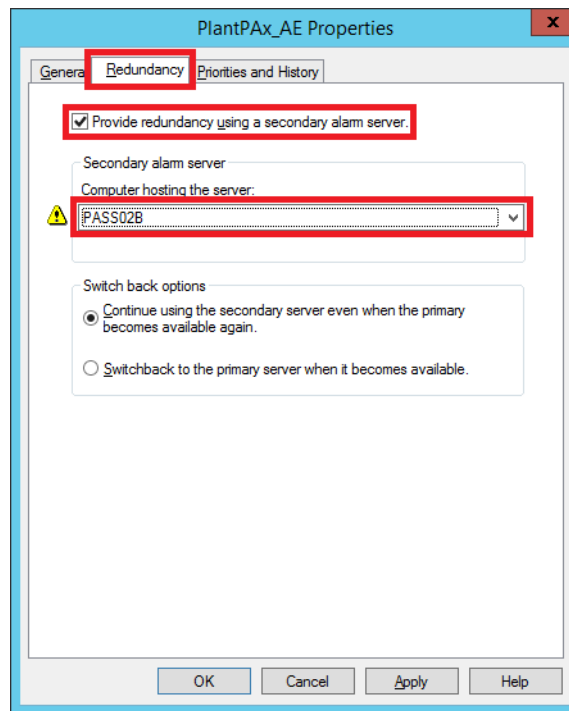
Complete these steps.

1. In FactoryTalk View Studio, right-click PlantPAx>Area>Alarm>PlantPAx_AE and choose Properties.

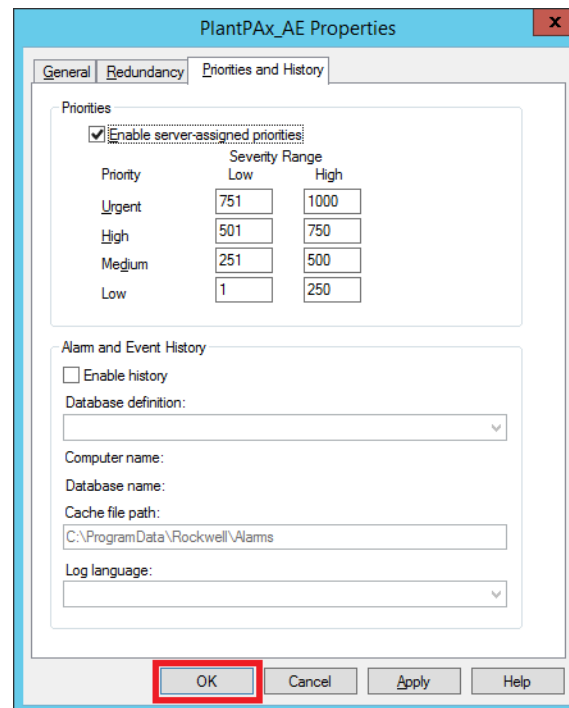


The Tag Alarm and Event Server Properties dialog box appears.

- On the Redundancy tab, check 'Provide redundancy using a secondary alarm server.



- From the pull-down menu, select the Secondary server.
- On the Priorities and History tab, verify the alarm severity ranges and click OK.



Create Alarm and Event Database

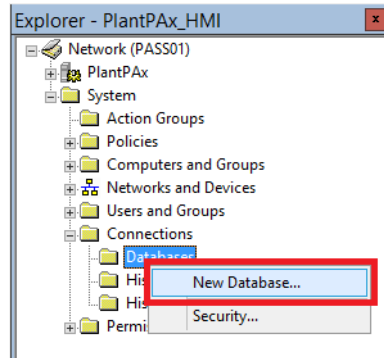
Use an Engineering Workstation with these procedures



You must create a database to enable Alarm and Event history.

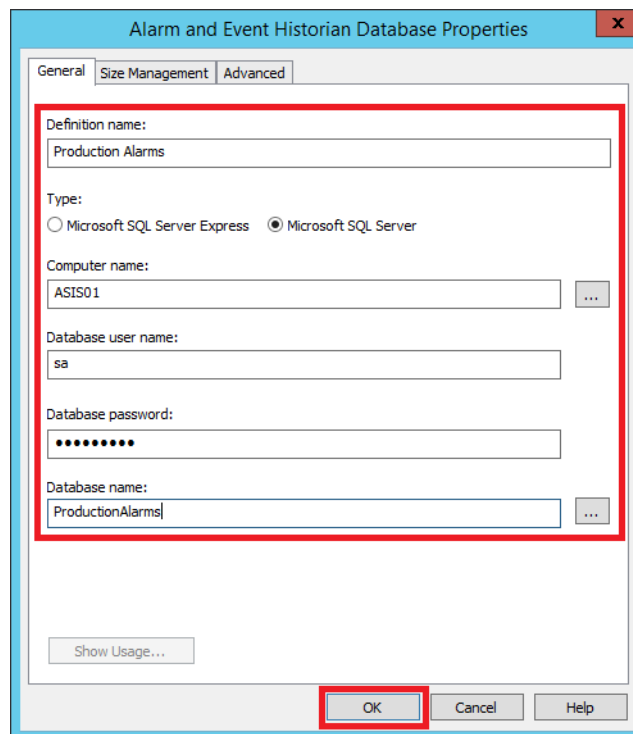
Complete the following steps:

1. From FactoryTalk View Studio Explorer, right-click **System>Connections>Databases** and choose **New Database**.



The Alarm and Event Historian Database Properties dialog box appears.

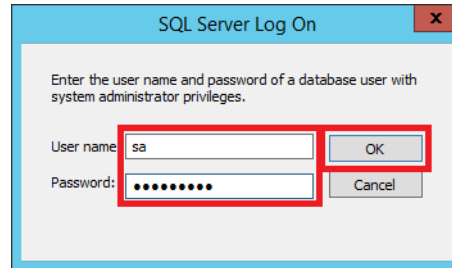
2. Configure the new database.
 - a. Type a definition name.



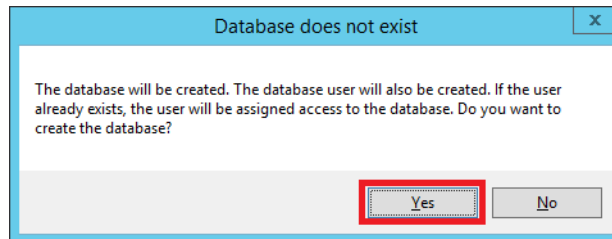
- b. Click the type of SQL Server you want to use.
- c. Type the Computer name or click Browse (ellipsis '...') to navigate to the computer name.
- d. Type a Database user name.
- e. Type 'SA' for the user and the SA password, or use other known credentials.

- f. Type a new Database name or click Browse (ellipsis '...') to navigate to a database name.
3. Click OK.
A log on popup window could appear.
4. Type the user name ('sa' for the dedicated database).

IMPORTANT The user name **must** match the SQL server user account.



5. Type the password and click OK.
A popup window appears and asks if you want to create the database.



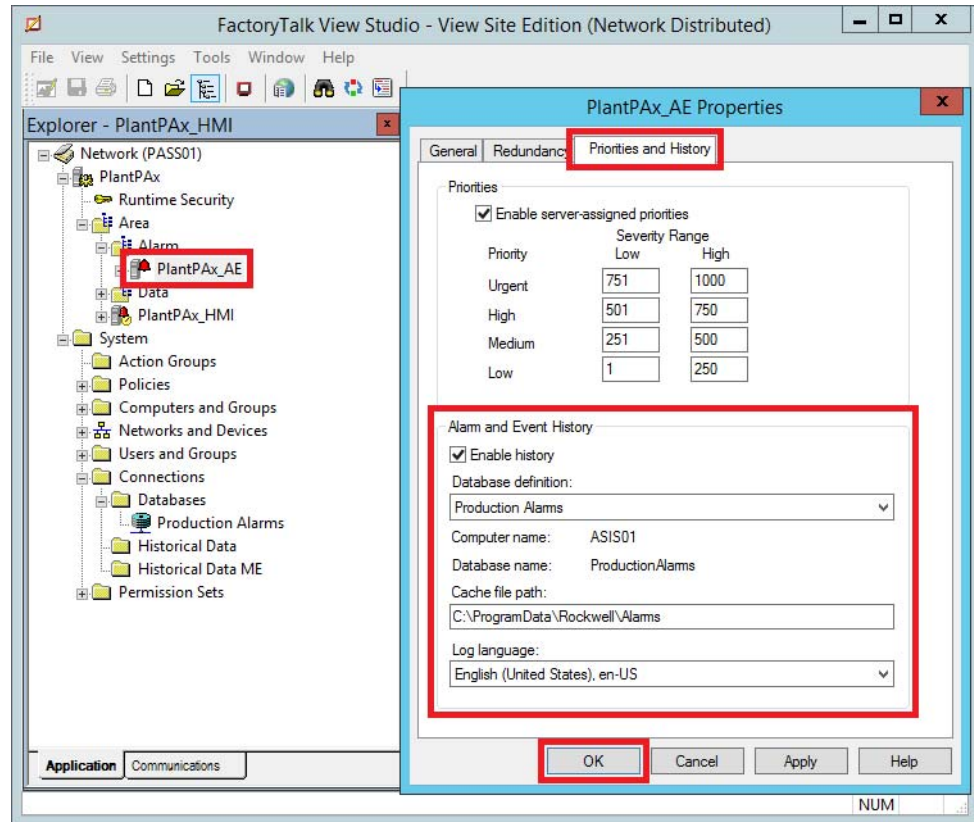
6. Click Yes.

The SQL Server Log On dialog box appears.

7. Right-click the Alarm and Event server.

The Server Properties dialog box appears.

8. On the Priorities and History tab, check 'Enable history'.



9. From the pull-down menu, select the database definition.
10. Accept the default Cache file path.
11. From the pull-down menu, select the Log Language.
12. Click OK.

Define HMI Security

This section describes how to configure security for the FactoryTalk View Site Edition (SE) software.

Configure FactoryTalk SE Security

Runtime security must be set up to provide each account or user group with the correct FactoryTalk View security codes. The security codes verify that operators, maintenance personnel, and engineers have permission to run secured commands, open secured graphic displays, or write to secured tags at runtime.

IMPORTANT See Rockwell Automation Library of Process Objects, publication [PROCES-RM002](#), for a list of security codes and descriptions.

Use a PASS with these procedures.

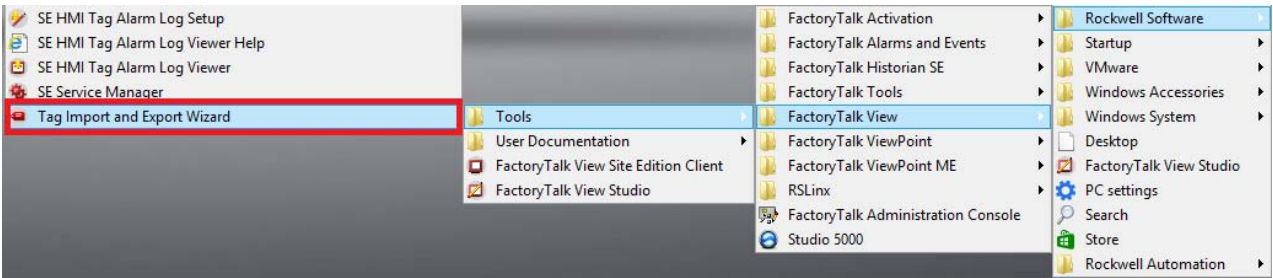


PASS02A

Import FactoryTalk Site Edition Security Tags

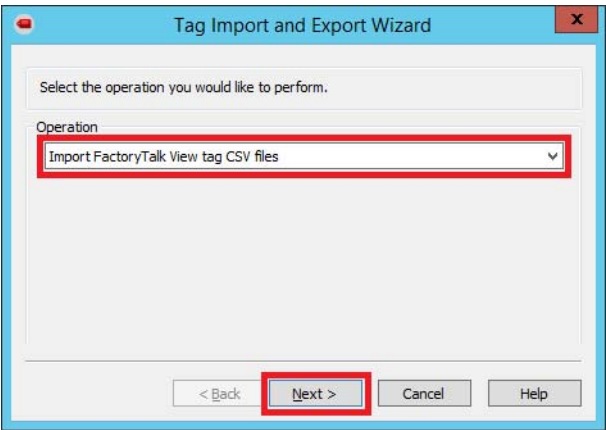
Complete the following steps to import security tags on the PASS.

1. Click the Programs >> symbol and choose Rockwell Software>FactoryTalk View>Tools>Tag Import and Export Wizard.

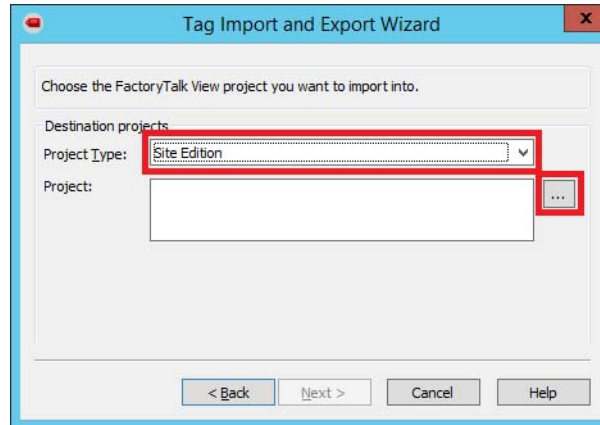


The Tag Import and Export Wizard dialog box appears.

2. From the Operation pull-down, select Import FactoryTalk View tag CSV files and click Next.

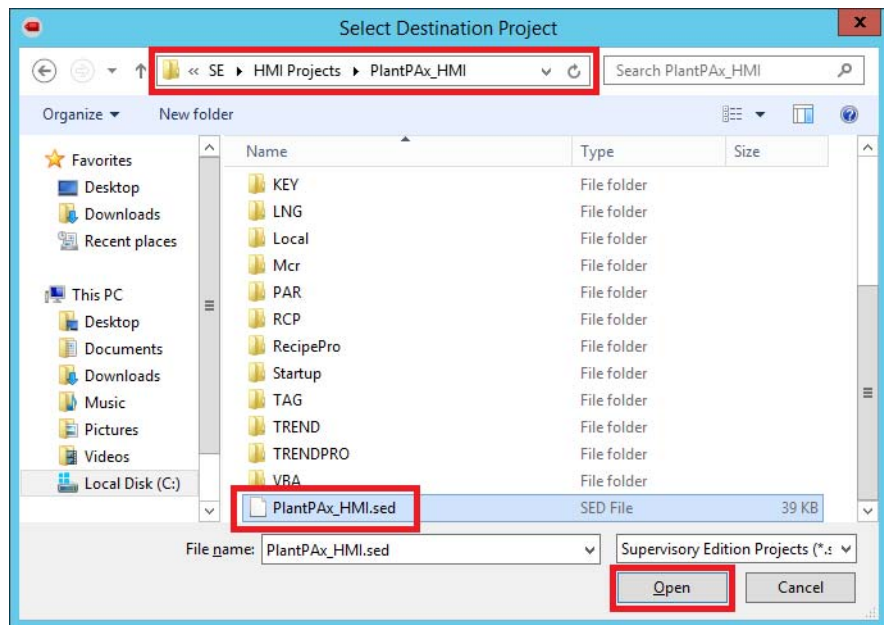


- From the Project Type pull-down, select Site Edition and click Browse (ellipsis '...').



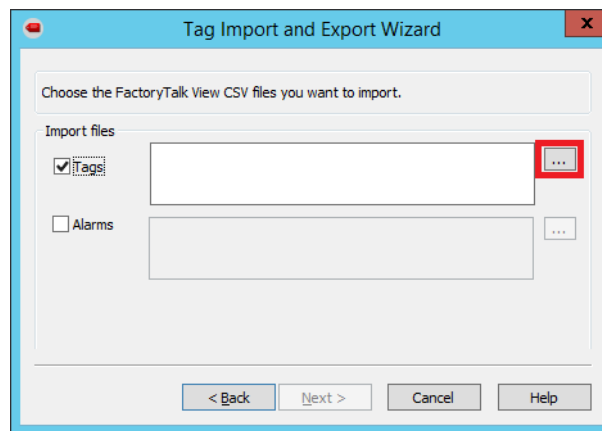
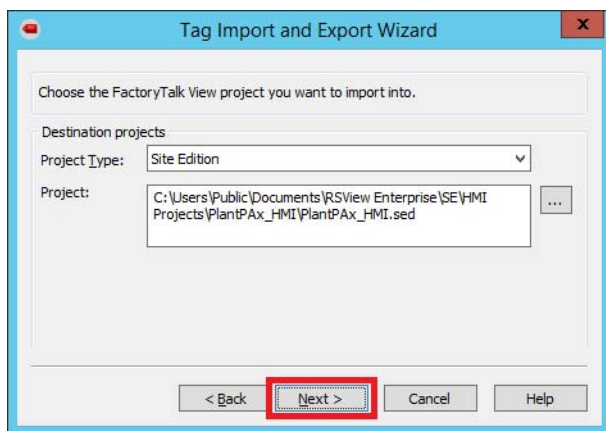
The Select Destination Project dialog box appears.

- Select the path of SE>HMI Projects>PlantPAx_HMI.

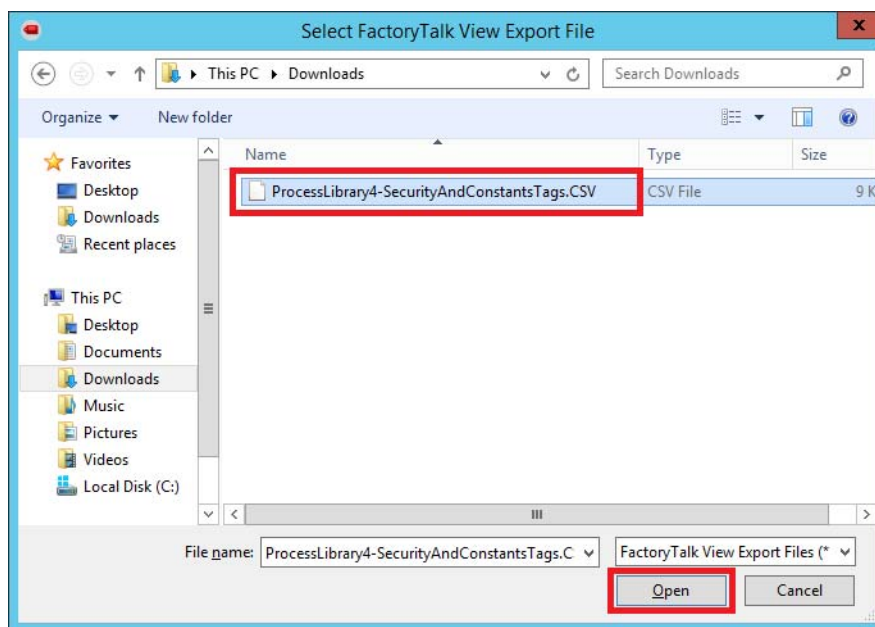


- Select PlantPAx_HMI.sed and click Open.

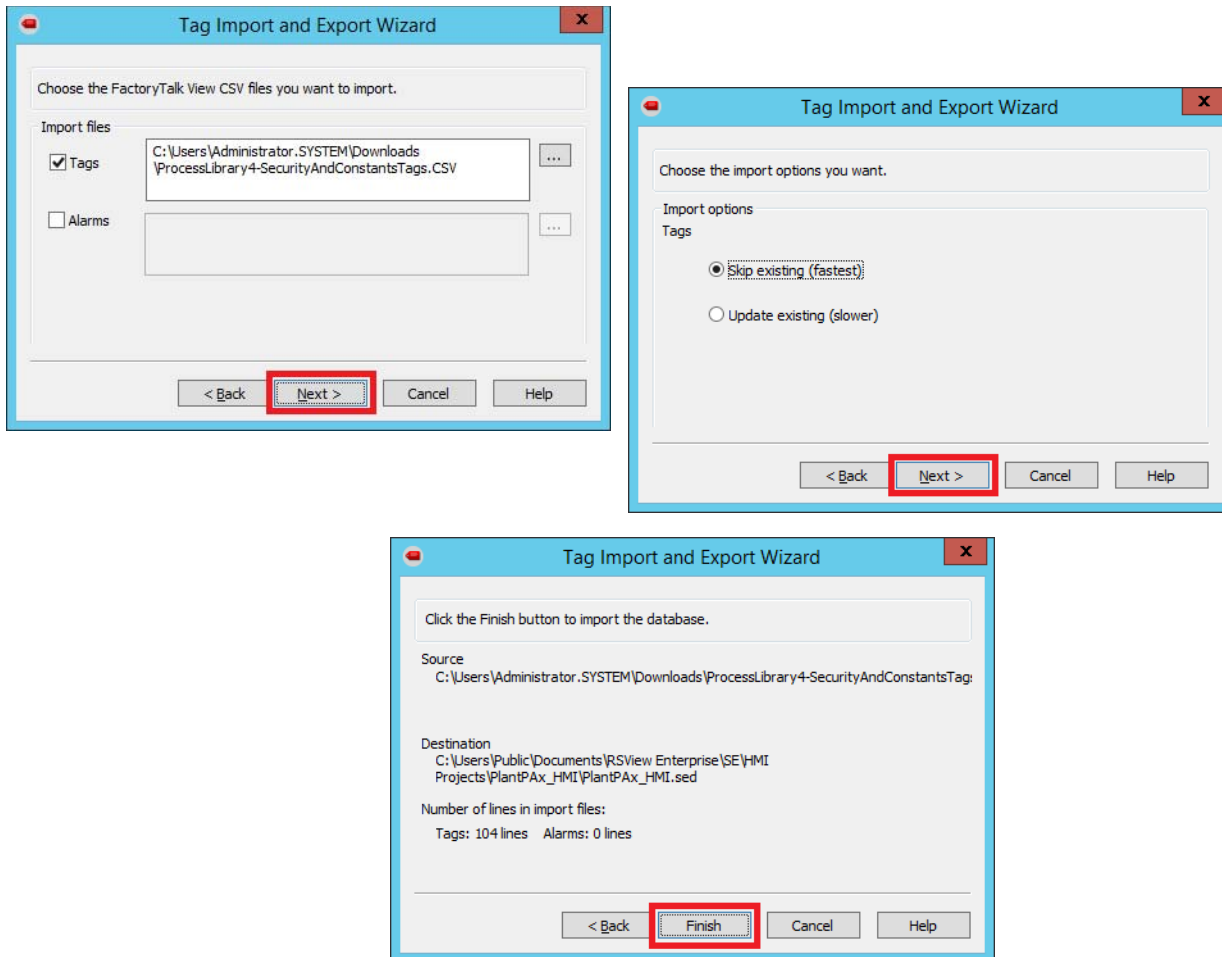
6. Click Next and Browse (ellipsis '...') for the ProcessLibrary4-SecurityAndConstantsTags.CSV file. This file is distributed with the PlantPAx Library of Process Objects Library.



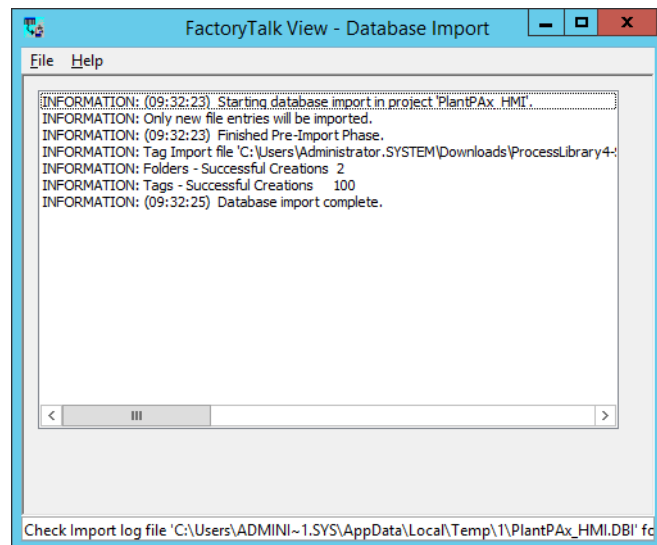
7. Click Open.



8. Click Next twice, and then click Finish.



The import results appear on the Database Import window.



9. To close the window, click 'X'.

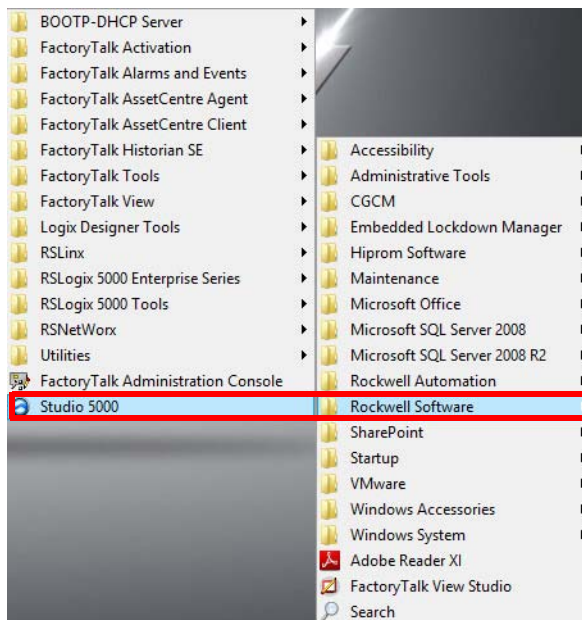
Setting Group Security

Use an Engineering Workstation with these procedures.



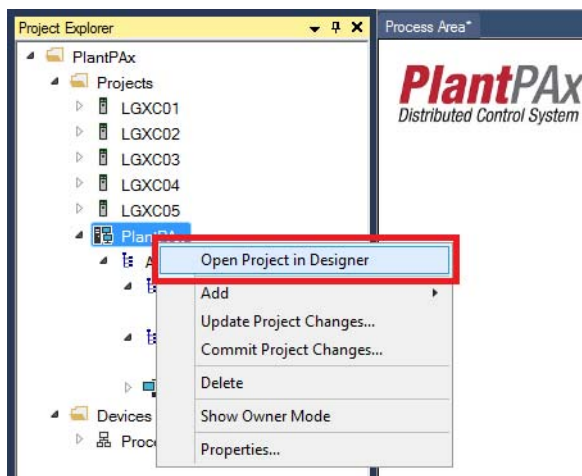
Complete these steps to set security permissions to groups on the workstation.

1. Click the Programs >> symbol and choose Rockwell Software>Studio 5000.



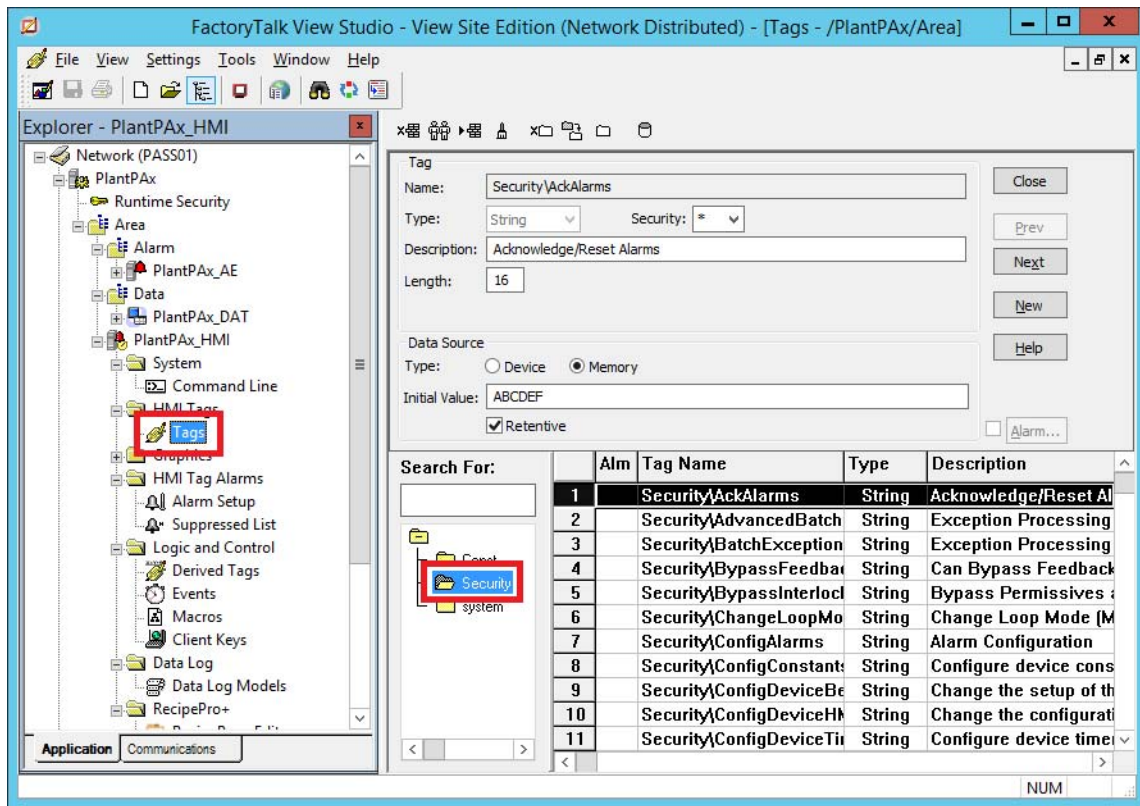
The Studio 5000 splash screen appears.

2. In the Studio 5000 splash page, select a recent project (PlantPax in the example).
3. In the Project Explorer, right-click PlantPax>Projects>PlantPax and choose Open Project in Designer.



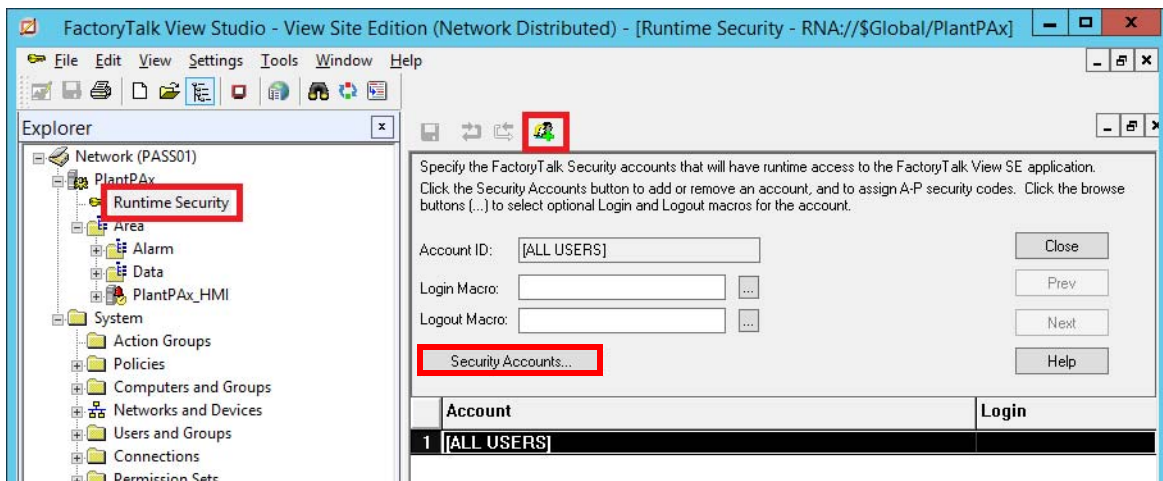
The FactoryTalk View Studio dialog box appears.

4. To verify that the security tags have been imported, choose PlantPAx>Area>PlantPAx_HMI>HMI Tags and double-click Tags.



IMPORTANT If the security tags have not been imported, see [Import FactoryTalk Site Edition Security Tags on page 284](#) for procedures.

5. In the FactoryTalk View Studio window, double-click PlantPAx>Runtime Security.

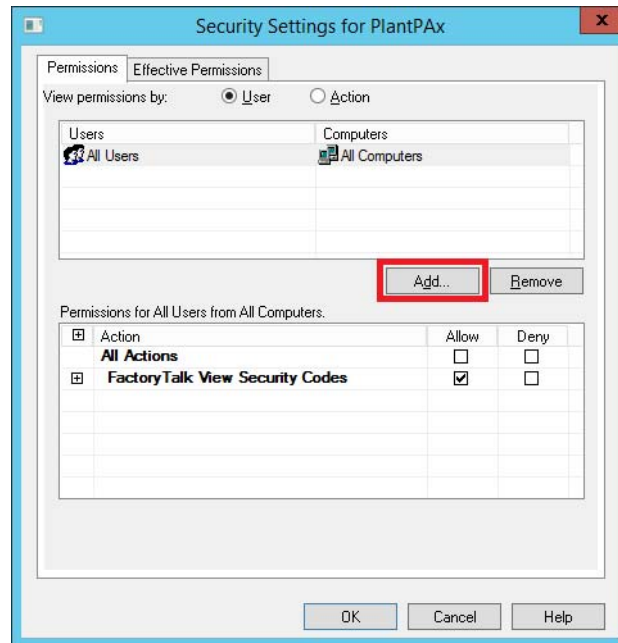


The Runtime Security panel appears on the right side of the window.

6. Click Security Accounts .

The Security Settings dialog box appears.

7. Click Add.

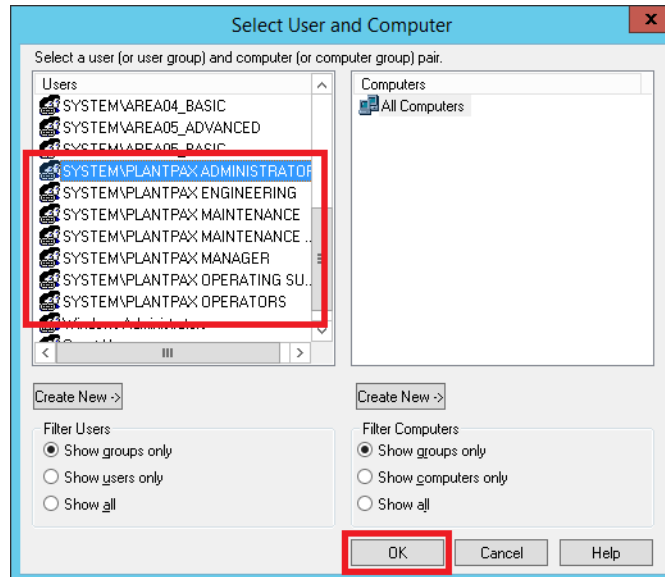


The Select User and Computer dialog box appears.

8. Click a PlantPAx group and click OK.

Each group has its own security code.
For example, 'A' for Operators, 'B' for
Operating Supervisory.

See a list of security codes on [page 291](#).

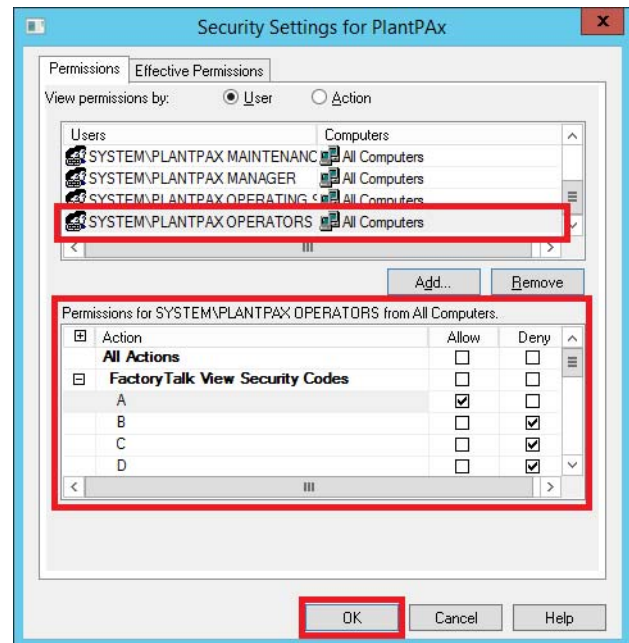
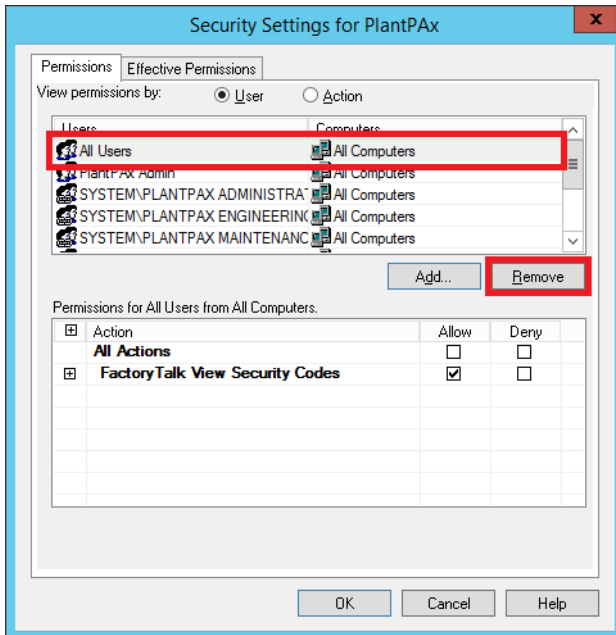


The group name appears in the top half of the Security Settings dialog box.

9. Repeat step 7 and step 8 until all PlantPAx groups are selected.

10. Select 'All Users' and click Remove.

You can assign security to each PlantPAx group based on letters (A...G).



11. Select a group from the Users list.

The default is that all FactoryTalk View Security Codes are checked Allow.

12. Click the Deny checkbox beside the FactoryTalk View Security Codes that you do not want to allow permission for the selected account.

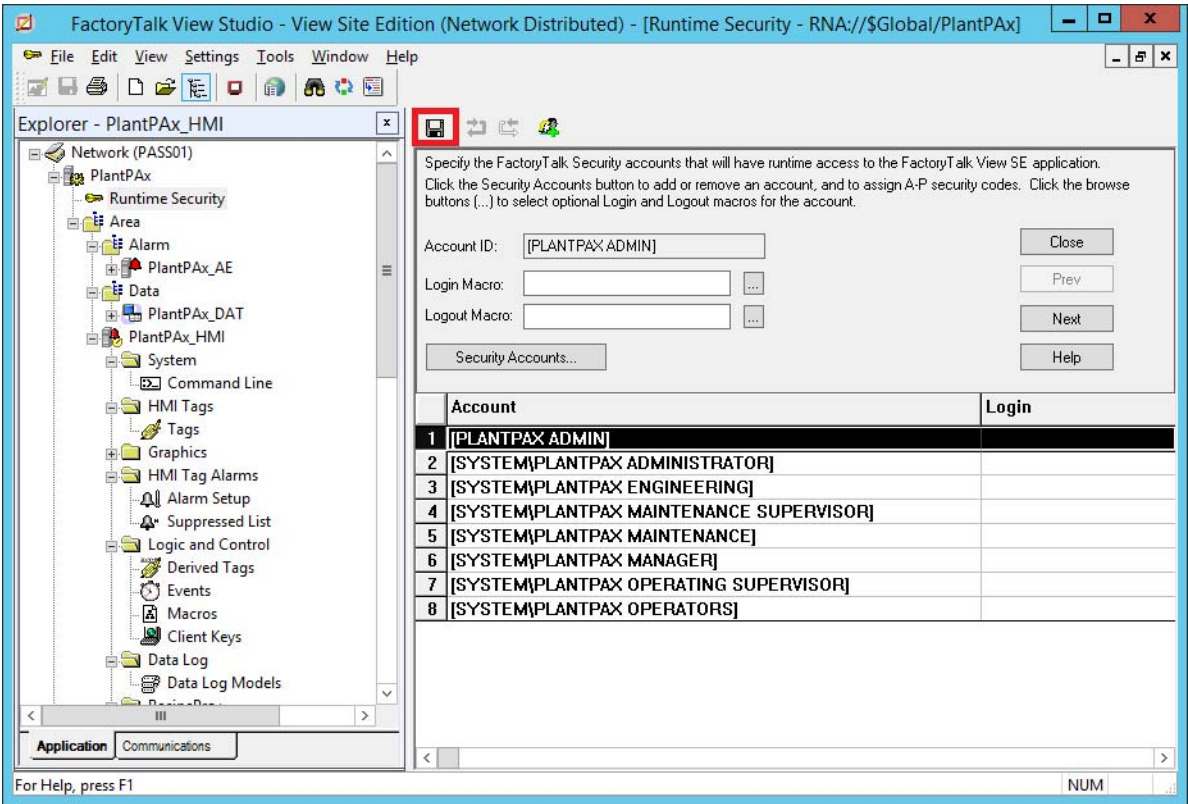
For example, allow security of 'A' for an Operator but deny 'B', 'C', 'D'.

Table 27 - Recommended Group Security Codes

Group	Security Code
Operators	A
Operating Supervisor	B
Maintenance	C
Maintenance Supervisor	D
Engineering	E
Manager	F
Administrator	G

13. Click OK.
14. Repeat step [11](#) through step [13](#) for each user or group account that you want to set up with runtime security.

The PlantPax groups that you set up with runtime security appear in the Account section of the Runtime Security dialog box.



15. Click Save .

Configure PanelView Plus

This section describes how to configure the HMI Machine Edition software for use with PanelView applications.


Use an Engineering Workstation with these procedures

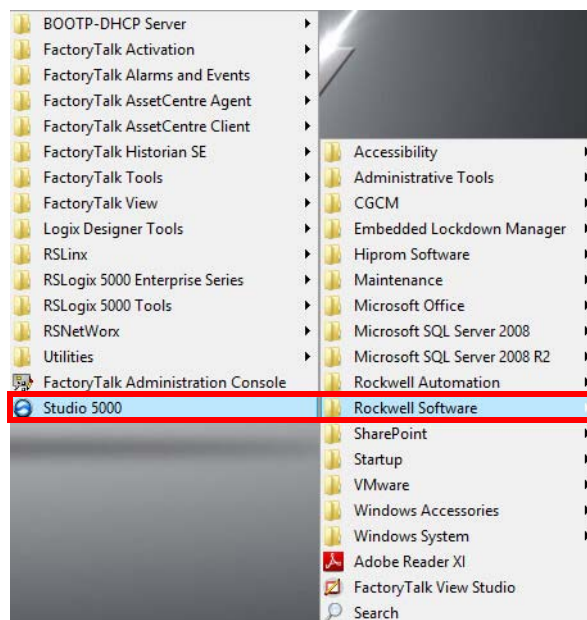


Create a FactoryTalk View ME Project

In this section, you create a FactoryTalk View ME project.

Complete the following steps:

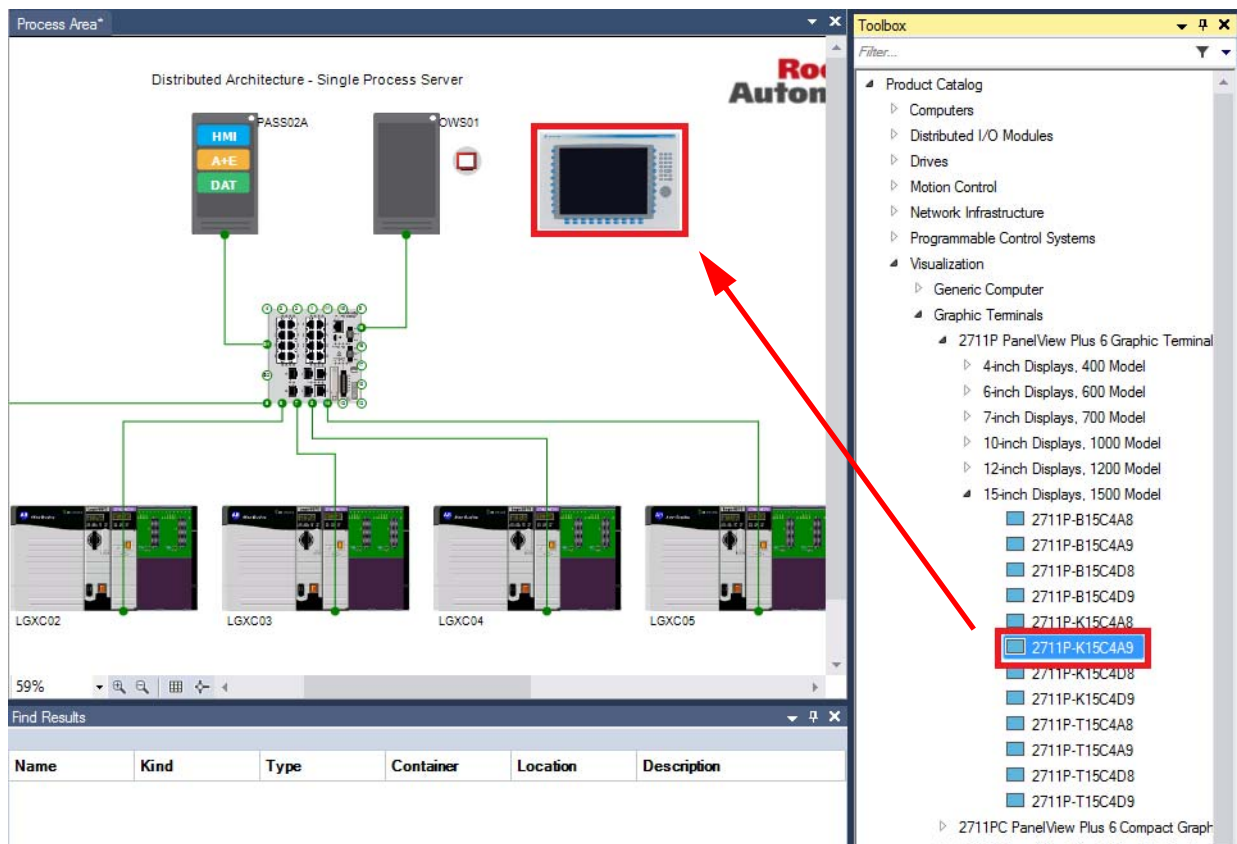
1. Click the Programs  symbol and choose Rockwell Software>Studio 5000.



The Studio 5000 splash screen appears.

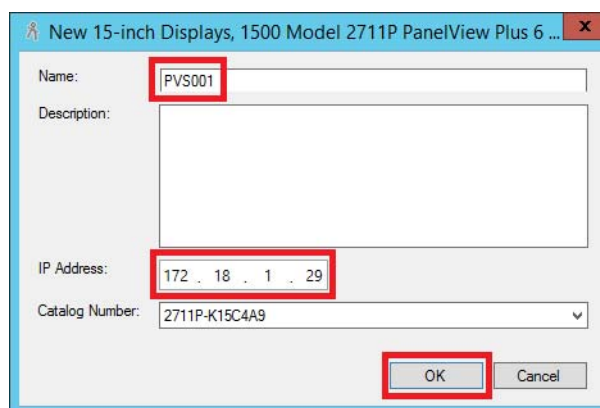
2. In the Studio 5000 splash page, select a recent project (PlantPAx in the example).

3. Drag the desired PanelView object (2711P-K15C4A9 in the example) from the Library Management panel and drop it in the Process Area panel.



The new graphic dialog box for the PanelView object you selected (1500 PanelView Plus 6 in the example) appears.

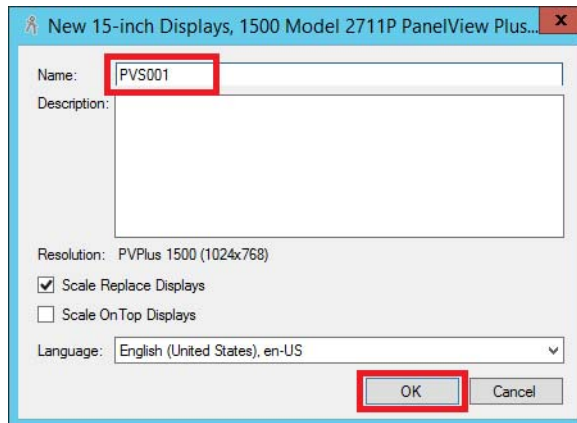
4. Type the name of the PanelView graphic (PVS001 in the example).



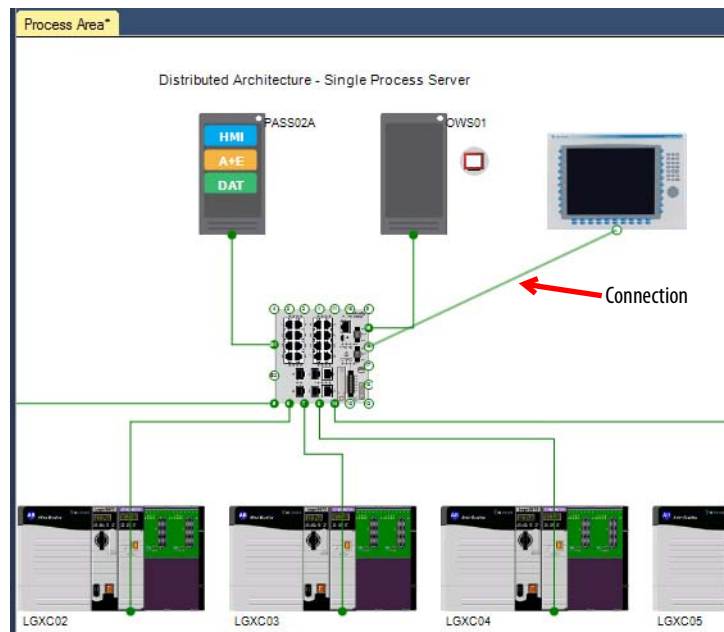
5. Type the IP address of the PanelView object and click OK.

The new project dialog box for the PanelView object appears.

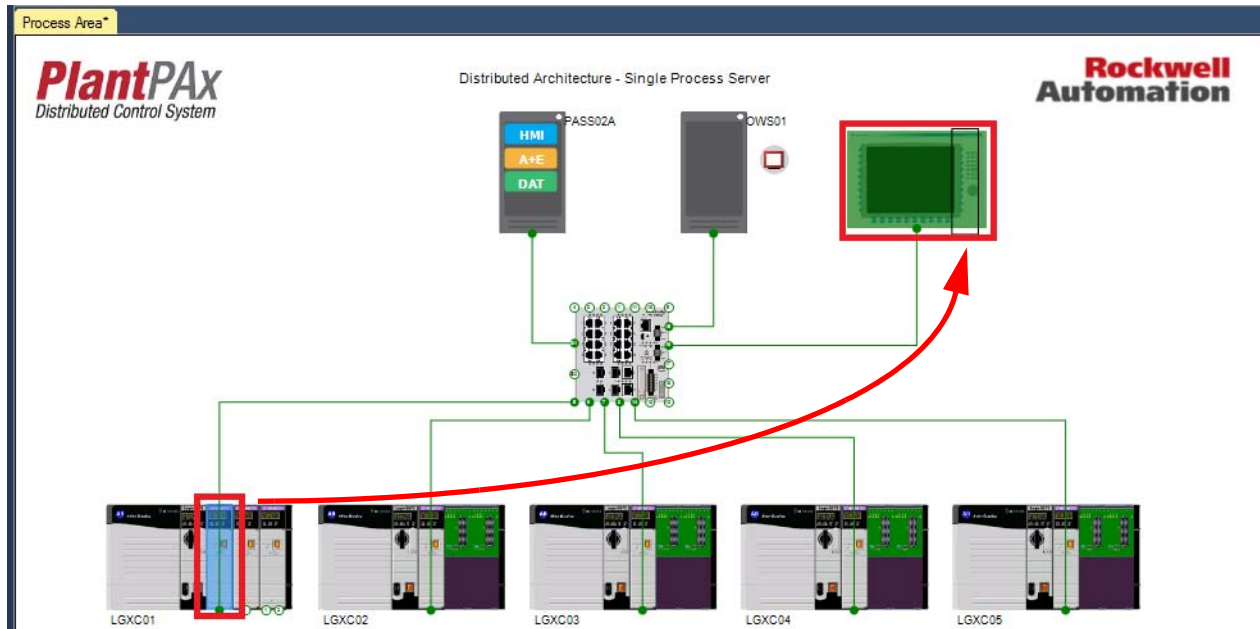
6. Type the name of the PanelView project (PVS001 in the example) and click OK.



7. Connect any port on the switch to the PanelView.

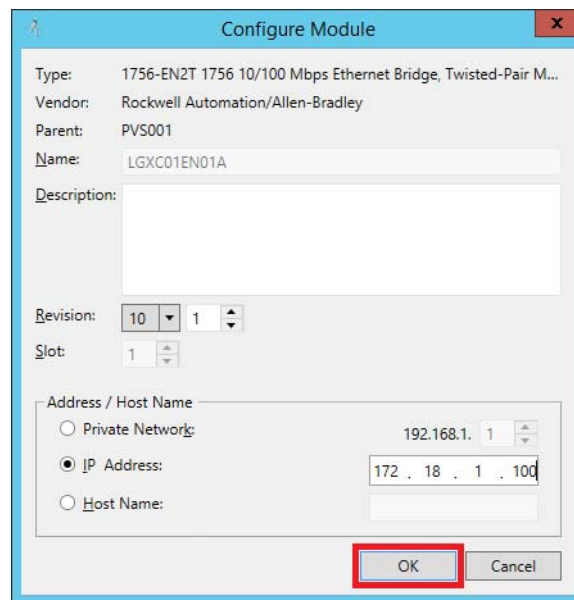


8. Drag the communications module from the chassis (LGXC01 in the example) and drop it on the PanelView.

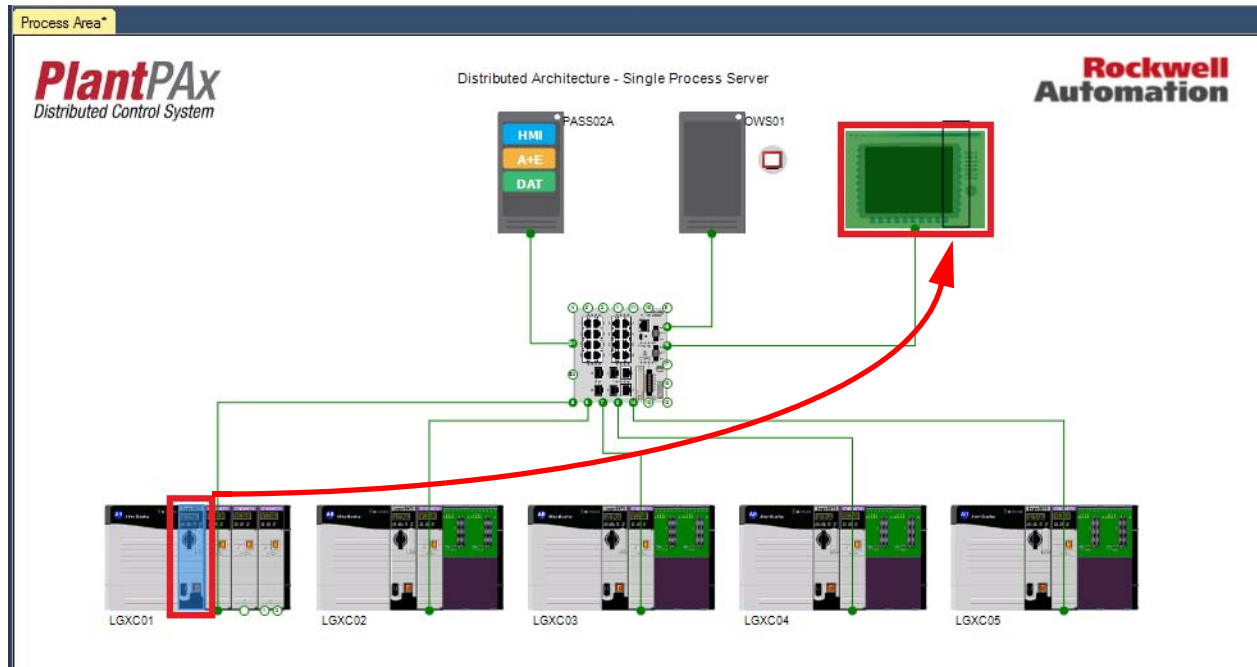


The Configure Module dialog box appears.

9. Click OK.

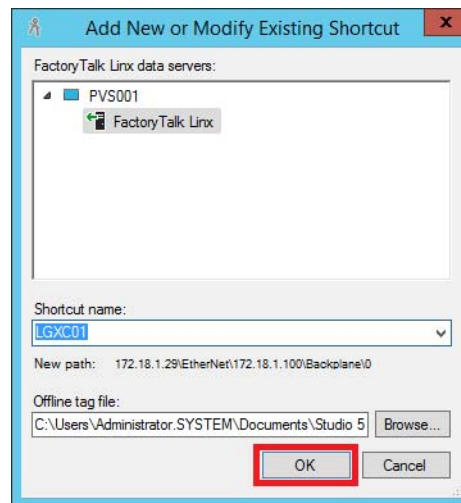


10. Drag the controller module from the chassis (LGXC01 in the example) and drop it on the PanelView module.

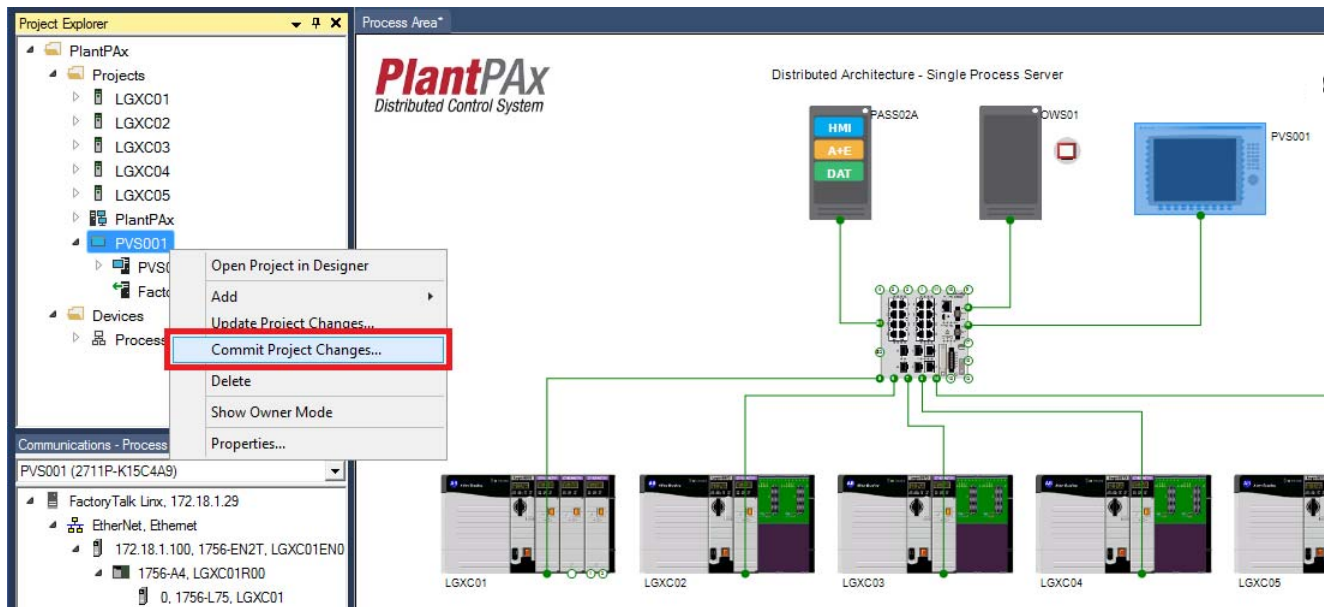


The Add New or Modify Existing Shortcut dialog box appears.

11. Click OK.

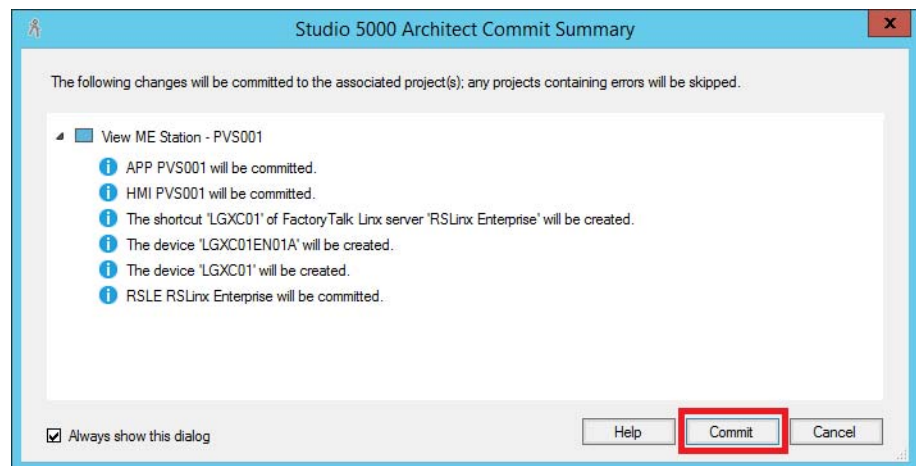


12. In the Project Explorer panel, right-click the project name (PVS001 in the example) and choose Commit Project Changes.

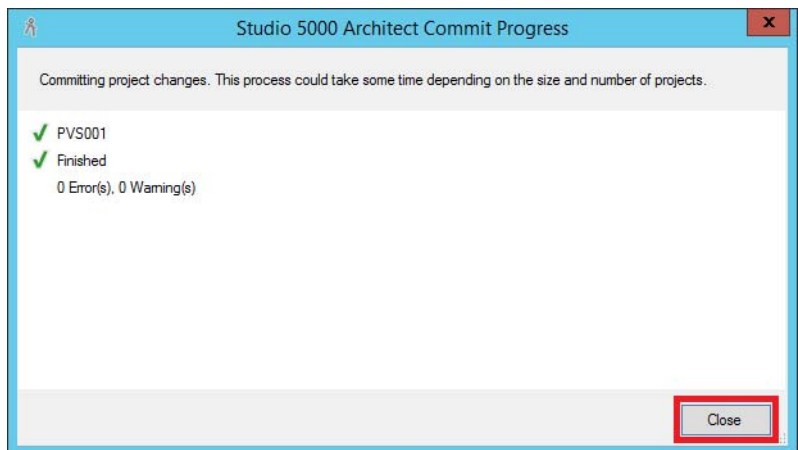


The Commit Summary dialog box appears.

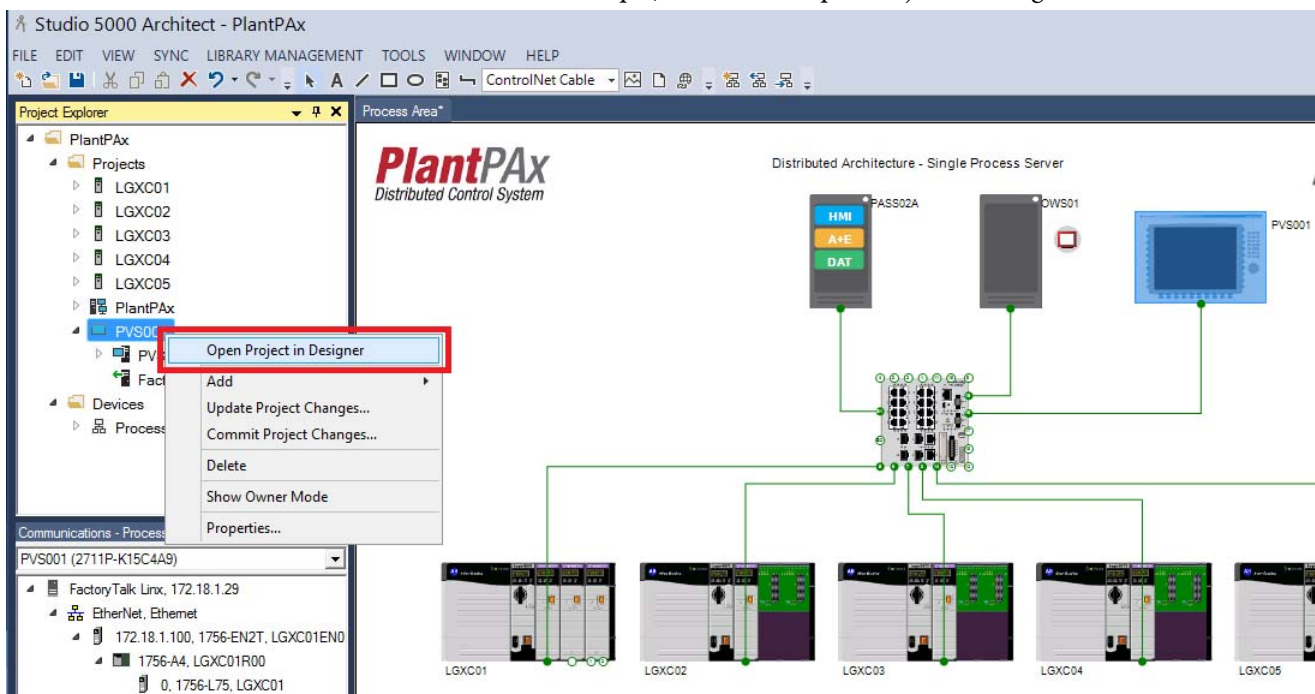
13. Click Commit.



14. Click Close to close the Committing Projects dialog box.



15. In the Project Explorer panel, right-click the project name (PVS001 in the example) and choose Open Project in Designer.




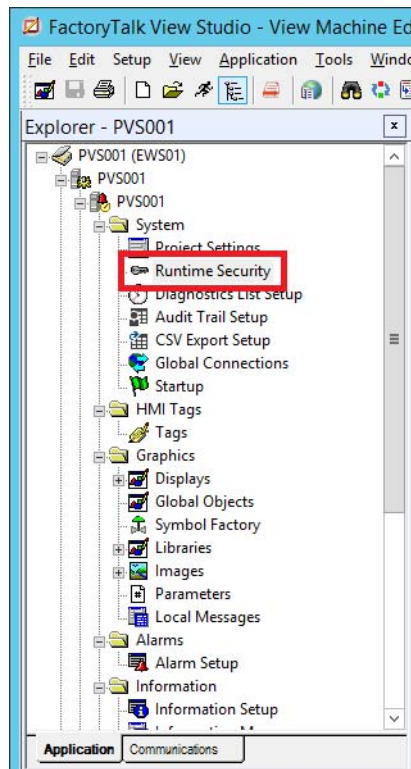
The FactoryTalk View Studio window appears.

TIP Do not close this window as it is used in later procedures.

Configure FactoryTalk View ME Security

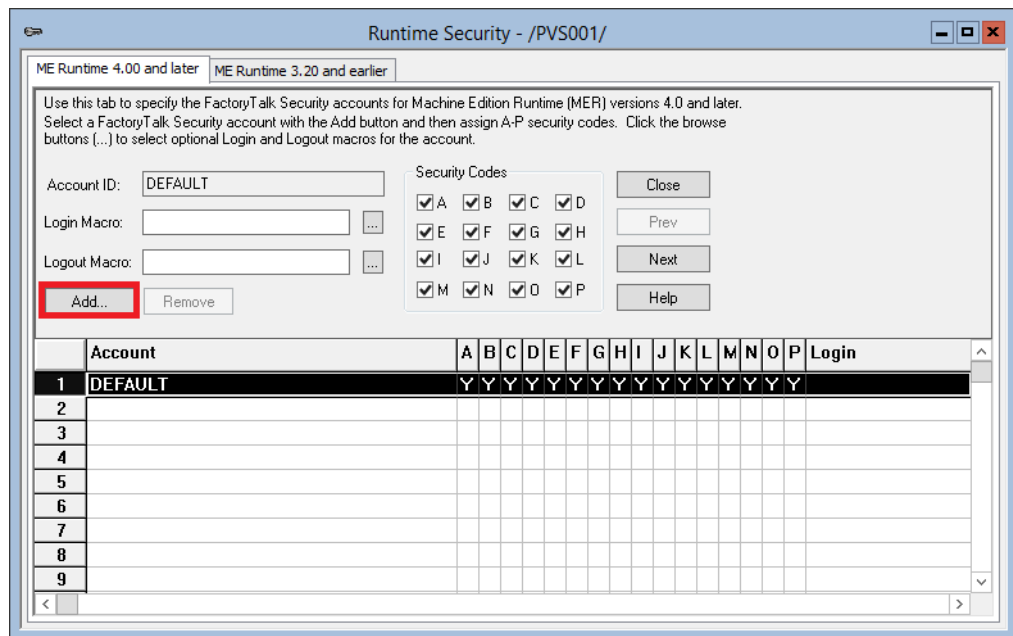
Runtime security must be set up to provide each account or user group with the correct FactoryTalk View security. Complete these steps.

1. If the FactoryTalk View Studio window is not already open, do the following:
 - a. Click the Programs  symbol and choose Rockwell Software>Studio 5000.
 - b. In the Studio 5000 splash page, select the PanelView project.
 - c. In the Project Explorer, right-click on the PanelView project and choose Open Project in Designer.
2. In the Explorer panel of the FactoryTalk View Studio window, double-click PVS001>PVS001>PVS001>System>Runtime Security.

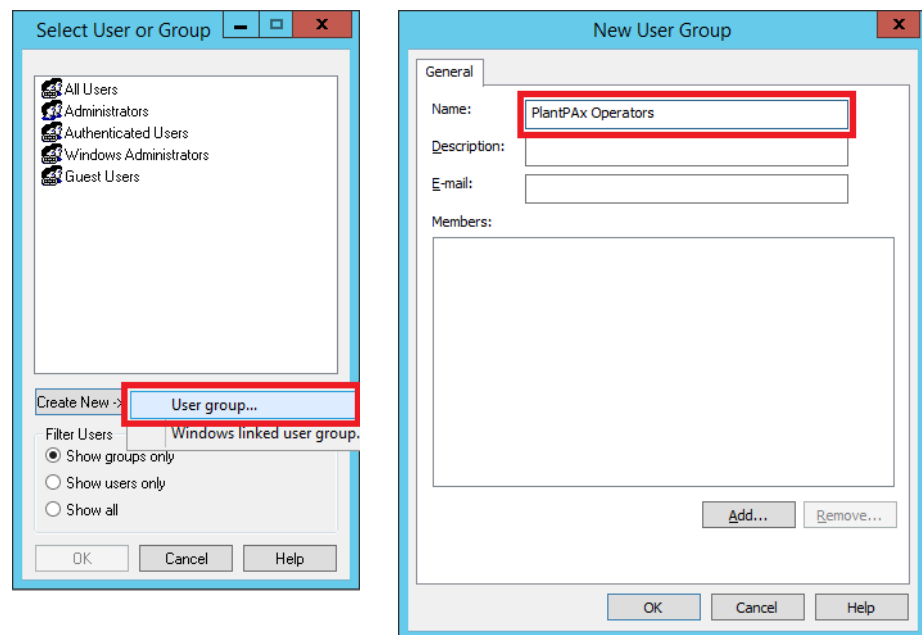


The Runtime Security window appears.

3. Click Add to insert local users groups.



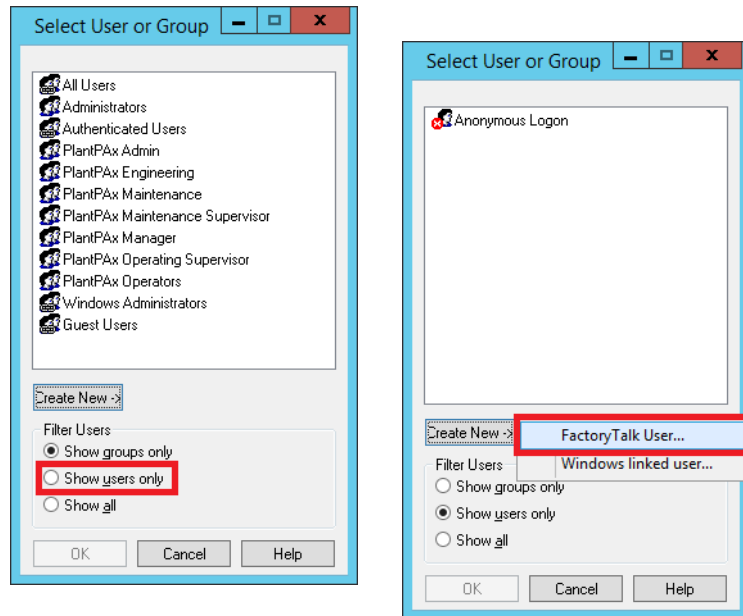
4. Choose Create New>User group in the Select User or Group window to create PlantPax user groups.



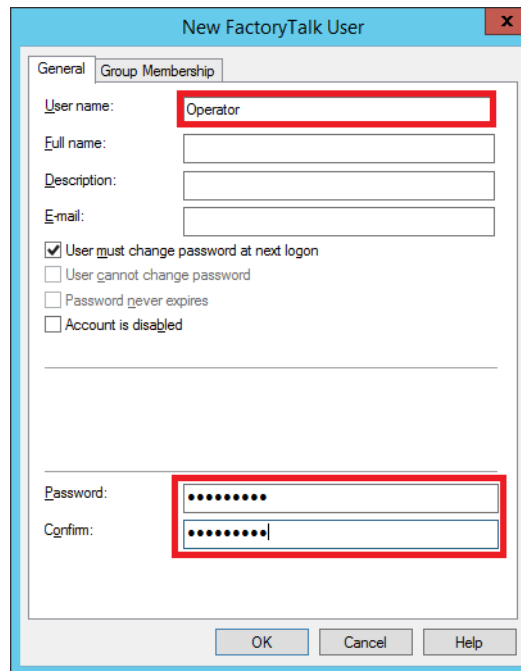
The New User Group dialog box appears.

5. Type the user group name and click OK.
6. Repeat step 4 and step 5 for all desired PlantPax user groups.

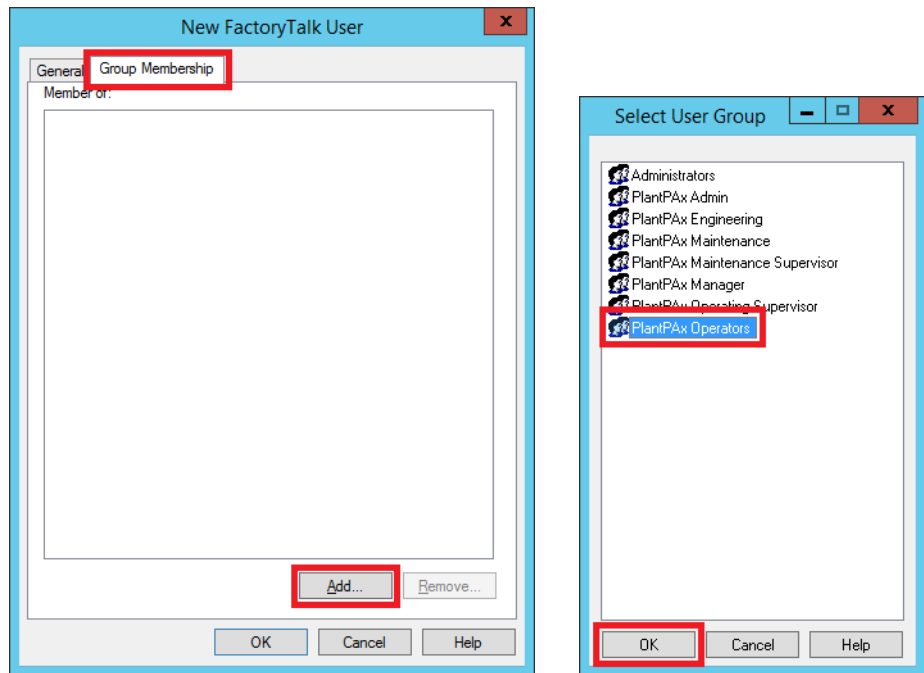
7. Click 'Show users only' and then click Create New>FactoryTalk User to create a user.



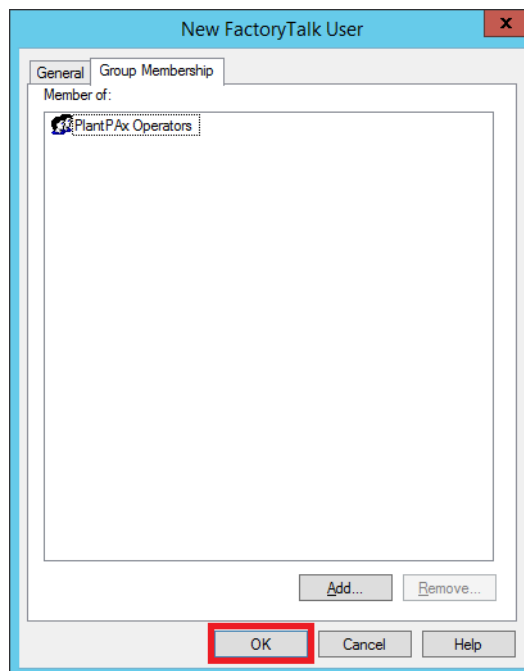
8. In the General tab of the New User dialog box, type the PanelView user name followed by a password.



9. In the Group Membership tab, click Add.
10. Select a PlantPAx group and click OK.



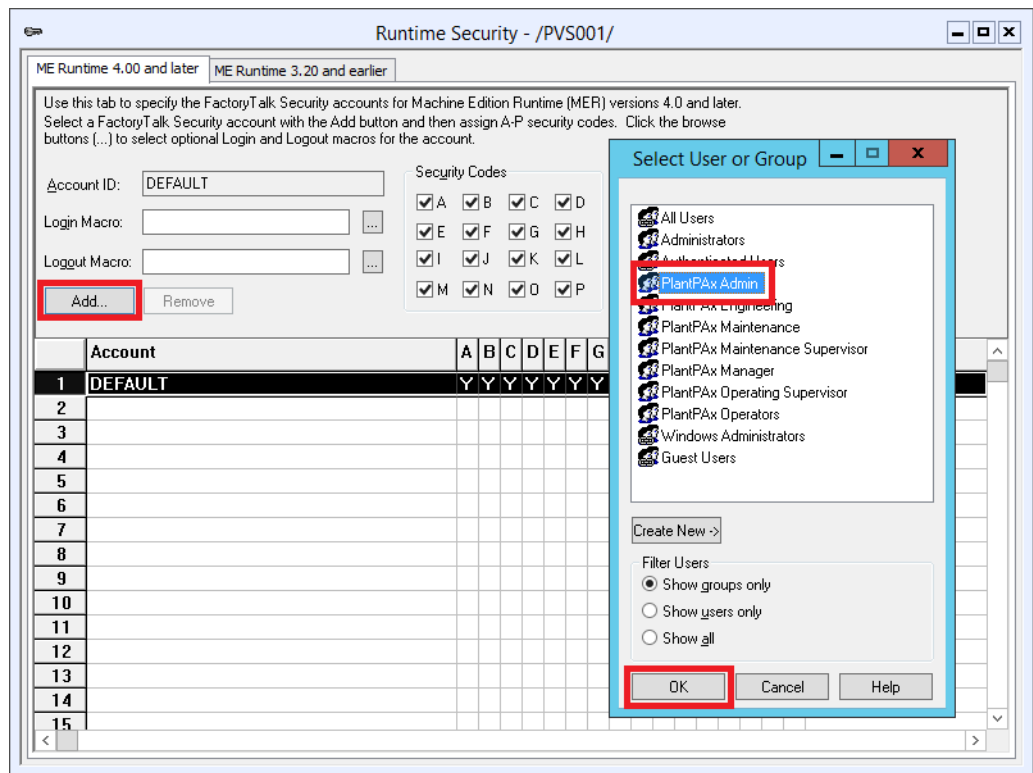
11. Click OK.



IMPORTANT Observe that the selected group is being added to the user; the user is not being added to the group.

12. Repeat step 8 through step 11 for all desired users.

13. Click Add to insert all PlantPAx user groups.



14. In the Select User or Group dialog window, select a User Group and click OK.

The group name appears in the Account list.

15. Repeat step 13 and step 14 for all desired groups.

We recommend that you remove the default security codes if you are using the Process Library objects. For more information, see the Rockwell Automation Library of Process Objects Reference Manual, publication [PROCES-RM002](#).

ME Runtime 4.00 and later ME Runtime 3.20 and earlier

Use this tab to specify the FactoryTalk Security accounts for Machine Edition Runtime (MER) versions 4.0 and later. Select a FactoryTalk Security account with the Add button and then assign A-P security codes. Click the browse buttons (...) to select optional Login and Logout macros for the account.

Account ID: DEFAULT

Login Macro: ...

Logout Macro: ...

Add... Remove

Security Codes

☐ A ☐ B ☐ C ☐ D ☒ E ☐ F ☐ G ☐ H ☐ I ☐ J ☐ K ☐ L ☐ M ☐ N ☐ O ☐ P

Close Accept Discard Help


Account	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Login
1 DEFAULT	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
2 [PLANTPAX ADMIN]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
3 [PLANTPAX ENGINEERING]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
4 [PLANTPAX MAINTENANCE SUPERVISOR]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
5 [PLANTPAX MAINTENANCE]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
6 [PLANTPAX MANAGER]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
7 [PLANTPAX OPERATING SUPERVISOR]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
8 [PLANTPAX OPERATORS]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

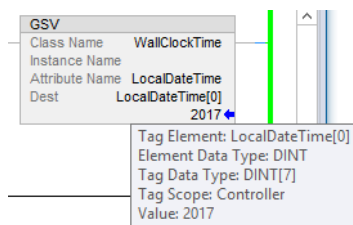
16. For each of the user groups, click a user group in the account section and type 'Y' (yes) or 'N' (no) for the respective security codes.
17. Click Close when all security codes are assigned to the groups.
18. When asked, confirm that you want to save Runtime Security.

Configure Time Synchronization for PanelView Terminals

PanelView terminals are used for applications that monitor, control, and display information graphically. The terminals provide operators a quick and efficient status of their application.


Complete the following steps for the controller project:

1. If the Studio 5000 Logix Designer® application is not already open, do the following:
 - a. Click the Programs  symbol and choose Rockwell Software>Studio 5000.
 - b. In the Studio 5000 splash page, select the controller project.
 - c. In the Project Explorer, right-click on the controller project and choose Open Project in Designer.
2. When not using the 1756 HP -TIME module, create a Get System Value (GSV) instruction to capture the controller clock, according to the example that follows.
 - Class Name – WallClockTime
 - Attribute Name – LocalDateTime
 - Dest – Create a DINT array [7] (LocalDateTime[0]...[6])

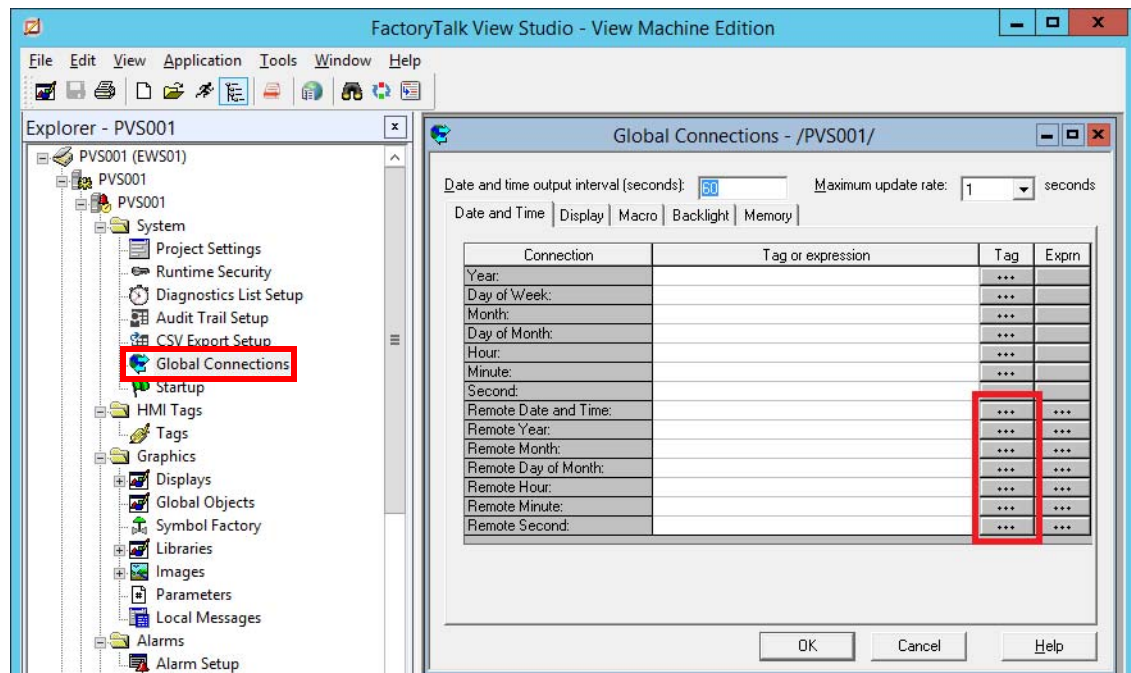


TIP We recommended that this GSV instruction be triggered every minute (60 seconds).

Complete the following steps for the PanelView project:

1. If FactoryTalk View Studio is not already open, do the following:
 - a. Click the Programs  symbol and choose Rockwell Software>Studio 5000.
 - b. In the Studio 5000 splash page, select the PanelView project.
 - c. In the Project Explorer, right-click on the PanelView project and choose Open Project in Designer.

2. In the FactoryTalk View Studio window, double-click PVS001>PVS001>PVS001>System>Global Connections.



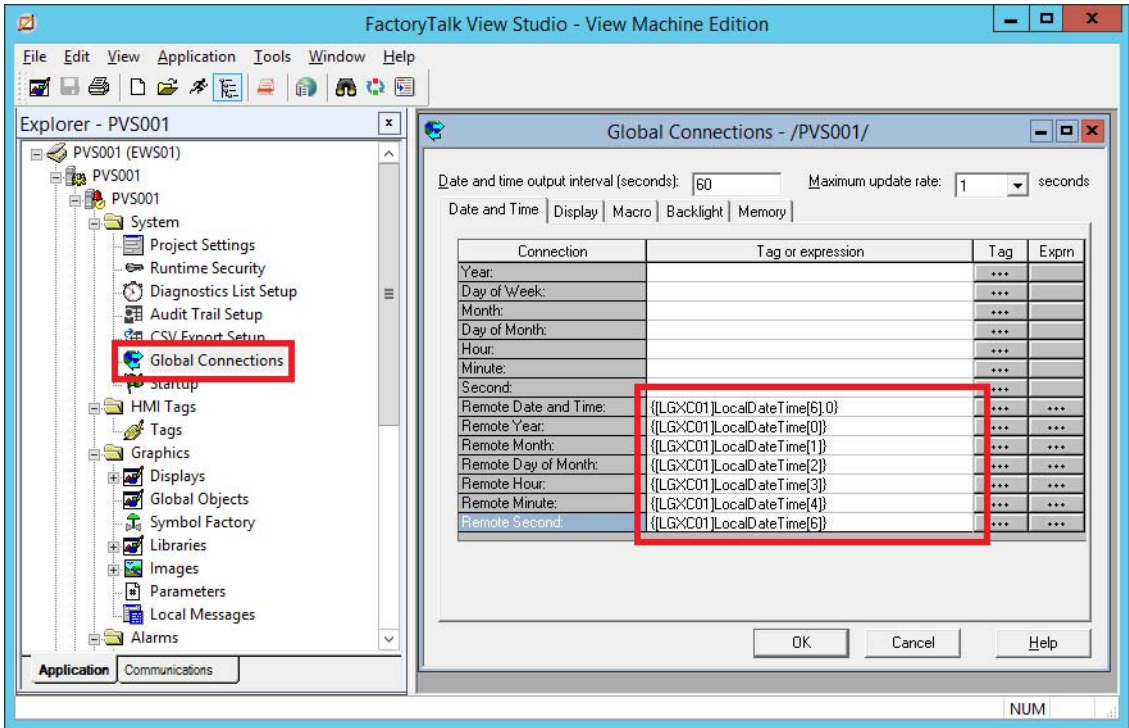
The Global Connections panel appears at the right side of the window.

The following steps create Remote Time references.

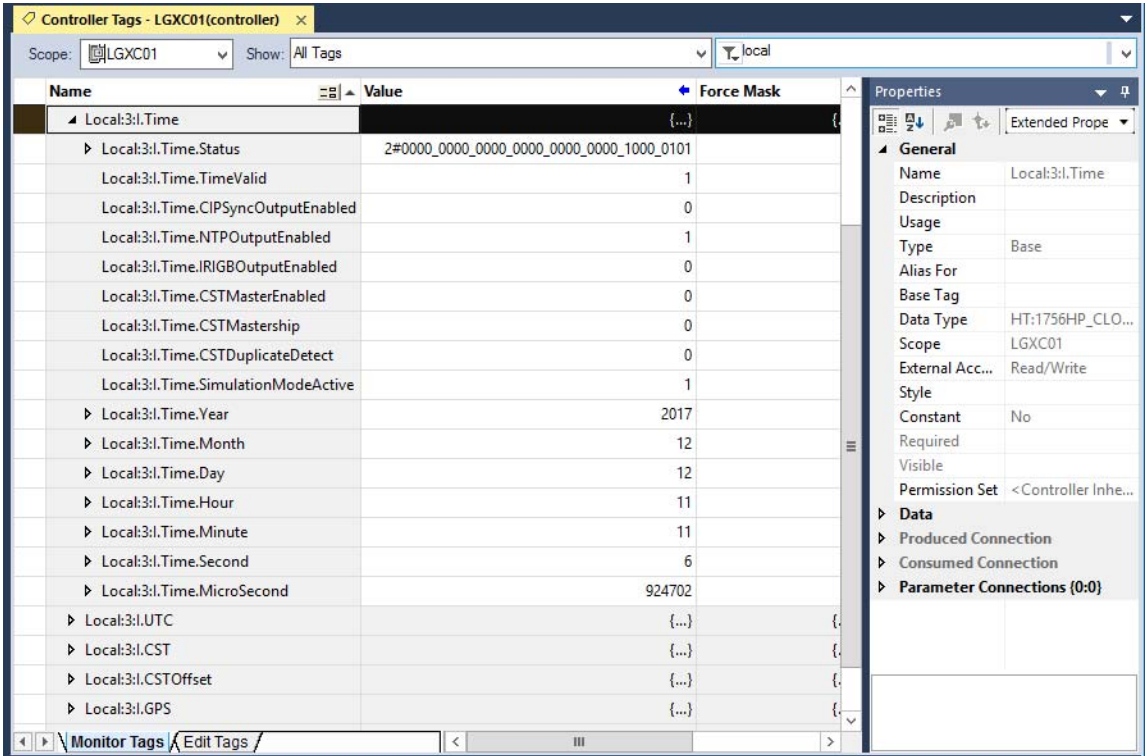
3. For the first remote connection, click the Browse button (ellipsis '...').
4. Find the proper tag and click Open.

The tag appears in the Tag expression column.

5. Repeat step [step 3](#) and [step 4](#) for the rest of the remote connections.




When using the 1756 HP -TIME module, information is available.

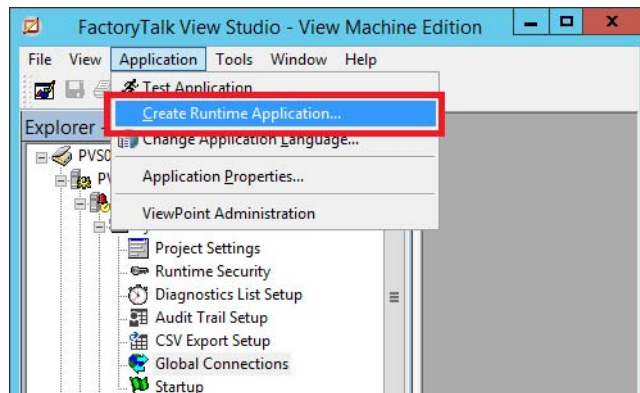


Download the Application

This procedure downloads the runtime application file from the workstation to the PanelView.

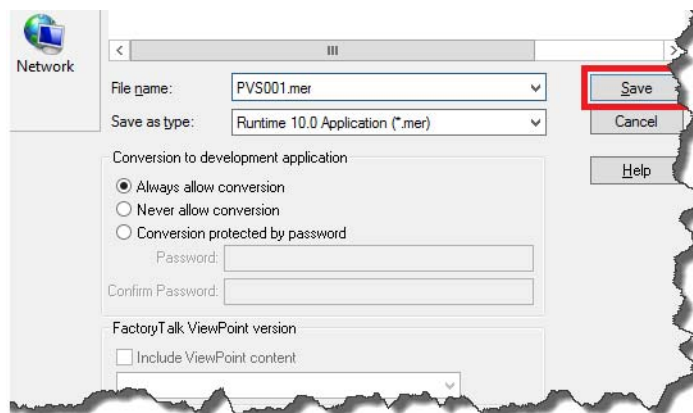
Complete the following steps:


1. If the FactoryTalk View Studio window is not already open, do the following:
 - a. Click the Programs  symbol and choose Rockwell Software>Studio 5000.
 - b. In the Studio 5000 splash page, select the PanelView project.
 - c. In the Project Explorer, right-click on the PanelView project and choose Open Project in Designer.
2. From the Application menu, choose Create Runtime Application.

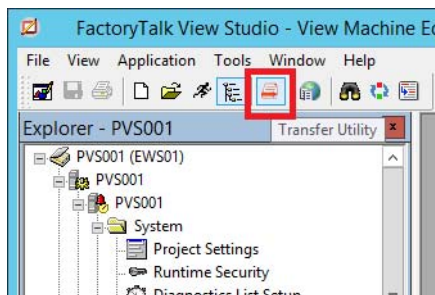


The Create Runtime Application dialog box appears.

3. Click Save to accept the default file name.

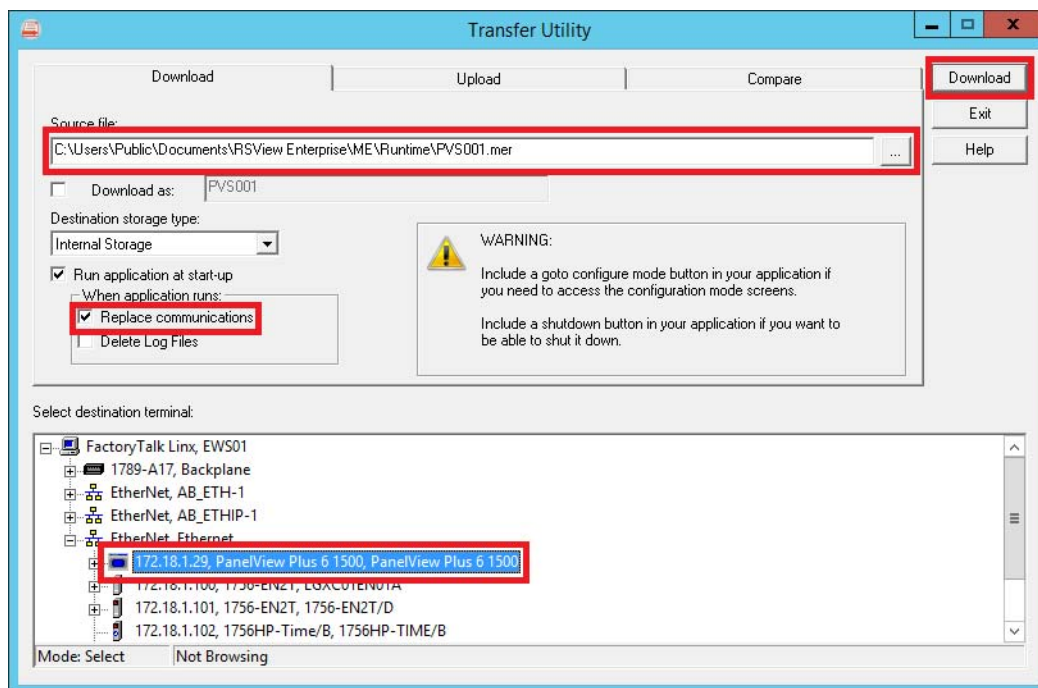


4. In the FactoryTalk View Studio ME window, click the Transfer Utility  icon.

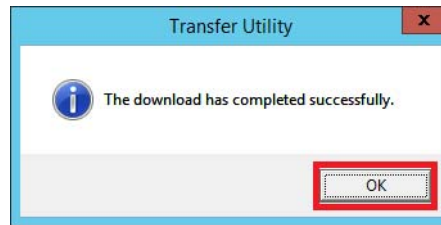


The Transfer Utility window appears.

5. Verify the Source file default path and select the destination PanelView terminal.
6. The first time that you download this file, click Replace Communications.
7. Click Download.



8. When the download completes, a dialog box notifies you that the download is successful.



9. Click OK.

Notes:

Configure an Application Server Information Server (AppServ-Info)

IMPORTANT Before starting this chapter, make sure that the FactoryTalk® Historian template has been deployed and initialized. If you are not using the Historian template, refer to Knowledgebase Answer ID 491889 - Migrating and/or Upgrading to FactoryTalk Historian Site Edition at <https://www.rockwellautomation.custhelp.com>.

This chapter describes procedures for configuring the Information Management application server (AppServ-Info) with the FactoryTalk View Historian Site Edition (SE) software and the FactoryTalk® VantagePoint® server.

The Historian SE tool lets you collect, manage, and analyze real-time data from the PlantPAx® system.

IMPORTANT We do not recommend installing data management (Historian) and decision reporting (VantagePoint) software on the same AppServ-Info server for small-scale applications. Use separate servers to maximize performance.

The VantagePoint software tool helps make informed business decisions with the plant floor data used as a gauge of the manufacturing process. You can use the VantagePoint software with mobile devices, tablets, and phones to generate reports via importing historical data tags.

Considerations

Consider the following suggestions before starting this chapter:

FactoryTalk Historian

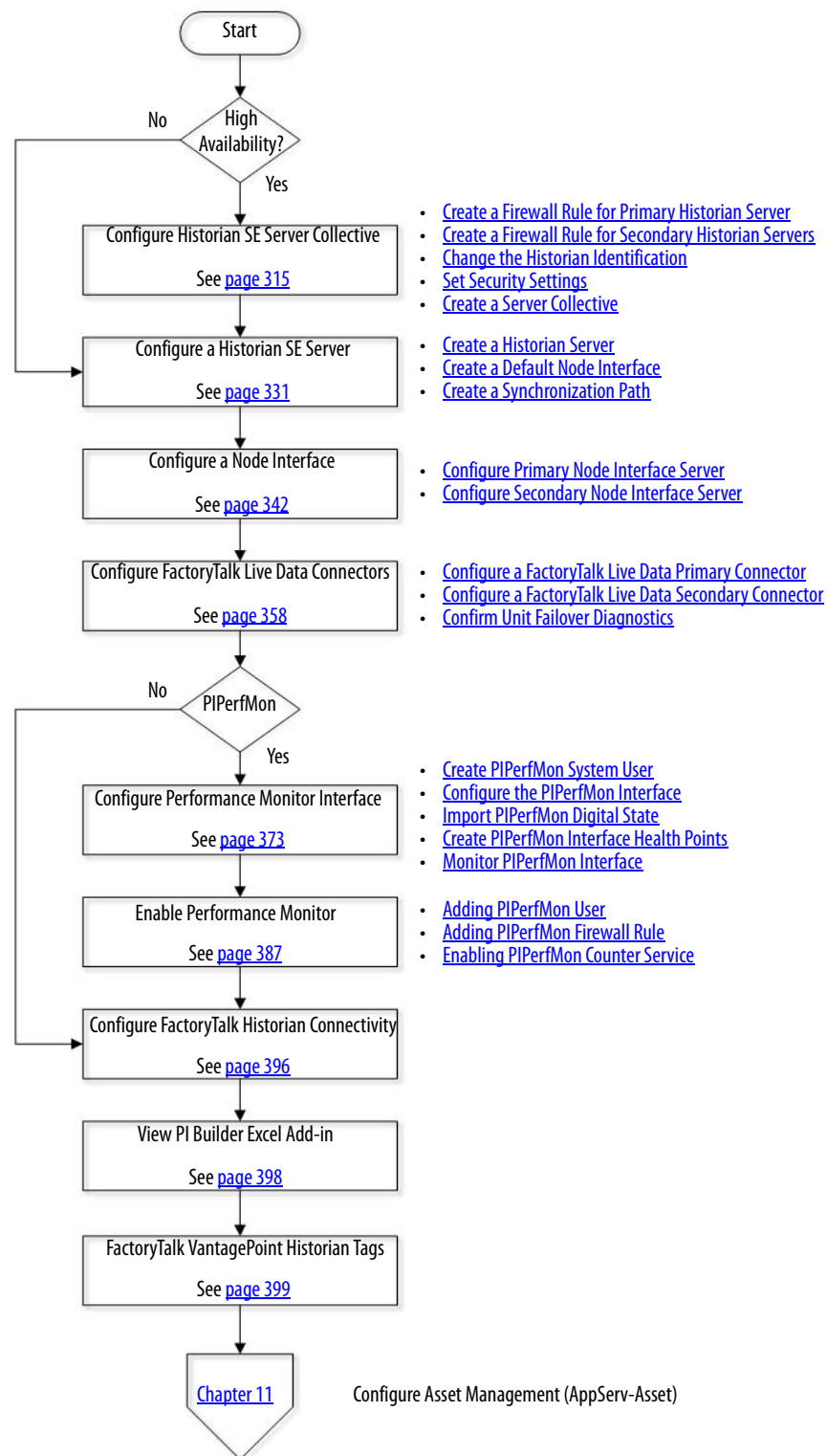
- When you plan your FactoryTalk Live Data location, be sure to enable buffering and high availability with failover capability.
- Consider a collective if you want high availability with redundant Historian servers.

FactoryTalk VantagePoint

Although the procedures in this chapter only expose historical data, you must decide the type of report variables that are required to generate your manufacturing intelligence.

[Figure 17](#) shows the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 17 - AppServ-Info (Historian) Workflow



Configure Historian SE Server Collective

Use the Historian servers with these procedures.



ASIH01A ASIH01B

IMPORTANT A server collective is required for high availability. If you are not using a collective, skip to [Configure a Historian SE Server on page 331](#).

A server collective consists of two FactoryTalk Historian SE servers (primary and secondary) that have the same configuration database. The collective provides the same association between the key values in the FactoryTalk Historian SE tables on all servers. The collective also helps confirm that the archive data files have the same structure on all servers.


Keep the following in mind regarding server collectives:

- When creating a server collective, you must always use fully qualified host names, not IP addresses. Therefore, the name resolution functionality must work on the network.
- If you make one or more FactoryTalk Historian SE servers members of a collective, you must restart them after the server collective is created. Otherwise, FactoryTalk Administration Console does not recognize any of the third-party tag licenses you have on your servers.
- To create a server collective on computers that have the Windows Firewall turned on, you must manually open the TCP 445 port between the two computers. See the Microsoft documentation for more information.
- The Windows user that configures server collectives must be a domain user and must be mapped to the piadmin user.
- The same 'Windows user to piadmin user mapping' must be performed on both the primary and secondary server in the collective.
- Activate your server collective in the FactoryTalk Administration Console.

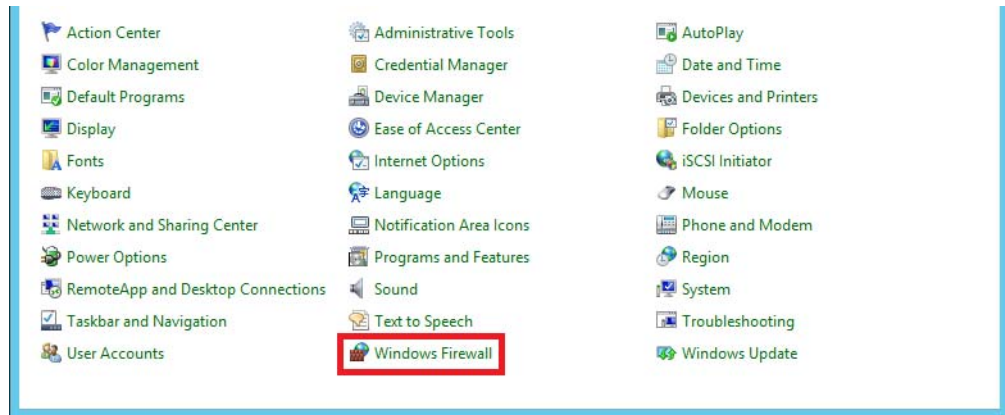
Create a Firewall Rule for Primary Historian Server

This section describes how to create an inbound rule for your Windows firewall on the primary Historian server (ASIH01A). Be sure to add the 445 rule for FactoryTalk SE even if you see existing rules that allow port 445.

Complete the following steps.

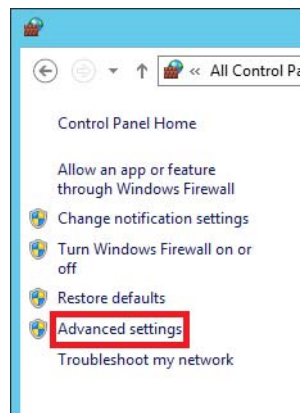
1. In the bottom left corner of the Windows Desktop, click the Windows  icon.

2. Click Control Panel and choose Windows Firewall.



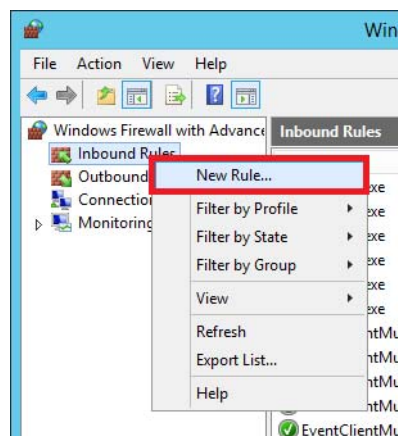
The Windows Firewall Window appears.

3. Click Advanced Settings.



The Windows Firewall with Advanced Security window appears.

4. Right-click Inbound Rules and choose New Rule.



The New Inbound Rule Wizard - Rule Type window appears.

5. Click Port and then click Next.

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back **Next >** Cancel

6. Click Specific local ports, type '445' in the text box, and then click Next.

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

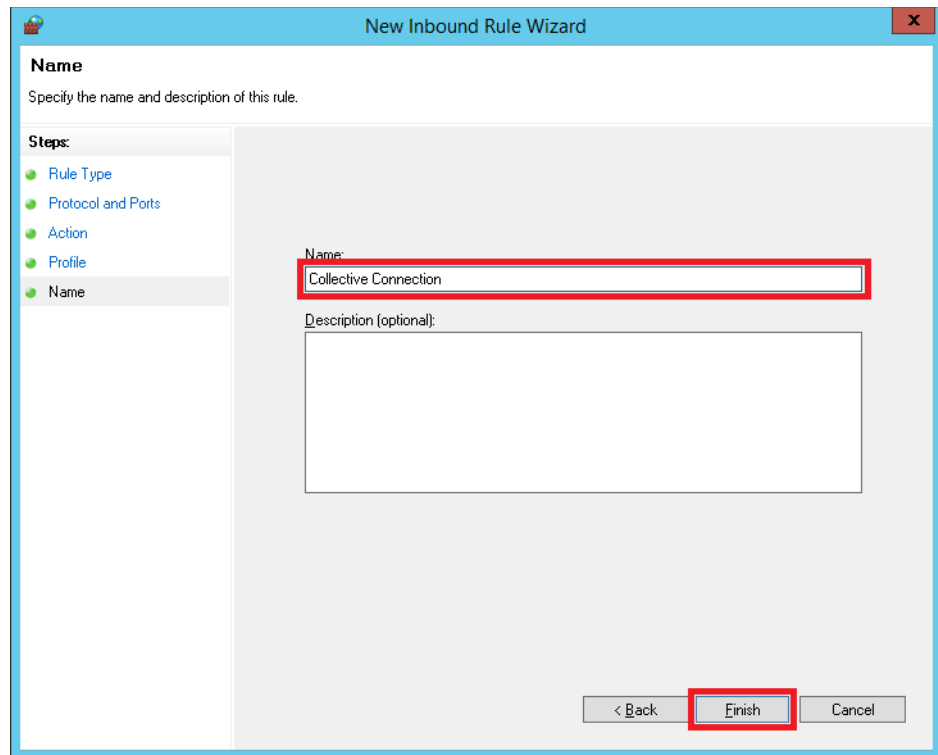
☒ **Specific local ports:**
Example: 80, 443, 5000-5010

< Back **Next >** Cancel

7. Click Next on each of the successive dialog boxes to do the following:
 - Allow the connection
 - Apply the rule to the Domain, Private, and Public

The New Inbound Rule Wizard - Name appears.

8. Type a name for this rule (Collective Connection in the example) and click Finish.



Your inbound rule for your firewall is created.

Create a Firewall Rule for Secondary Historian Servers

To create an inbound rule for your Windows firewall on secondary Historian servers, repeat [step 1](#) through [step 8](#).

Change the Historian Identification

Use a Historian server with these procedures.



ASI01A or ASI01B

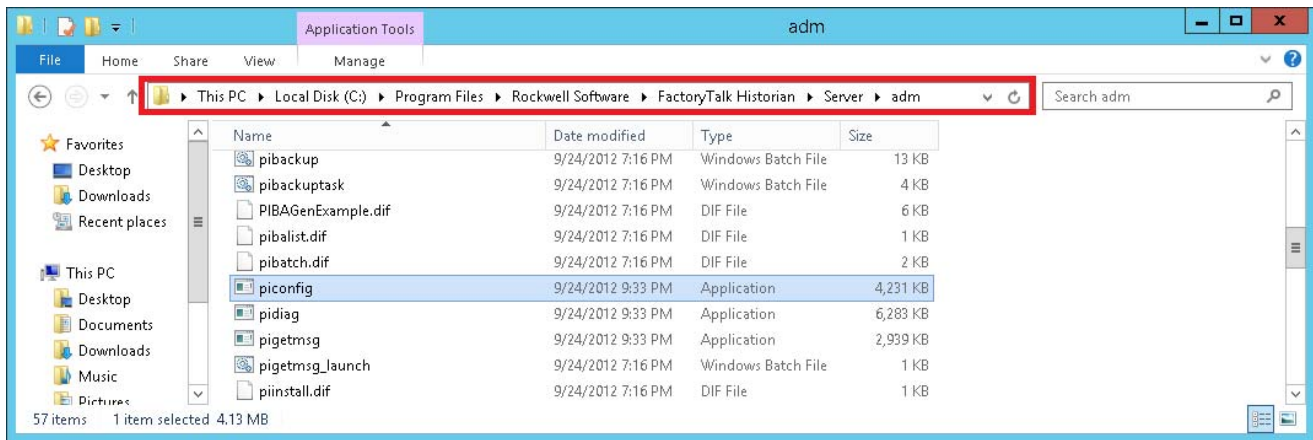
IMPORTANT Perform this section only if you are running VMware Template or if you have cloned a FactoryTalk Historian server.

Otherwise, continue to [Set Security Settings on page 321](#)

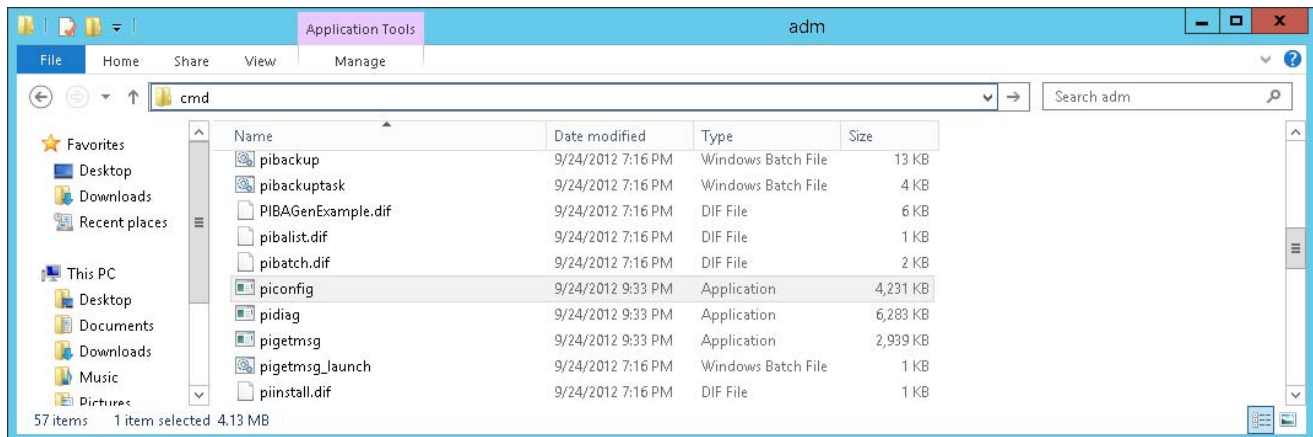
In this section, you create a ServerID for one of the FactoryTalk Historian servers.

Complete the following steps.

1. In Windows desktop, click File Explorer and navigate to `c:\Program Files\Rockwell Software\FactoryTalk Historian\Server\adm`.



2. Type 'cmd' and press Enter.



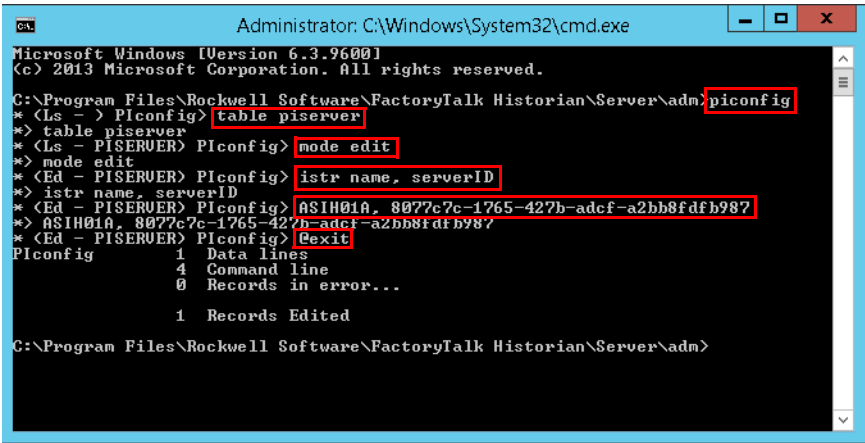
The Command window appears and is in the `c:\Program Files\Rockwell Software\FactoryTalk Historian\Server\adm` directory.

IMPORTANT Make sure that you press 'Enter' after typing each command in the following table.

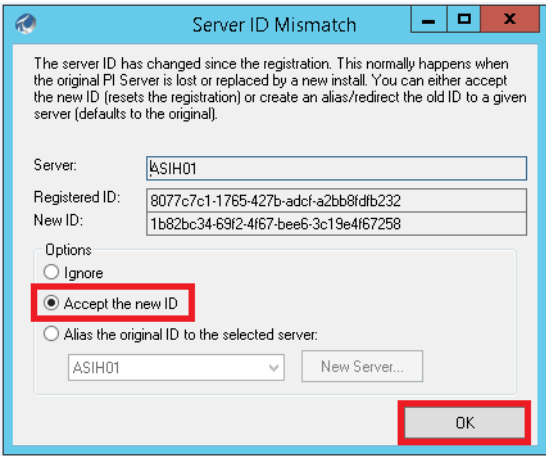
See [Figure 18 on page 320](#) for reference as you type the commands in the following table:

Command
piconfig
table piserver
mode edit
istr name, serverID
<hostname>, <new serverID>
@exit

Figure 18 - Command Window



If you have connected before, the next time you access this FactoryTalk Historian server, you see the following window.



- 3. Click 'Accept the new ID' and click OK.

Set Security Settings

Use the Historian servers with these procedures.



ASIHO1A



ASIHO1B

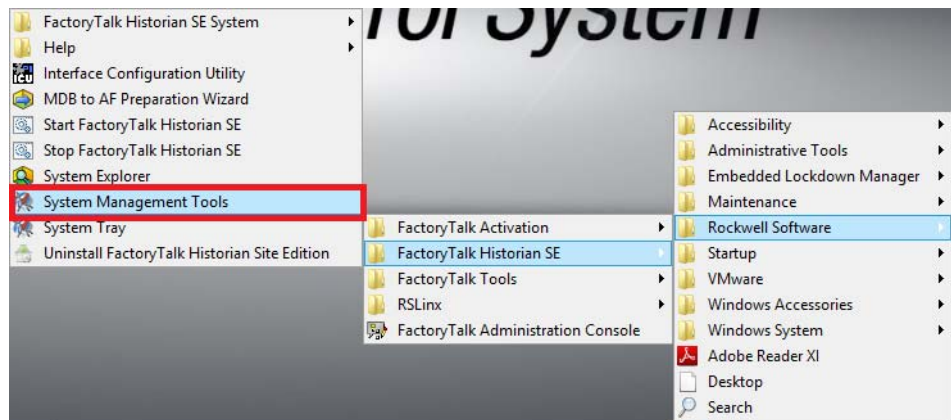
In this section, the security settings for the primary and secondary FactoryTalk Historian servers are set.

Security Settings for the Primary Historian Server

Set the security settings for the primary FactoryTalk Historian servers.

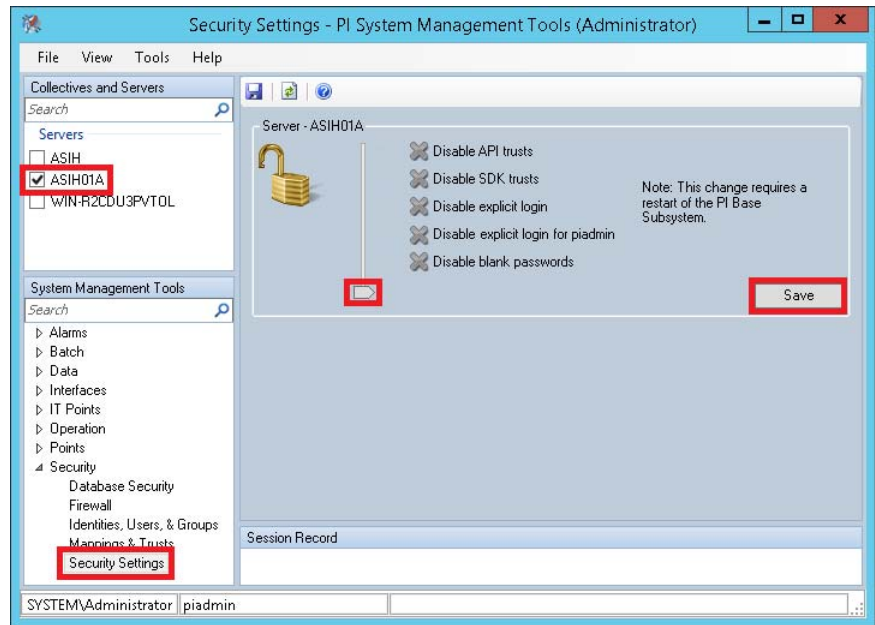
Complete the following steps.


1. Click the Programs  symbol and choose Rockwell Software®>FactoryTalk Historian SE>System Management Tools.

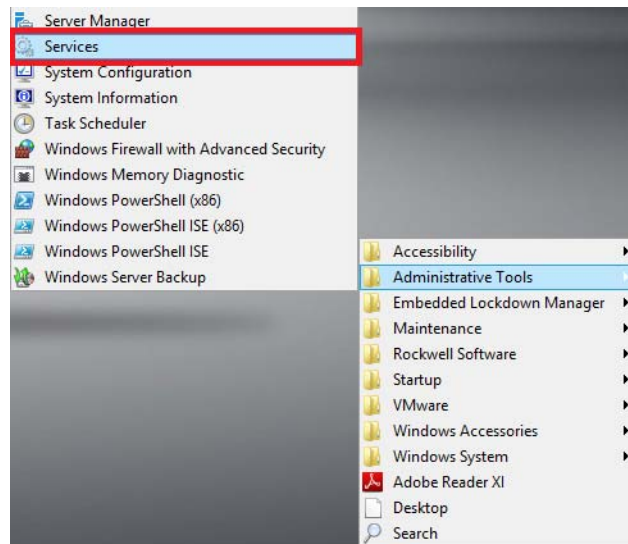


The 'Security Settings - PI System Management Tools (Administrator)' window appears.

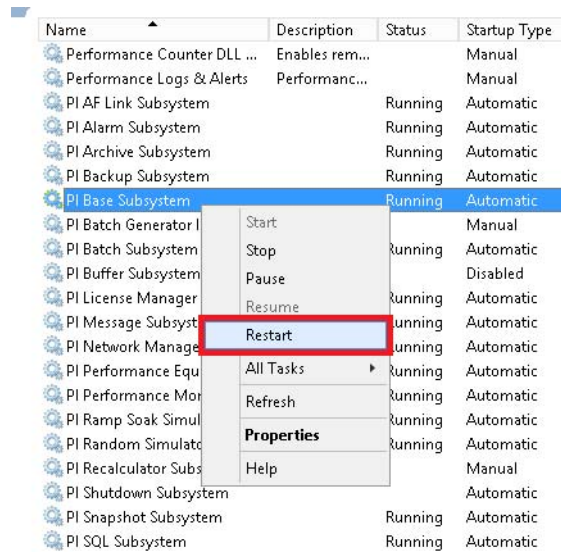
2. Under Collectives and Servers, check the server that you want to set the security settings for.



3. Under System Management Tools, choose Security>Security Settings.
The Security Settings slider appears on the right side of the window.
4. Set the slider to its lowest point and click Save.
5. In the Windows desktop, click the Programs  symbol and choose Administrative Tools>Services.



6. Right-click PI Base Subsystem and choose Restart.



The PI Base Subsystem service restarts. When the status is 'running', continue with the next step.

7. Close the Services and Administrative Tools windows.

Security Settings for the Secondary Historian Server

In this section, the security settings for the secondary FactoryTalk Historian server are set.

Repeat [step 1](#) through [step 7](#) for the secondary Historian server.

Connect Primary Historian Server to Secondary Historian Server

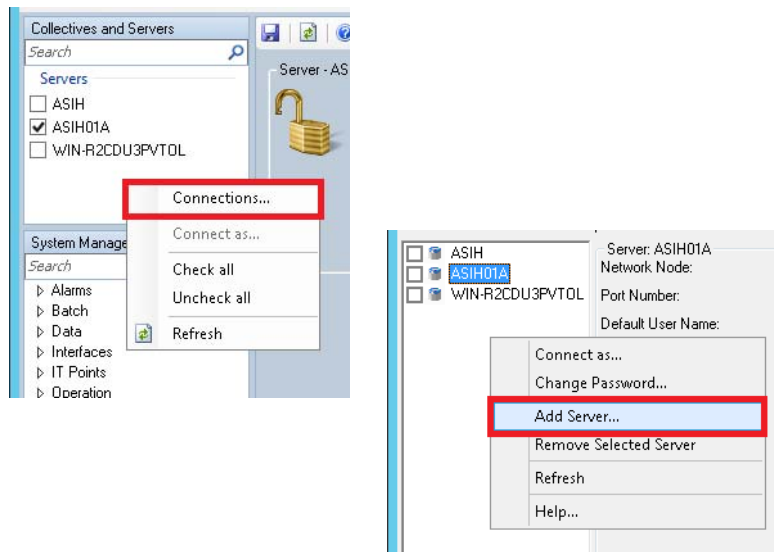
Use the Historian server with these procedures.



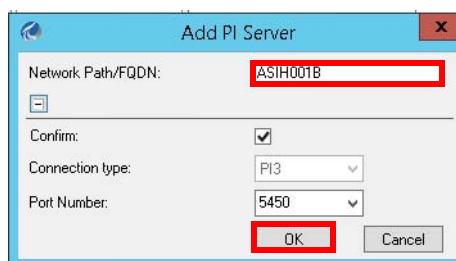
In this section, you make a connection from the primary Historian server (ASIH01A) to the secondary Historian server (ASIH01B).

Complete the following steps:

1. Open the PI SDK utility and click Connections.
2. Click in the white space and then click Add Server.

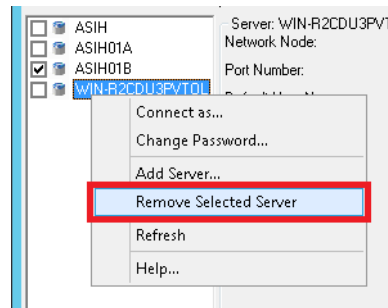


3. Type the server name (ASIH01B in the example) in the Network Node text box.



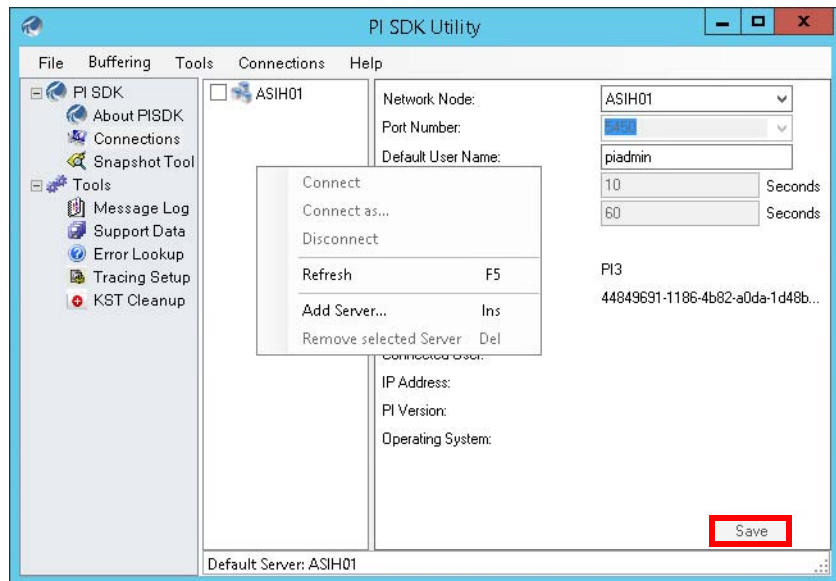
4. Accept the rest of the default entries and click OK.

5. In the PI Connection Manager window, right-click a server that is not necessary and choose Remove Selected Server.



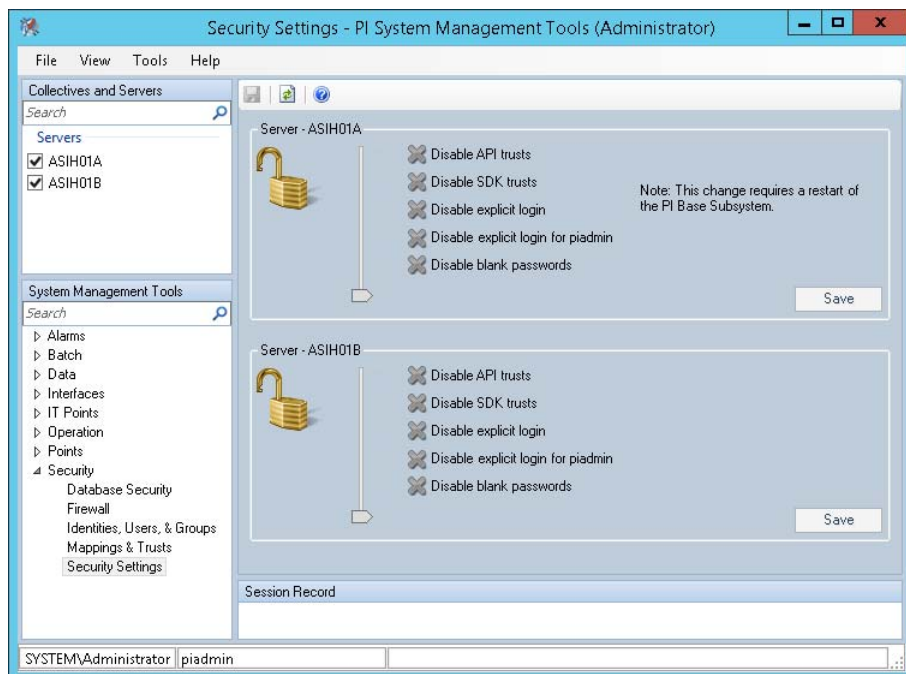
6. Repeat this step for servers only that you do not need.

Once you have deleted all unnecessary servers, the PI SDK Utility window looks similar to the following figure.



7. Click Save.

8. In the 'Security Settings - PI System Management Tools (Administrator)' window, make sure both FactoryTalk Historian servers (ASIH01A and ASIH01B in the example) are checked. The window appears similar to the following figure.



Connect Secondary Historian Server to Primary Historian Server

Use the Historian server with these procedures.



ASIH01B

To connect the secondary Historian server (ASIH01B) to the primary Historian server (ASIH01A), repeat [step 1](#) through [step 8](#) on the secondary server (ASIH01B).

IMPORTANT When you repeat step 3, type ASIH01A in the Network Node text box on the Add Server dialog box.

Create a Server Collective


Use the Historian servers with these procedures.

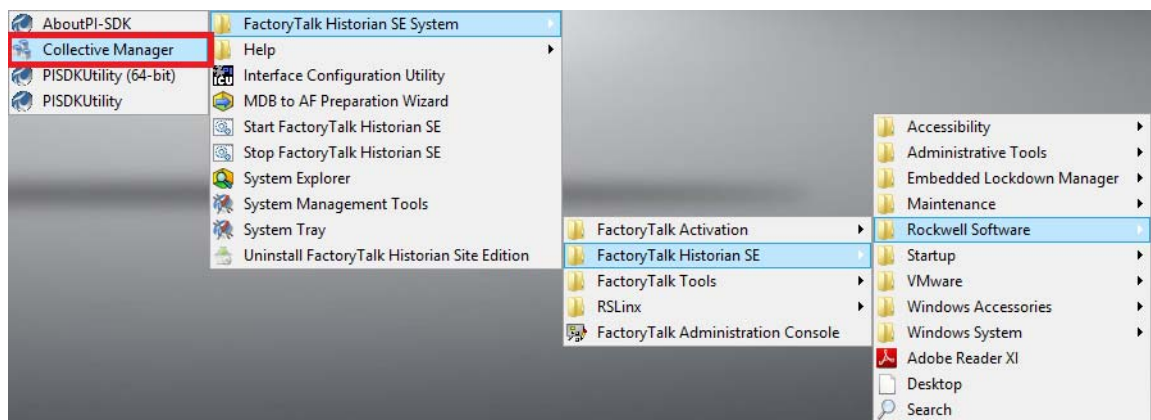


In this section you create a FactoryTalk Historian collective (ASIH01) that includes FactoryTalk Historian servers ASIH01A and ASIH01B.

Create Collective and Add Historian Servers

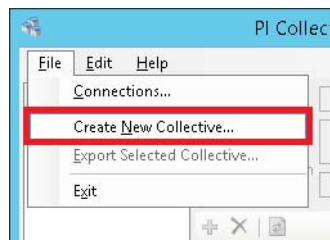
Complete the following steps.

1. In the Windows desktop, click the Programs  symbol and choose Rockwell Software®>FactoryTalk Historian SE>FactoryTalk Historian SE System>Collective Manager.



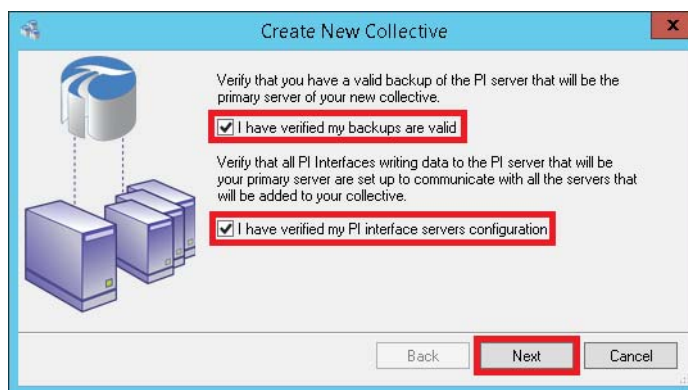
The PI Collective Manager (Administrator) window appears.

2. Click File and choose Create New Collective.



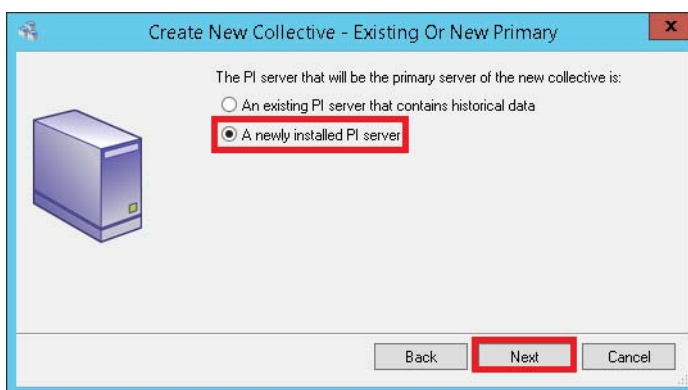
The Create New Collective dialog box appears.

3. Check both boxes and click Next.



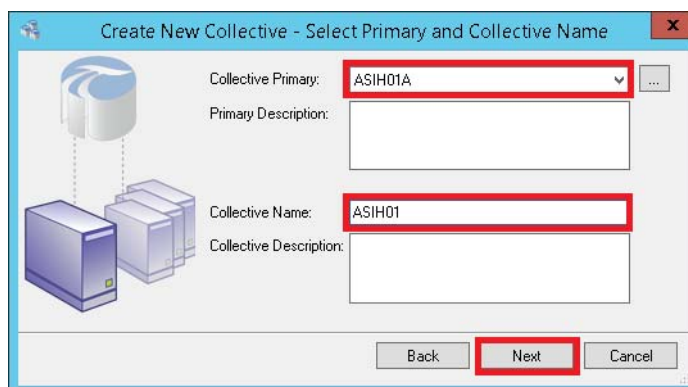
The Existing or New Primary dialog box appears.

4. Check 'A newly installed PI server' and click Next.



The Select Primary and Collective Name dialog box appears.

5. Select the primary FactoryTalk Historian server from the pull-down list.
If the server name does not appear in the pull-down list, click the ellipses [...] and select the server from the Connection Manager dialog box.

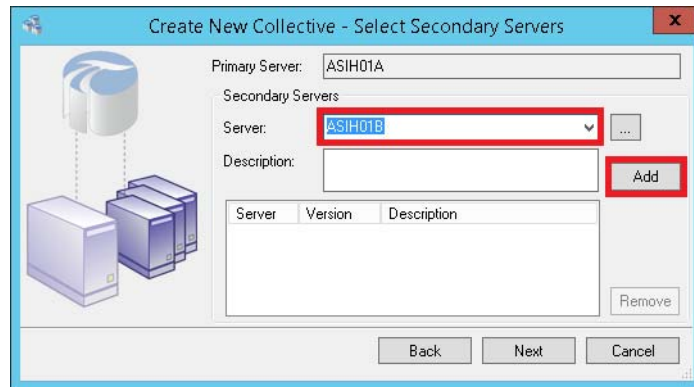


6. (Optional) Type a description for the collective primary.
7. Type a unique name for the new collective.
8. (Optional) Type a description for the collective and click Next.

The Select Secondary Servers dialog box appears.

9. Select the secondary FactoryTalk Historian server from the pull-down list.

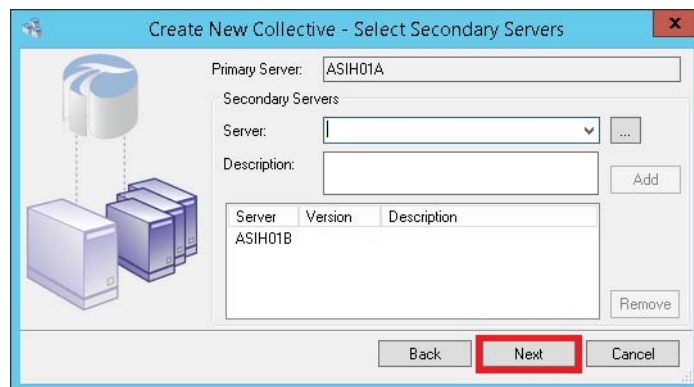
If the server name does not appear in the pull-down menu, click Browse (ellipses '...') and select the server from the Connection Manager dialog box.



10. (Optional) Type a description for the collective secondary.
11. Click Add.

The server is added to the server list.

12. (Optional) Add additional secondary servers by repeating step 9 through step 11 with another server.
13. When you are finished adding secondary servers, click Next.

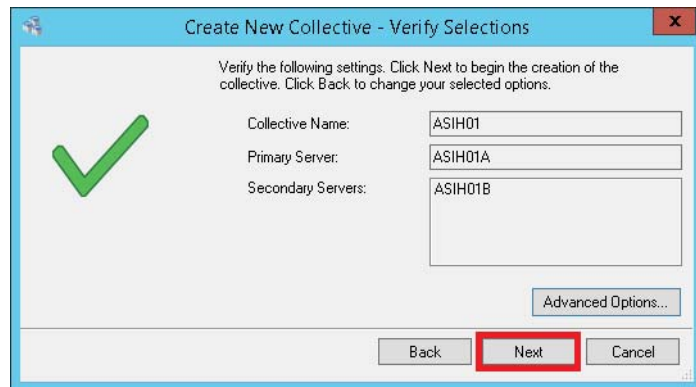


The Select Archives dialog box appears.

14. Click Next on each of the successive dialog boxes to do the following:
 - Accept the default number of archives to be copies
 - Accept the default location for the temporary backup

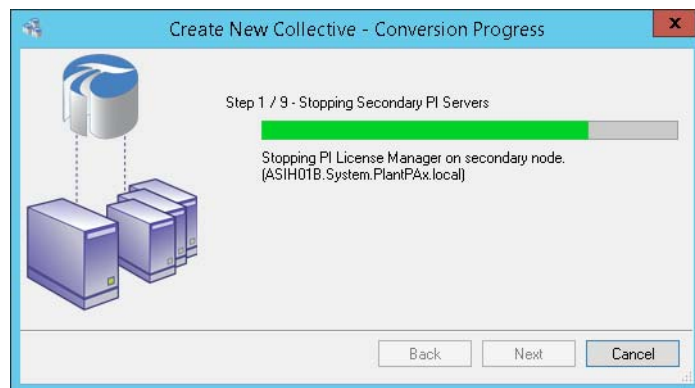
The Verify Selections dialog box appears.

15. Verify the information on this screen and click Next.

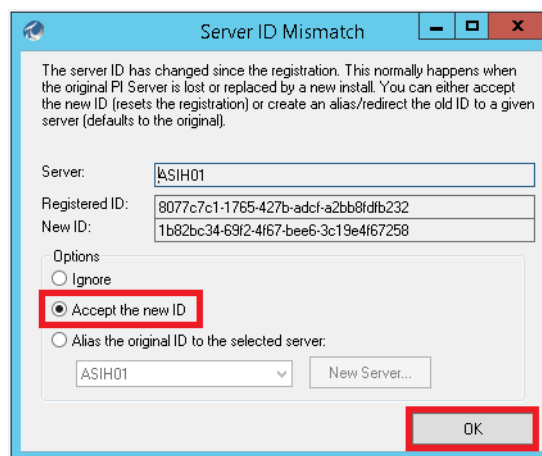


The Conversion Process dialog box appears.

The Conversion Process page displays the status and individual steps of the conversion process.



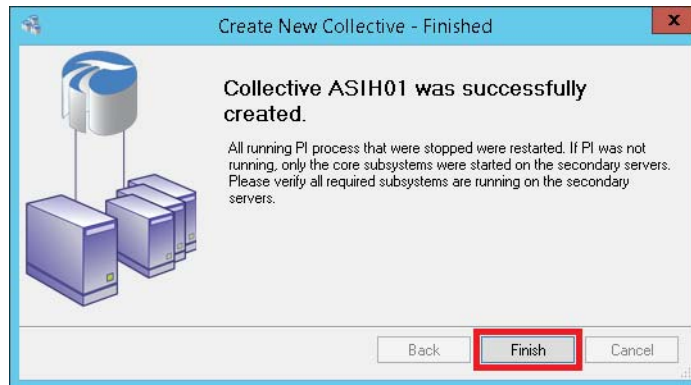
The Server ID Mismatch window appears when the process completes.



16. Click 'Accept the new ID' and click OK.

The Finished page appears.

- Click Finish to complete the Create New Collective process.



Configure a Historian SE Server

This section describes how to create a FactoryTalk Historian SE server.

Create a Historian Server

IMPORTANT To perform this procedure, make sure that you have completed [step 1](#) through [step 7](#) on pages [321](#)...[323](#).

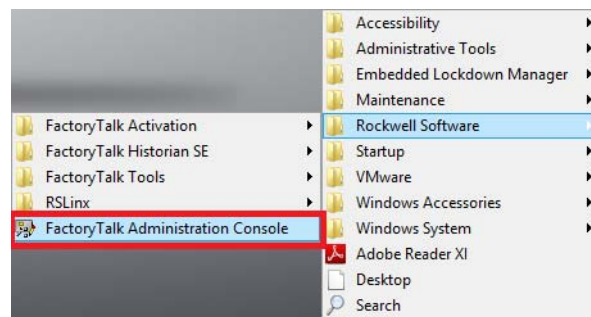
Use the Historian server with these procedures.



ASIH01 or ASIH01A (If working with a collective)

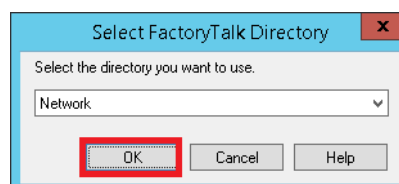
This section describes how to configure, test, and name a Historian server connection.

- Click Start and choose Rockwell Software®>FactoryTalk Administration Console.



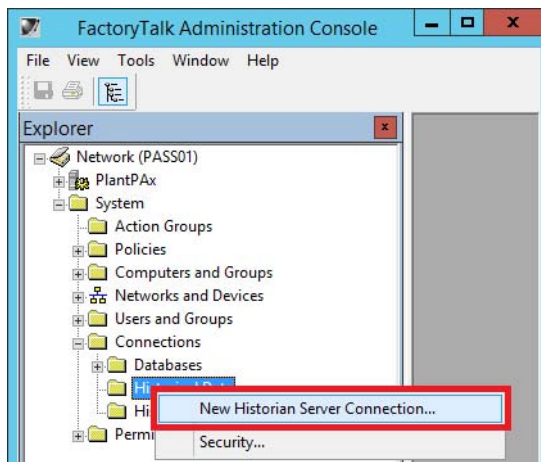
The Select FactoryTalk Directory dialog box appears.

- Click Network and then click OK.



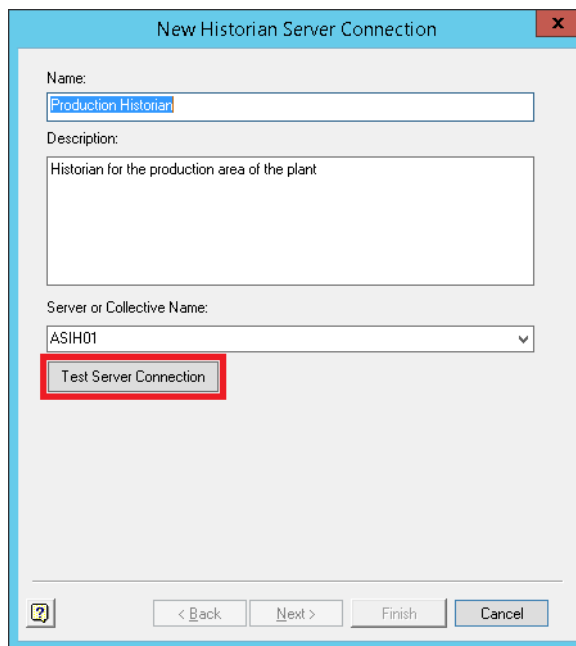
The FactoryTalk Administration Console dialog box appears.

3. In the FactoryTalk Administration Console, right-click Network>System>Connections>Historical Data and choose New Historian Server Connection.

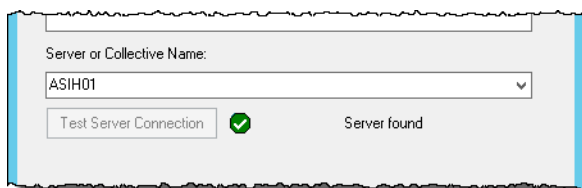


The 'New Historian Server Connection' dialog box appears.

4. From the pull-down menu, select the Server or Collective Name.
5. Click Test Server Connection.



If the connection is good, a green check mark appears along with the text 'Server Found!'.



If the connection is not good, a yellow triangle appears along with the text 'No server found'.



TIP If the connection to the server is not good:

- Make sure that the correct Historian server is called out
- Make sure that the Historian server is installed correctly

6. Click Finish.

IMPORTANT This step also creates an instance of the FactoryTalk Live Data (FTLD) interface on the host.

7. In the FactoryTalk Administration Console, right-click Network>System>Connections>Historical Data>'<Production Historian>' and choose Properties.

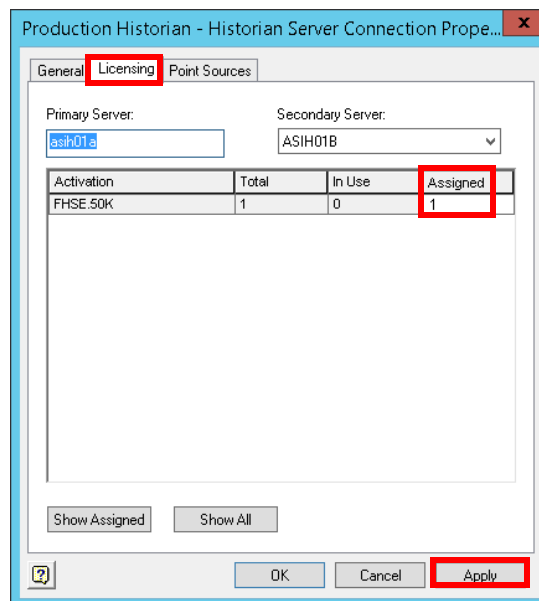
The Historian Server Connection Properties dialog box appears.

8. Click the Licensing tab.

The dialog box now shows both the Primary and Secondary servers.

IMPORTANT Depending on your licensing, the dialog box could appear differently. But, use the fhse.xxxK activation.
If using a collective, you must have two total and assigned licenses.

9. Type '1' in the Assigned column and click Apply.



The example shows '1' license stored locally in each collective server. If both activation licenses are on the activation server, you need to type '2'. This applies to a collective **only**.

10. Click Apply.

Create a Default Node Interface

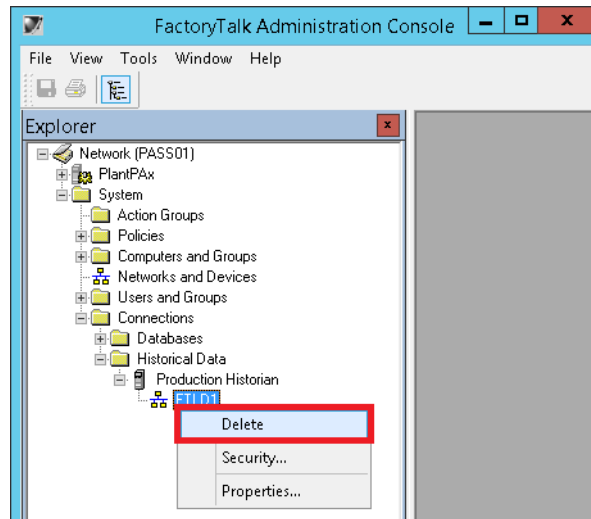
Use the Historian server with these procedures.



ASIH01 (no collective)
ASIH01A (with collective)

Node interface FTLD1 is automatically created when the Historian server is created. This interface must be deleted and two interfaces created on the proper servers.

1. In the FactoryTalk Administrative Console, right-click on FTLD1 and choose Delete.

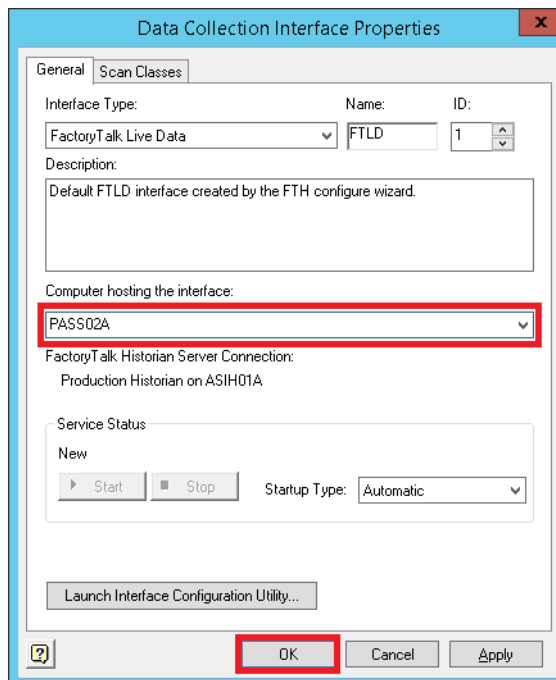


2. To confirm the deletion, click Yes on the popup window.
3. To create an interface to collect data, right-click the Historian server and choose New Data Collection Interface.

You are creating a connector to the correct Historian server.

The Data Collection Interface Properties dialog box appears.

4. On the General tab, select the PASS hosting the interface (PASS02A in the example) from the pull-down.
5. Click OK.



IMPORTANT You need a host for both node interfaces. For a redundant pair, the primary only is referenced.

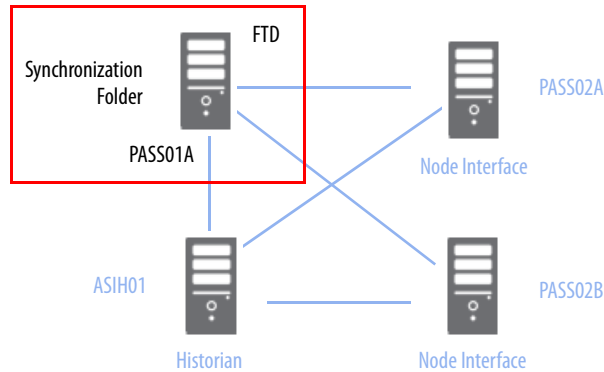
Use a PASS server with these procedures.



PASS01

Create a Synchronization Path

A common folder is used for files that are used for handshaking and redundancy.

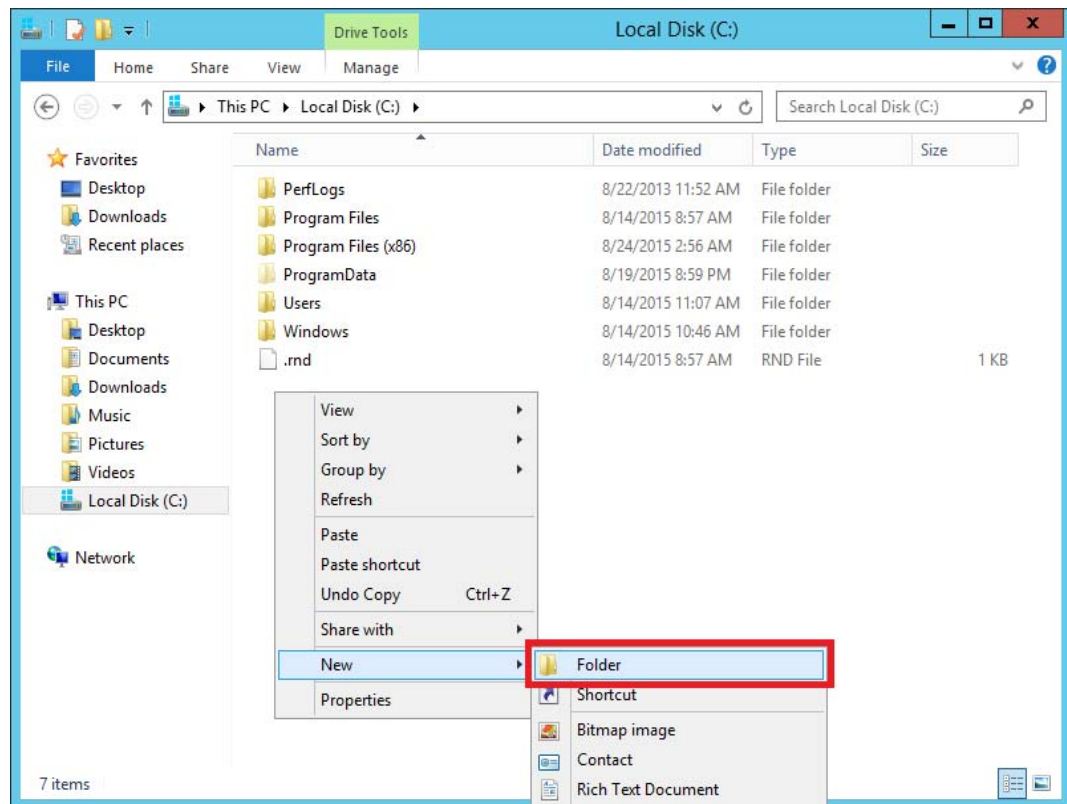


See [page 342](#) for connecting node interfaces.

IMPORTANT We recommend that you use a server that is not running LiveData.

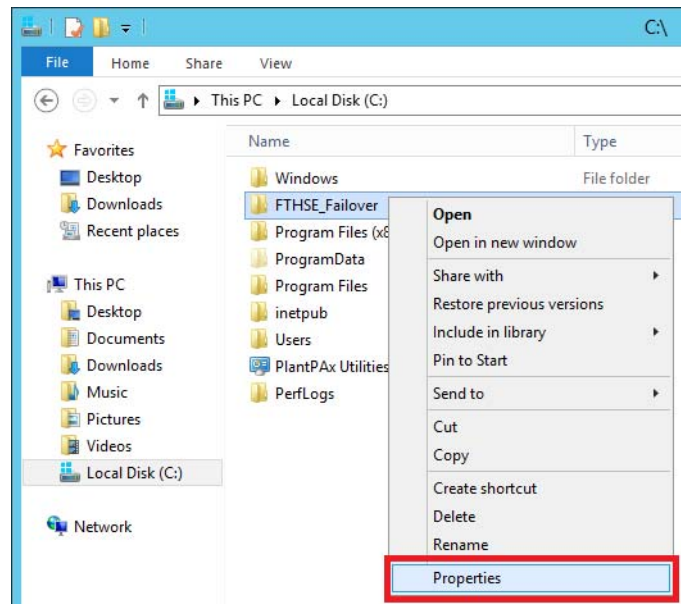
Complete the following steps.

1. In File Explorer, right-click Local Disk (C:) and choose New>Folder.

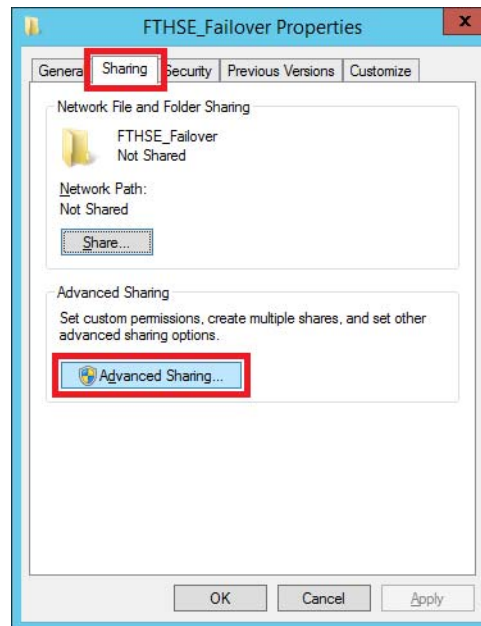


2. Name the new folder FTHSE_Failover.

3. Right-click the new folder and choose Properties.

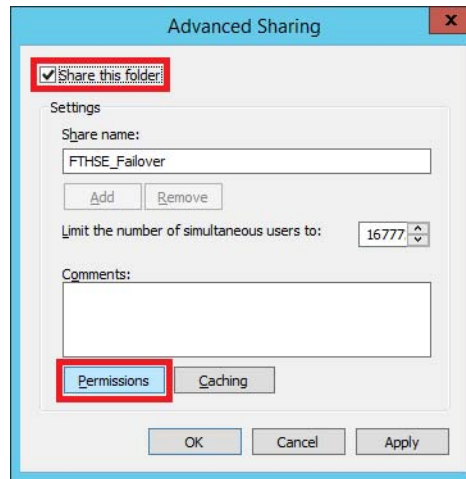


The FTHSE_Failover Properties dialog box appears.

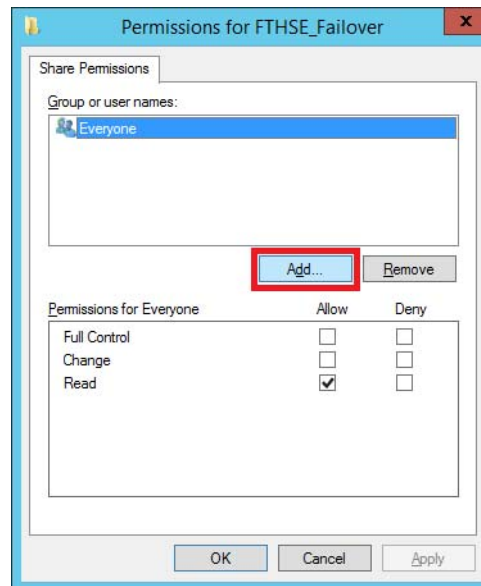


4. From the Sharing tab, click Advanced Sharing.

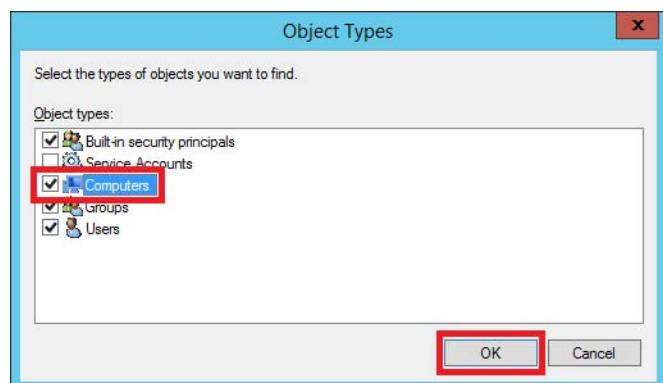
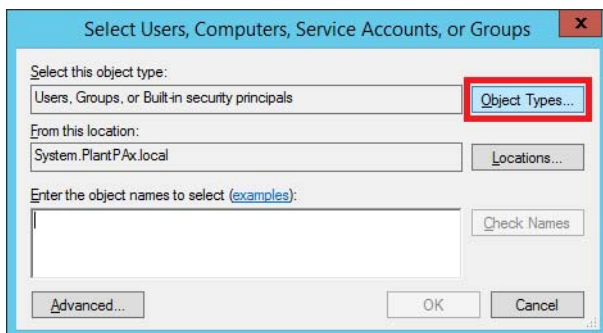
- From the Advanced Sharing dialog box, click Share this folder, and then click Permissions.



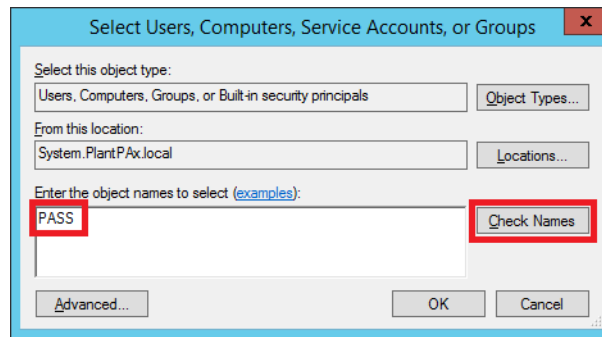
- Select 'Everyone' and click Add.



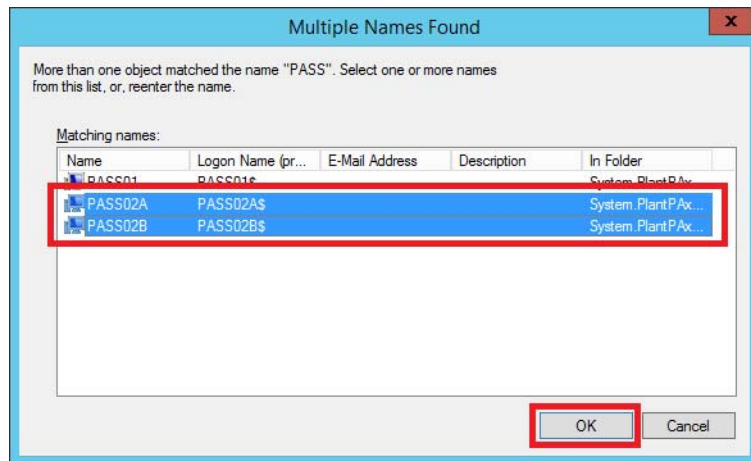
- Click Object Types.
- Select Computers and click OK.



9. Type PASS into the text box, and click Check Names.

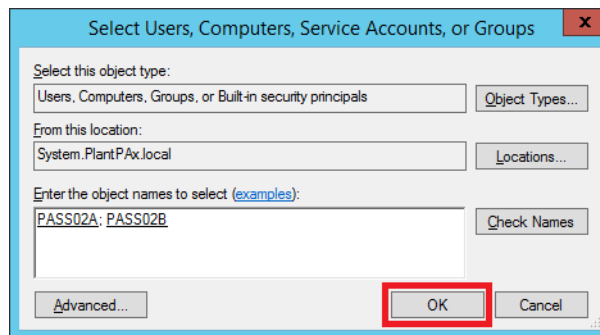


10. Select a match from the search and click OK.

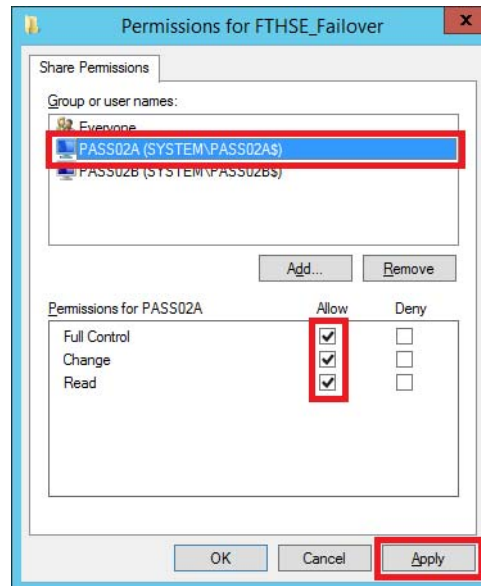


The example shows a primary and secondary server selected to create a folder for a redundant pair.

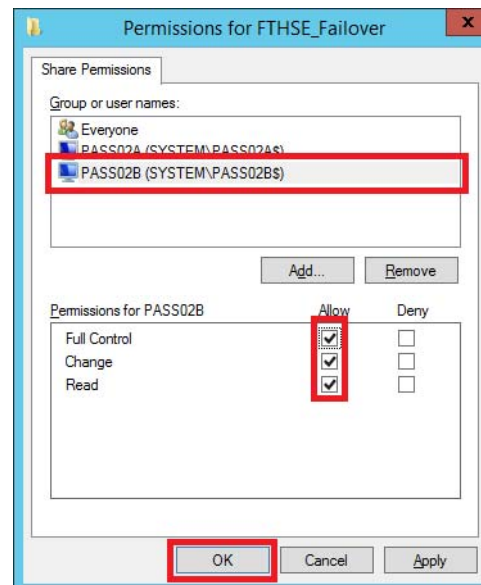
11. Click OK.



12. To provide Read/Write access to the folder, select the primary server and click all three Allow checkboxes.

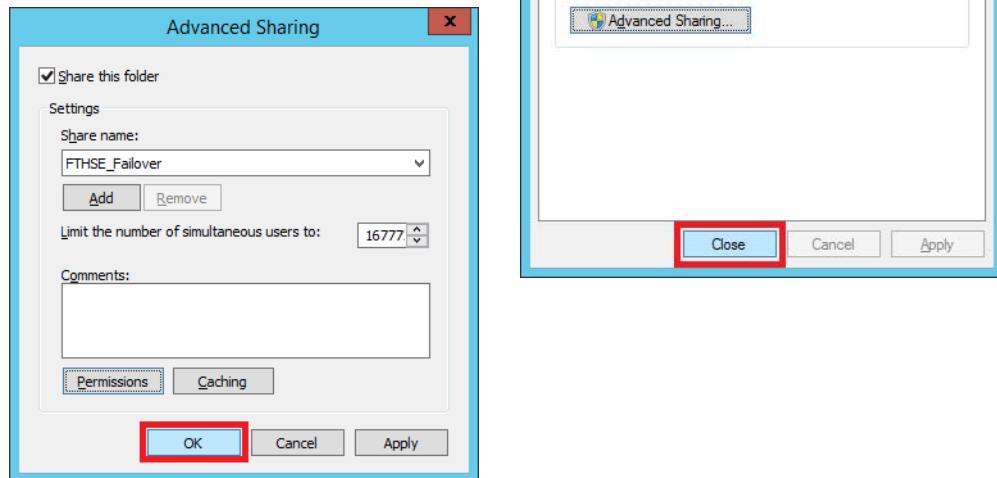


13. Click Apply.
14. Select the secondary server and click all three Allow checkboxes.



15. Click OK.

16. To complete the procedure, click OK and Close.



Proceed to [page 342](#) for procedures on how to configure a data pipeline between FactoryTalk data servers and FactoryTalk Historian servers.

Configure a Node Interface

Use a PASS server with these procedures.



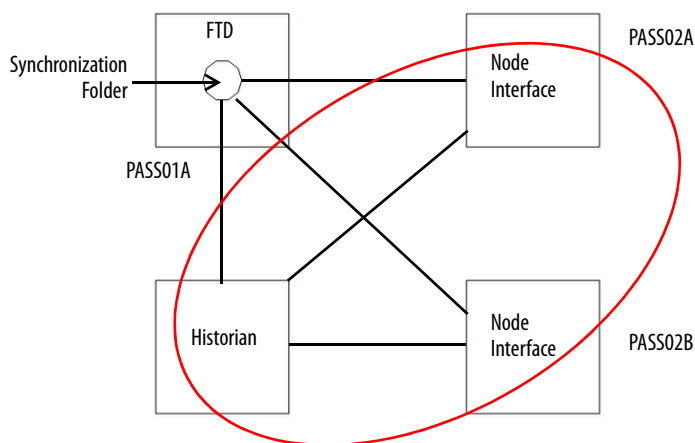
PASS02A

This section describes how to configure FactoryTalk Live Data (FTLD) connectors. The FTLD interface is a FactoryTalk Live Data client that enables process data to be passed between a FactoryTalk Live Data server (for example, FactoryTalk Linx) and a FactoryTalk Historian server. Each instance of the FTLD Interface can provide data to a single FactoryTalk Historian SE server or collective.

Configure Primary Node Interface Server


This section describes how to connect the Historian server to the PASS server with node interfaces.

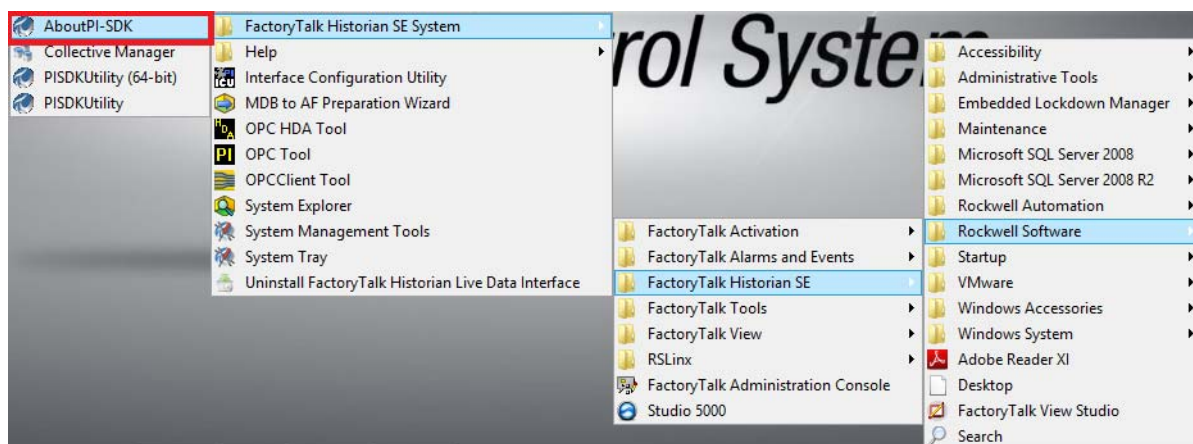
See [page 336](#) for creating a synchronization folder.



Configure the Server Connection

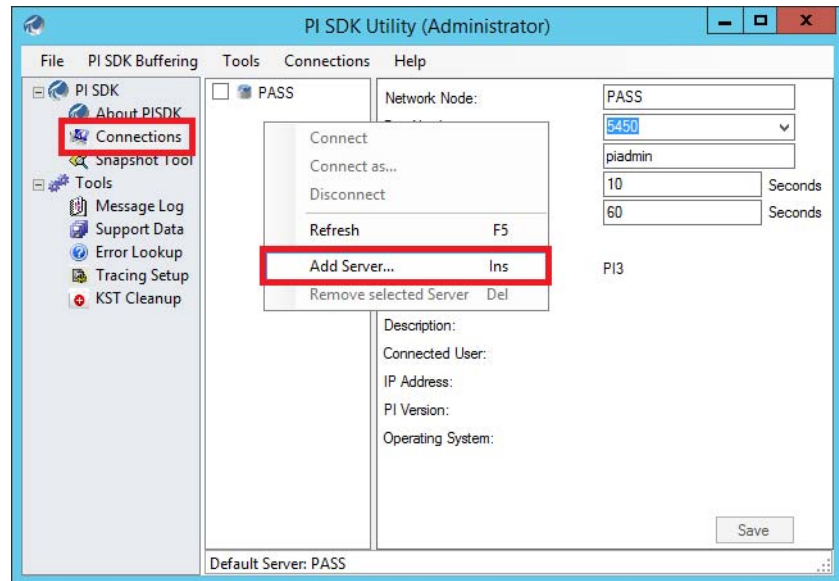
Complete the following steps:

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>FactoryTalk Historian SE System>AboutPI-SDK.



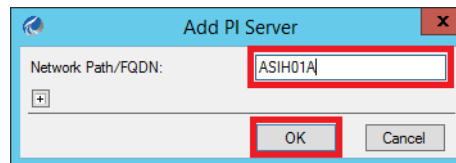
The PI SDK Utility window appears.

2. Expand PI SDK and click Connections.
3. Right-click anywhere in the white space and choose Add Server.

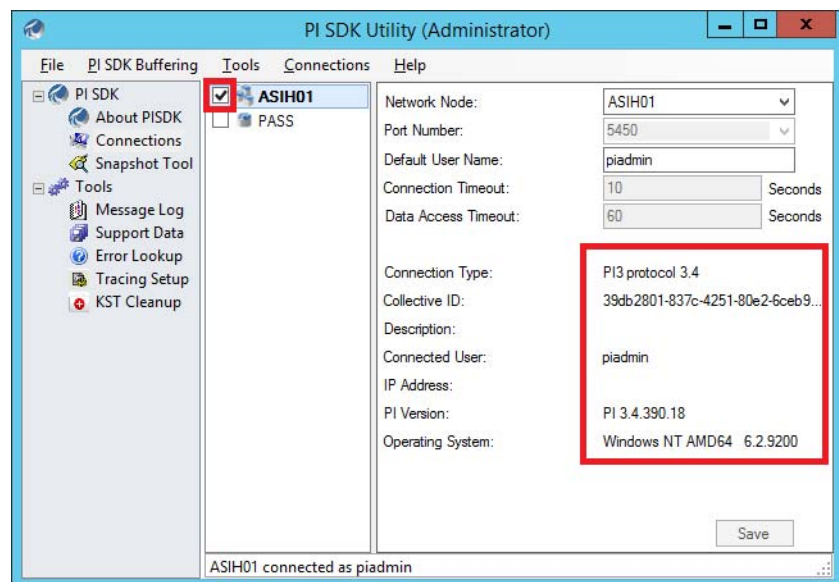


The Add PI Server dialog box appears.

4. Type the Network Path (If you are using a collective, type the primary machine name) and click OK.

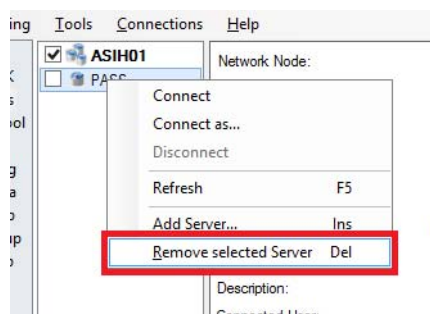


5. Click the box next to the new server (ASIH01 in the example).



If the connection is successful, the connection information appears in the same window.

6. If there are servers listed that are not required, right-click the server name and choose 'Remove selected server'.



7. When asked if you want to delete the server, click Yes.
8. Close the PI SDK Utility window.

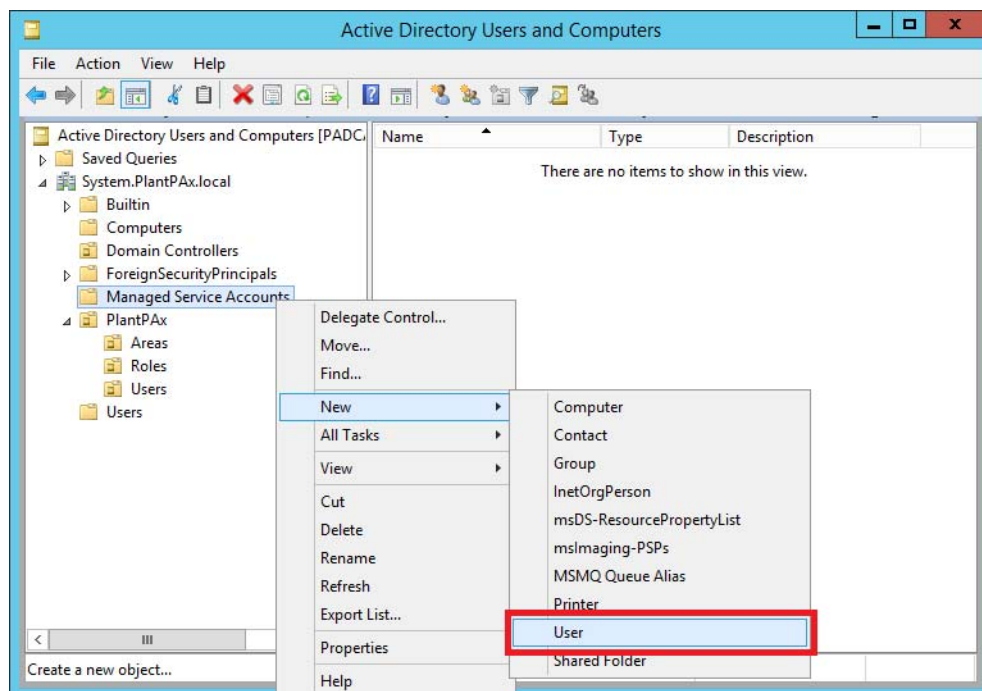
Creating a PI Buffer Service User

Use a domain controller with these procedures.



You must create a service user to enable PI buffering service.

1. From the Server Manager, click Tools and choose Active Directory Users and Computers.
2. Expand the domain folder (System.PlantPAx.local), right-click Managed Service Accounts and choose New>User.



The New Object - User dialog box appears.

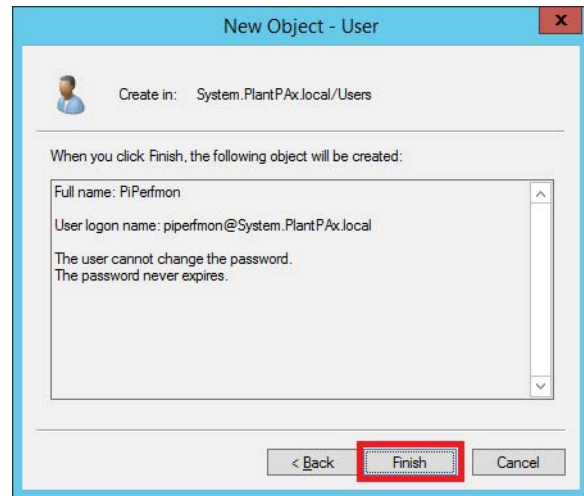
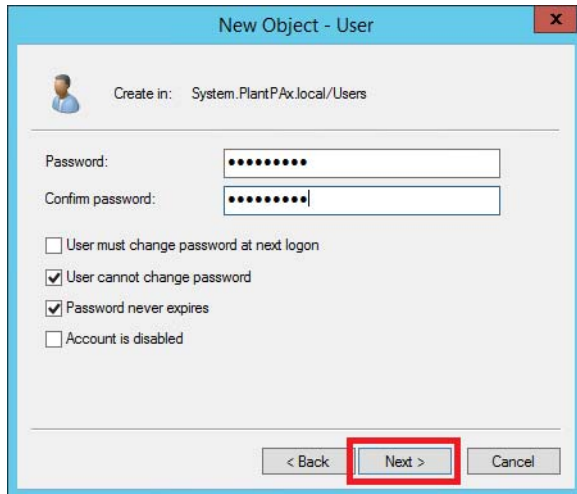
3. Complete the User text boxes.

Item	Description
First name	Type a name for the PI buffering service. IMPORTANT: The 'PI' preface is the name of the OSIsoft product.
Initials	Optional; you can leave blank.
Full name	Type the same name for the PI buffering service.
User login name	Type the same name for the PI buffering service and click the pull-down to select your domain folder.
User login name (pre-Windows 2000)	Use the SYSTEM\ default and type the same name for the PI buffering service.

IMPORTANT The logon password creates a service user, not a person. The service user grants access to system computers for placing data into memory (buffer).

4. Click Next.

5. Type your password twice, and make sure that there is a check mark in the following boxes:
 - User cannot change password
 - Password never expires (indefinite service for system access)



6. Click Next and then click Finish.

Creating Security Mappings

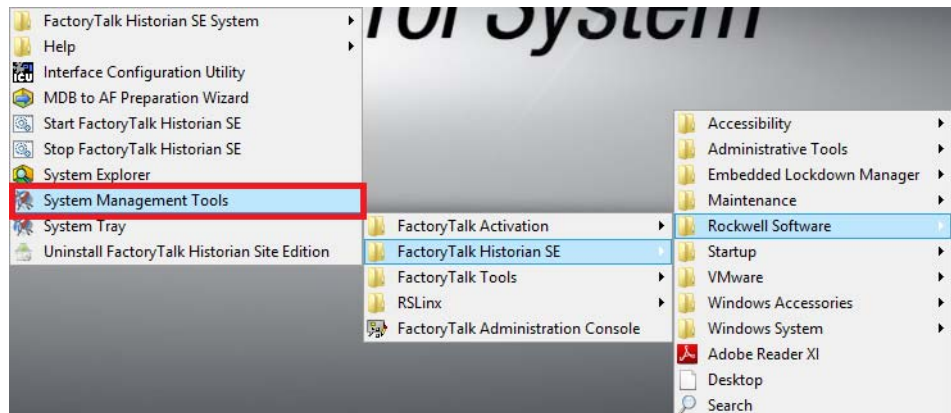
Use an AppServ-Info server with these procedures.



ASIHO1A

This procedure associates the service user identity with the Historian mapping and trusts.

1. Click the Programs >> symbol and choose Rockwell Software>FactoryTalk Historian SE>System Management Tools.



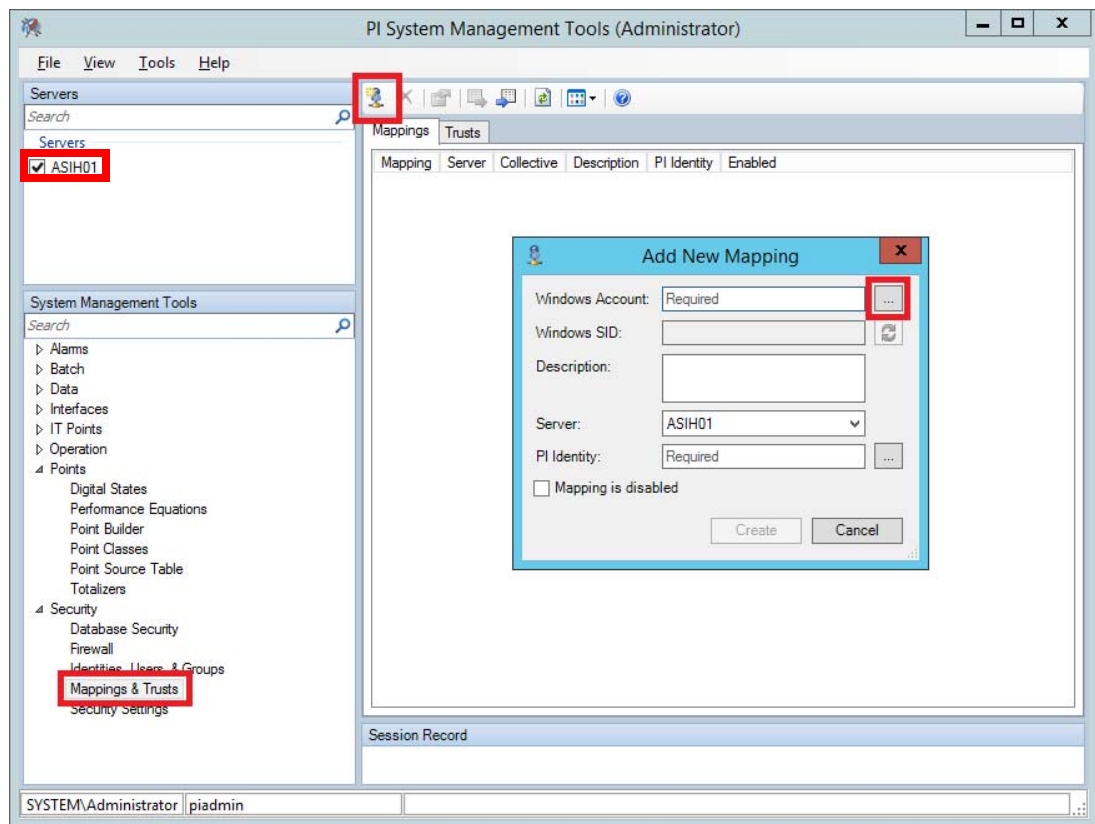
The PI System Management Tools window appears.

2. Do the following steps:
 - a. Under Servers, check the server that you want to set the security settings for.
 - b. Under System Management Tools, choose Mappings & Trusts.

- c. Click Add Mapping icon .

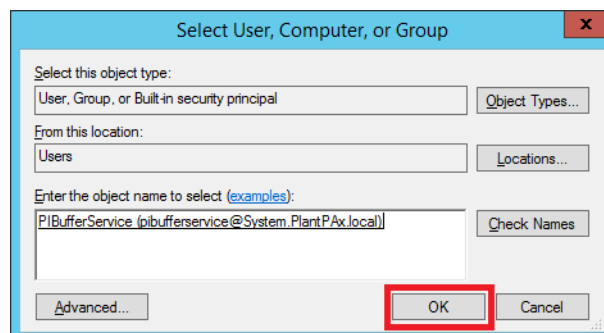
The Add New Mapping dialog box appears in the right pane.

- d. Click Browse (ellipsis '...').

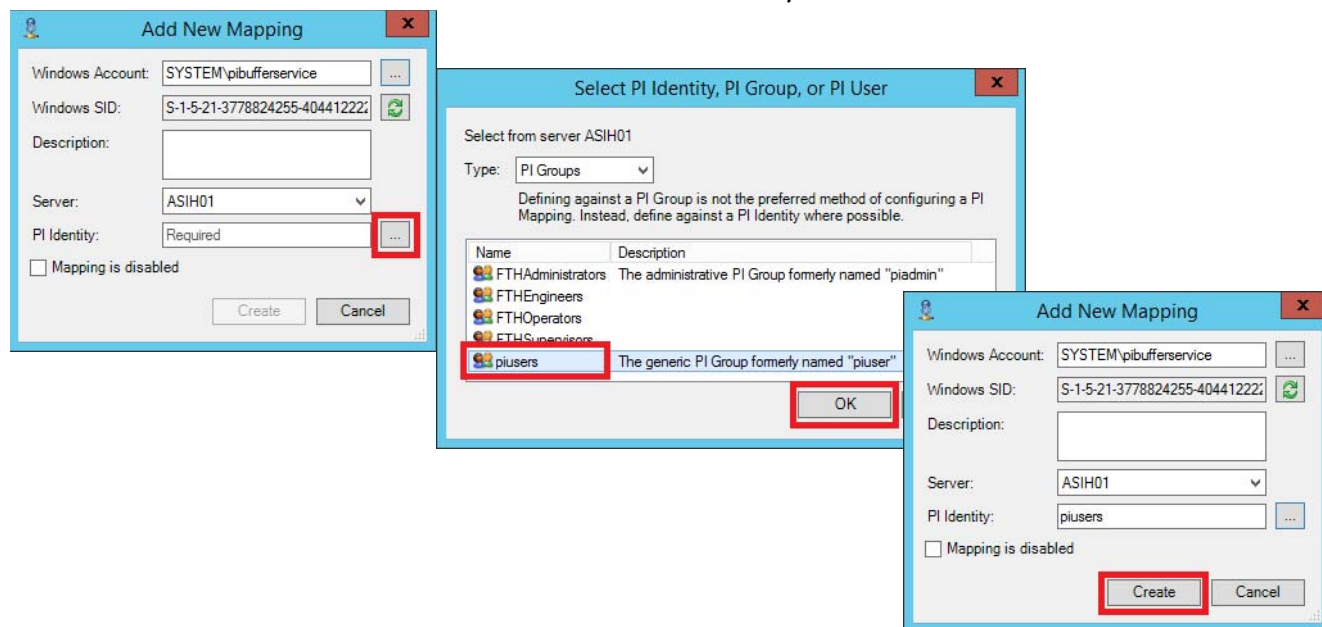


The Add New Mapping dialog box appears in the right pane.

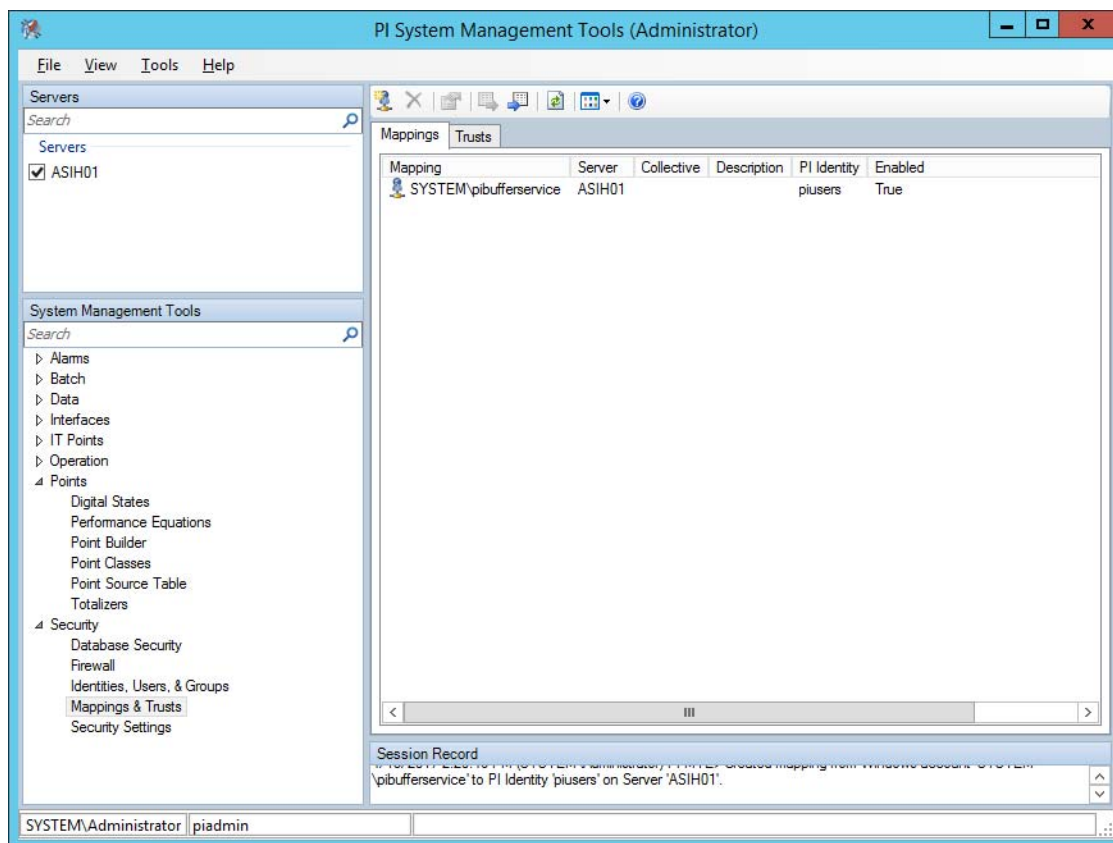
3. Select the PIBufferService user that you created earlier.
4. Click OK.



5. Click Browse, then select a group from the Type pull-down men.
6. Select a desired identity and click OK.



7. Click Create.



Use a PASS server
with these procedures.

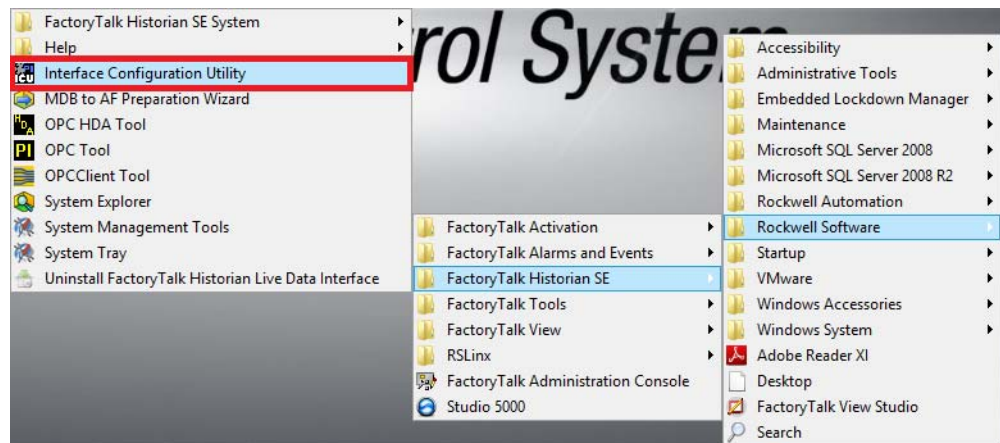


PASS02A

Configuring the Interface

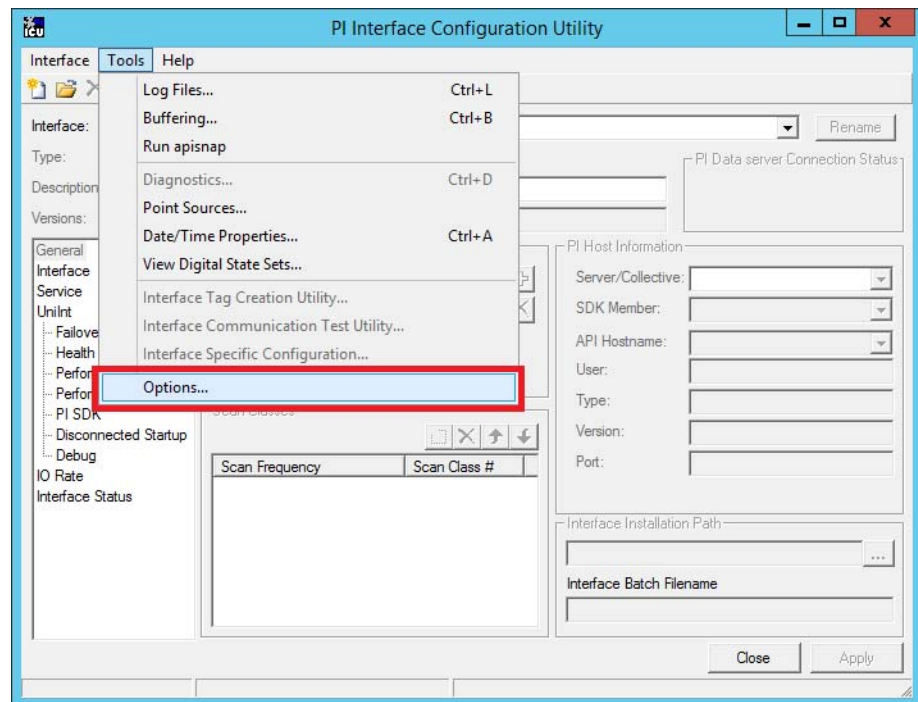
Complete the following steps to configure buffering for the server that you connected.

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>Interface Configuration Utility.

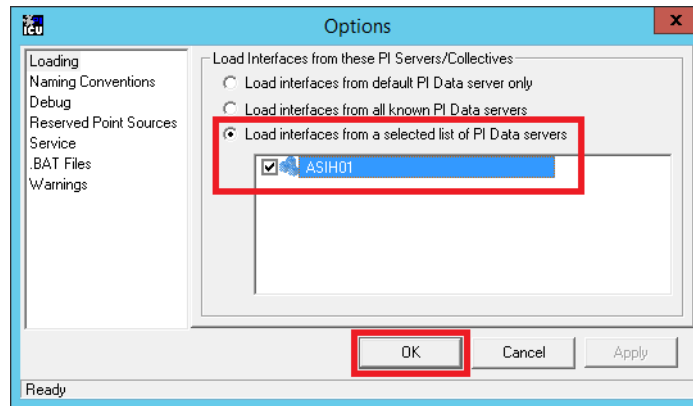


The PI Interface Configuration Utility window appears.

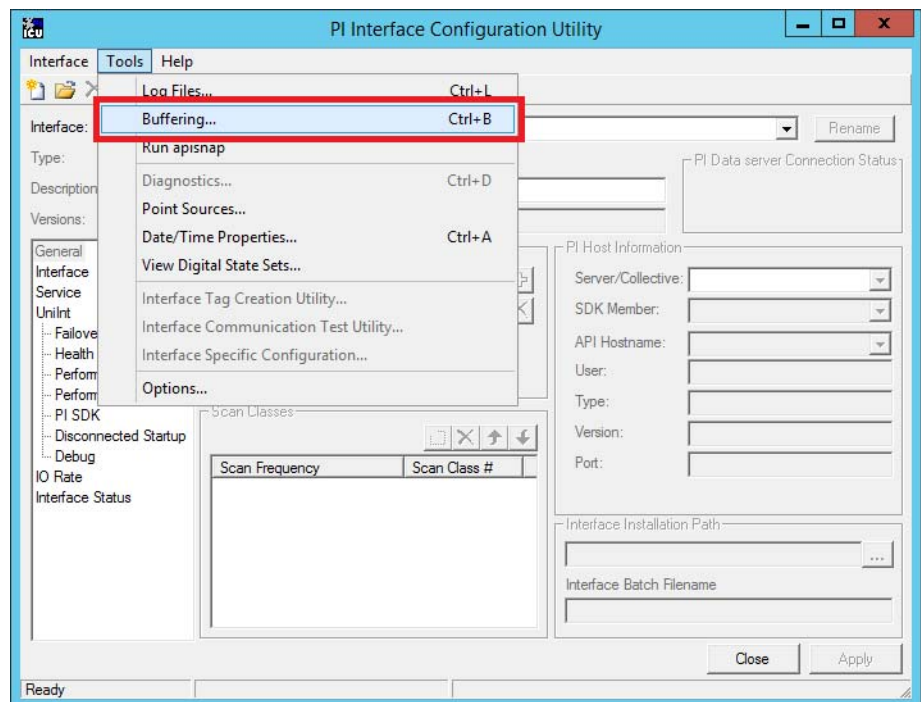
2. From the Tools menu, choose Options.



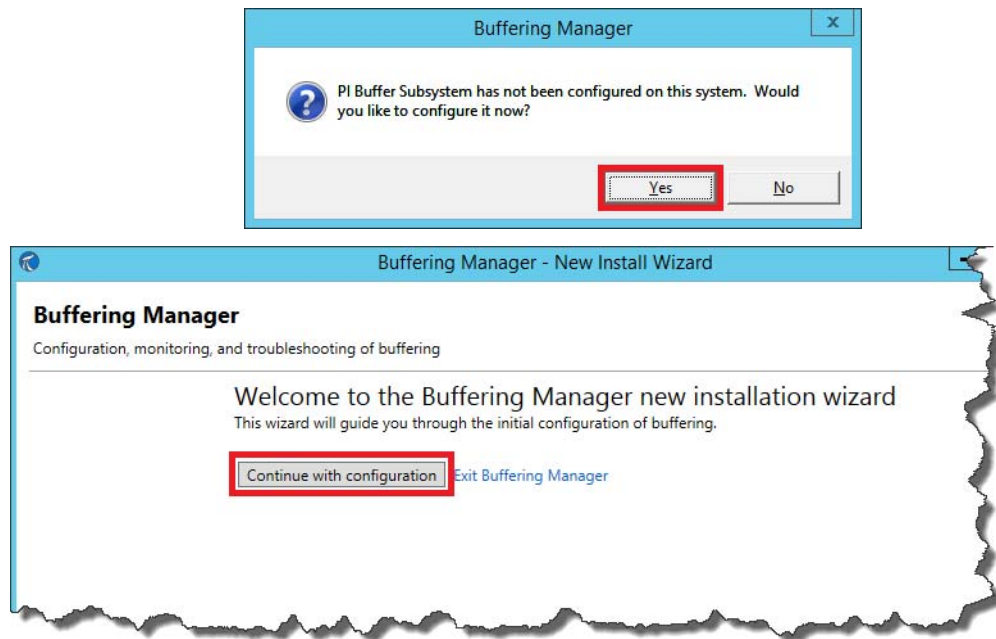
- Click 'Load interfaces from a selected list of PI Data servers'.



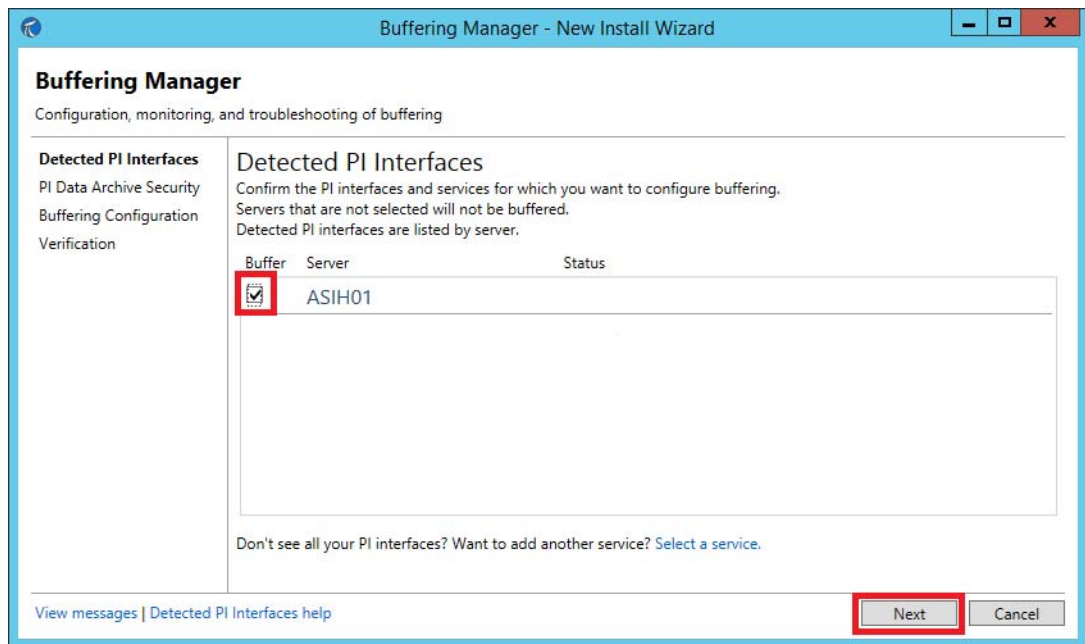
- Click a server box and then click OK.
- From the Tools menu, choose Buffering.



6. Click Yes, and then 'Continue with configuration' to initiate the Buffering Manager wizard.

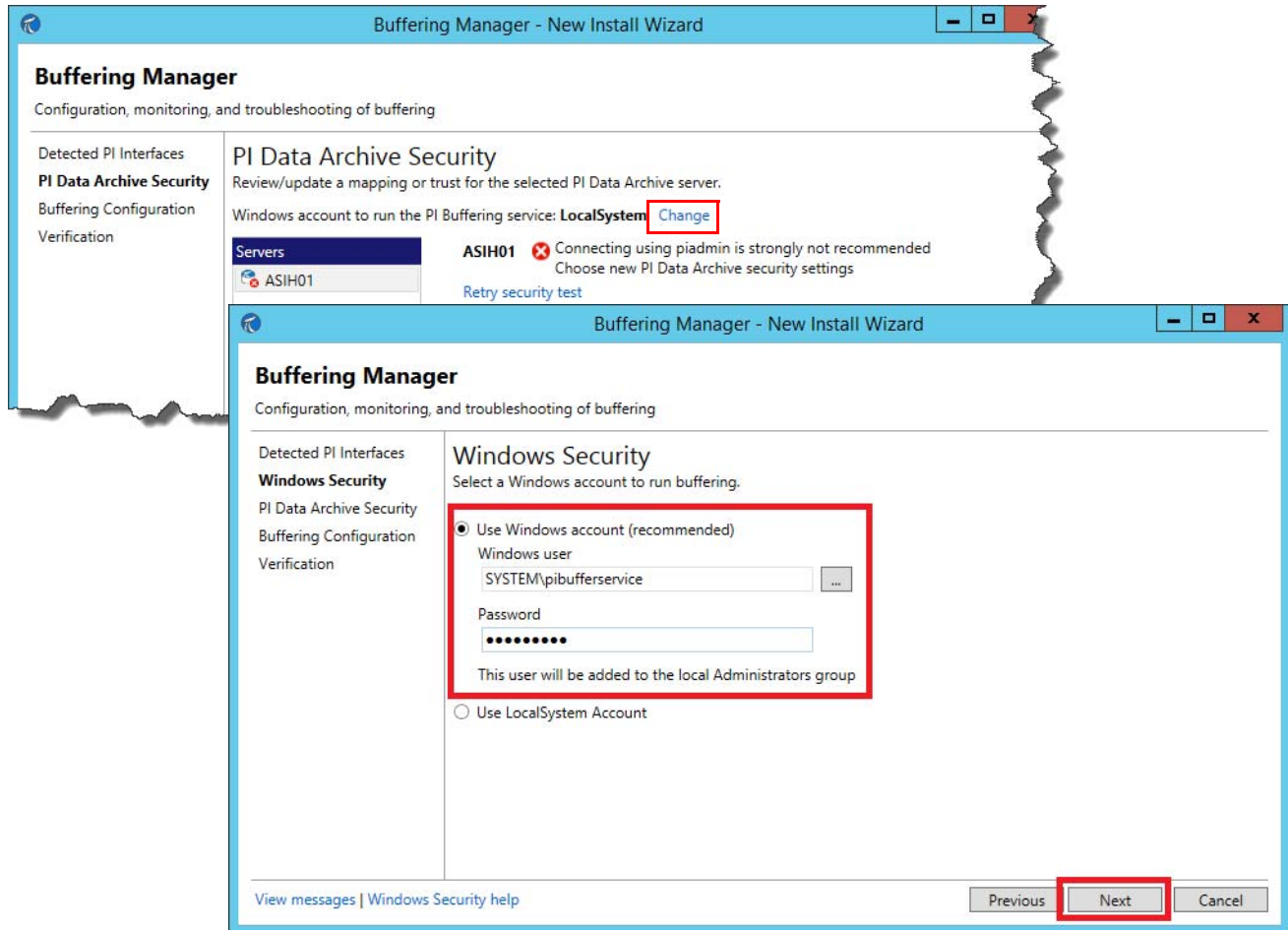


7. Select Buffer and click Next.



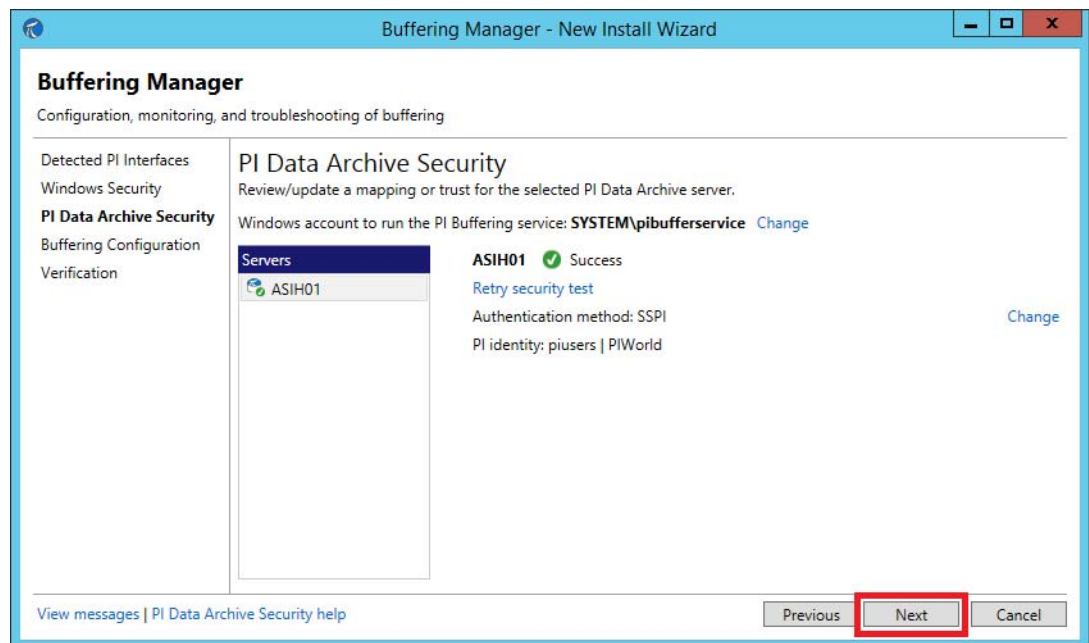
IMPORTANT Do [step 8](#) and [step 9](#) on the Buffering Manager, if applicable. Otherwise, skip to [step 10](#).

8. Click Change, type the user name and password (that you created earlier), and click Next.

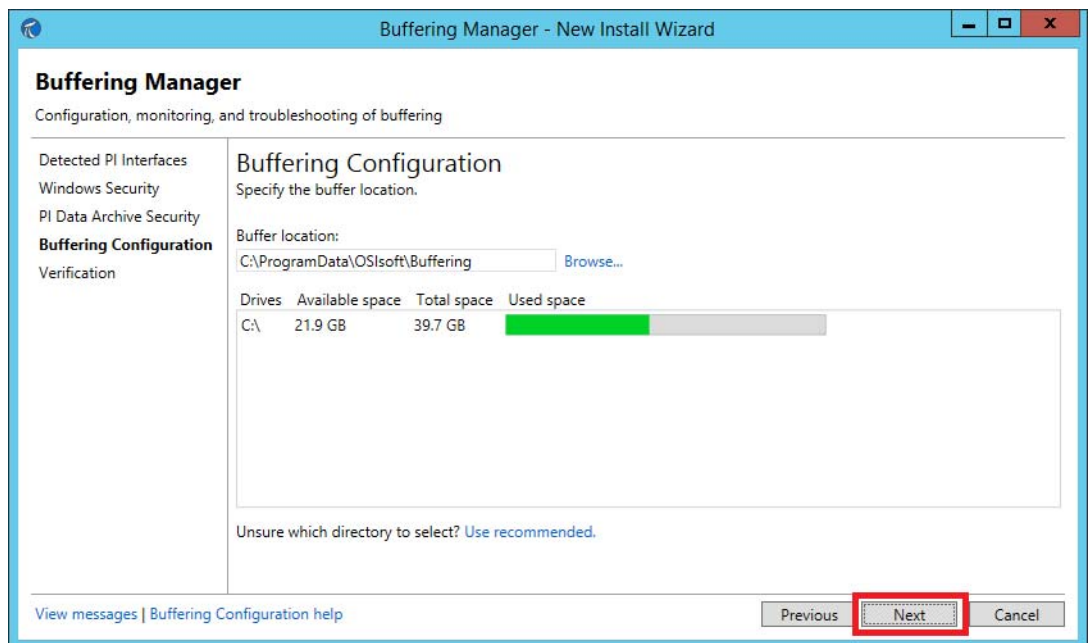


IMPORTANT If you miss the Change option on the New Install Wizard (or the option does not appear), you must configure the Service logon. For procedures, see [Configure Service Logon on page 357](#).

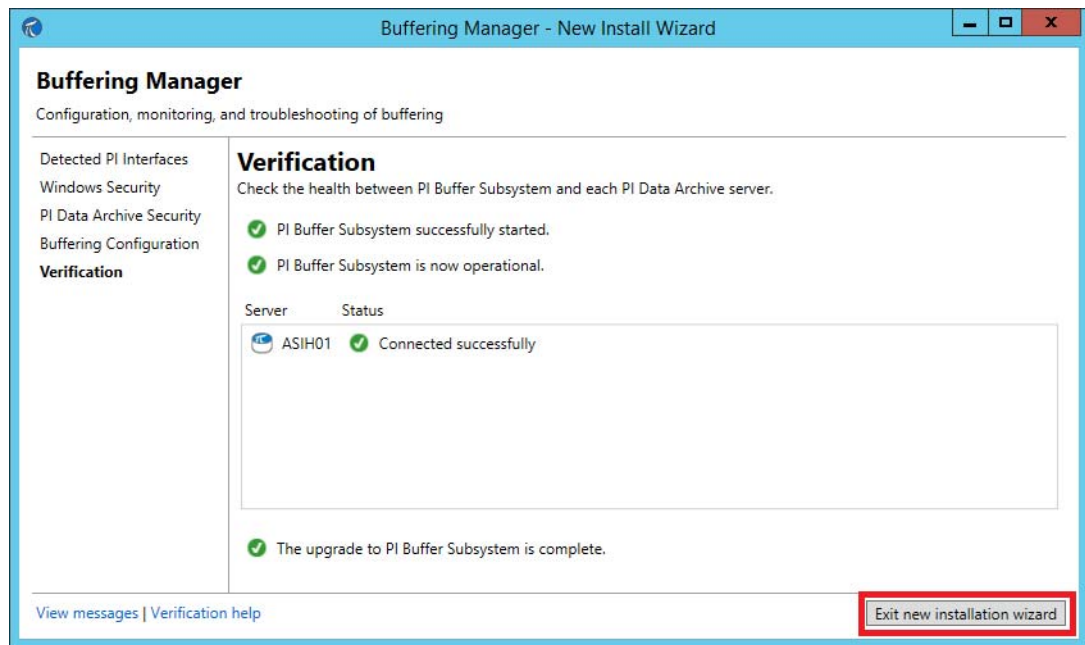
9. Click Next.



10. Click Next again.

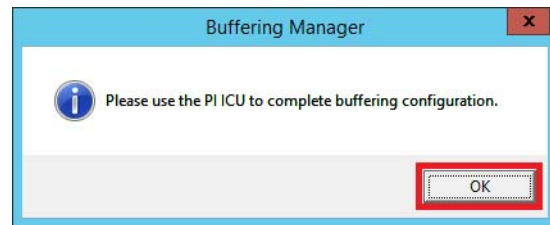
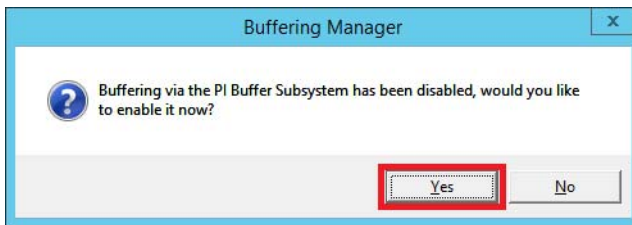


11. Click 'Exit new installation wizard'.




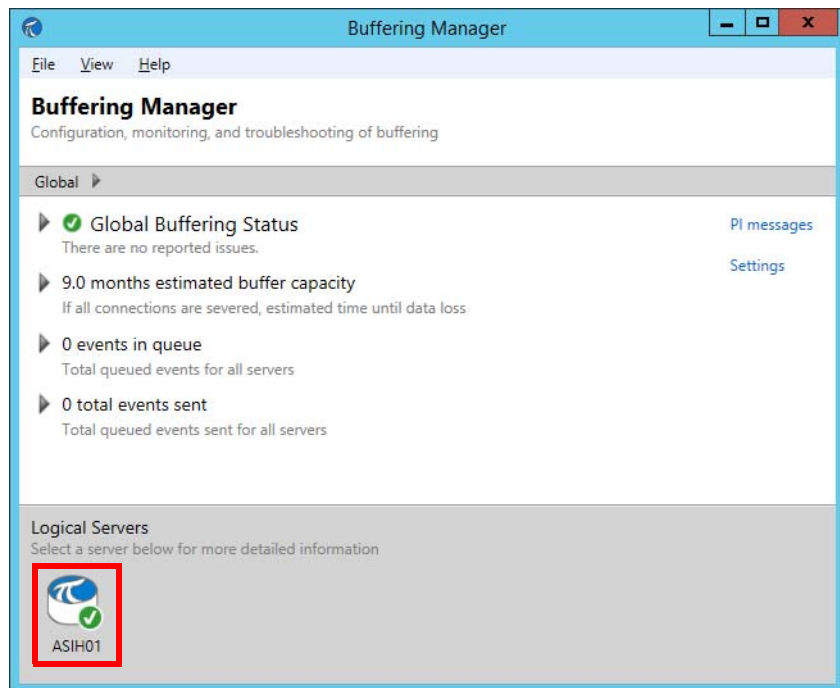
The following messages appear to complete the buffering configuration.

12. Click Yes and OK to confirm the PI ICU dependency.



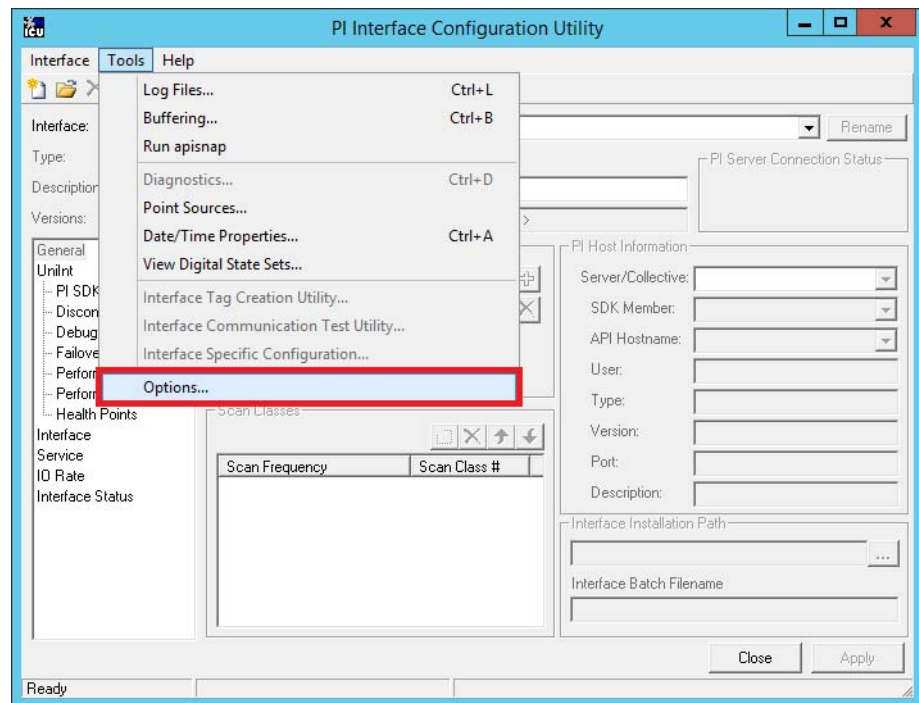
13. From the Tools menu, choose Buffering and verify that your information matches the dialog box shown.

IMPORTANT If your Buffering Manager dialog box does **not** show a server with a green check mark , choose File>Add Server and repeat [step 8](#) and [step 9](#) on pages [352-353](#).



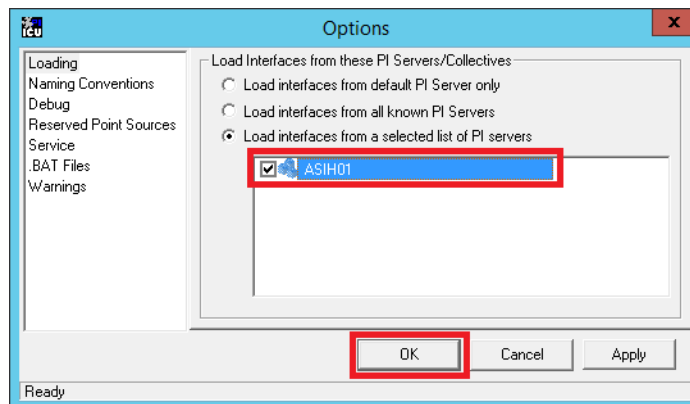
14. Close the Buffering Manager.

15. In the PI Interface Configuration Utility window, from the Tools menu choose Options.



The Options dialog box appears.

16. Check 'Load interfaces from a selected list of PI servers.'

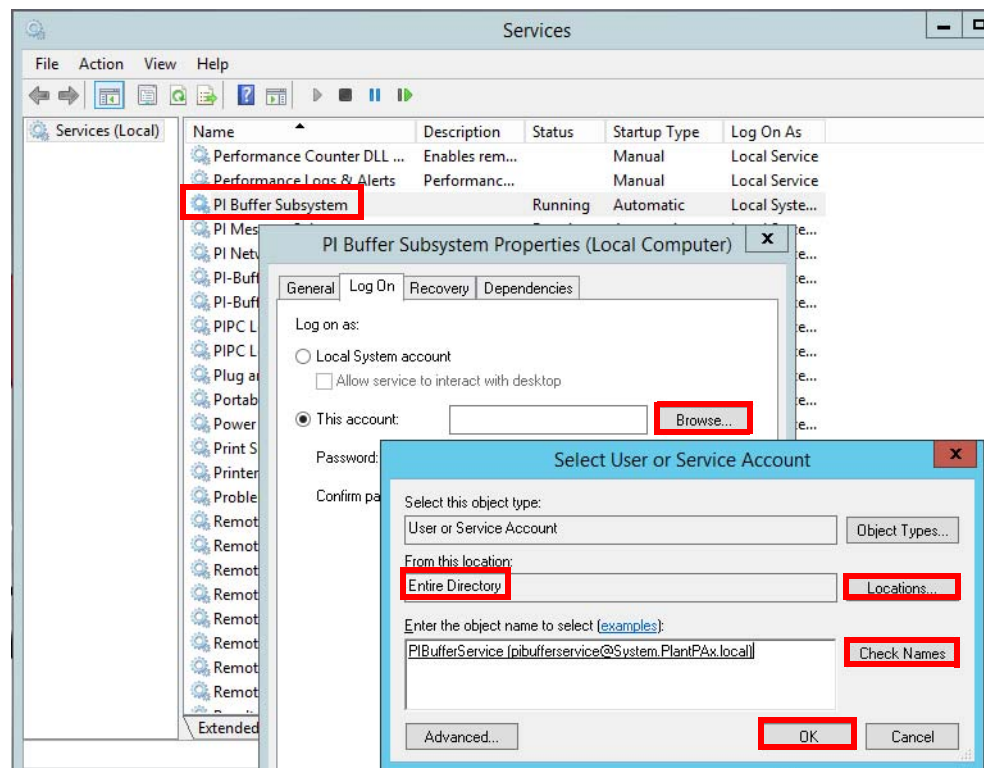


17. Make sure that the server is checked.
18. Click OK.

Configure Service Logon

The following procedure is applicable only if the Change Option was not available on the New Install Wizard dialog box.

1. On the PASS server, right-click Start menu and choose Computer Management.
2. In the left pane, open Local Users and Groups and right-click Groups and choose Administrators.
3. Click Add and type 'SYSTEM\pibufferservice'.
4. Click Check Names.
5. Click OK.
6. To assign the logon service account, from the Start menu, click Programs and choose Administrative Tools>Services.
7. Right-click PIBuffer Subsystem and choose Properties.
8. On the Log On tab, click Browse.



9. Click Locations, choose 'Entire Directory', and click OK.
10. Type 'SYSTEM\pibufferservice' and click Check Names.
11. Click OK.

Use a PASS server
with these procedures.



PASS02B

Configure Secondary Node Interface Server

In this section, you connect to the PASS02A servers and configure buffering for the server.

Configure Server Connection

Repeat [step 1](#) through [step 8](#) on pages [342](#)...[344](#) for the PASS02B server.

Configure the Interface

Repeat [step 1](#) through [step 18](#) on pages [349](#)...[356](#) for the PASS02B server

Configure FactoryTalk Live Data Connectors

Use PASS servers
with these procedures.



PASS02A



PASS02B

UniInt (Universal Interface) provides generic functions required by most interfaces, such as establishing a connection to the Historian Server node and monitoring the Historian Point Database for changes.

To minimize data loss during a single point of failure within a system, UniInt provides two failover schemas: (1) synchronization through the data source (Phase 1) and (2) synchronization through a shared file (Phase 2).

Phase 1 UniInt Failover uses the data source itself to synchronize failover operations and provides a hot failover, no data loss solution when a single point of failure occurs.

Phase 2 UniInt Failover uses a shared file to synchronize failover operations and provides for hot, warm, or cold failover. The Phase 2 hot failover configuration provides a no data loss solution for a single point of failure similar to Phase 1.

IMPORTANT In this section, only Phase 2 UniInt Failover is addressed.

The UniInt failover scheme requires the data source be able to communicate and service data to two interfaces simultaneously. Additionally, the failover configuration requires that the interface supports outputs. A redundant solution requires two separate interface nodes communicating with the data source.

In a hot failover configuration, the interface copy that is in a backup role collects and queues data in parallel to the interface that is in the primary role. The interface in the backup role does not send the data that is collected to the Historian server. However, if a failover occurs, the interface immediately sends its data to the Historian server.

Use a PASS Server with these procedures.




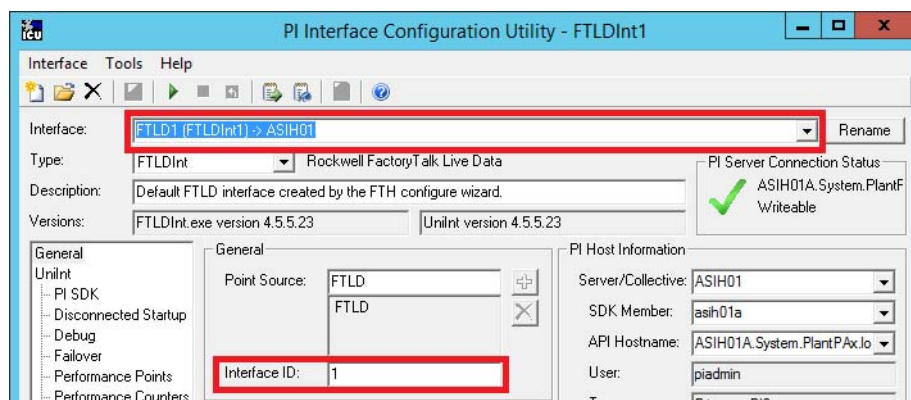
PASS02A

Configure a FactoryTalk Live Data Primary Connector

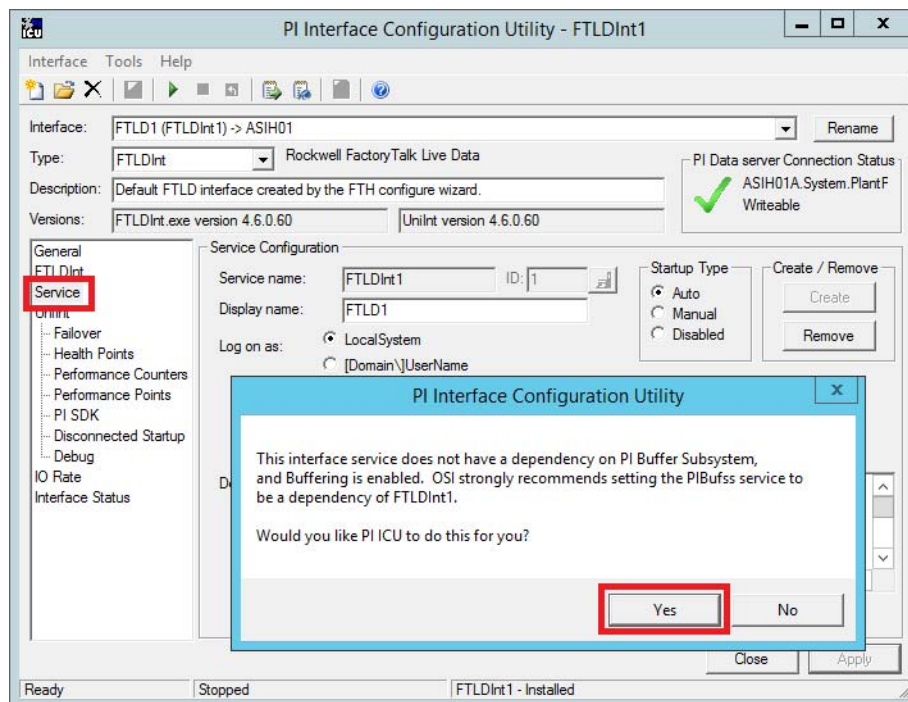
The FactoryTalk Live Data 1 (FTLDDint1) is in the primary server (PASS02A in the example).

Complete the following steps.

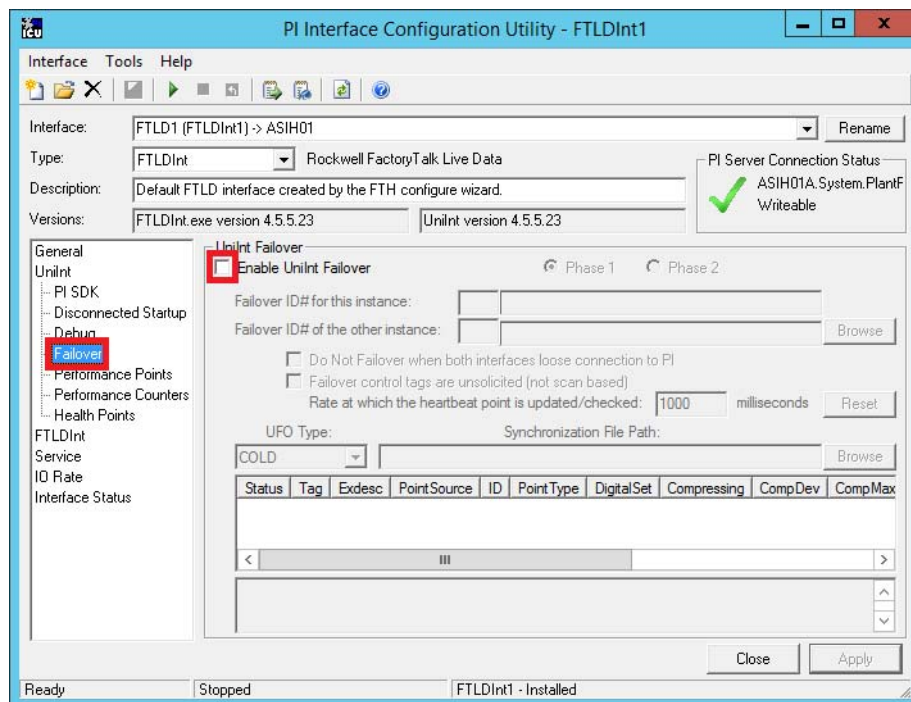
1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>Interface Configuration Utility.
2. In the PI Interface Configuration Utility window, choose 'FTLDDint1 (FTLDDint1)->ASIH01' from the Interface pull-down list.



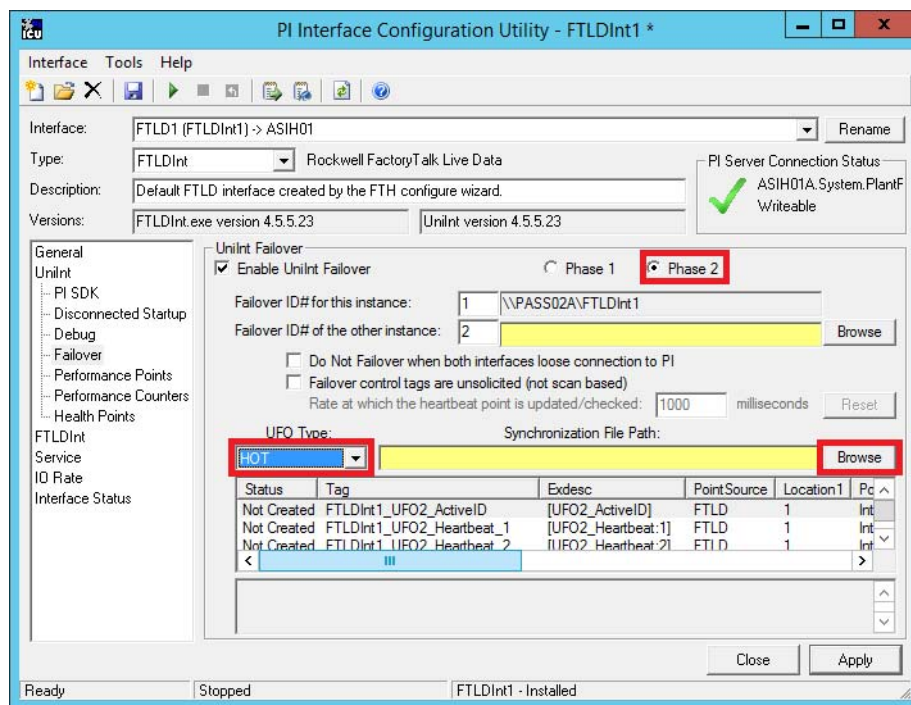
3. If the Interface ID is not already '1', change it to '1'.
4. Click Service, and then Yes on the popup window.



5. Select Failover from the list on the left.
6. Check Enable UniInt Failover.



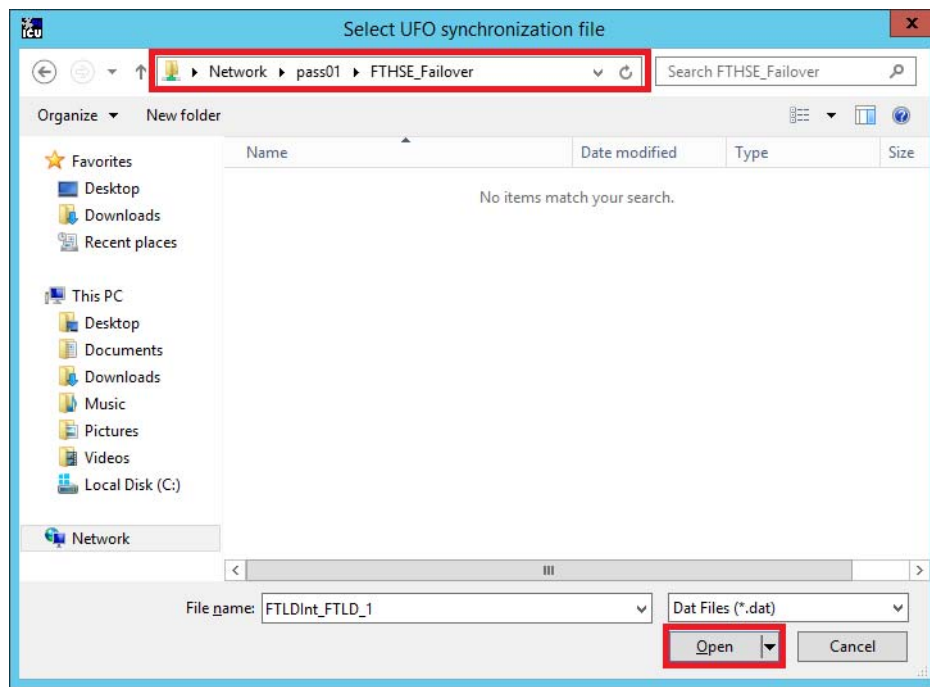
7. Click 'Phase 2'.



8. From the UFO Type pull-down list, choose HOT.
9. Click Browse to search for the Synchronization File path for the secondary instance.

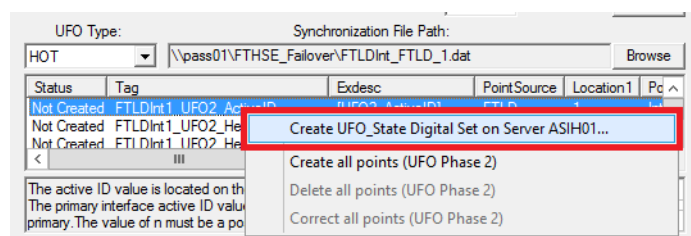
The 'Select UFO synchronization file' dialog box appears.

10. Navigate to the Network>pass01>FTHSE_Failover directory (that was created in the previous section).
11. Click Open.

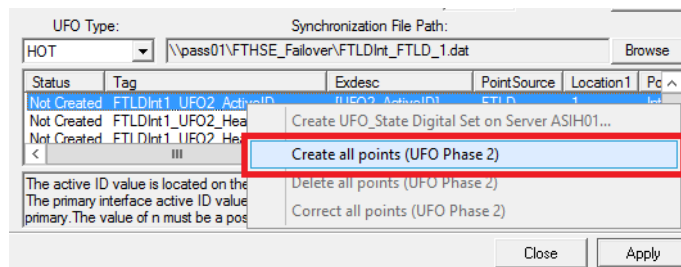


The 'Select UFO synchronization file' dialog box closes.

12. Right-click in the tag area and choose 'Create UFO_State Digital Set on Server ASIH01'.



13. When you receive the Successfully created Digital Set 'UFO_State' on server ASIH01 message, click OK.
14. Right-click in the tag area and choose 'Create all points (UFO Phase 2)'.



15. When the status for FTLDInt1_UFO2_ActionID tags changes to 'Created', click Apply.

The 'UniInt Failover' configuration is not complete until the 'Other' interface is selected' message appears.

16. Click OK.

Another popup message appears that 'changes made to the interface settings will not take effect until the interface service is stopped and started'.

17. Click OK.

Configure a FactoryTalk Live Data Secondary Connector

Use a PASS server with these procedures.

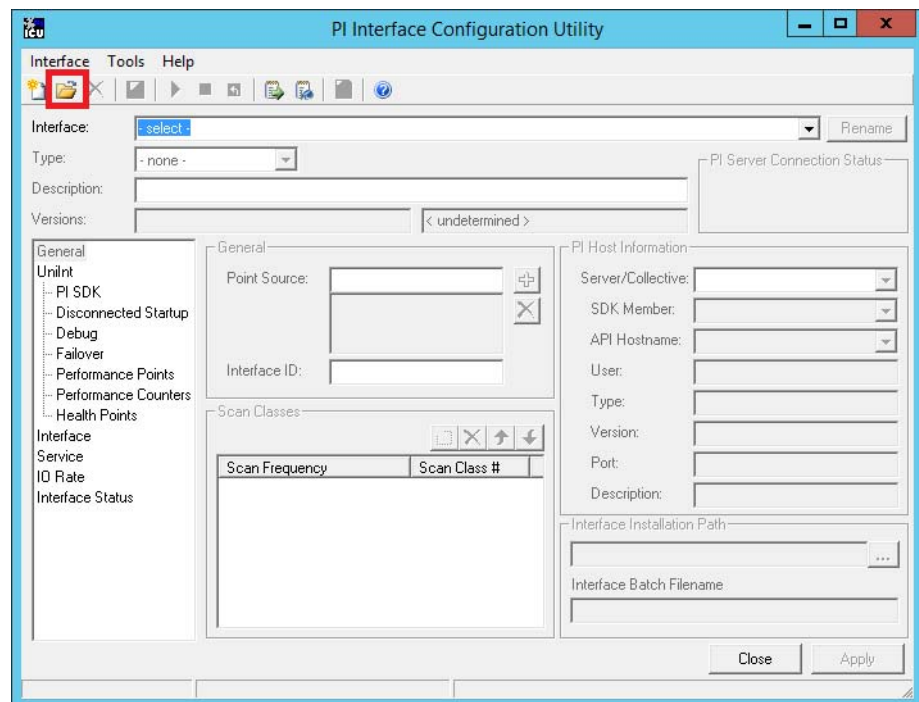


PASS02B

In this section you configure FactoryTalk Live Data Secondary connector.

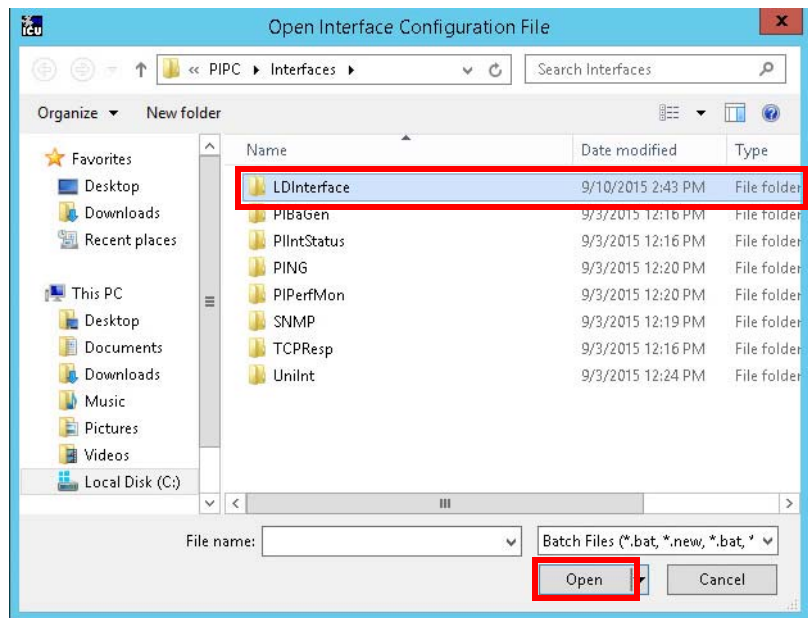
Complete the following steps.

1. In the PI Interface Configuration Utility window, click the folder symbol (Create a New Interface instance from a .BAT file).

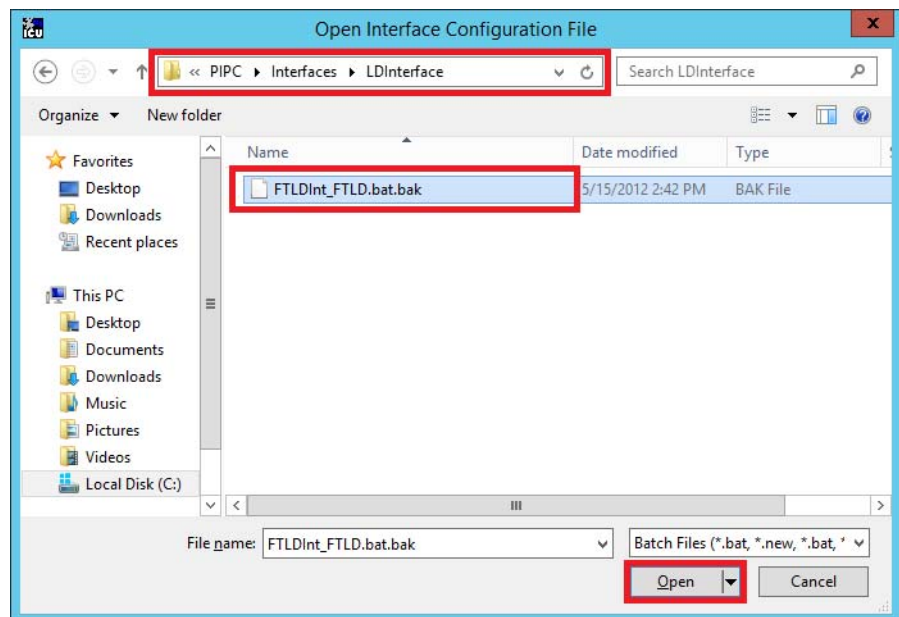


The Open Interface Configuration File dialog box appears.

2. Select LDInterface and click Open.

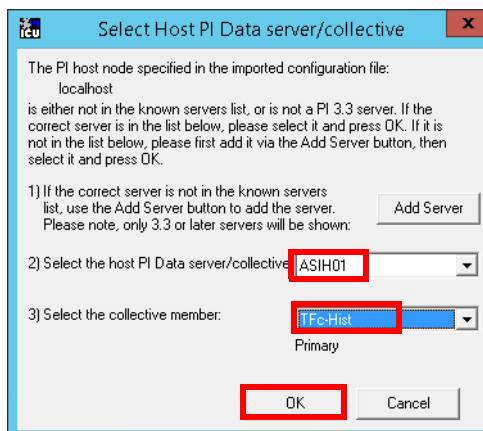


3. Select the 'FTLDDInt_FTLDD.bat.bak' file and click Open.

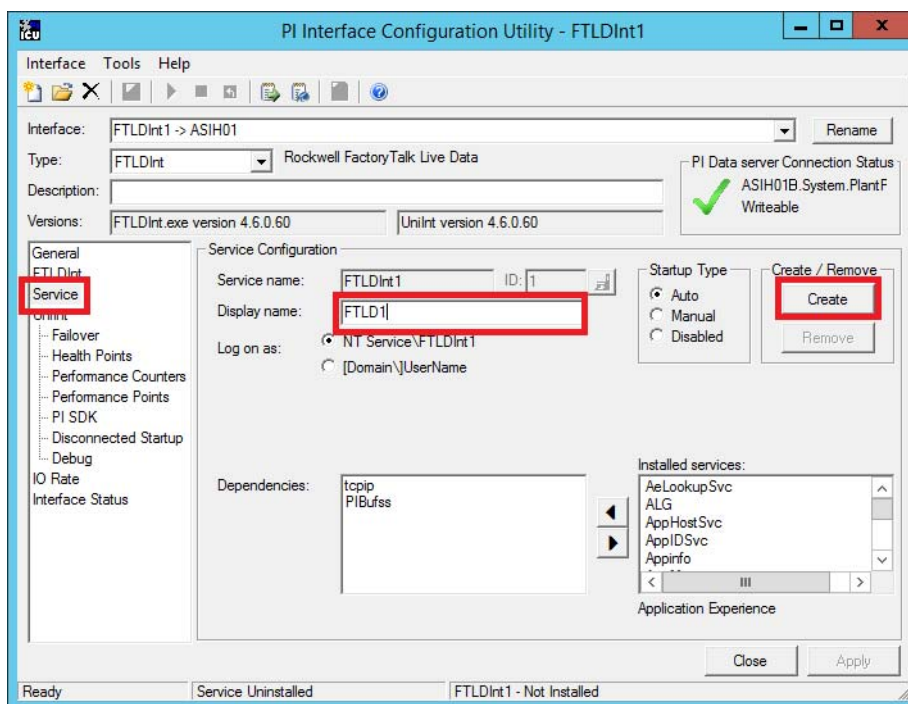


The Select Host PI Server dialog box appears.

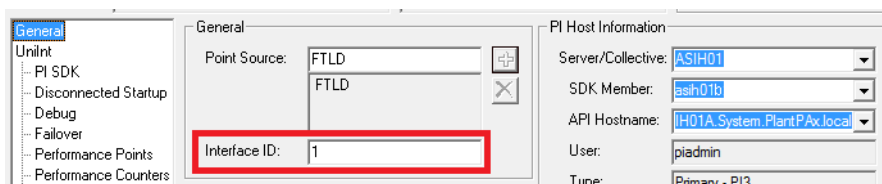
4. Make certain that the appropriate server is selected for each pull-down menu.
5. Click OK.



6. Select Service from the list on the left of the PI Interface Configuration Utility - FTLDInt1 window.

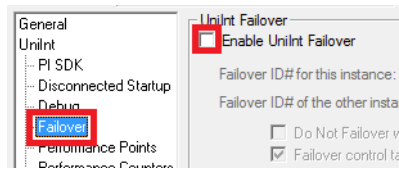


7. Type 'FTLD1' for the Display name and click Create.
8. Select General from the list on the left.

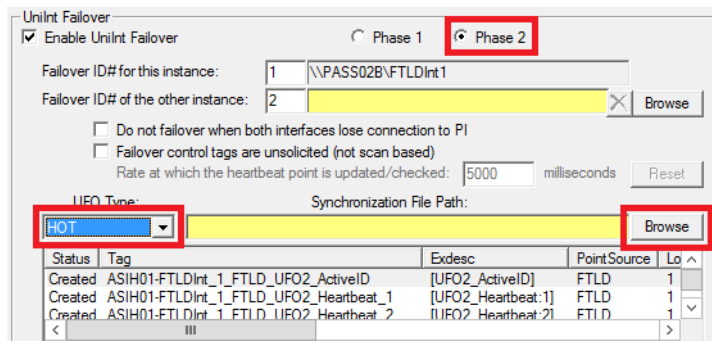


9. If the Interface ID is not already '1', change it to '1'.

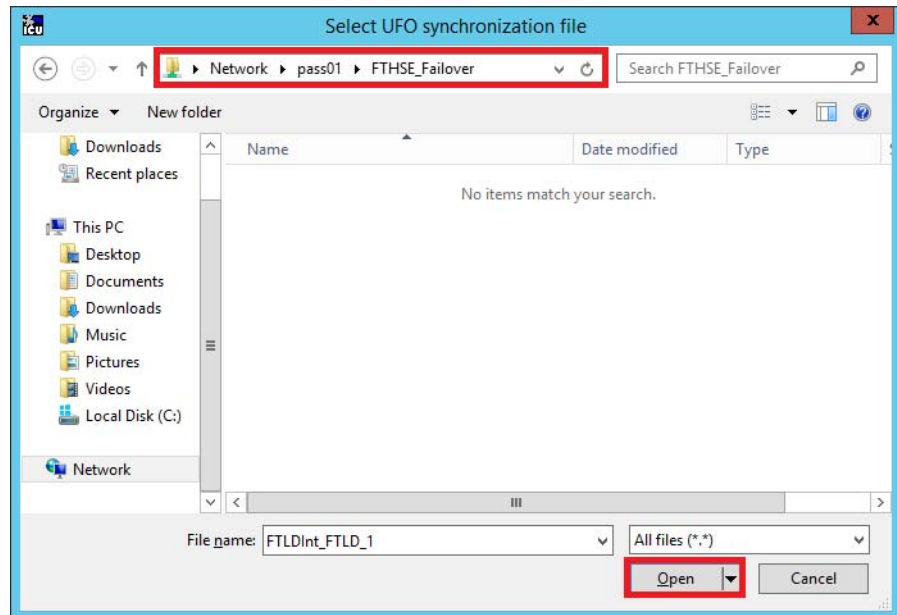
10. Select Failover from the list on the left.



11. Check 'Enable UniInt Failover'.
12. Check 'Phase 2'.

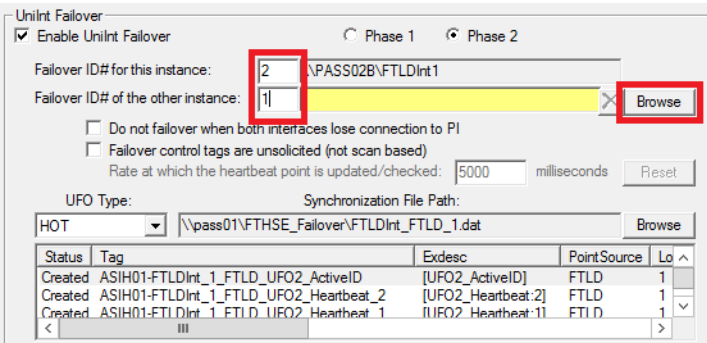


13. From the UFO Type pull-down list, choose HOT.
14. Click Browse to search for the UFO synchronization File Path.
15. Navigate to the Network>pass01>FTHSE_Failover directory and click Open.

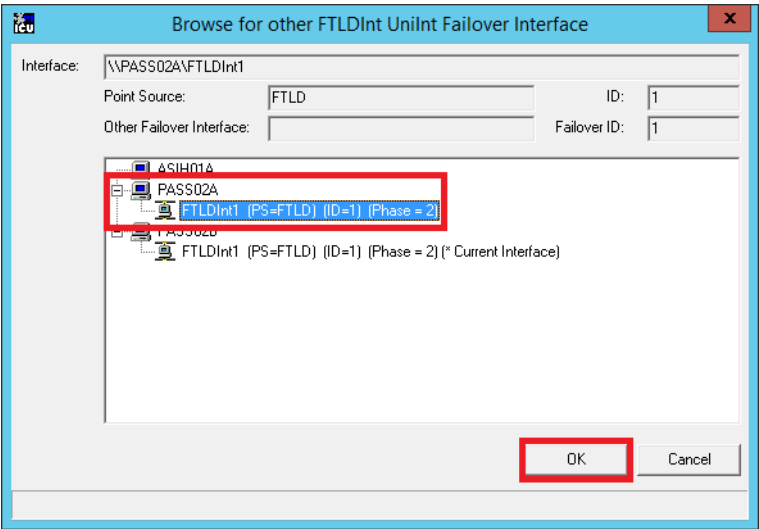


The Select UFO synchronization file dialog box closes.

16. Set the Failover IDs as shown in the following image.

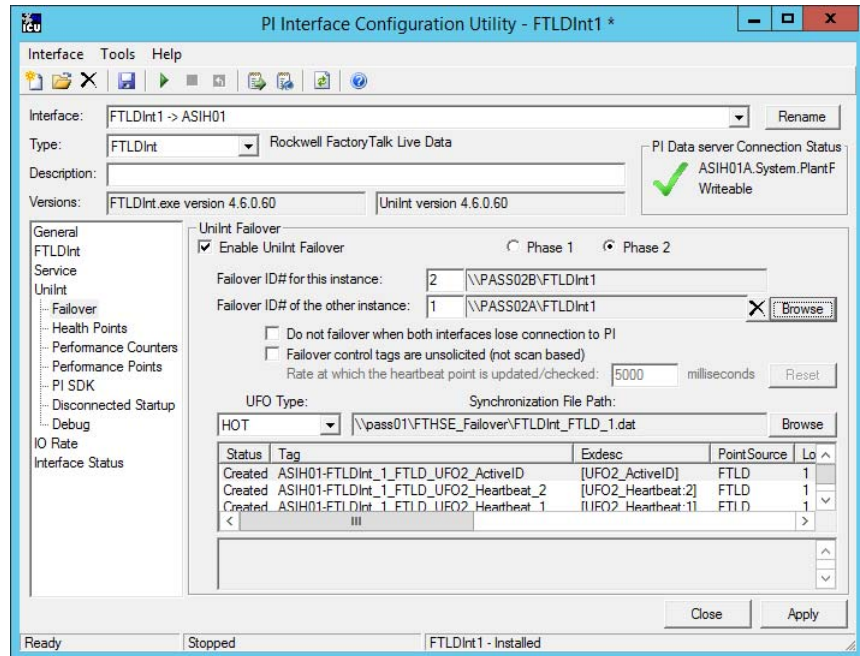


17. Click Browse to search for the secondary instance.
18. Select FTLDDInt1 (under PASS02A in the example) and click OK.



- A synchronize UFO settings popup window appears.
19. Click Yes to synchronize the UFO settings for this instance.

The failover and synchronization information appears in the respective fields.



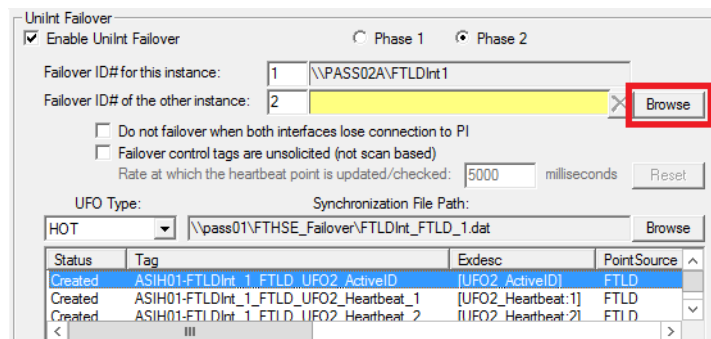
Use a PASS server with these procedures.



PASS02A

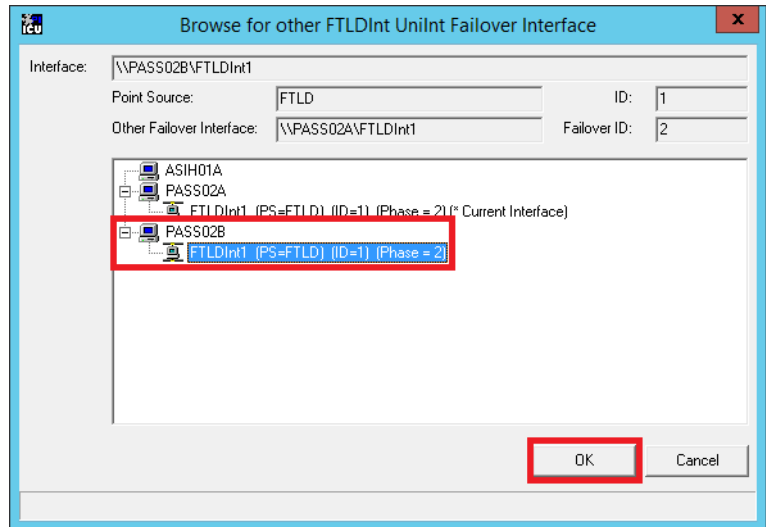
Return to the primary server for the following steps.

1. In the PI Interface Configuration Utility window, click Apply.
2. In the PI Interface Configuration Utility window, click Browse.

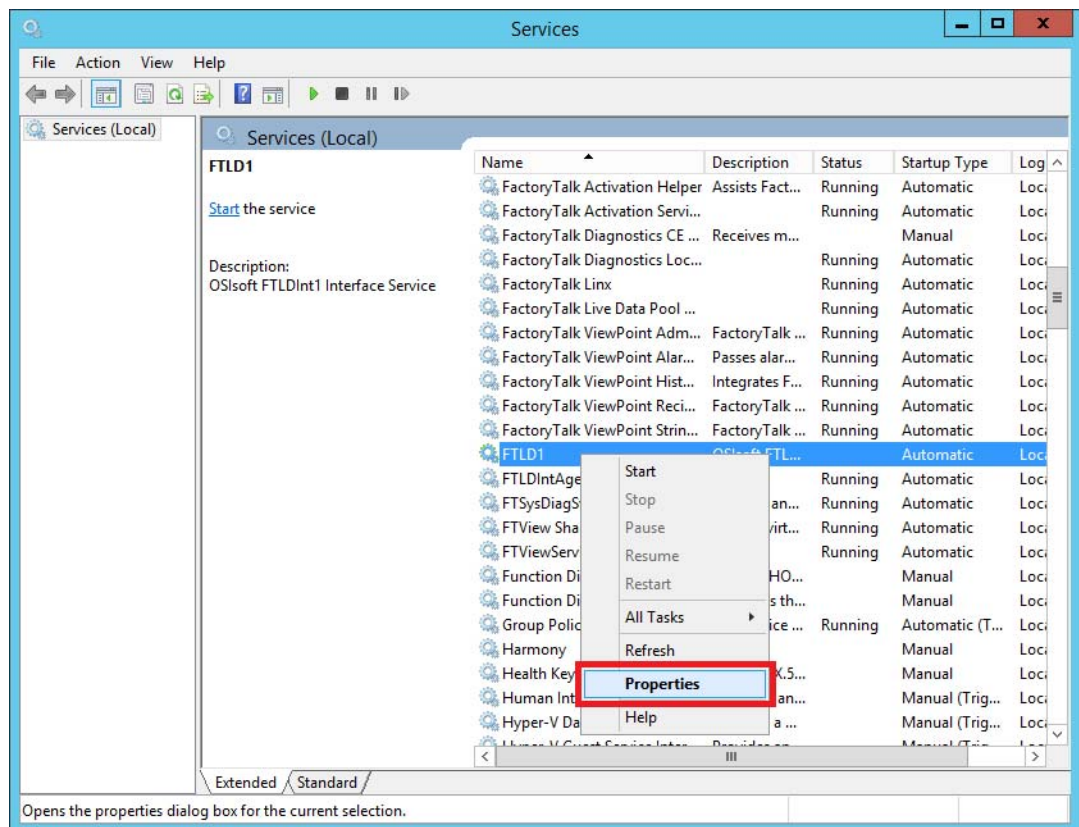


The Browse for other FTLDInt IniInt Failover Interface dialog box appears.

3. Select the 'FTLDInt1 (PS=FTLD) (ID=1) (Phase=2)' line under PASS02B and click OK.

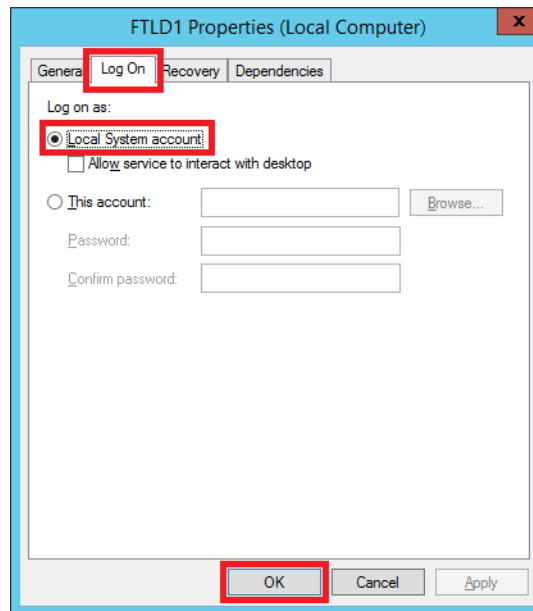


4. Click the Programs >> symbol and choose Administration Tools>Service.

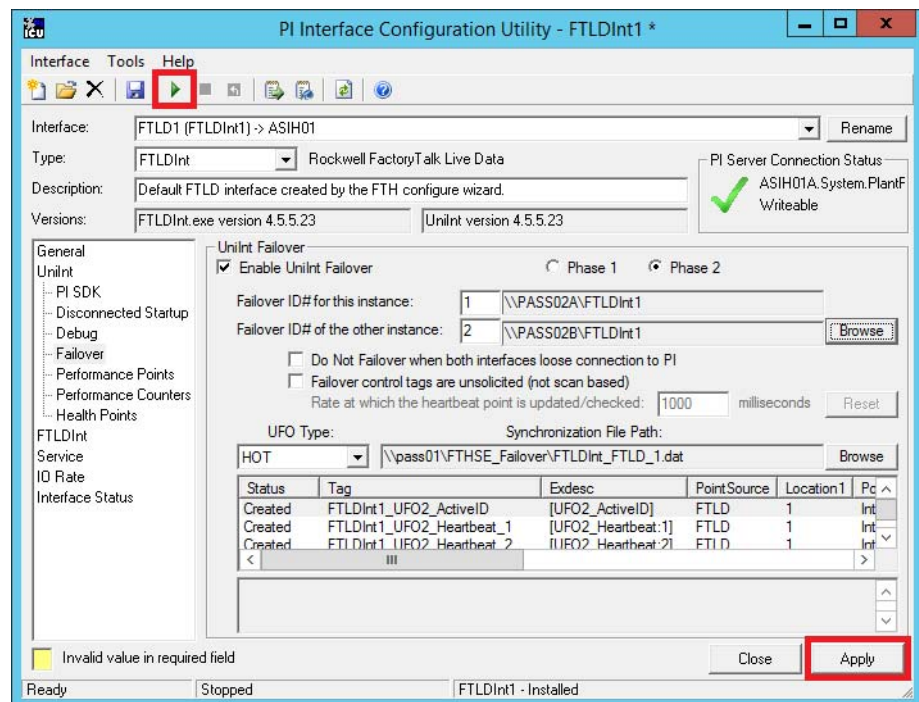


5. Right-click FTLD1 and choose Properties

6. From the Log On tab, click “local System account” and click OK.



7. In the PI Interface Configuration Utility window, click Apply and then Play ► to start the primary service (if not already running).




8. If asked 'Would you like ICU to start this service for you?', click Yes.

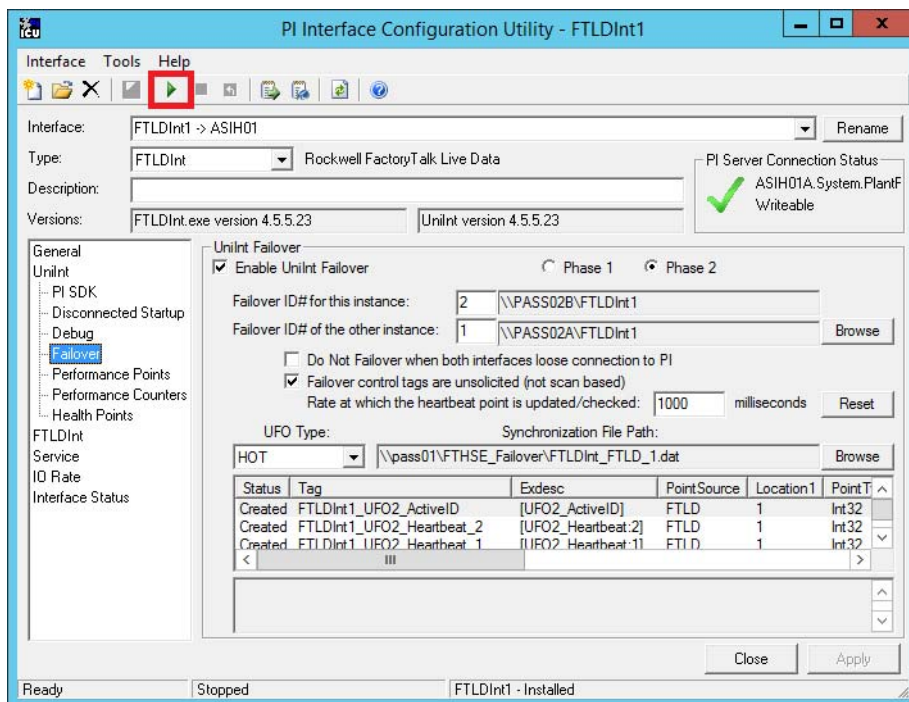
Return to the secondary server for the following steps.

Use a PASS server with these procedures.




PASS02B

1. Select the Interface that is shown in the following image and click Play  to start the secondary service.



2. If asked 'Would you like ICU to start this service for you?', click Yes.

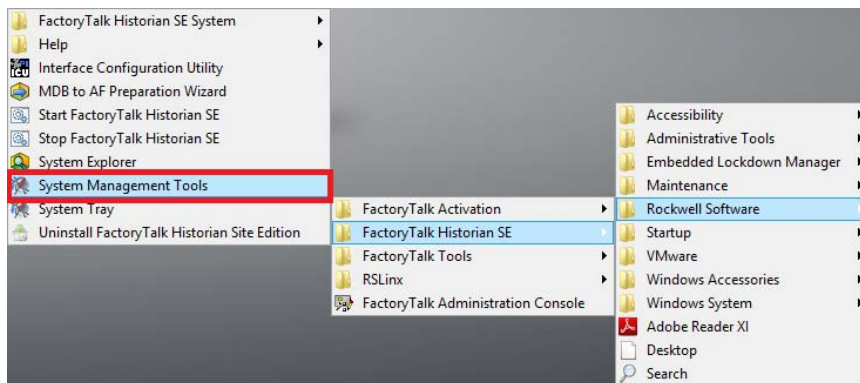
Confirm Unit Failover Diagnostics

1. In the Windows desktop, click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>System Management Tools.

Use an AppServ-Info server with these procedures.

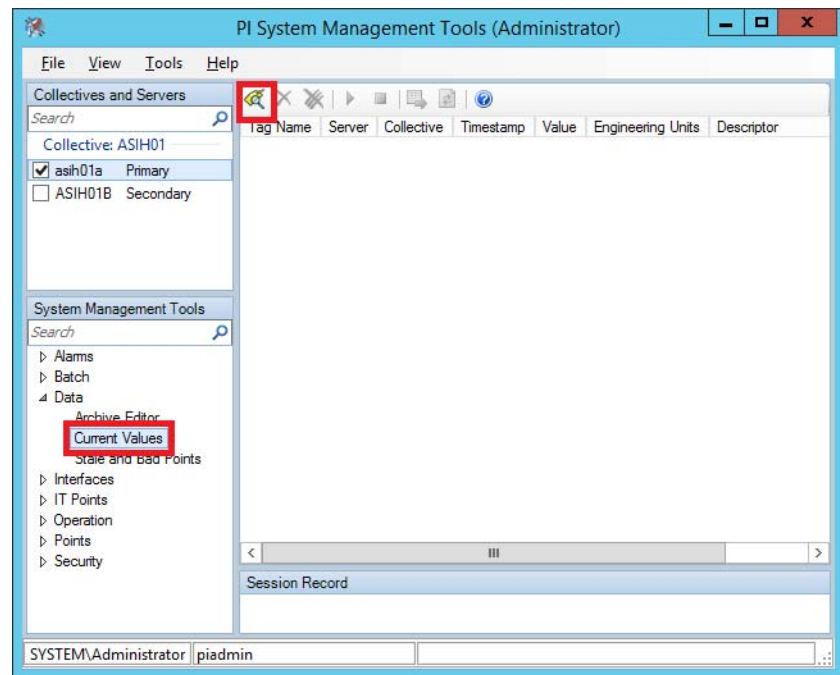


ASIH01A



The PI System Management Tools (Administrator) window appears.

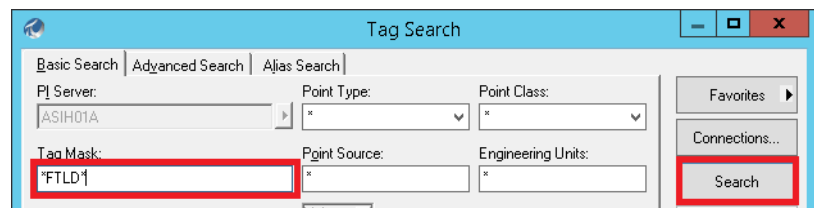
2. Click Data>Current Values.



3. Click the Tag Search  icon.

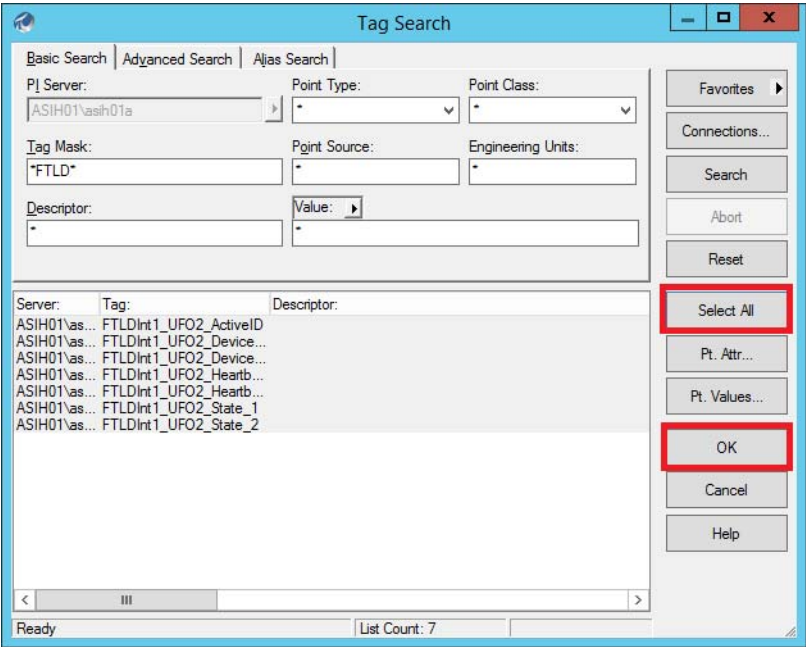
The Tag Search window appears.

4. Type *FTLD* in the Tag Mask and click Search.



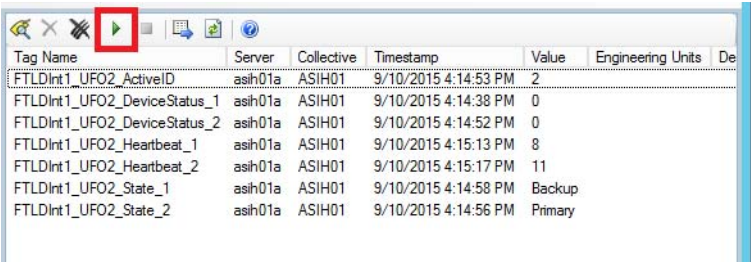
All *FTLD* tags are displayed.

5. Click Select All and OK.



The Tag Search window closes and all *FTLD* tags are displayed in the Current Values - PI System Management Tools (Administrator) window along with their values.

6. If desired, click Play ▶ to see the online status.



IMPORTANT We recommend that you use PerfMon for all computers and proceed to [Configure Performance Monitor Interface on page 373](#).
If your system does not require this option, proceed to [page 396](#) to configure FactoryTalk Historian connectivity.

Configure Performance Monitor Interface

The Windows Performance Monitor (PerfMon) interface provides continuous monitoring of historical data to evaluate the performance of a computer. The 'PI' preface is the name of the OSISoft product.

Use a Domain controller with these procedures.



PADCA

Create PIPerfMon System User

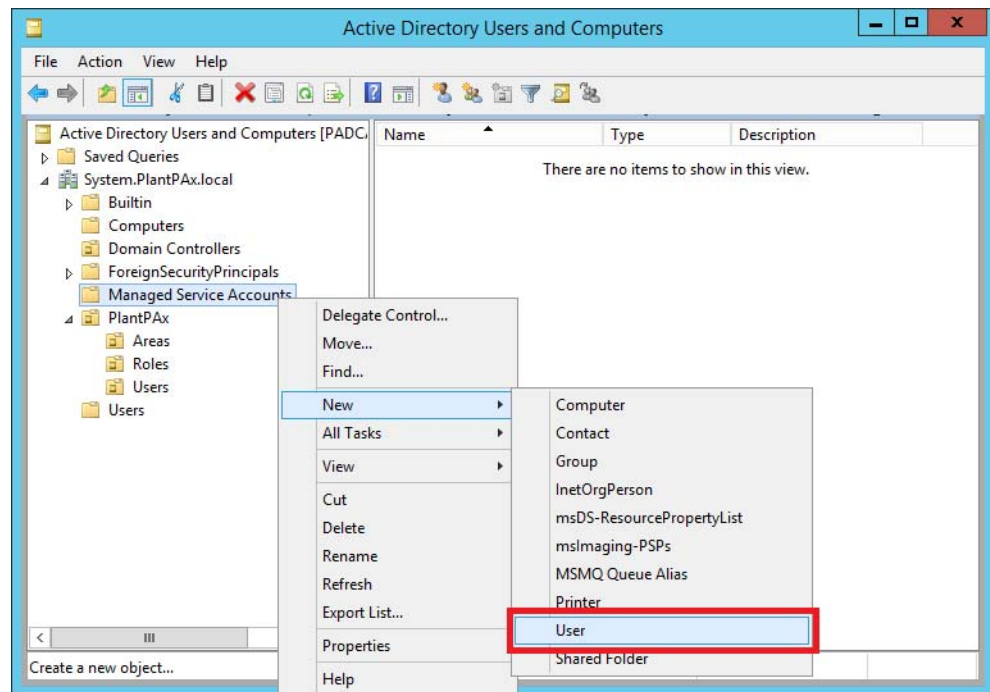
You must create a user that is actually a service to have privileges within other computers on your system. This 'user' permits the system to access computers to obtain data for a performance capture.

Complete these steps.

1. From the Server Manager, click Tools and choose Active Directory Users and Computers.

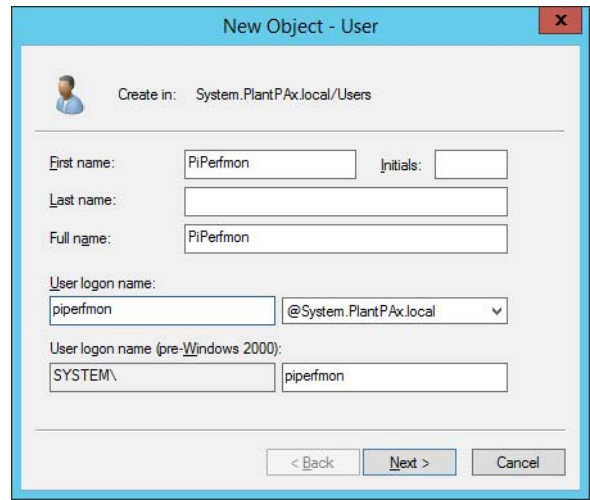
The Active Directory Users and Computers dialog box appears.

2. Expand the domain folder (System.PlantPAx.local).



3. Right-click Managed Service Accounts and choose New>User.

The New Object - User dialog box appears.



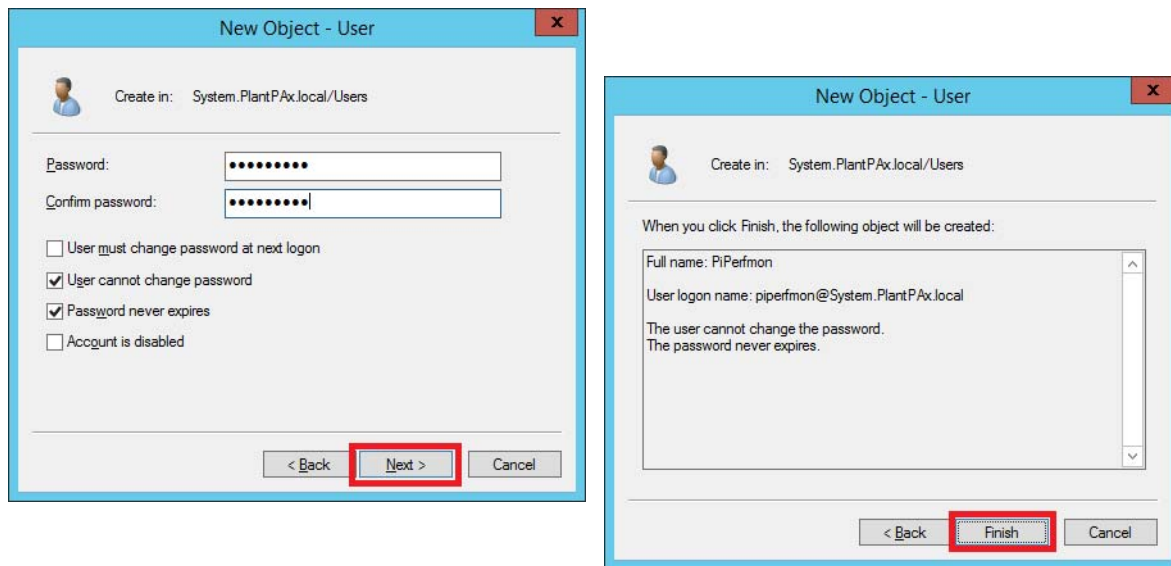
4. Complete the User text boxes.

Item	Description
First name	Type a name for the PI PerfMon service. IMPORTANT: The 'PI' preface is the name of the OSISoft product.
Initials	Optional; you can leave blank.
Full name	Type the same name for the PI PerfMon service.
User login name	Type the same name for the PI PerfMon service and click the pull-down to select your domain folder.
User logon name (pre-Windows 2000)	Use the SYSTEM\ default and type the same name for the PI PerfMon service.

IMPORTANT The logon password creates a service user, not a person. The service user grants access to system computers for placing data into memory (buffer).

5. Click Next.

6. Type your password twice, and make sure that there is a check mark in the following boxes:
- User cannot change password
 - Password never expires (indefinite service for system access)



7. Click Next and then click Finish.

Configure the PIPerfMon Interface

Use an AppServ-Info server that has the interface with these procedures.




ASIHO1

You must enter an interface name and a points value. The points are the limit the interface uses based on the number of computers in your system. Each variable – CPU usage, RAM, disk space – is one point. You can use the number of points up to 20% of your FactoryTalk Historian SE software license.

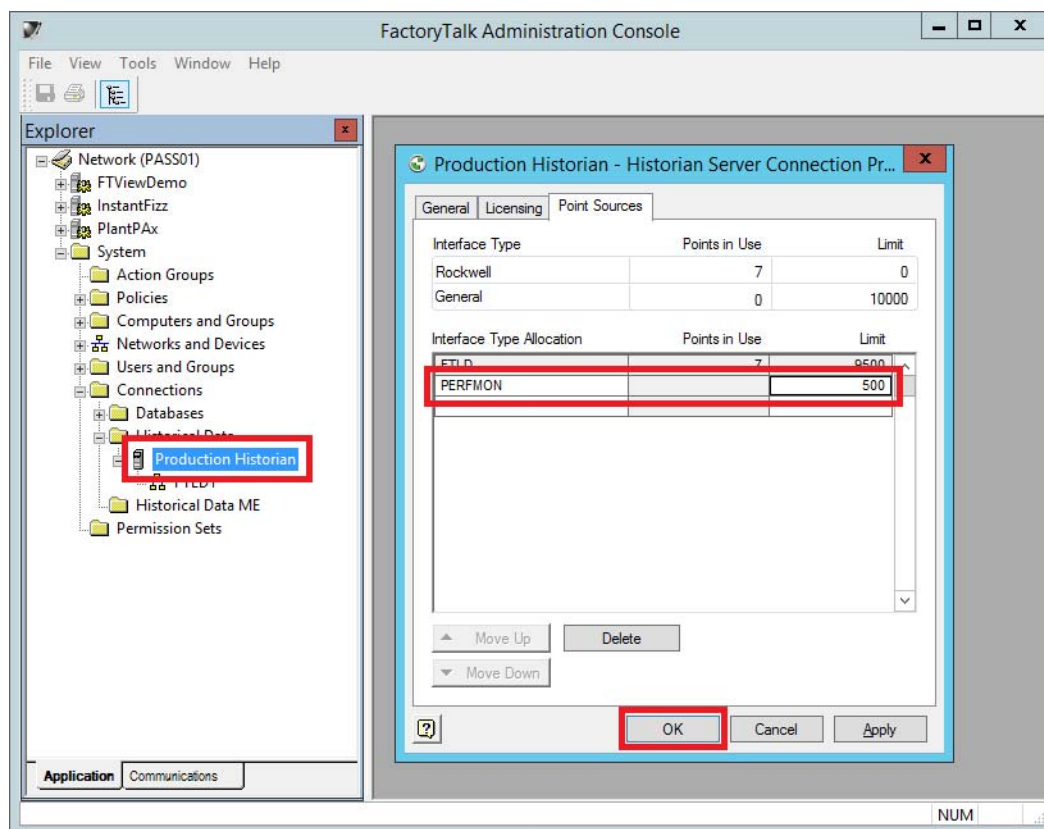
Assign the License

Complete these steps to assign the interface license.



1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Administration Console.
2. Select Network and click OK.

3. Expand the System>Connections>Historical Data folders and right-click Production Historian.
4. Select Properties.




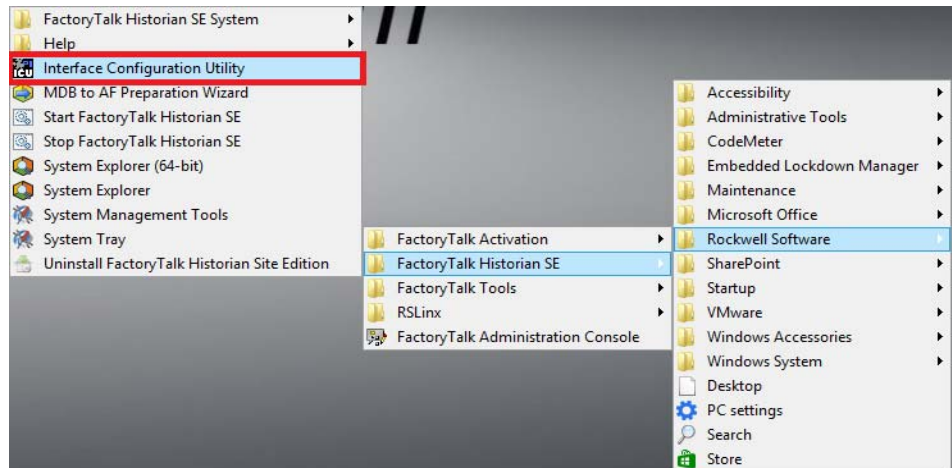
IMPORTANT Be patient because this dialog box could take a few minutes to appear.

5. On the Point Sources tab, type an interface name (such as PerfMon) and a value for the points limit.
The value is the expected number of performance points in the system.
6. Click OK.
7. Close the FactoryTalk Administration Console.

Configure the Interface Utility

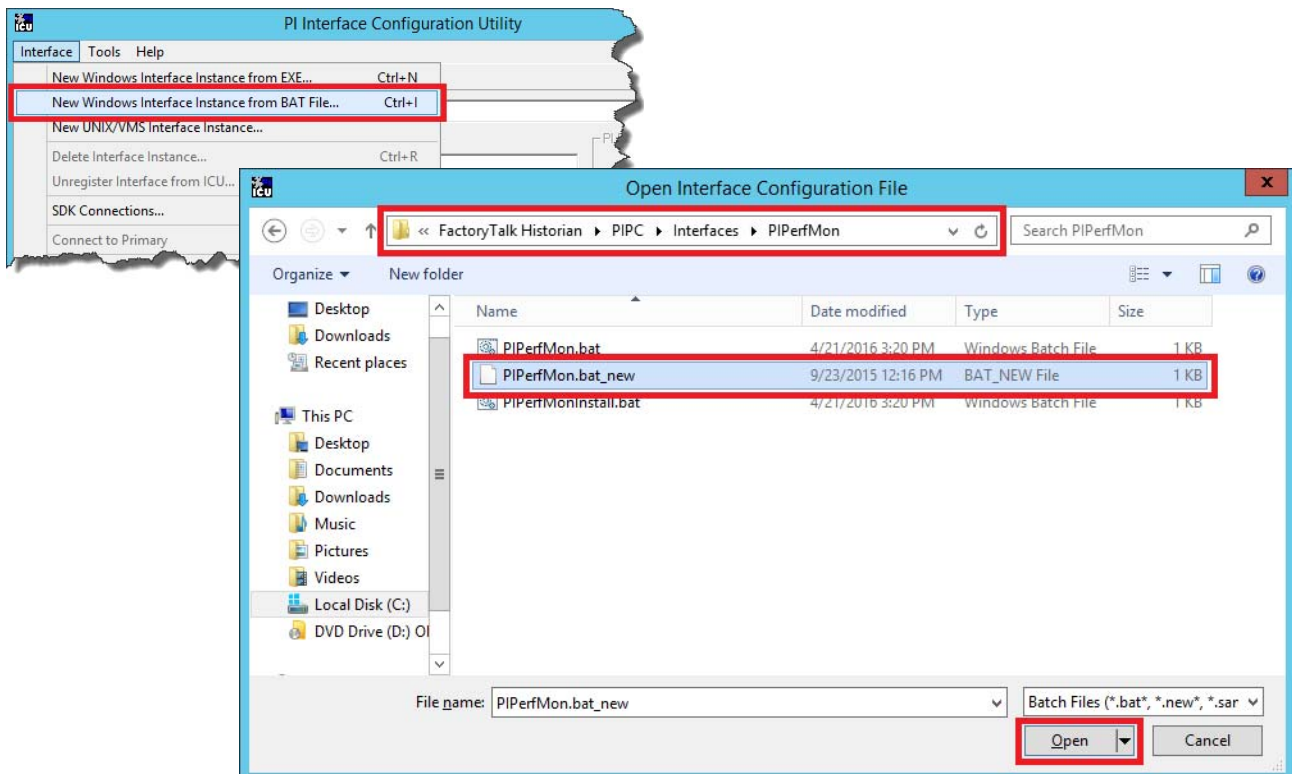
Complete these steps to configure the PIPerfMon interface.

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>Interface Configuration Utility.

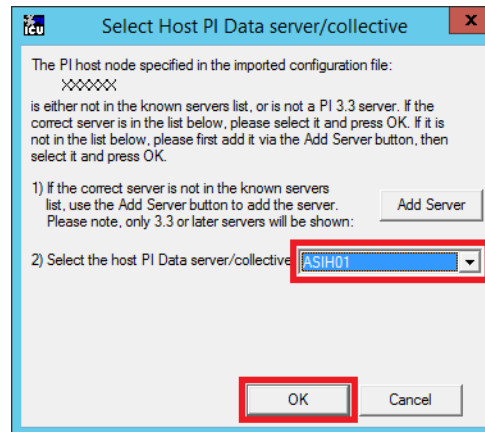


The Interface Configuration Utility dialog box appears.

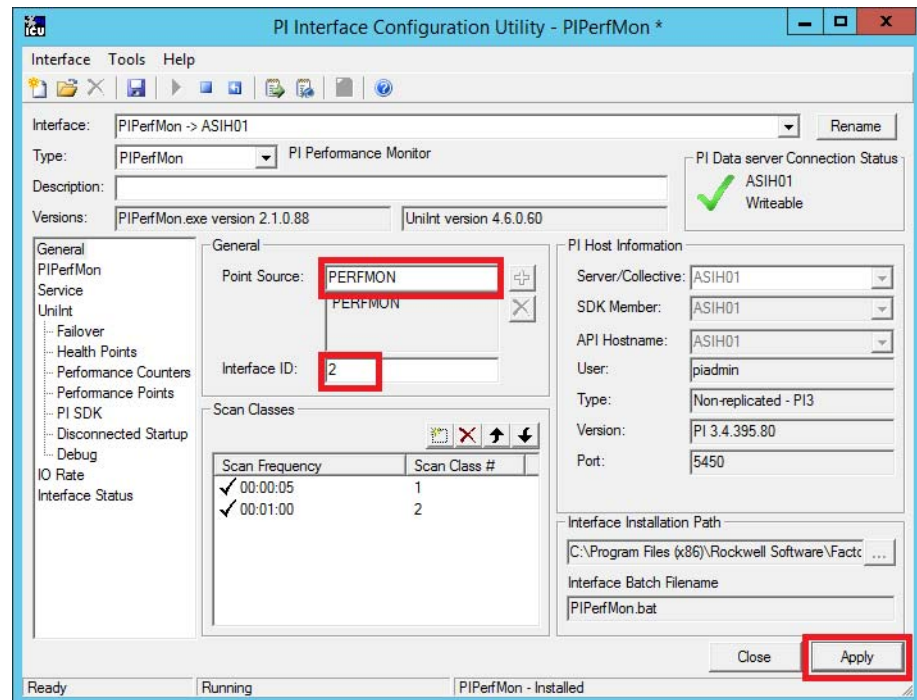
2. Choose New Windows Interface Instance from BAT file from the Interface menu.
3. Select the PiPerMon.bat_new file under FactoryTalk Historian/PIPC/Interfaces/PIPerfMon.



4. Click Open.
5. Select the FactoryTalk Historian server and click OK.



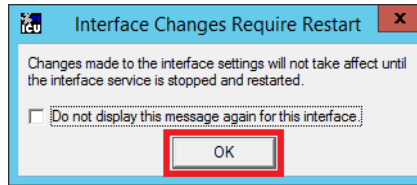
6. Type a Point Source name and an Interface ID number.



IMPORTANT The Point Source name **must** match the interface name that you typed in the Historian Production dialog box on [page 376](#). The Interface ID number must be unique in the system.

7. Click Apply.

8. Click OK to restart the interface service.




Import PIPerfMon Digital State

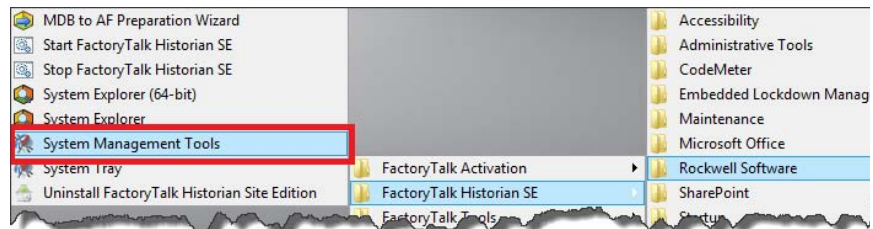
Use these procedures with an AppServ-Info server or an Engineering Workstation that has FactoryTalk Historian installed.



Complete these steps to import digital sets and states for the Performance Monitor service. Digital states create a relationship between values and text state names.

For example, 0 = Good, confirmed good quality; 1 = Good, assumed good quality.

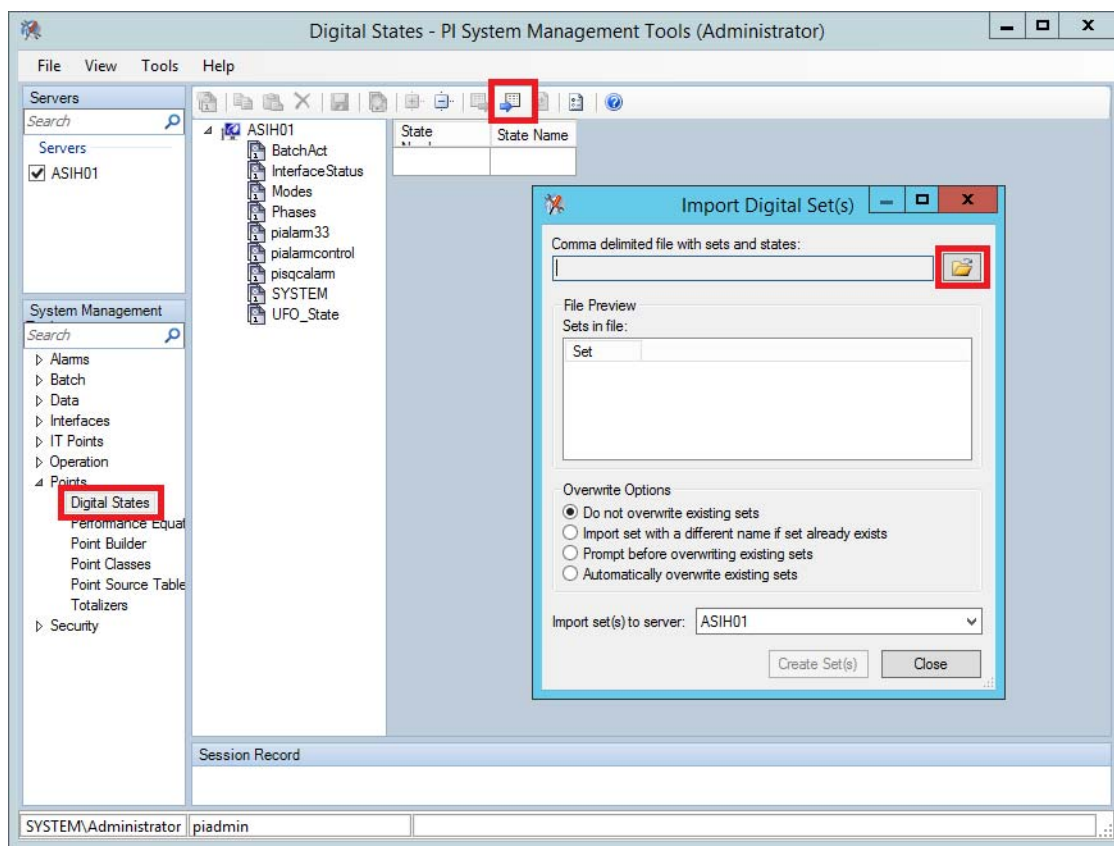
1. Open the Historian folder by clicking the Program button  and choosing Rockwell Software>FactoryTalk Historian SE>System Management Tools.



The Digital States - PI System Management Tools dialog box appears.

2. Under Servers, select the server that is being configured for the PIPerfMon interface.

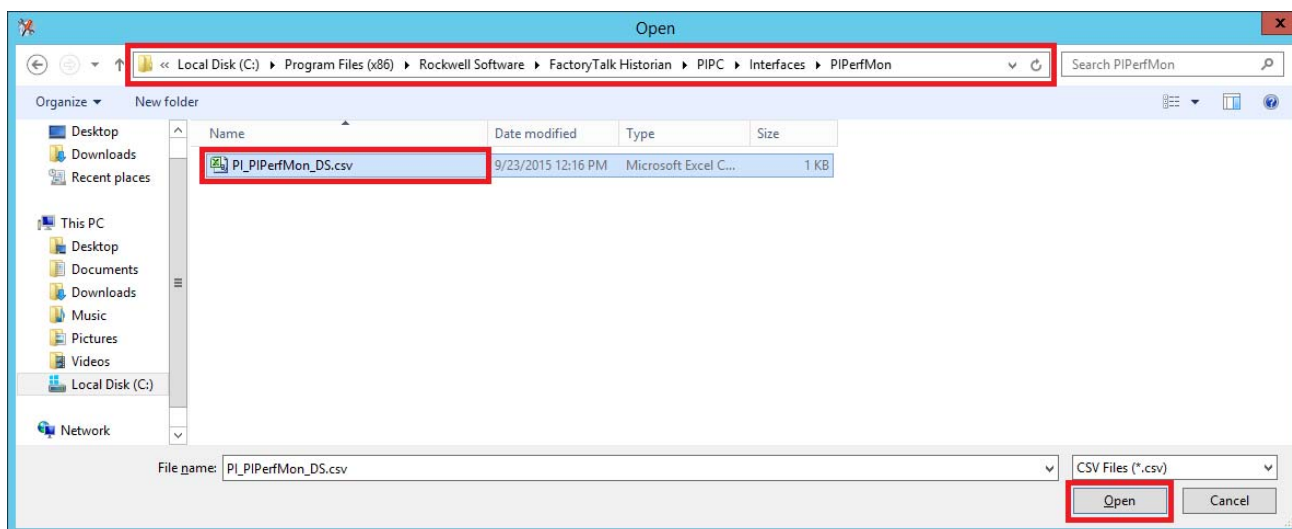
3. Under Points, open Digital States and click the Import button.



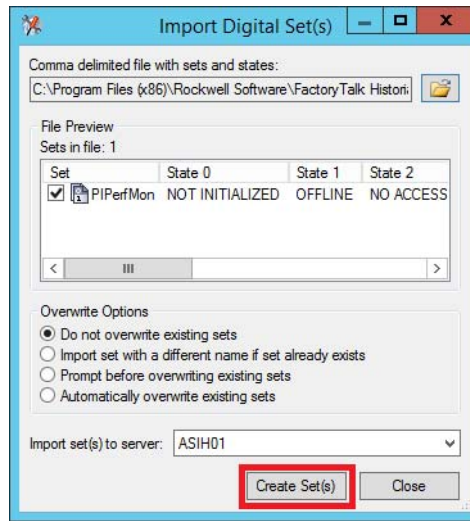
4. From the Import Digital Set(s) dialog box, click the folder icon.

5. Navigate to C:\Program Files (x86)\Rockwell Software\FactoryTalk Historian\PIPC\Interfaces\PIPerfMon

6. Select the PI_PIPerfmon_DS.csv and click Open.



7. Click Create Set(s).



8. Click Close.


Create PIPerfMon Interface Health Points

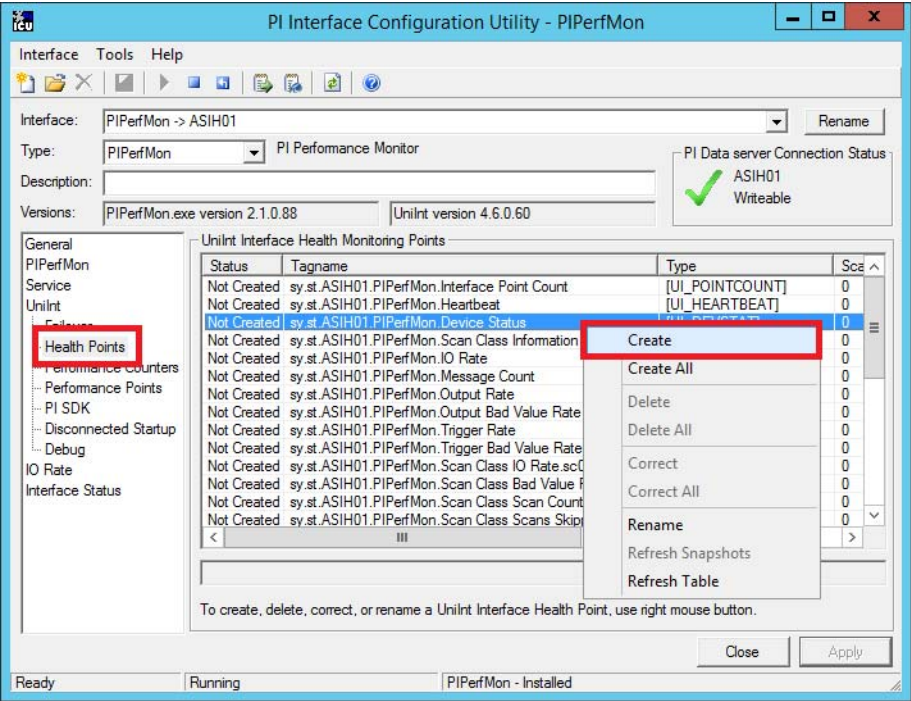
Use an AppServ-Info server that has the interface with these procedures.



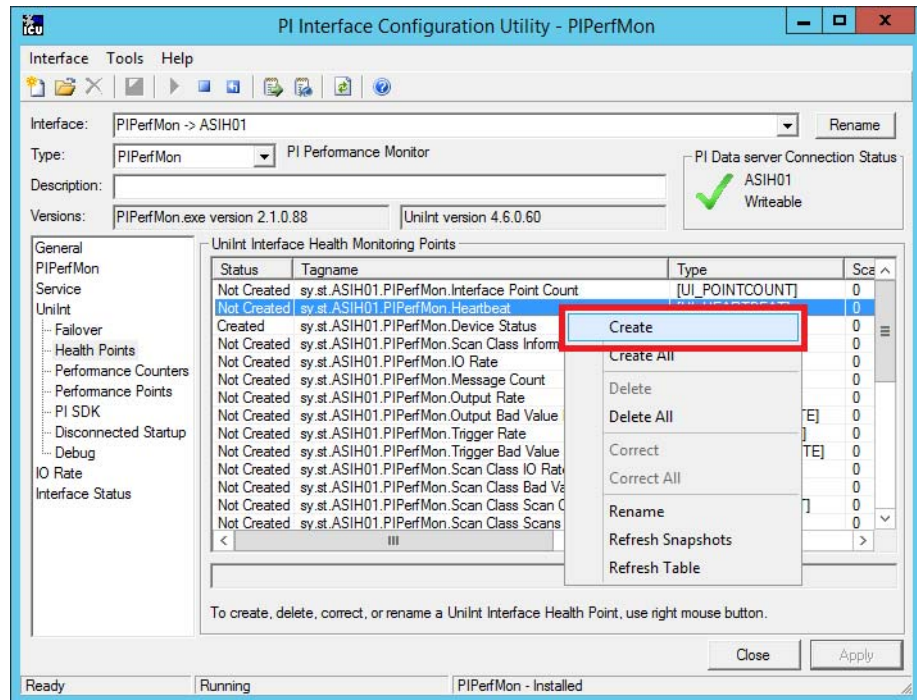
ASIH01

Complete these steps to associate the PerfMon interface with the health tags that monitor a device heartbeat for diagnostics. The heartbeat count determines if the system is working. If there is a stoppage, you can analyze what prompted the fault or device error.

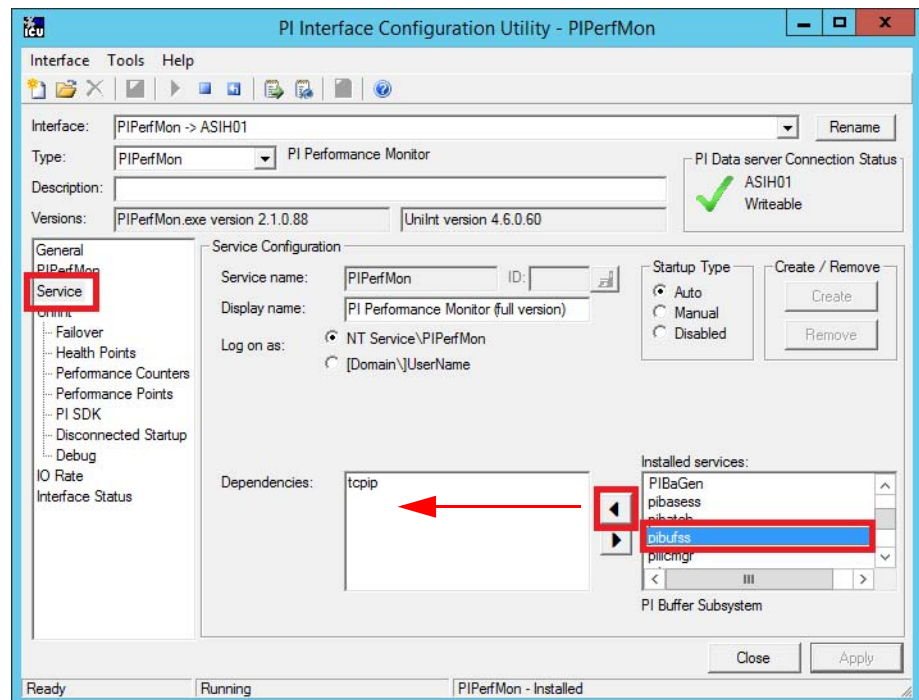
1. Click the Program button  and choose Rockwell Software>FactoryTalk Historian SE>Interface Configuration Utility.
2. From the Interface pull-down, select PIPerfMon.
3. From Health Points on the left, right-click PIPerfMon.DeviceStatus and choose Create.



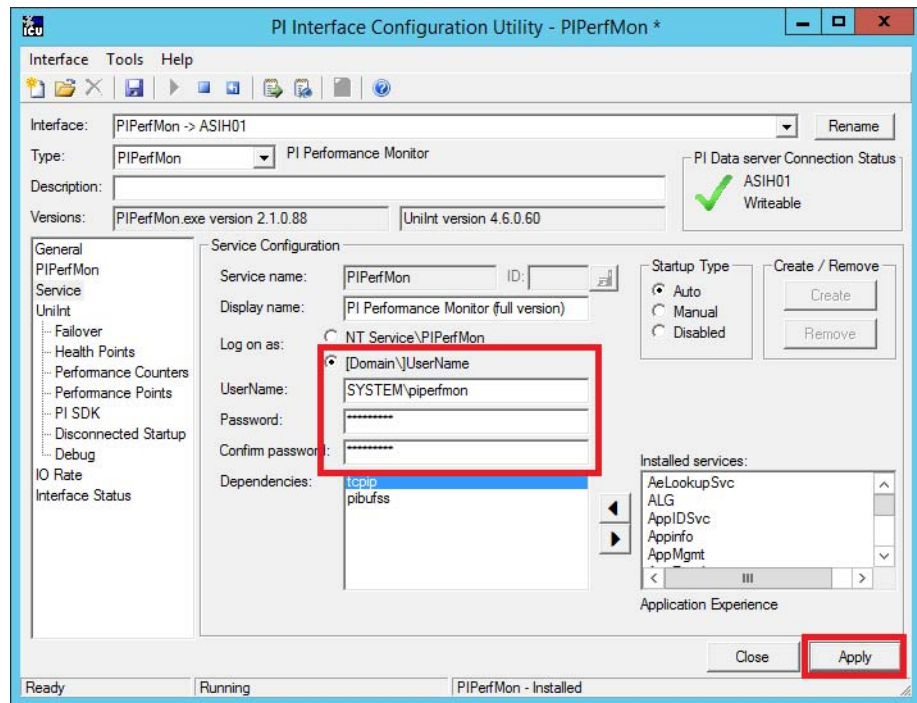
4. Right-click PIPerfMon.Heartbeat and choose Create.



5. Under Service, choose pibufss and click the left arrow to move to the Dependencies box.

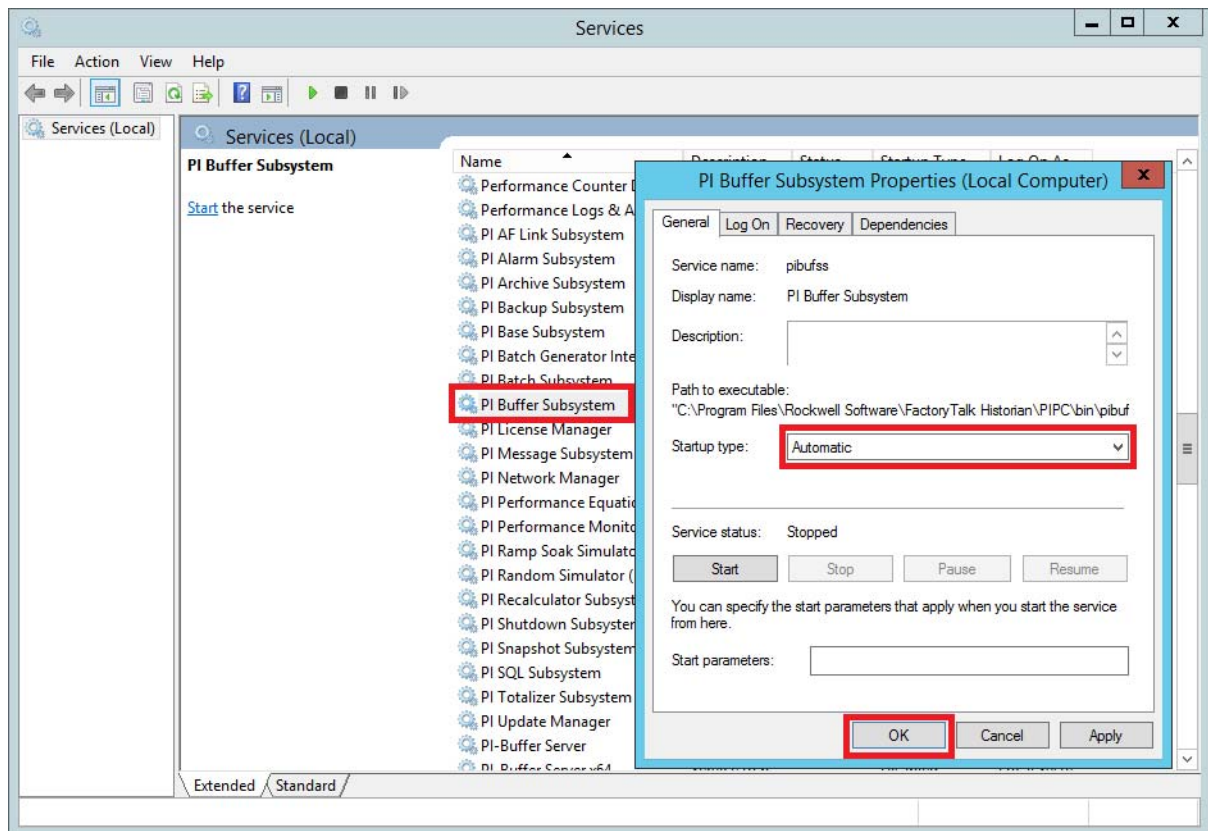


6. Type the same user name and password that you initially created for the service. See [page 374](#).

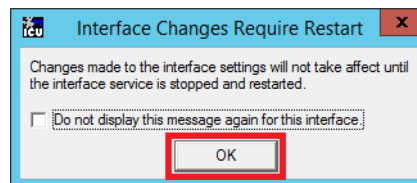


7. Click Apply.

8. Open Services, right-click PI Buffer Subsystem, and select 'Automatic' as the Startup type.

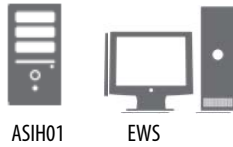


9. Click OK.
10. To restart the interface service, click OK.




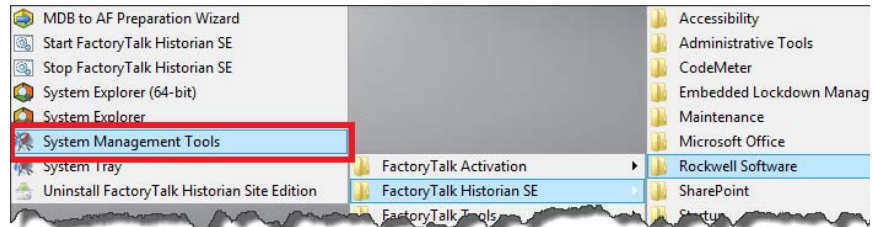
Monitor PIPerfMon Interface

Use these procedures with an AppServ-Info server or an Engineering Workstation that has FactoryTalk Historian installed.



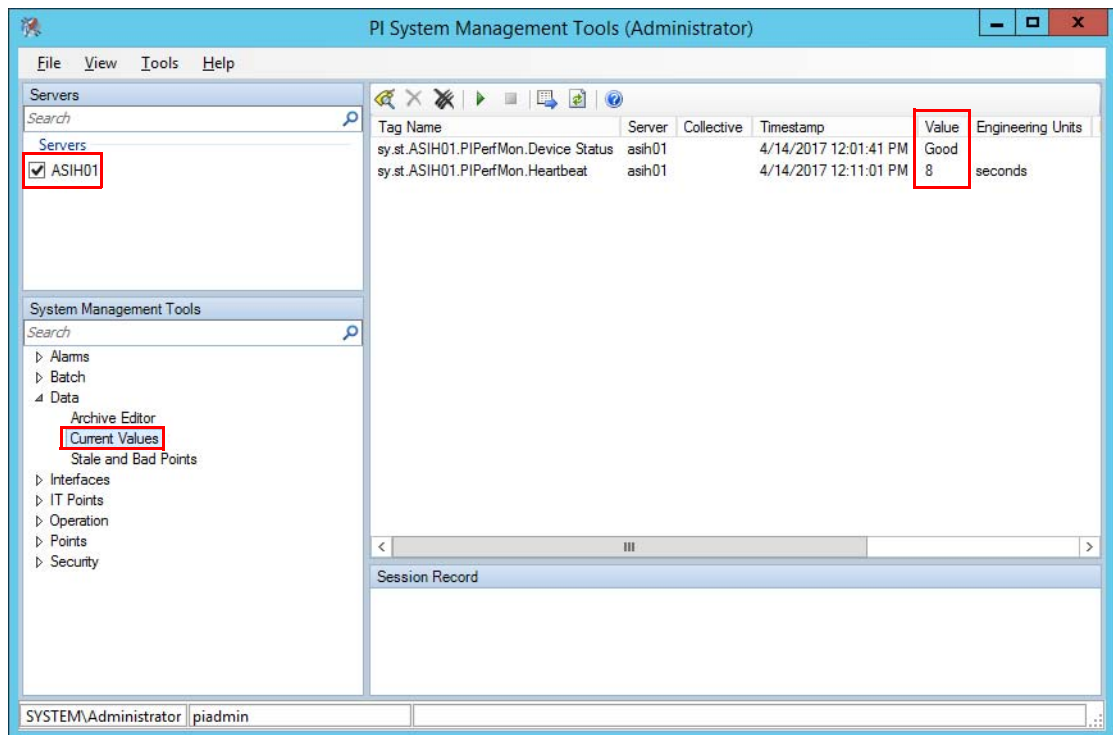
Complete these steps to verify that the interface has a good working status.

1. Click the Program button  and choosing Rockwell Software>FactoryTalk Historian SE>System Management Tools.



The PI System Management Tools dialog box appears.

2. In left, top pane, search for the appropriate server with the interface.



3. In the lower, left pane, expand the Data folder and click Current Values.

After you search for tags you need, the Value category displays the health state of the interface and the number of seconds between the heartbeat counts.

Enable Performance Monitor

This section describes how to enable PIPerfMon to collect data from system computers.

Perform this procedure in all system computers.



All servers ...



... and workstations

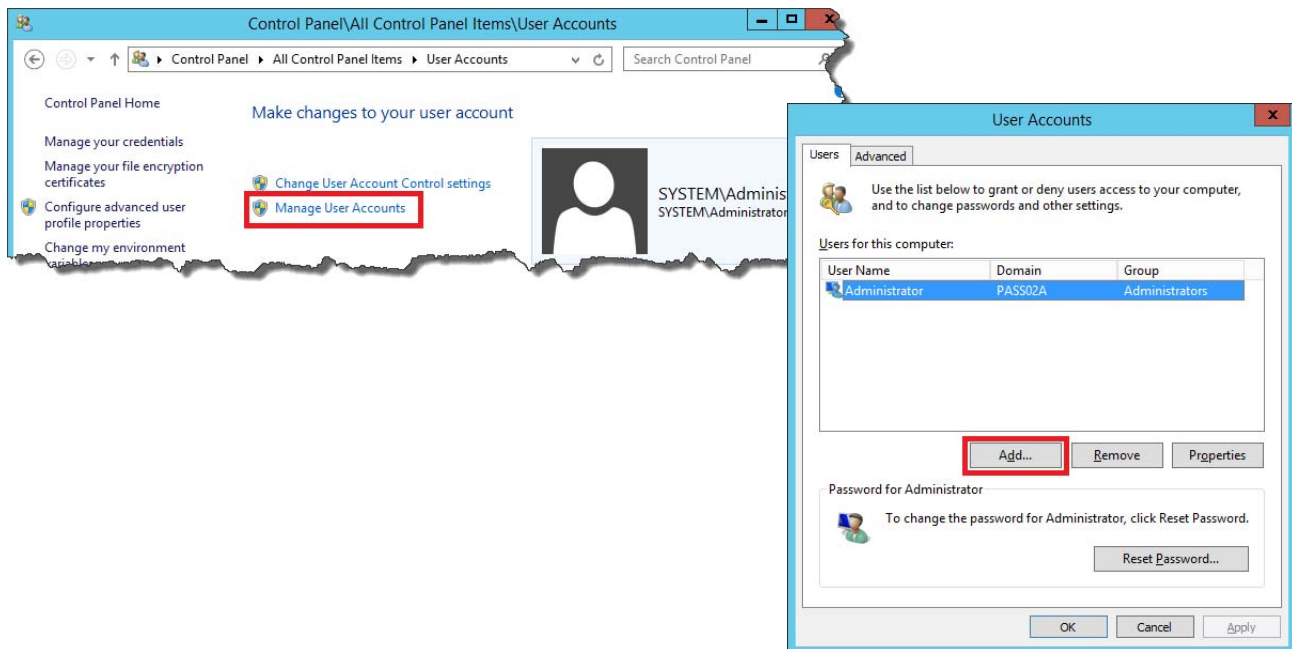
Adding PIPerfMon User

Complete these steps to create a performance monitor user.

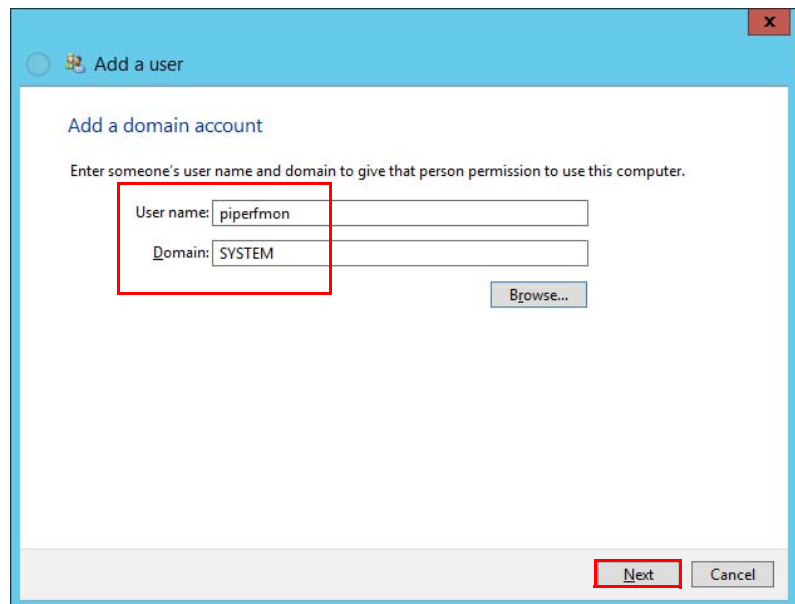
1. Click the Windows  symbol.
2. Click Control Panel and choose User Accounts.



3. Click Manage User Accounts and click Add.

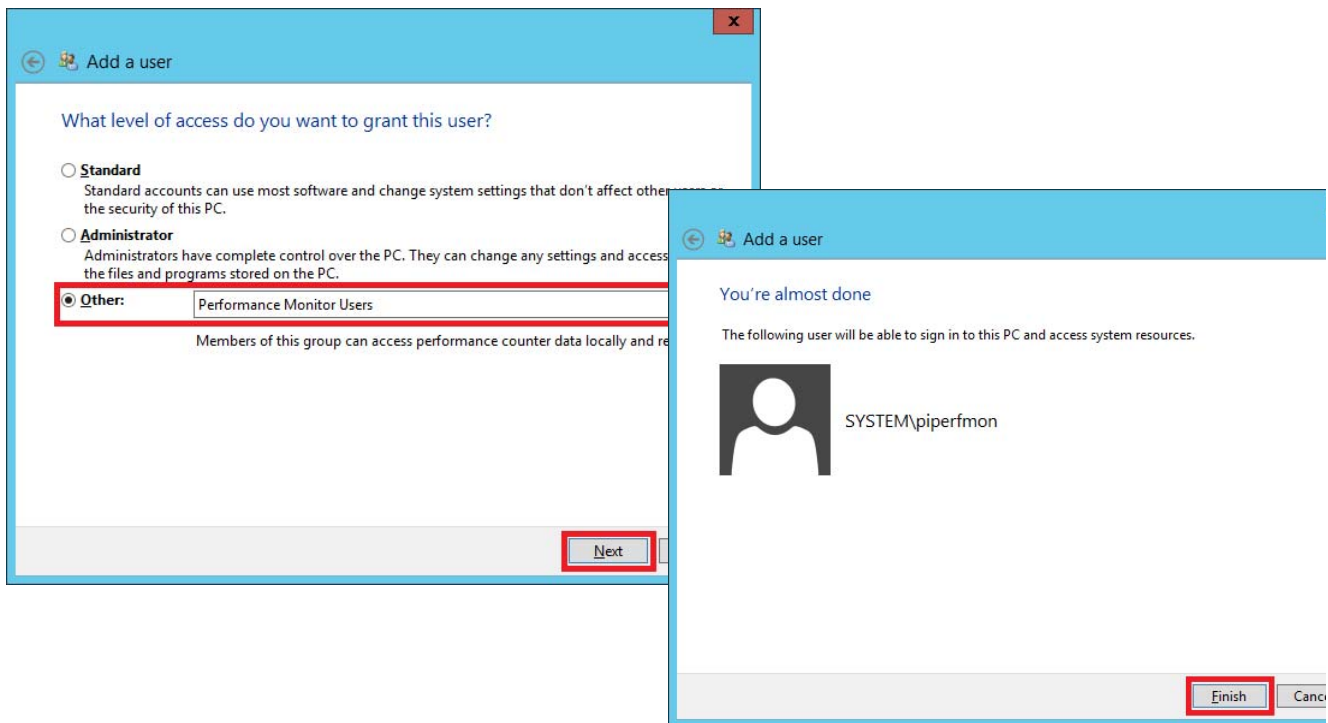


4. Type the same user name and Domain that you did to grant system access for the PerfMon service. See [page 384](#).



5. Click Next.

6. Click Other and choose Performance Monitor Users.




7. Click Next and Finish.

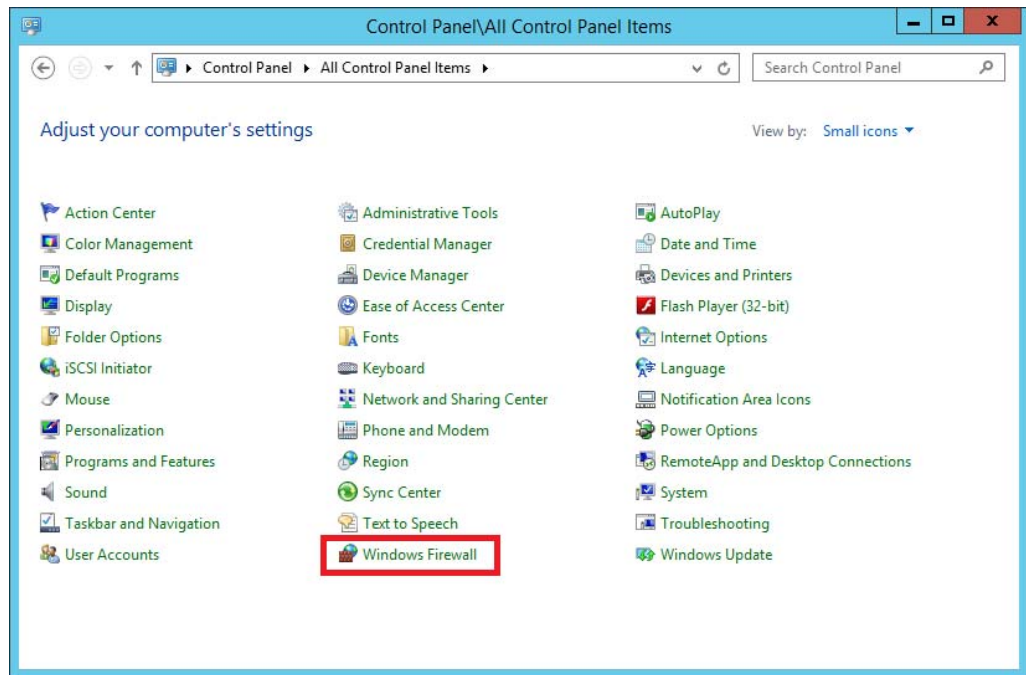
Adding PIPerfMon Firewall Rule

Perform this procedure in all system computers.

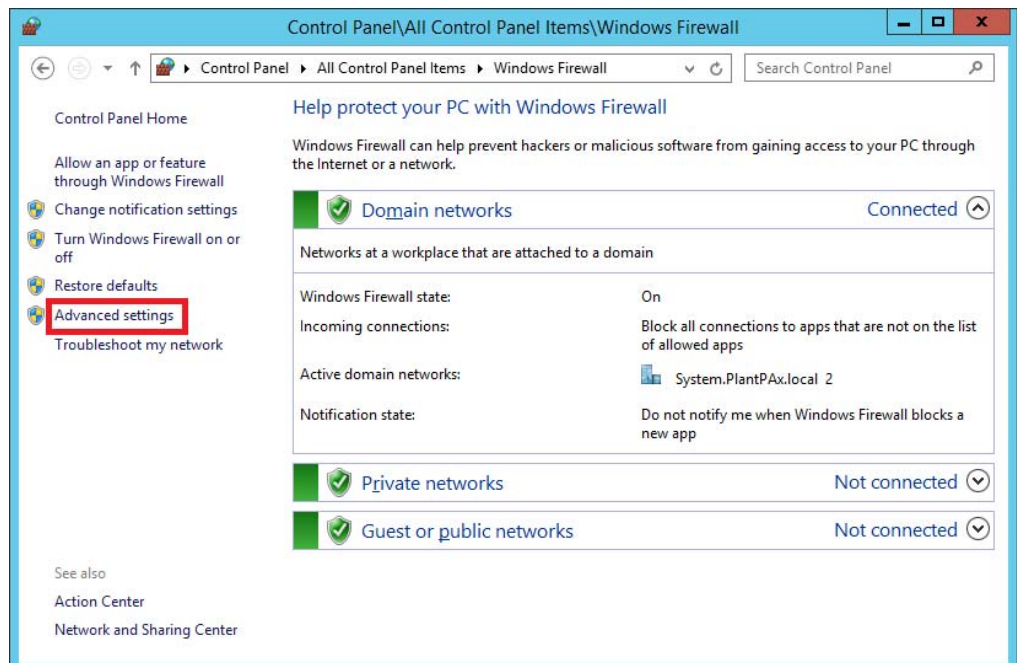


Complete these steps to configure port settings to allow external computer connections to extract system data.

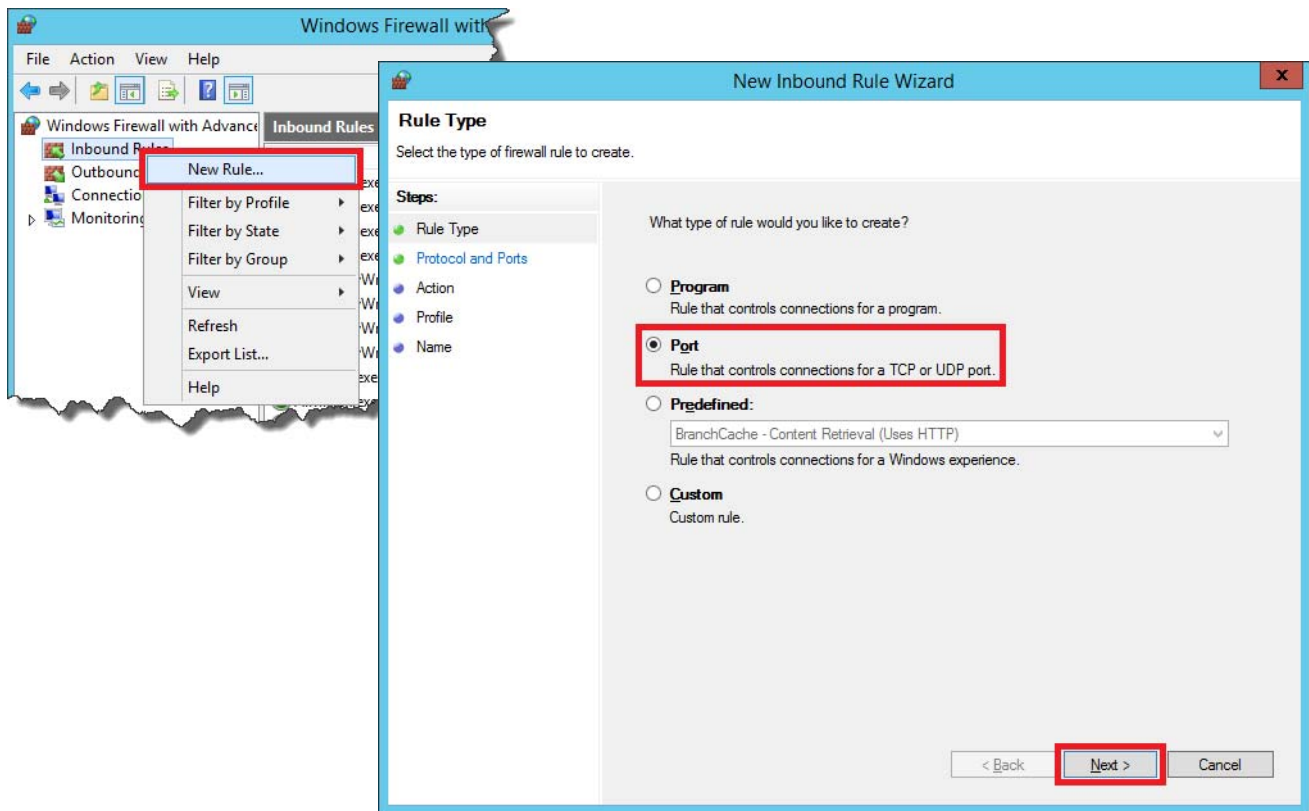
1. Click the Windows  symbol.
2. Click Control Panel and choose Windows Firewall.



3. Click Advanced Settings.



4. Expand the Windows Firewall folder, right-click Inbound Rules, and choose New Rule.
5. Click Port and then click Next.



6. For TCP, click Specific local ports and type 135, 445.

IMPORTANT The two port numbers listed in step 6 **must** be configured to allow system data exchanges with external computers.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a blue title bar and a sidebar on the left with steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains the following options:

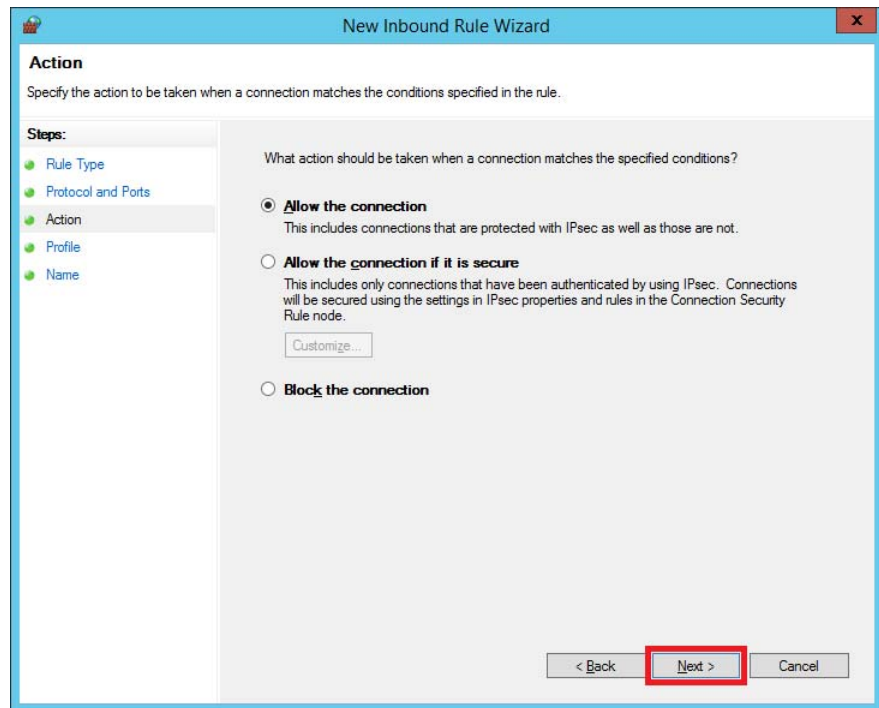
- Does this rule apply to TCP or UDP?
 - ☒ TCP
 - ☐ UDP
- Does this rule apply to all local ports or specific local ports?
 - ☐ All local ports
 - ☒ Specific local ports:

Below the text input field is an example: 'Example: 80, 443, 5000-5010'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

7. Click Next.

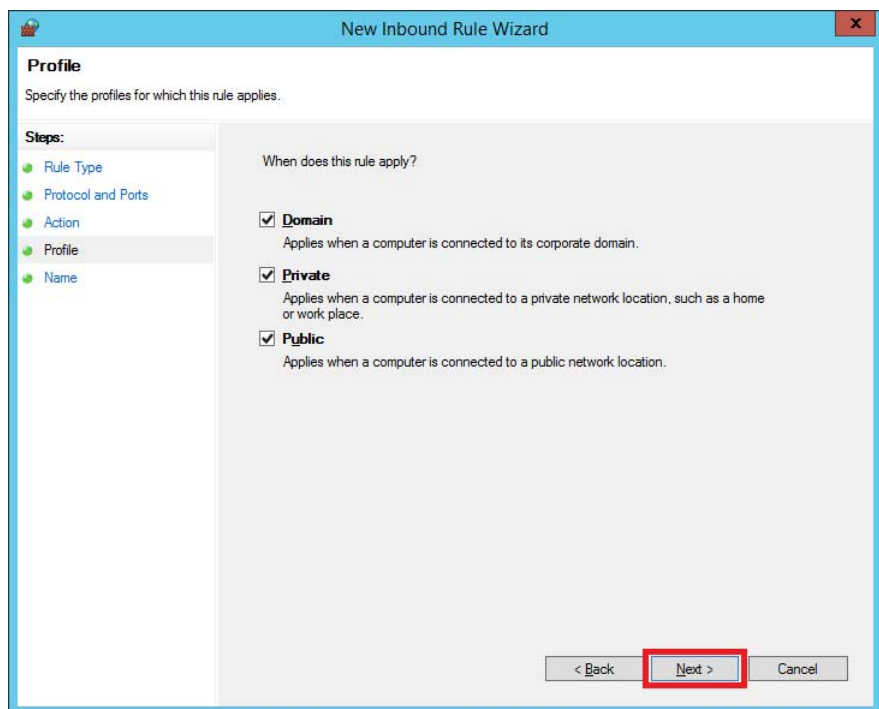
8. Click Next for the Action step.

Do **not** change any settings.



9. Click Next for the Profile step.

Do **not** change any settings.



10. Type a name and click Finish.

The screenshot shows a 'New Inbound Rule Wizard' window. On the left, a 'Steps' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Name' being the current step. The main area is titled 'Name' and contains the instruction 'Specify the name and description of this rule.' Below this, there is a 'Name:' label followed by a text box containing 'Perfmon Connection'. Underneath is a 'Description (optional):' label followed by a larger text box. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red box.

Enabling PIPerfMon Counter Service

Perform this procedure in all system computers.



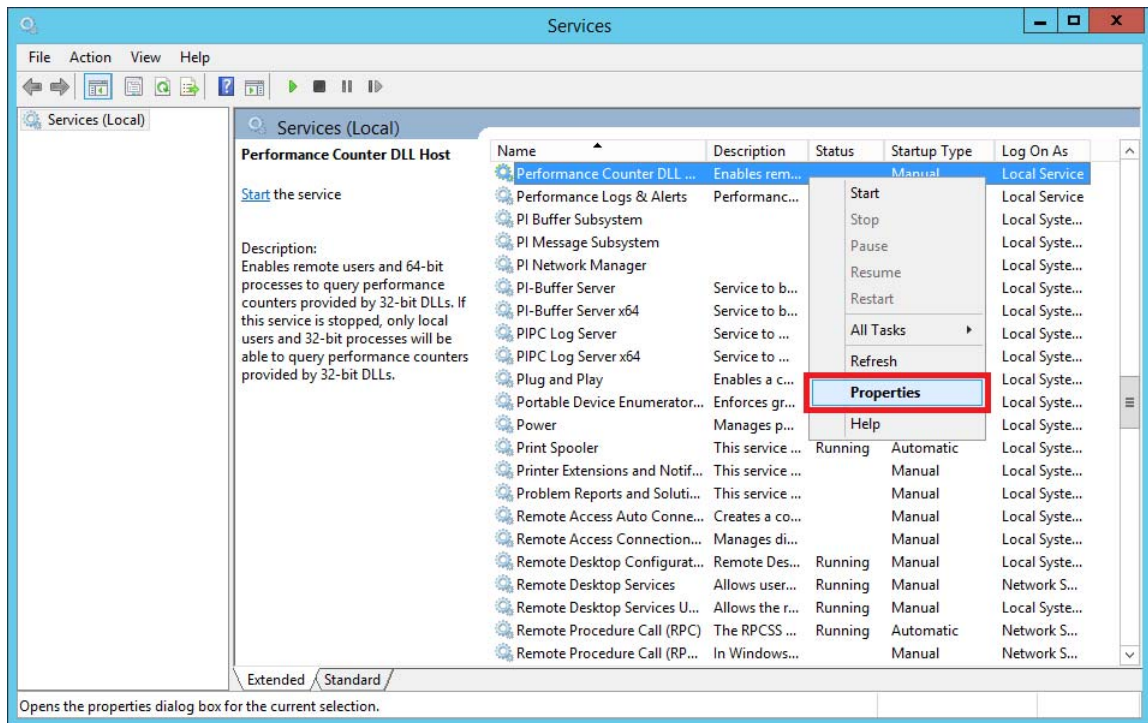
All servers ...



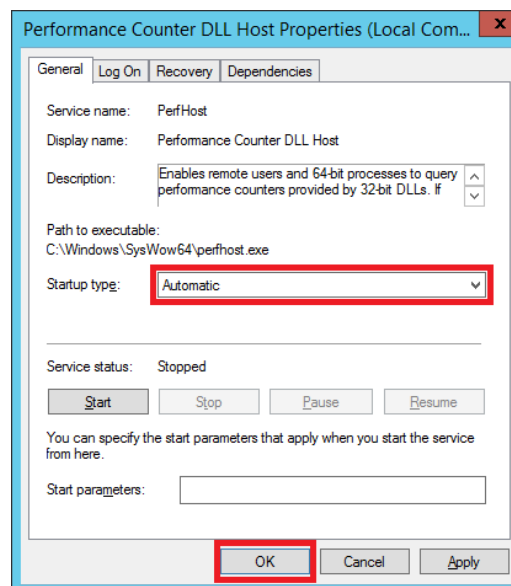
... and workstations

Complete these steps to enable the PIPerfMon service to start collecting information from system computers.

1. From the Start menu, click Programs and choose Administrative Tools>Services.
2. Right-click Performance Counter DLL Host and choose Properties.



3. Select Automatic as the Startup type and click OK.




Configure FactoryTalk Historian Connectivity

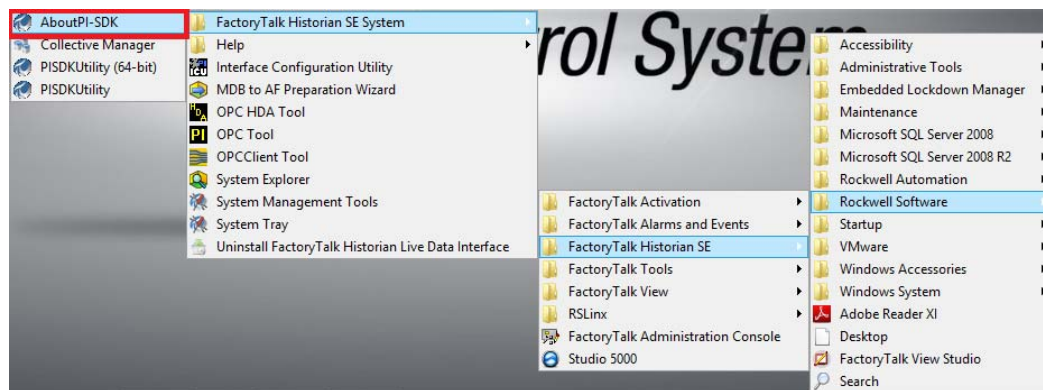
Use all workstations with these procedures.



This section describes how to connect the system elements with the Historian server.

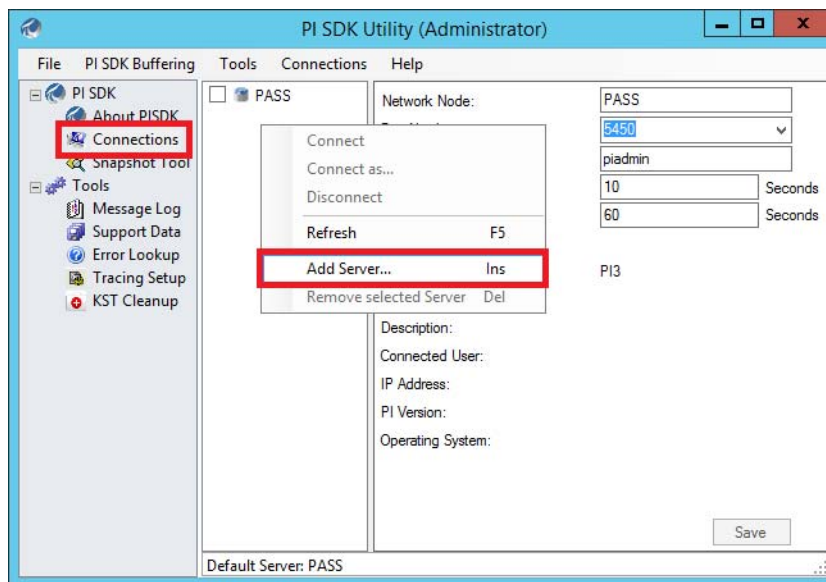
Complete the following steps.

1. On the Windows desktop, click the Programs  symbol and choose Rockwell Software>FactoryTalk Historian SE>FactoryTalk Historian SE System>AboutPI-SDK.



The PI SDK Utility window appears.

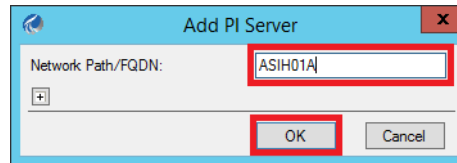
2. Click the '+' to expand the PI SDK folder and click Connections.
3. Right-click anywhere in the white space and choose Add Server.



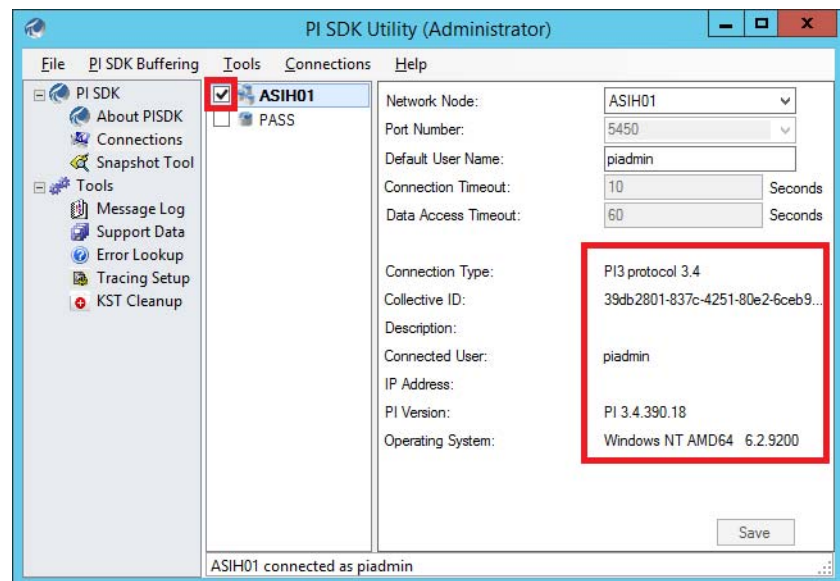
The Add PI Server dialog box appears.

4. Type the Network Path and click OK.

TIP If you are using a collective, type the primary server.

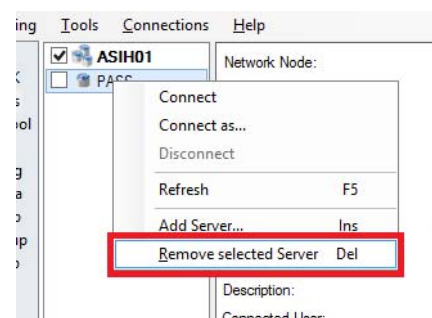


5. Click the box next to the new server.



If the connection is successful, the connection information appears in the same window.

6. If there are other servers listed that are not required, right-click on the server name and choose 'Remove selected server.'



7. When asked if you want to delete the server, click Yes.
8. Close the PI SDK Utility window.

View PI Builder Excel Add-in

Use an Engineering Workstation with these procedures.

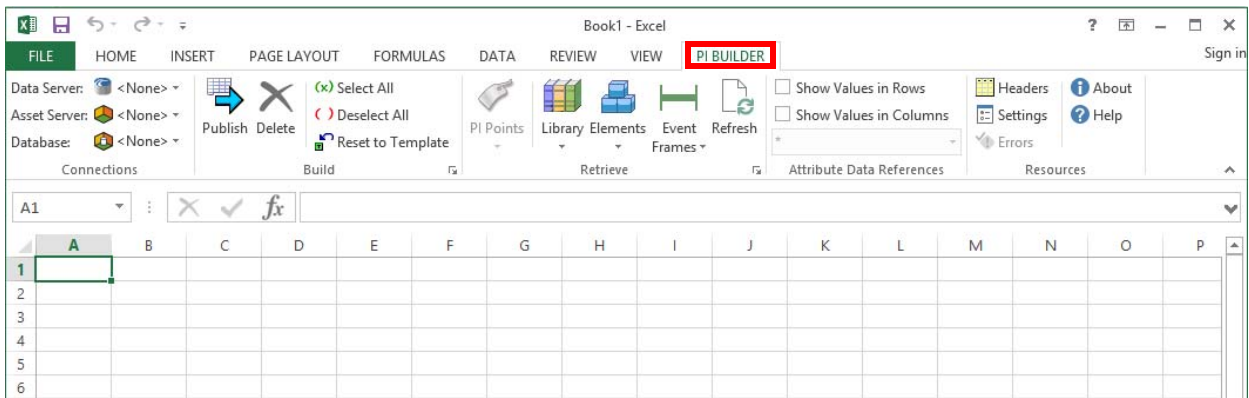


PI Builder lets you import and export PI points and Asset Framework objects to and from Microsoft Excel Add-in spreadsheet.

IMPORTANT Microsoft Excel 32-bit software must be installed for these procedures. This section uses Microsoft Excel 2013. Your version could be different.

To view the information in an Excel spreadsheet, complete these steps.

1. Open your version of Microsoft Excel.
2. Click the PI Builder tab.



You can select the desired server to generate a report in the top, left corner of the spreadsheet.

IMPORTANT PI Builder installation instructions are documented in the Virtualization User Manual, publication [9528-UM001](#).

Configure FactoryTalk VantagePoint Historian Tags

Use the Reporting Application server with these procedures.




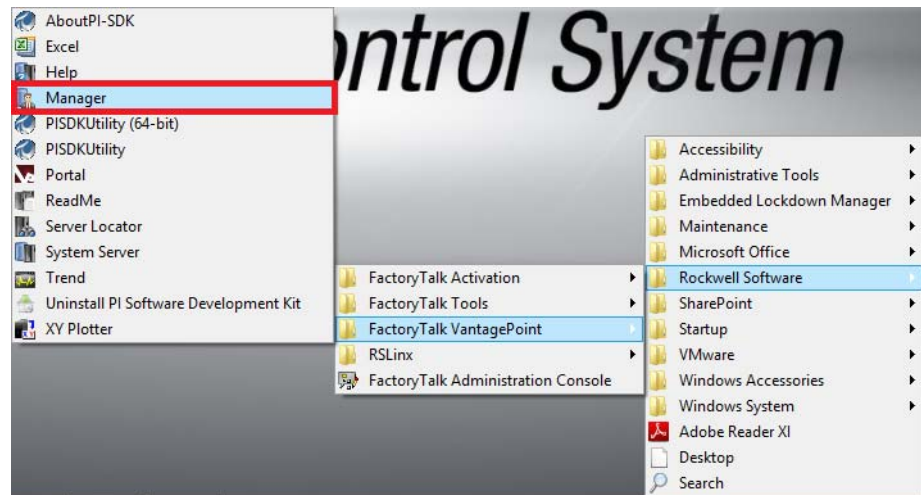
ASIV01

This section shows how to import FactoryTalk Historian data tags. Data from multiple Historian SE servers can be brought together into a single decision support system by using VantagePoint as the information reporting software.

IMPORTANT Before proceeding with this section, make sure that FactoryTalk Historian is installed and configured.

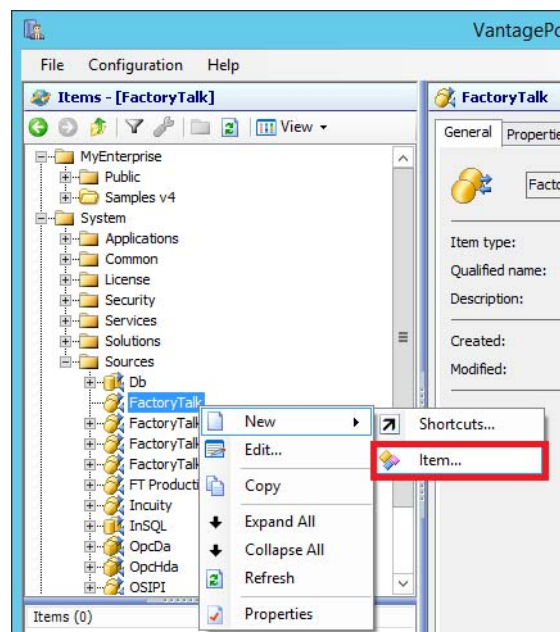
Complete the following steps.

1. On the Windows desktop, click the Programs  symbol and choose Rockwell Software>FactoryTalk VantagePoint>Manager.



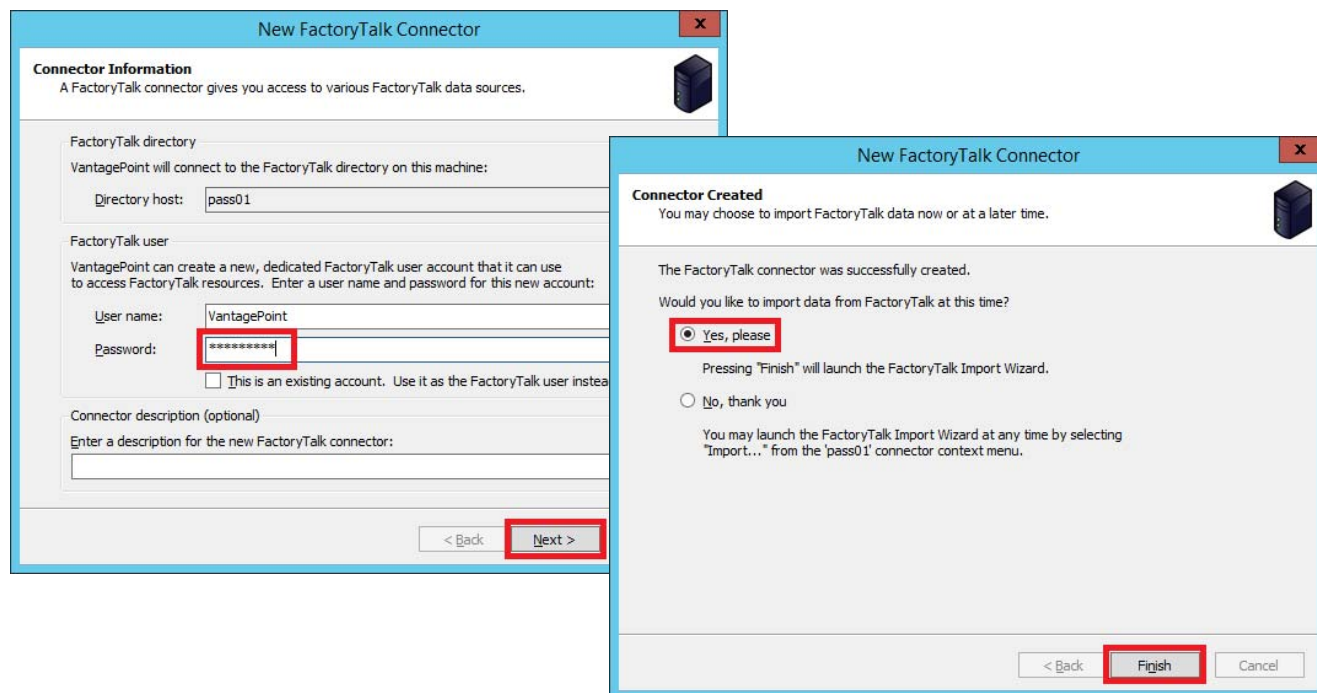
The VantagePoint Manager window appears.

2. In the directory tree under Sources, right-click FactoryTalk and choose New>Item.



The New FactoryTalk Connector - Connector Information dialog box appears.

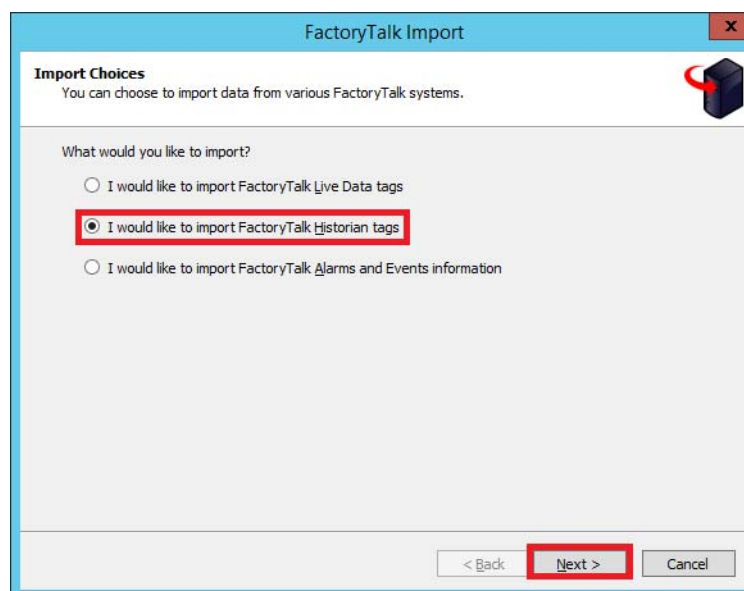
3. Type the VantagePoint user password and click Next.



4. Click 'Yes, please' and Finish.

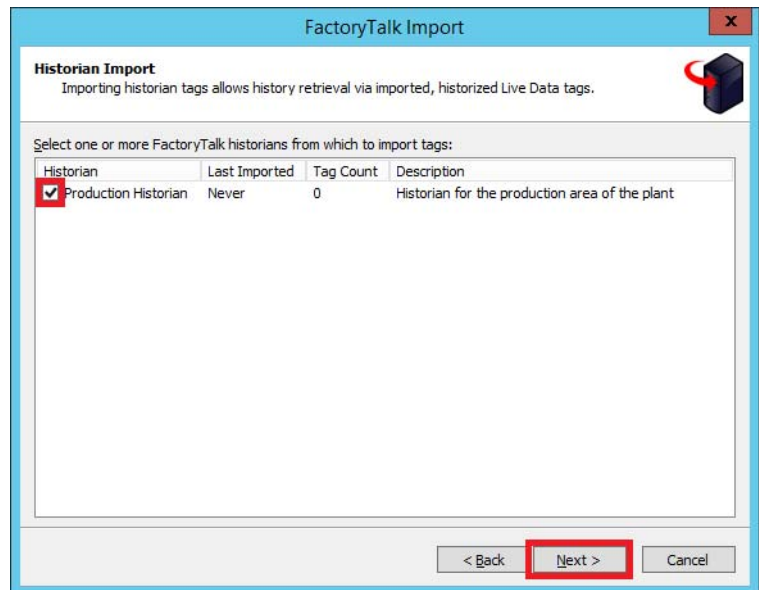
The FactoryTalk Import - Import Choices dialog box appears.

5. Click 'I would like to import FactoryTalk Historian tags', and then click Next.

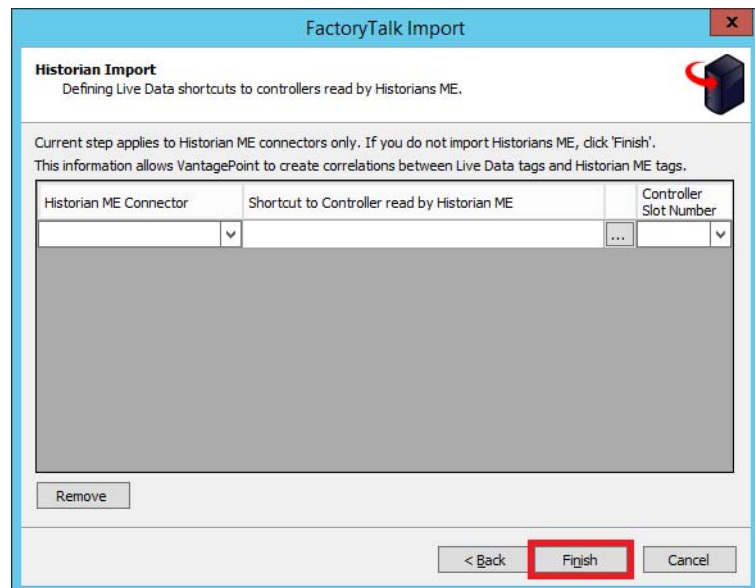


The Historian Import dialog box appears.

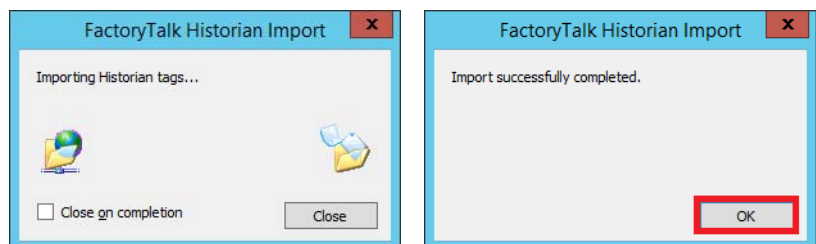
6. Check the Historian that you want to use and click Next.



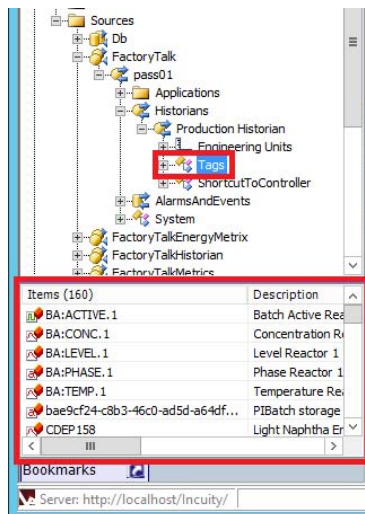
7. If you are not using an ME connector, click Finish.



8. When the 'Import successfully completed' dialog box appears, click OK.

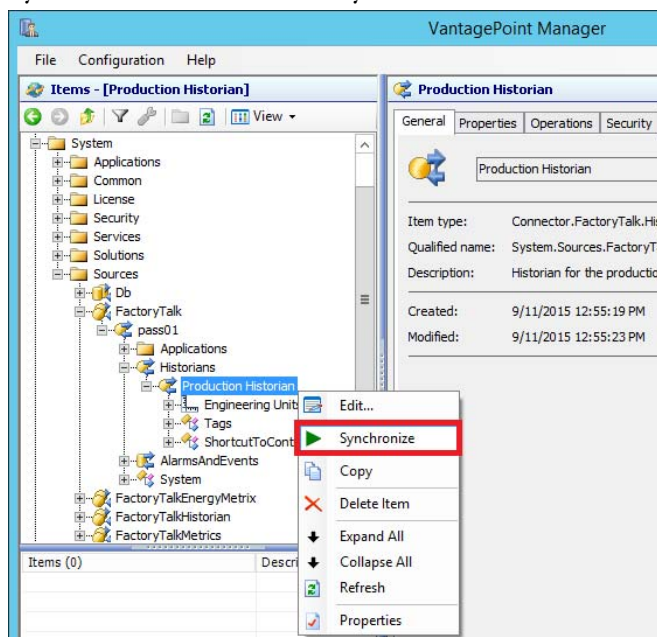


9. To confirm the import, click
System>Sources>FactoryTalk>pass01>Historians><Production
Historian> and look for 'Tags', where:
 - Server = pass01
 - Your Historian = Production Historian in the example.



IMPORTANT Adding new Historian points in the system requires a synchronization action.

10. To synchronize the Historian, right-click
System>Sources>FactoryTalk><server>>Historians>
<your Historian> and choose Synchronize.



Synchronizing lets you update the VantagePoint references.

You are finished configuring the FactoryTalk VantagePoint Historian tags and synchronizing the Historian.

Configure Asset Management (AppServ-Asset)

The Asset Management server (AppServ-Asset) provides a centralized tool to secure, manage, and track asset-related information. The pool of information provides analysis of system resources, including source controls, audits, and change notifications.

This section describes how to configure an audit log. The log monitors and records user interactions with FactoryTalk® software products. For example, if an operator changes a setpoint in a controller, the change is logged for future reference.

FactoryTalk AssetCentre software includes Device Type Manager interfaces and disaster recovery back-up files. For procedures on these tools, see Chapter 8 in the PlantPAx® DCS Application Configuration User Manual, publication [PROCES-UM003](#).

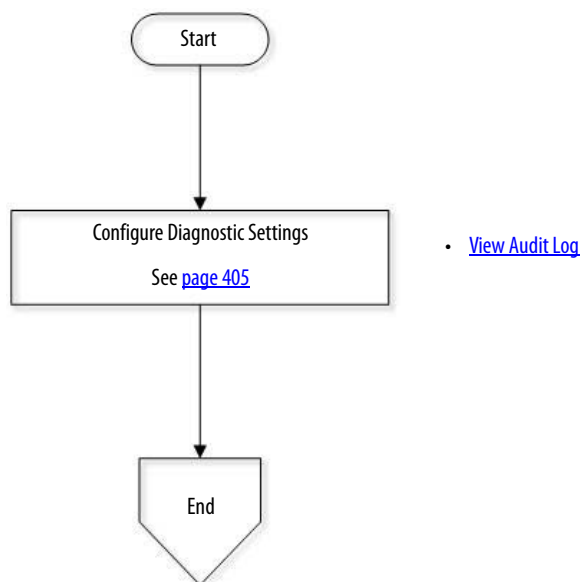
Considerations

Consider the following suggestions before starting this chapter:

- For more information on the PanelView™ audit log, refer to Knowledgebase Answer ID 58977, Using FactoryTalk AssetCentre to receive audits from a PanelView Plus, at <http://www.rockwellautomation.custhelp.com>.
- We strongly recommend additional licensing for disaster recovery that automatically backs up supported devices.

[Figure 19](#) shows the topics that are described in this chapter. Click or see the page number for quick access to a section.

Figure 19 - AppServ-Asset Workflow



Configure Diagnostic Settings

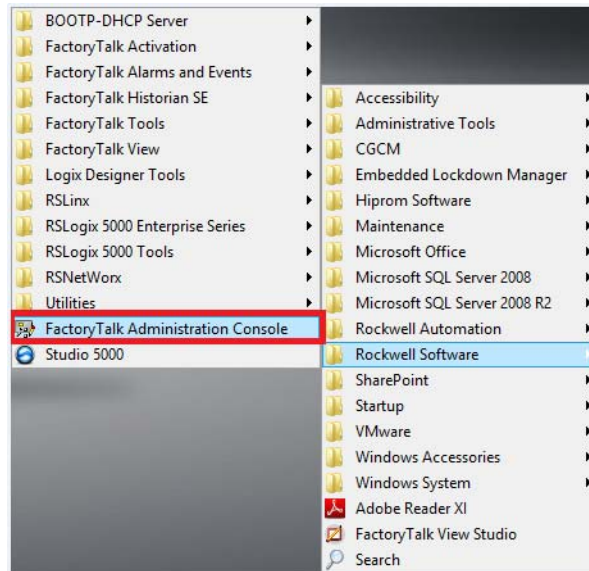
Use all servers and workstations with these procedures.



The Audit Log monitors FactoryTalk-enabled software products and logs user actions. Complete these steps to configure the Audit Log so that it can be viewed in FactoryTalk AssetCentre.

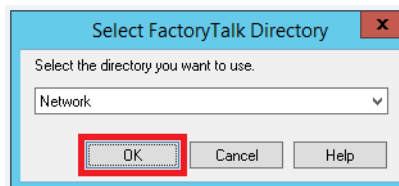
IMPORTANT All servers and workstations must be configured by using FactoryTalk Administration Console or FactoryTalk View Studio. The examples in this section use the FactoryTalk Administration Console.

1. Click the Programs  symbol and choose Rockwell Software®>FactoryTalk Administration Console.



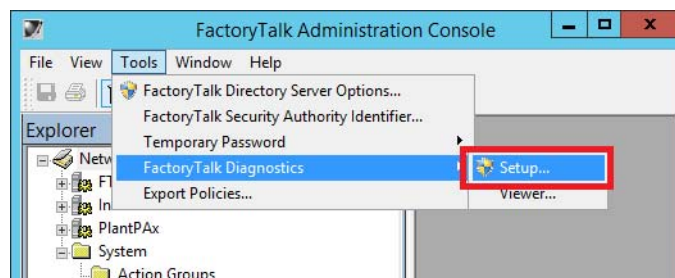
The Select FactoryTalk Directory dialog box appears.

2. Select Network and click OK.



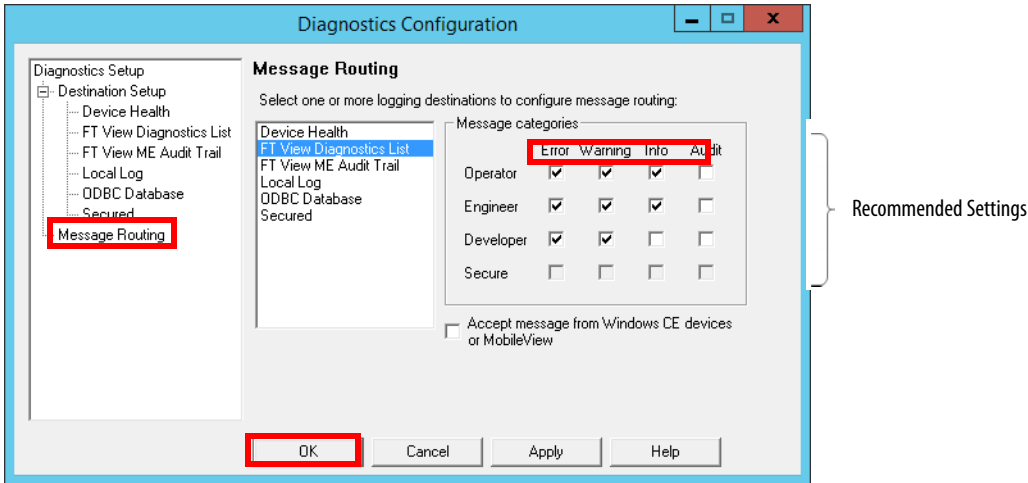
The FactoryTalk Administration Console window appears.

3. Right-click Tools>FactoryTalk Diagnostics and choose Setup.



The Diagnostics Configuration window appears.

4. In the Message Routing section, click FT View Diagnostics List.

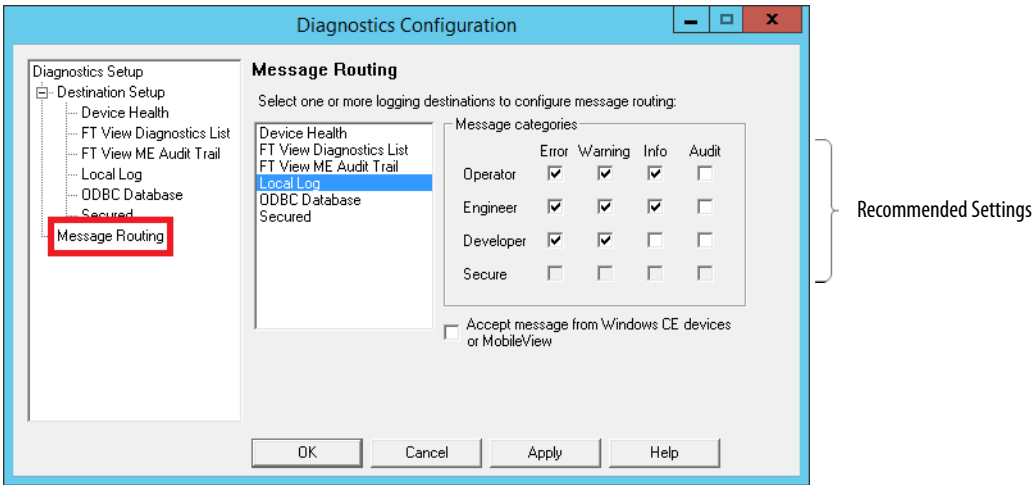


5. In the 'Message categories' section, configure the desired level of diagnostics.

Message Categories	Notes
Operator	If Info is checked, screen access is stored as an Event. If Secured also is checked, the information is logged into the Event tag of FactoryTalk AssetCentre software. IMPORTANT: This setting does not show which computer accesses the system; only on FactoryTalk Diagnostics Viewer.
Engineer	If Audit is checked, Alarm acknowledgments are audited and displayed regardless of the destination. HMI display changes (on FactoryTalk View Studio software) also are logged.
Developer	If Audit is checked, HMI tag value changes are audited regardless of the destination.
Secure	If Audit is checked, any changes on Studio 5000® are audited under the Secured destination.

TIP Click Help for more information on the message categories.

6. In the Message Routing section, click Local Log.




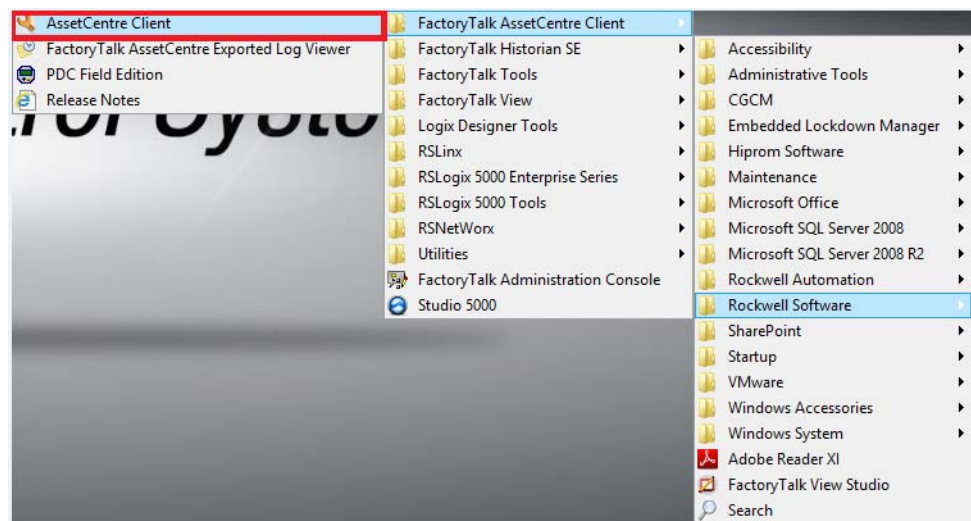
7. Repeat [step 5](#).
8. Click Apply and then click OK.

The Diagnostics Configuration window closes.

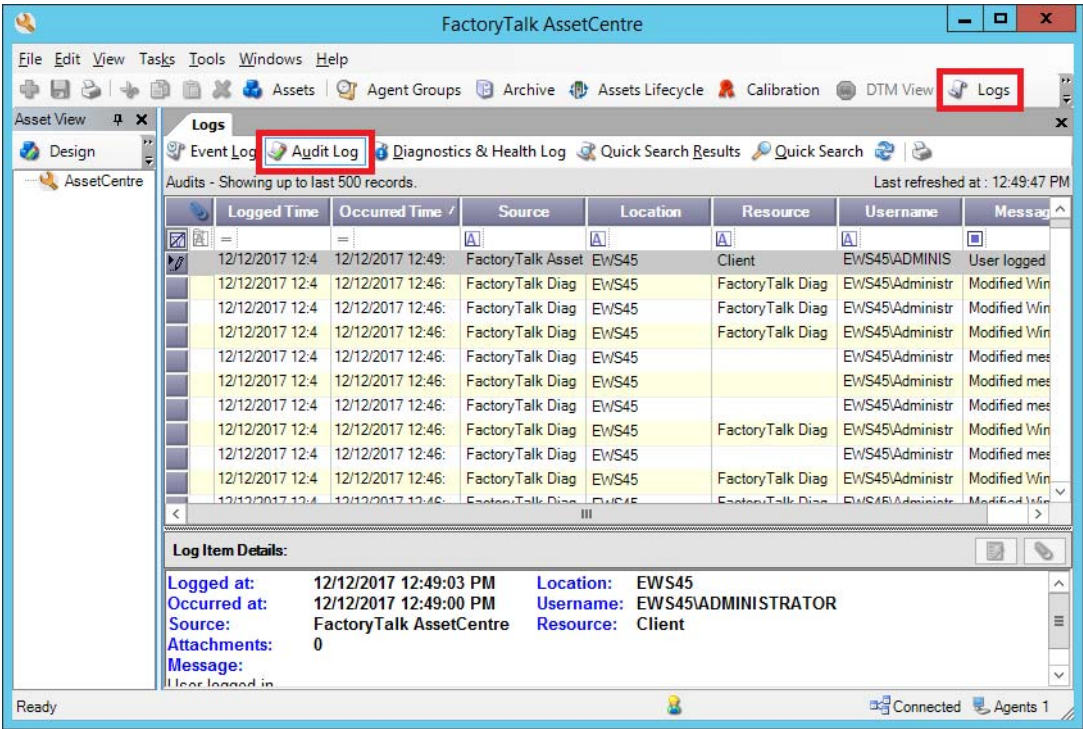
View Audit Log

A log of activity lets you view the messages. Complete these steps.

1. Click the Programs  symbol and choose Rockwell Software>FactoryTalk AssetCentre Client>AssetCentre Client.



2. Click Logs and then Audit Log.



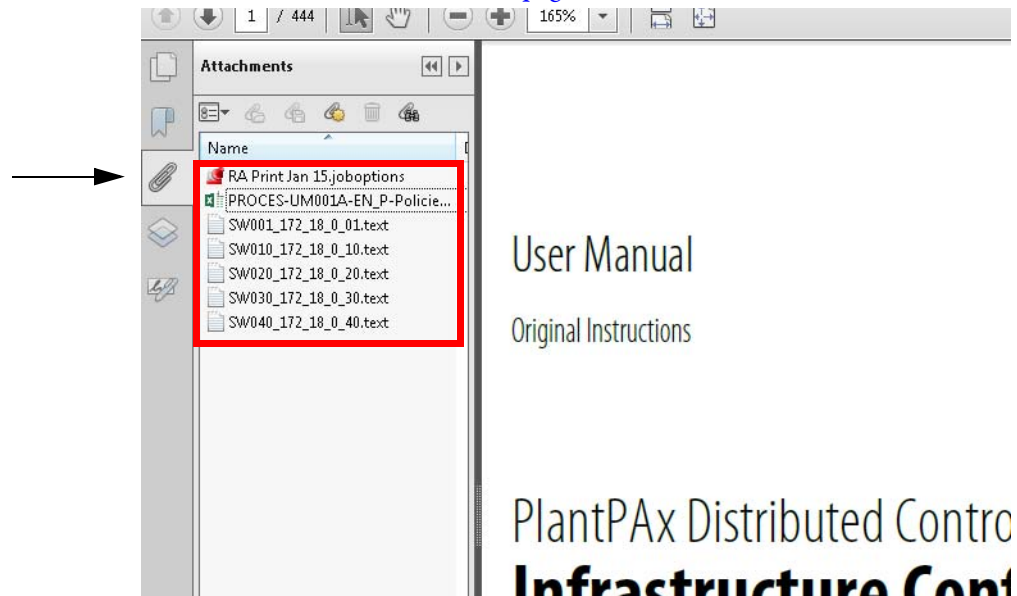
3. Click 'X' to Close.

Access the Attachments

The Microsoft Excel spreadsheet and text files that are attached to this PDF file contain security and switch information to customize application requirements. Each security tab in the Excel spreadsheet has specific 'Allow' and 'Deny' security permissions.

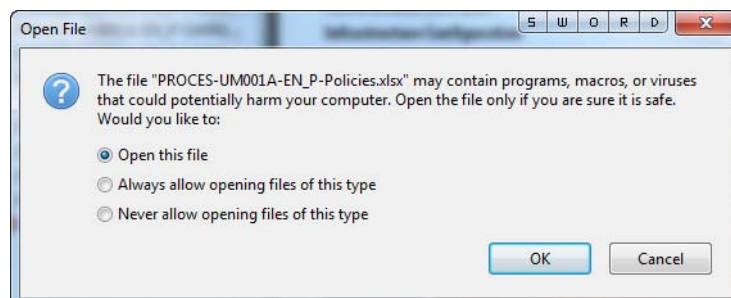
To use the attachments, click the Attachments link (paper clip) and double-click the desired file.

See [How to Use Attachments on page 410](#).



Open Content

As a precaution when you open programs or files, select one of the choices and click OK.



How to Use Attachments

The Excel spreadsheet contains several tabs to access security permissions for policy groups. Click a desired tab and use the suggested security along with the procedures in [Define FactoryTalk System Policies on page 193](#).

	A	B	C	D	E	F	G	H
	Product Policies	Operators	Operator Supervisor	Maintenance	Maintenance Supervisor	Manager	Engineer	Administrator
1	Product Policies							
2	RSLogix5000							
3	Feature Security							
4	Project: New	Deny	Deny	Allow	Allow	Allow	Allow	Allow
5	Print: Modify Options	Deny	Deny	Allow	Allow	Allow	Allow	Allow
6	Controller: Secure	Deny	Deny	Allow	Allow	Allow	Allow	Allow
7	Toolbar: Configure	Deny	Deny	Allow	Allow	Allow	Allow	Allow
8	Firmware: Update	Deny	Deny	Allow	Allow	Allow	Allow	Allow
9	Workstation: Modify Options	Deny	Deny	Allow	Allow	Allow	Allow	Allow
10	Studio 5000 Architect							
11	Feature Security							
12	Create	Deny	Deny	Allow	Allow	Allow	Allow	Allow
13	Open	Deny	Deny	Allow	Allow	Allow	Allow	Allow
14	Save	Deny	Deny	Allow	Allow	Allow	Allow	Allow
15	Batch							
16	. Batch Campaign							
17	.. Commands							

The four text files contain switch configuration information. Double-click the .txt file to open the respective file in a text editor, such as Notepad. Copy and paste the switch configuration data into the CLI interface in the PuTTY software.

You can use these files to directly configure your switches according to this manual's directions by downloading the file contents into each of your switches. If you use these files to configure your switch, we strongly recommend that you verify all switch settings by logging into the switches and viewing/verifying switch configuration by using the Device Manager.

See [Using a Terminal Emulator \(PuTTY\) on page 41](#) for procedures.

Define a Workgroup and DeskLock Utility

Use all system computers with these procedures.



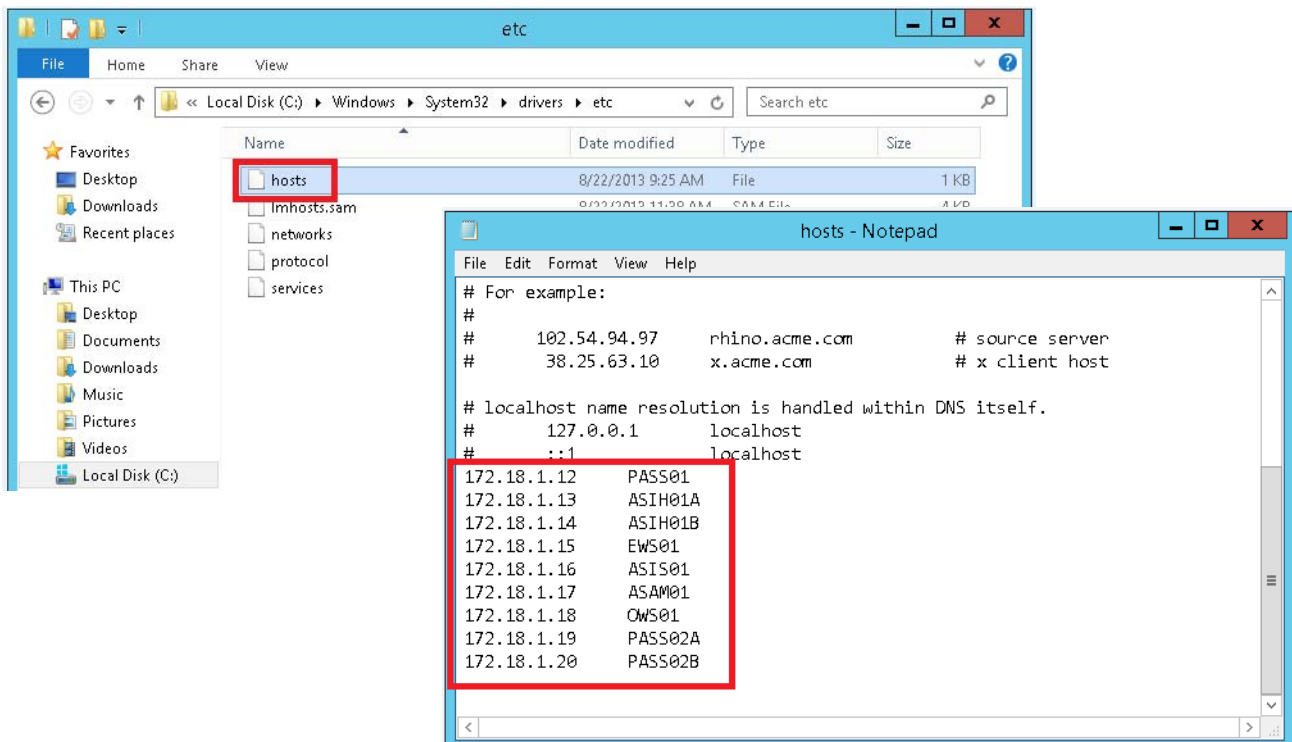
If you don't use a domain, you must configure a workgroup to make sure that the name resolution is correct for the network. Workgroups are supported for systems with 10 or fewer workstations and servers.

This appendix also includes procedures for how to enable an optional DeskLock Utility.

Complete the following steps.

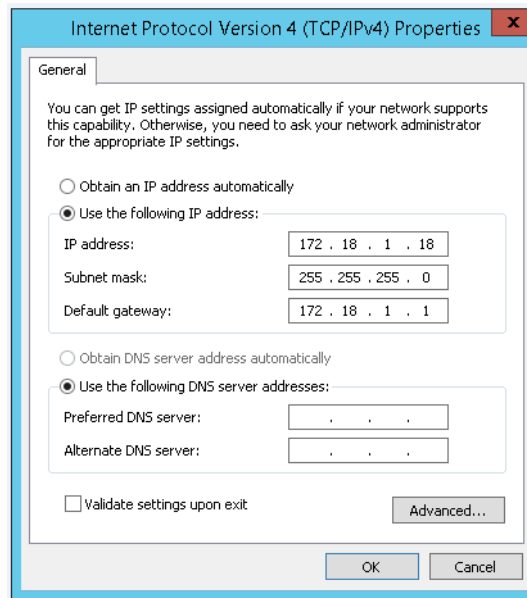
1. In Windows Notepad, open the file C:\Windows\System32\Drivers\Etc\host and enter the IP addresses and machine names for the computers in the workgroup.

Use a tab between each IP address and machine name.

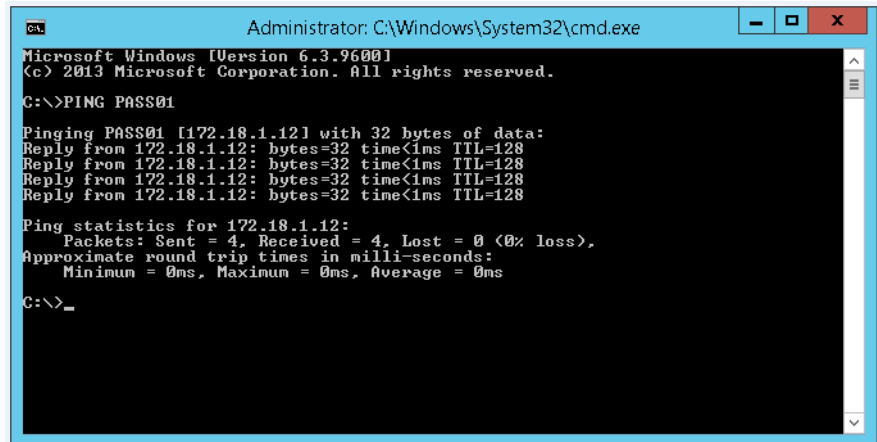


2. Copy the revised host file to all computers in the system.

3. Configure each server network adapter with the correct IP address.



4. Use a ping command to test name resolution, for example, ping PASS01.



5. Click 'X' to close.

Enable the Windows DeskLock Utility (optional)

Use all workstations with these procedures.



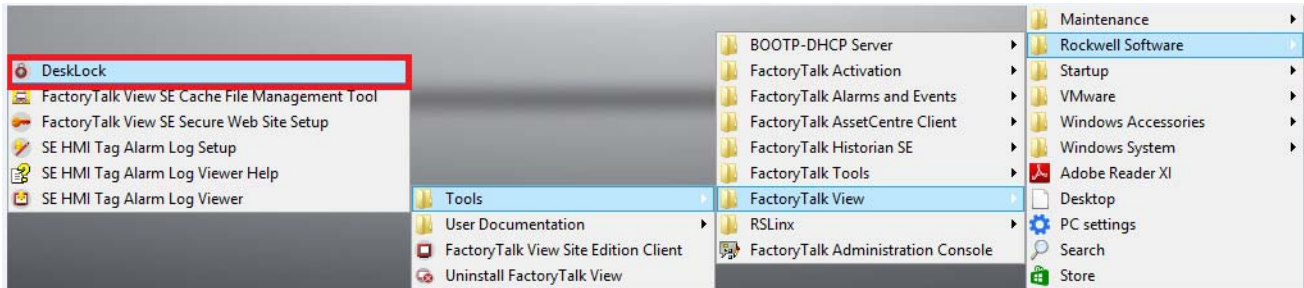
The FactoryTalk® View DeskLock utility, which is available for any workstation computer, provides control options for smaller environments that do not use domain management.

DeskLock is installed with FactoryTalk View software.

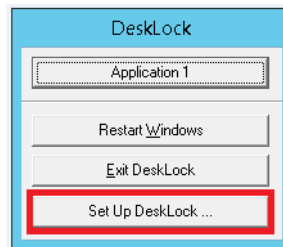
Complete these steps.

1. Click the Programs symbol and choose Rockwell Software®>FactoryTalk View>Tools>DeskLock.

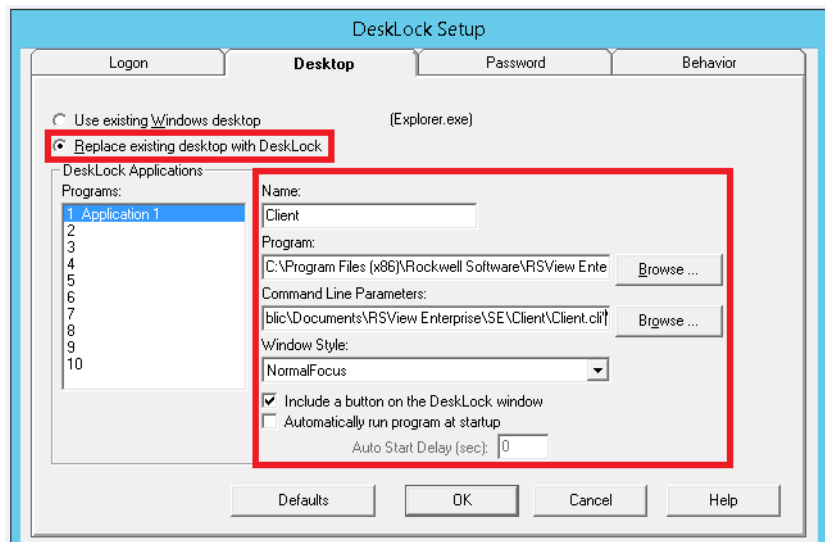
2.



3. Click Set Up DeskLock.

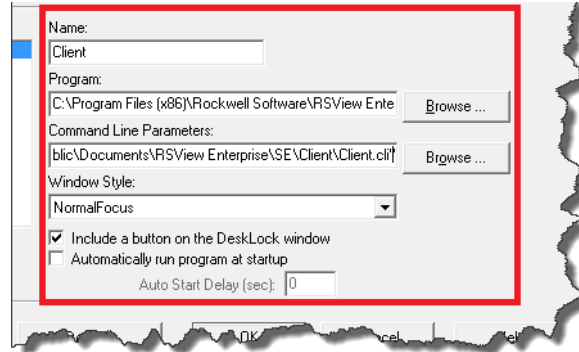


4. Login and click the Desktop tab.
5. Select 'Replace existing desktop with DeskLock' and click OK.



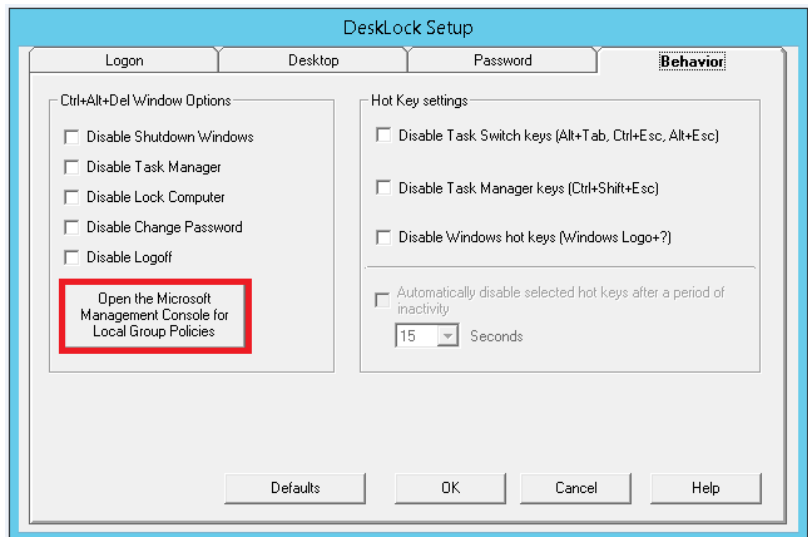
- In the popup window, type the name of the application option in the Name text box.

For example, type 'Client' if FactoryTalk View Client is to be an application.

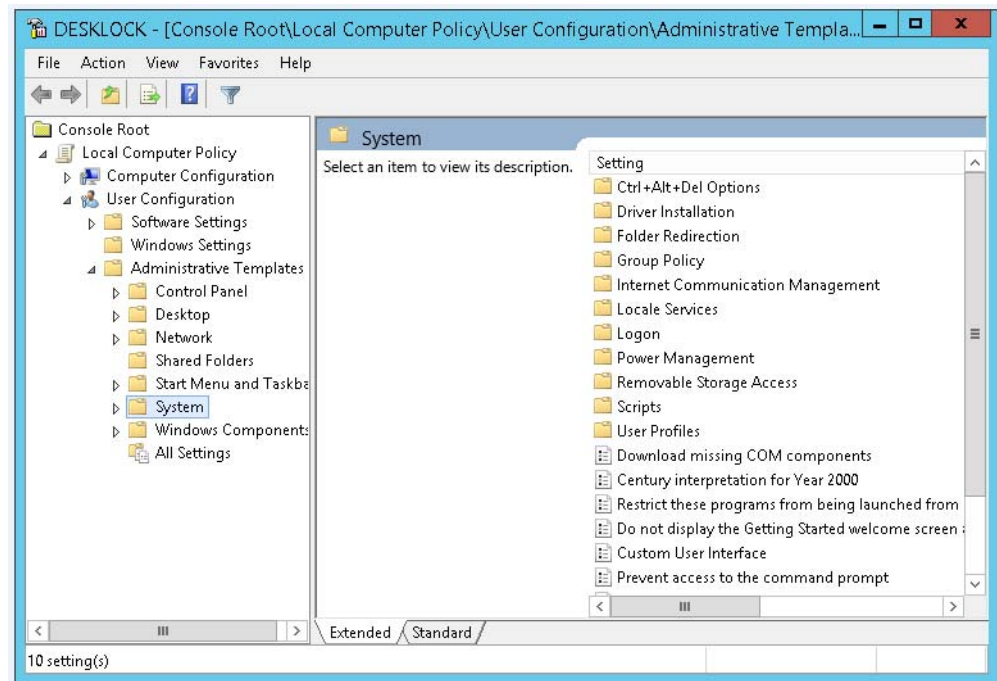


You can enable up to 10 applications in the DeskLock.

- Click the Password tab to configure local password management.
- Click the Behavior tab to configure Hot Key settings and the Ctrl+Alt+Del options.



9. To open the DeskLock under the Local Computer Policy, click Microsoft Management Console.



10. To enable DeskLock options and settings, restart your computer.

Notes:

Firewall Configurations

Common Ports

[Table 28](#) shows the most common ports that need to be considered during the firewall configuration.

Table 28 - Common Firewall Port Descriptions

Port	Type	Usage
25	TCP	SMTP mail
80	TCP	Standard WWW port
123	UDP	Network Time Protocol
135	TCP	Remote process calls
137	UDP	File and printer sharing
138	UDP	
139	TCP	
445	TCP	Use in the Collective configuration and file and print sharing
1433	TCP	Communication to SQL server
1434	UDP	Browsing for SQL server
21060	UDP	Rockwell Automation® trace diagnostics
21061	UDP	

Rockwell Automation TCP/UDP Ports

[Table 29](#) shows the TCP/UDP ports for Rockwell Automation® firmware and software products.

For periodic updates, see the Knowledgebase Answer ID 29402 at <http://www.rockwellautomation.custhelp.com>.

Table 29 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments
23	TCP	Telnet	Trusted® AADvance before release 1.3	Diagnostic command-line interface (see also 55555)
25	TCP	SMTP	1769-L35E, 1769-L32E, 1756-ENBT, 1756-EN2T, 1756-EWEB, 1768-ENBT, 1768-EWEB, 1788-ENBT, 1763-L16x 1766-L32x, FactoryTalk® AssetCentre, FactoryTalk® Transaction Manager, RSSQL	Outbound email only
67...68	UDP	DHCP/BOOTP	1756-ENET, 1756-ENBT, 1756-EWEB, 1756-EN2T, 1794-AENT, 1734-AENT, 1769-L35E, 1769-L32E, 1788-ENBT, 1761-NET-ENI, 1785-LXXE, 1785-ENET, 1791ES, 1763-L16x, 1766-L32x, PowerFlex® Drives, PowerMonitor™ 3000, PanelView™	Client only

Table 29 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments
69	UDP	TFTP	5820-EI	For binary download, used in conjunction with BOOTP
80	TCP	HTTP	1756-ENET, 1756-ENBT, 1756-EWEB, 1794-AENT, 1734-AENT, 1769-L35E, 1769-L32E, 1788-ENBT, 1761-NET-ENI, 1785-LXXE, 1785-ENET, 1747-L55x, 1763-L16x, 1766-L32x, PowerFlex Drives, PowerMonitor 3000, PanelView, RSBizWare™, RSView®32, FactoryTalk View SE, FactoryTalk® VantagePoint®, FactoryTalk ViewPoint	FactoryTalk ViewPoint and VantagePoint EMI server can use any other custom assigned port
123	UDP	NTP	PowerMonitor 3000, AADvance	Network time protocol
135	TCP	RPC/Endpoint Mapper	FactoryTalk, RSMACC™	DCOM endpoint mapper
161	UDP	SNMP	1756-ENET, 1756-ENBT, 1794-AENT, 1734-AENT, 1769-L35E, 1769-L32E, 1788-ENBT, 1761-NET-ENI, 1785-LXXE, 1785-ENET, 1747-L55x, 1766-L32x, 5820-EI, PowerFlex Drives, PowerMonitor 3000, PanelView	
300...400	UDP	Proprietary	PowerMonitor 3000	Master/slave configuration
400...402	TCP	RPC	FactoryTalk Transaction Manager, RSSQL	Transaction manager, compression server, and configuration server
443	TCP	HTTPS	FactoryTalk ViewPoint	When using web server with secure certificate
502	TCP	ModbusTCP	AADvance, Trusted®	Master or slave (AADvance), Slave only (Trusted)
1001...1009	UDP	Proprietary	1426 PowerMonitor 5000	Waveform synchronized broadcast
Dynamic (1024...65535+)	TCP	DCOM	FactoryTalk	DCOM dynamic ports
1089	TCP/UDP	ff-annunc	1788-EN2FFR	FOUNDATION Fieldbus
1090		ff-fmx		
1091		ff-sm		
1132	TCP	SNCP	AADvance	Safety Network Control Protocol, used by OPC, workbench debugger, and binding networks
1330	TCP	rnprpc	FactoryTalk	Object RPC
1331	TCP	rnaserv	FactoryTalk	Service control
1332	TCP	rnaserveping	FactoryTalk	Server health
1433	TCP	N/A	FactoryTalk® AssetCentre (server), FactoryTalk VantagePoint RSMACC	SQL server communication (default port)
1434	UDP	N/A	FactoryTalk AssetCentre (server), FactoryTalk VantagePoint	Recommended static destination port for MSSQL to minimize the number of ports open on a firewall See the Knowledgebase Answer ID 287932 at http://www.rockwellautomation.custhelp.com
1947	TCP/UDP	N/A	SafeNet Sentinel Local License Manager	Windows Service installed by Sentinel USB HASP driver. This service is not required for USB dongle to function. See the Knowledgebase Answer ID 570831 at http://www.rockwellautomation.custhelp.com
2000	TCP	Modbus RTU	AADvance (Slave only), Trusted (Master or slave, used for OPC and SOE)	RTU packaged in serial stream. Other ports can be assigned

Table 29 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments	
2010...2011	UDP	Discover tool	AADvance	Used to configure systems. The tool sends broadcast to 2010 and systems reply to port 2011	
2222	UDP	EtherNet/IP	1756-ENBT,1794-AENT,1734-AENT,1769-L35E, 1769-L32E,1788-ENBT	I/O communication that is used by products that only support I/O over EtherNet/IP	
2222	TCP	CSP	1785-Lxxe,1785-ENET,1771-DMC(x),1747-L55x,5820-EI, PowerMonitor II, RSLinx® Classic, INTERCHANGE™	This is the source port for connections	
3060	TCP	rnadirft	FactoryTalk	Directory server file transfer	
3622	TCP/UDP	ff-lr-port	1788-EN2FFR	FOUNDATION Fieldbus	
4000	UDP	Peer-to-peer	Trusted	Original simplex protocol	
4120	TCP	RPC	RSBizWare	Production server	
4121				Server manager	
4122				PlantMetrics™ server	
4123				Task manager	
4124				Scheduler server	
4125				Scheduler CTP server	
4446	TCP	TCP/IP	FactoryTalk Diagnostics (CPR SR3)	See the Knowledgebase Answer ID 68260 at http://www.rockwellautomation.custhelp.com	
5000	UDP	Peer-to-peer	Trusted, AADvance	Enhanced (new) protocol	
5241	TCP	TCP/IP	FactoryTalk Diagnostics (CPR9 SR4 and greater)	See the Knowledgebase Answer ID 68260 at http://www.rockwellautomation.custhelp.com	
5450	TCP		FactoryTalk Historian Site Edition	PI network manager	
5454				Analysis Framework v1.x	
5455					
5456				ACE 2 scheduler	
5457				Asset Framework server	
5458				PI notifications	
5459				Asset Framework to OLEDB Enterprise	
6000	TCP	Workbench	Trusted	Online debugger	
6543	TCP	rnaalarming	FactoryTalk	Alarming server	
7002...7004	TCP		FactoryTalk AssetCentre (default)	FactoryTalk AssetCentre services	
7600	TCP		FactoryTalk	Event multiplexor	
7700				Event server	
7710				Directory server	
7720	TCP		RSView SE, FactoryTalk View SE	HMI server	
7721				Server Framework	
7722				HMI activation	
7723				Historical Data Log reader	
8080	TCP		HTTP	RSBizWare	Production server, reports
8081					Server manager
8083	TCP	HTTP	CTP Server		

Table 29 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments
10001...10006	TCP	Serial data	AADvance	Transparent communication interface, where an Ethernet host can talk through AADvance to a serial port
27000...27009	TCP	TCP/IP	FactoryTalk® Activation Server, FactoryTalk Activation Manager	For more application required to run FLEXSVR.exe. and LMGRD.exe, see the Knowledgebase Answer ID 35717 and 184922 at http://www.rockwellautomation.custhelp.com
44818	TCP/UDP	EtherNet/IP	1756-ENET, 1756-ENBT, 1756-EWEB, 1794-AENT, 1734-AENT, 1769-L35E, 1769-L32E, 1788-ENBT, 1761-NET-ENI, 1785-LXXE, 1785-ENET, 1747-L55x, 1763-L16x, 1766-L32x, PowerMonitor3000, PanelView, RSLinx Classic, FactoryTalk Linx, INTERCHANGE (rsicd)	Messaging, data transfer, upload/download, peer messaging, and so forth; used mainly by RSLinx
49281	TCP	TCP/IP	FactoryTalk Live Data, FactoryTalk View SE HMI tag server	HMI tag server
55555	TCP	Telnet	AADvance from release 1.3	Diagnostic command-line interface
60093	TCP	TCP/IP	FactoryTalk Diagnostics (CPR9 SR2 and earlier)	See the Knowledgebase Answer ID 68260 at http://www.rockwellautomation.custhelp.com
65207	TCP	TCP/IP	FactoryTalk VantagePoint	Incuity® server advertiser

A

A and B

- LAN 63

access

- level
 - define for group 160
 - software restriction 165

activation

- FactoryTalk 175
- manager 175

adapter

- local communication 210
- network configuration 210

additional resources 14**aggregation**

- port link 38

alarm and event

- database 281
- enable redundancy 279
- server creation 254

AppServ

- Info Historian 313

area

- import active directory 189

assets

- central analysis 403
- central analysis tracking 403
- server configuration 405
- workflow 404

assign

- users to groups 125

audit 196

- view audit 407

authority

- identifier 220

C

canvas

- Logix 5000 Architect 206

central directory

- FactoryTalk 169

child domain controller

- configuration 86

CIP VLAN

- enable 31

code

- restrictions 224, 225

communication

- restriction 223
- restrictions 220

components

- FactoryTalk architecture 167

computers

- DHCP server 117
- DNS server 116

configuration

- asset management 403
- child domain controller 86
- code restrictions 224, 225
- communication restriction 223
- communication restrictions 220
- controller security 203
- data restrictions 223, 224
- DHCP server 99, 102
- Excel add-in 398
- FactoryTalk components 167
- FactoryTalk groups 185
- FactoryTalk security 183
- FactoryTalk users 185
- failover 110
- GPS time sync 236
- group policies 131
- Historian server 313
- HMI server 247
- initial switch setting 20
- IP address 86
- layer 2 switch 55
- live data connectors 358
- network overview 15
- node interfaces 342
- NTP server 133
- PanelView Plus 293
- parent domain 79
- PASS 243
- primary node interface server 342
- reporting server 399
- secondary node interface server 358
- smartports 47
- switch express setup 21
- system servers 77
- time sync 231
- users and groups 118
- workgroup 411

connectivity

- Historian server 358, 396

connectors

- live data connectors
 - configuration 358

control network

- overview 45

controller

- child domain 86
- directory name 219
- enable security 217
- modify properties 207
- PTP time sync 241
- redundant switches 73
- ring switches 59
- security 199, 203
- security workflow 204
- switches 54

conventions

- manual 10

copy

- primary HMI folder 260

create 41

- alarm and event server 254
- data server 250
- routing and HSRP 41
- VLAN 29

D**data**

- restrictions 223, 224
- server
 - enable redundancy 266
- server shortcut 250

database

- alarm and event 281

default

- domain controller policy 133
- domain policy (NTP) 143
- terminal server 193

description 47

- ports 47
- SW007 and SW008 55, 57, 60, 62, 65, 69

desklock

- Windows utility 413

DHCP

- enable scope 104
- server
 - computers 117
 - domain controller 99
- server configuration 102
- supervisory scope 107

directory

- areas 189
- FactoryTalk 169

disaster recovery

- software 403

DNS server

- computers 116

document

- conventions 10
- purpose 9

domain

- controller
 - default policy 133
 - DHCP 99
 - enforce policy 140
 - users and groups 118
- join 113
- NTP policy default 143
- policy enforcement 158

drive

- USB protection 161, 163

E**enable**

- CIP VLAN 31
- controller security 217
- DHCP scope 104
- DHCP supervisory scope 107
- PTP 35
- Rapid PVST+ 33
- switch routing 37

etherchannel

- port link aggregation 38

Ethernet

- bridges PTP 239

Excel

- add-in configuration 398

express setup

- switch 21

external

- security 183

F**FactoryTalk**

- activation 175
- directory
 - configuration 167
 - controller name 219
- ME configure security 300
- patches 177
- product security 199
- same log on 194
- SE security 284, 300
- security 183
- workflow 168

failover

- configuration 110

firewall

- Windows 171

FTD

- configuration 167, 169
- controller name 219
- network directory 172
- PASS 243

G**gateway**

- VLAN routing 43

GPS

- time sync 236
- time sync example 232

group

- add to group membership 303
- define access level 160
- membership
 - add groups 303
- policy
 - management 131
 - workflow 132
- security levels 198
- user assignment 125

H**Historian**

- configuration 313
- connectivity 358, 396
- create synchronization path 336
- workflow 314

HMI

- security 284
- server
 - configuration 247
 - enable redundancy 257
 - primary 247

hot standby routing

- protocol 41

hybrid group

- security 183

I**I/O**

- network star 57
- switches 55

I/O network

- switch configuration 52

identifier

- authority 220

interface

- delete node default 334

internal

- security 183
- users and groups 191

IP address

- check setting 20
- configuration 86
- VLAN 18

J**join**

- domain 113

L**LAN**

- A and B 63

layer 2

- switch 29, 31, 33, 35, 47, 54
- switch configuration 55
- switches 21

layer 3

- switch 29, 31, 33, 35, 47
- switches 21

local directory**log**

- view audit 407

log on

- FactoryTalk 194

Logix 5000 Architect

- canvas 206

lookup

- FactoryTalk directory 169

M**management**

- group policy 131

manager

- activation 175

manual

- conventions 10

MCC

- star switches 56
- switch 62
- switches 72

modify

- controller property 207

N**naming**

- controller directory 219
- conventions 10

network

- adapter 210
- directory 167
- directory definition 172
- I/O 57
- I/O switch configuration 52
- overview 15

node interface

- configuration 342
- delete default 334
- primary server configuration 342
- secondary server configuration 358

NTP

- default domain policy 143
- server configuration 133
- time sync example 231

O**overview**

- configuration network 15
- control network 45

P**PanelView**

- configure time sync 306
- download runtime application 309
- Plus
 - configuration 293

parent domain

- configuration 79

PASS

- configuration 243
- configure HMI server 247
- FTD 243
- workflow 244

patches

- FactoryTalk 177
- PCDC 177

PCDC

- patches 177

PlantPAx

- infrastructure
 - workflow 19, 46

policy

- domain controller default 133
- enforce domain 158
- enforce domain controller 140
- FactoryTalk security 199
- PlantPAx users object 160
- security 197

port 47

- descriptions 51
- link aggregation (etherchannel) 38

ports

- I/O network 57

Precision Time Protocol (PTP) 35**primary**

- copy folder to secondary 260
- HMI server 247

product

- FactoryTalk policies 199

property

- controller modification 207

protection

- USB drive 161, 163

protocol

- hot standby routing 41

PRP

- I/O switches 71
- reboxes 68

PTP

- controllers 241
- enable 35
- Ethernet bridges 239

purpose

- document 9

R

Rapid PVST+

- enable 33

redbox

- controller 64
- PRP distribution 68

redundancy

- data server 266
- enable on alarm and event server 279
- HMI server 257

redundant

- controller 73
- star switches 63

redundant star

- switches 63

reference

- manual scope 9

report

- server configuration 399
- spreadsheet 398

restrict

- code 224, 225
- communication 220, 223
- data 223, 224
- system access 195

restriction

- software access 165

ring

- controller switches 59
- topology 58

routing

- and HSRP 41
- enable switch 37
- hot standby 41
- VLAN gateway 43

runtime

- download to PanelView 309
- security 304

S

scope

- DHCP 104
- reference manual 9

security 196

- audit 196
- configure FactoryTalk View ME 300
- controller 203
- enable controller 217
- FactoryTalk 183
- FactoryTalk SE 284, 300
- HMI 284
- hybrid group 183
- levels for group 198
- runtime 304
- system policies 197
- workflow 184

server

- NTP configuration 133

setting

- check IP address 20
- configure switch 20

shortcut

- data server 250

smartports

- configuration 47

software

- access restriction 165

spreadsheet

- reports 398

star

- topology 53

static

- IP address' IP address
- static 74

supervisory

- DHCP scope 107

SW007 and SW008

- description 55, 57, 60, 62, 65, 69

switch

- check IP address 20
- controller 54
- controller ring 59
- enable routing 37
- express setup 21
- I/O 55
- initial setting 20
- layer 2 configuration 55
- MCC 56, 62, 72
- port descriptions 51
- PRP I/O (redbox) 71
- redboxes 64
- redundant star 63
- ring 58

switch configuration

- I/O network 52

sync

- time configuration 231

synchronization path

- Historian 336

system

- access restrictions 195
- security policies 197
- server
 - configuration 77
 - workflow 18

T**terminal server**

- default 193

time

- GPS sync 236
- PTP synced controllers 241
- sync 231
 - configure for PanelView 306
 - Ethernet bridges 239
 - workflow 233
- sync GPS reference 232
- sync NTP server 231

topology

- ring 58
- star 53
- workflow 46

track

- assets 403

U**USB drive**

- protection 161, 163

user manual

- overview 15

users

- assignment groups 125
- PlantPAx policy object 160

users and groups

- configuration 118, 185
- internal 191

V**visual**

- naming conventions 10

VLAN

- creation 29
- IP address range 18
- SW007 and SW008 55, 57, 60, 62, 65, 69

W**Windows**

- desklock utility 413
- firewall 171

workflow

- asset management 404
- controller security 204
- FactoryTalk
 - components 168
 - security 184
- group policy 132
- Historian server 314
- PASS 244
- PlantPAx
 - infrastructure 19, 46
- system servers 18
- time sync 233

workgroup

- configuration 411

Notes:

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Automation maintains current product environmental information on its website at <http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>.

Allen-Bradley, CompactLogix, ControlLogix, FactoryTalk, FactoryTalk Network Manager, Incuity, Integrated Architecture, INTERCHANGE, NetBIOS, Open Controller, PanelView, PlantMetrics, PlantPAx, PowerFlex, PowerMonitor, Rockwell Automation, Rockwell Software, RSBizWare, RSLinx, RSLogix 5000, RSMAC, Stratix, Studio 5000 Architect, Studio 5000 Logix Designer, Trusted, and VantagePoint are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies. Trademarks not belonging to Rockwell Automation are property of their respective companies.

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication PROCES-UM001B-EN-P - August 2018

Supersedes Publication PROCES-UM001A-EN-P - March 2016

Copyright © 2018 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.