This manual links to Knowledgebase Technote, PlantPAx System Release 5.20 Configuration and Implementation Tools, for multiple tools; download now for offline access.

PlantPAx Distributed Control System Configuration and Implementation

System Release 5.20

Allen-Bradley
by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PlantPAx Troubleshooting Scenarios

Notes:

About This Publication

Welcome to the PlantPAx® DCS, a single, plant-wide control system that helps to drive productivity, increase efficiencies and reduce costs in your plant or mill.

This manual helps you implement process control where controllers, HMI, and I/O are located in different areas of the plant. The PlantPAx system offers flexibility, using the latest technology and scalability to build only what you need to help reduce development time, downtime, and operational cost.

Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Adjusted system workflow for new documentation.	13
Added Antivirus information	20
Added PlantPAx View Only Role	Throughout
Updated PRP Topology	99
Updated DLR Topology	103
Split previous Chapter 5 for Process applications into three chapters. Chapter 5 - Configure Process Controller, Chapter 6 - Create Process Application, and Chapter 7 - Modify Process Applications.	As Noted.
Created Chapter 11 - Analytics	263

The following table lists the documentation resources that are available to help procure, configure, and maintain a PlantPAx system.

Table 1 - PlantPAx System Documentation

Stage	Publication	Description
Define and Procure	Selection Guide, publication PROCES-SG001	Helps you understand the elements of the PlantPAx system to make sure that you buy the proper components.
Install	Template User Manual, publication 9528-UM001	Provides direction on how to install and deploy PlantPAx virtual templates.
Develop and Operate	Configuration and Implementation User Manual, publication PROCES-UM100	Provides system guidelines and instructions to assist with the development of your PlantPAx system.
	Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200	Describes the Add-On Instructions, PlantPAx instructions, and associated faceplates that are available to develop applications.

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

Software and Firmware Updates

When you update software or firmware revisions, we recommend that you verify the impact on performance and memory utilization before implementing the upgrade on the production system. For FactoryTalk® View or ControlLogix® platforms, we recommend that you review the release notes and verify the impact of the upgrade on performance and memory utilization.

You can also verify the compatibility of an upgrade with the other software and operating systems in use in your PlantPAx system. See the Product Compatibility and Download Center.

Rockwell Automation Services and Support

System Support offers technical assistance that is tailored for control systems. Some of the features include the following:

- Highly experienced team of engineers with training and systems experience
- Process support at a systems-level that is provided by process engineers
- Use of online remote diagnostic tools
- Access to otherwise restricted TechConnect^{SM} Knowledgebase content
- 24-hour, 7 days per week, 365 days per year of phone-support coverage upgrade option

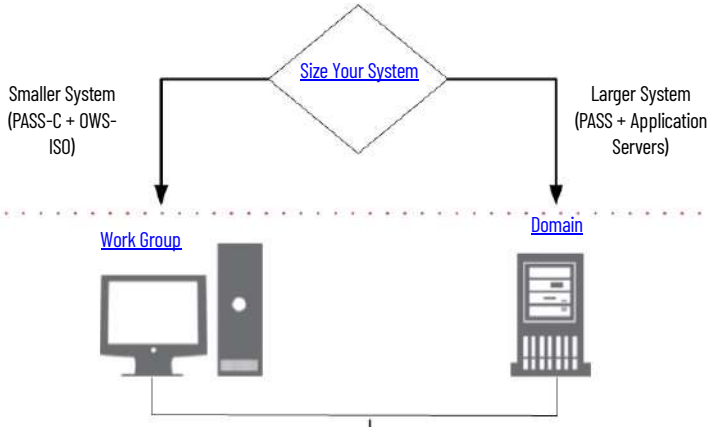
For more information, contact your local distributor or Rockwell Automation representative or see http://www.rockwellautomation.com/support.

System Workflow

The PlantPAx® distributed control system is an integrated control and information solution that helps manufacturers achieve Plant-wide Optimization in a wide range of industries. This single platform can run your entire plant and integrates all HMI, controls, optimization, engineering, information, and inputs/outputs into one common system architecture.

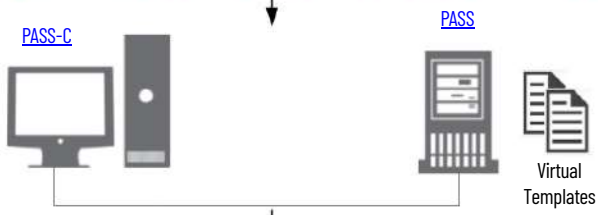
The following workflow shows the steps for how to size, design, and implement a scalable PlantPAx system. Click the links for the information that is related to each step.

1. Use the PlantPAx System Estimator (part of the Integrated Architecture® Builder tool) to size your application.



2. Manage servers and security policies.
   - Smaller systems = Work Group
   - Larger systems = Domain Controllers

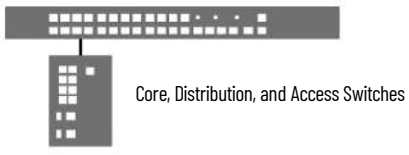
   See Process Controller Features on page 117 Chapter for security configurations



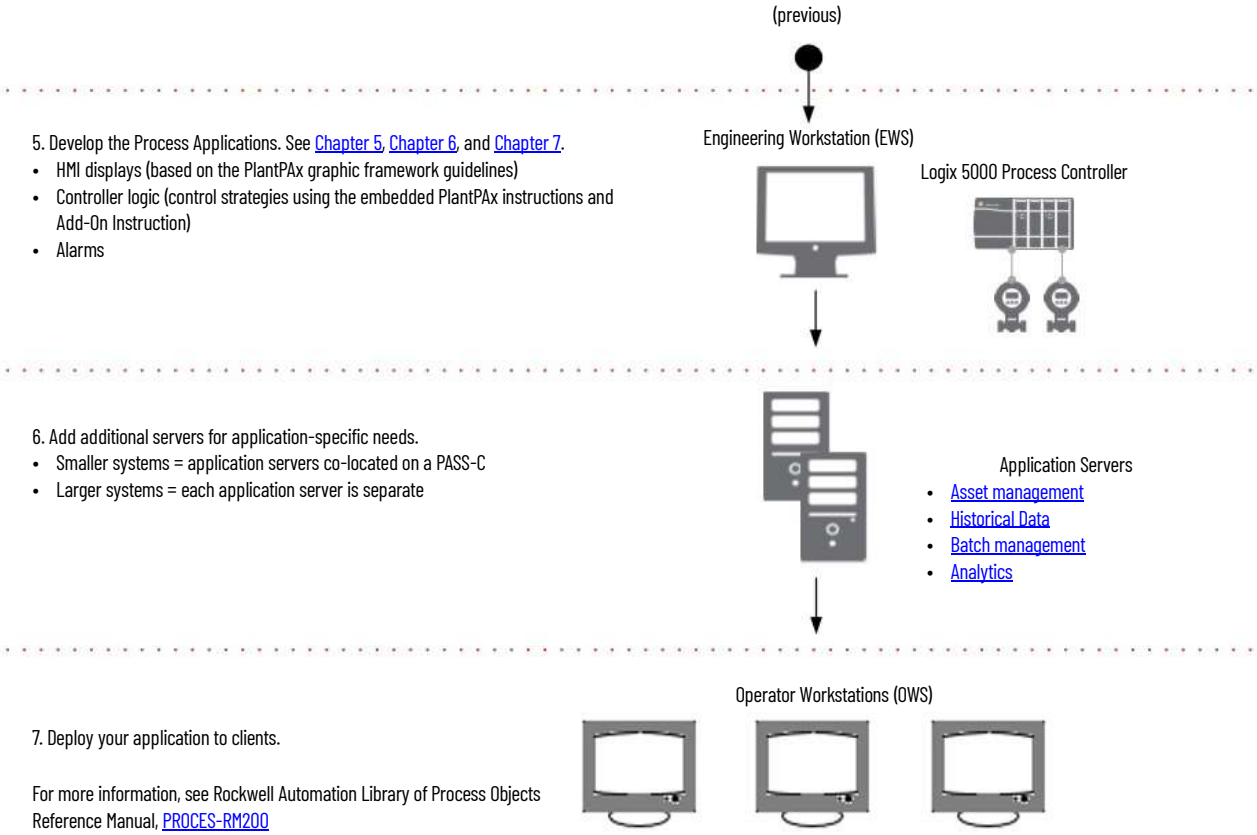
3. Configure the Process Automation System Server (PASS).
   - Smaller systems = PASS-C + OWS-ISO
   - Larger systems = Virtual templates

   See PlantPAx Virtualization User Manual, 9528-UM001, for template details

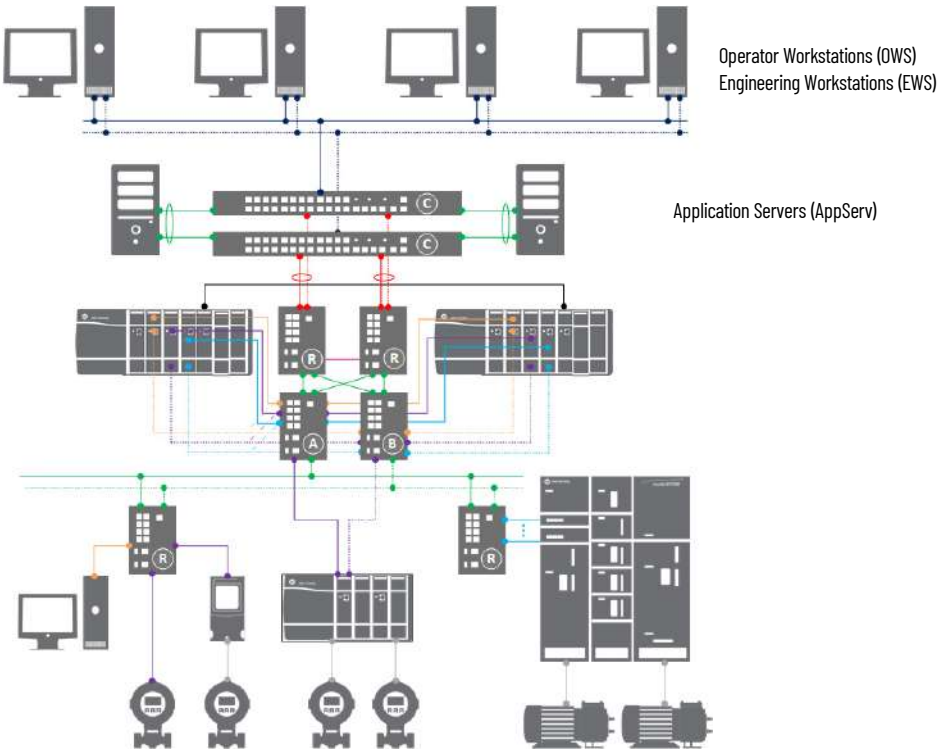
4. Design the Network Infrastructure
   - Select network topologies
   - Configure switches



(continued)



Example PlantPAx System



Size Your System

Rockwell Automation includes the PlantPAx System Estimator (PSE) tool as part of the Integrated Architecture® Builder software. The PSE Estimator tool helps define your PlantPAx system and verifies that your architecture and system elements are sized properly. The PSE includes online help that can assist you as you use the tool.

The PSE employs sizing guidelines that are based on the rules and recommendations from PlantPAx system characterization to achieve known performance and reliability. The PSE focuses on the critical system attributes of a PlantPAx system so you can verify that your system does not exceed system recommendations.

Before you run the PSE, you must plan the scope of your project so that you know the I/O requirements. This could be an equipment list or project database of devices. For more information, see Chapter 5, Process Applications.

Make sure that your PSE project has no errors. As much as possible, the project should accurately represent the physical layout of the system, such as the controllers, I/O, HMI, and data servers. The I/O locations and control rooms must align with your system architecture drawings.

- If you size based on I/O counts, the PSE makes assumptions as to the devices that I/O is connected to and assigns the I/O to control strategies.
- If you know the devices, the PSE results are more accurate if you size based on control strategies.
- Make sure that the logic execution rates accurately represent the requirements of the process.
- Reserve memory and CPU utilization in the controller for auxiliary logic (such as logic for batch applications).
- Accurately account for the process and device networks that are defined in the PSE. Also account for any networks not defined in the PSE.
- Select the execution periods in the PSE appropriate for your control strategies to verify the controller sizing meets the needs of the system.

The final PSE project only accounts for devices, not the programming that automates the devices. Extra programming can include batch, recipe control, or sequencing of any other logic used in the system. Make sure to consider any extra programming so that the system does not overload the controller.

IMPORTANT The PSE, along with the IAB, gives you a high-level Bill of Materials. You must complete a panel design to house, mount, and power the equipment for your environmental needs.

The PSE provides pre-engineered enclosures for PlantPAx systems are available from Rockwell Automation.

Select the Process Automation System Server

Use the sizing results from the PSE, the number of I/O points, and the overall size of the process to determine the Process Automation System Server (PASS) that best suits your PlantPAx system.

The PASS is the main component for PlantPAx computing. A PASS supports an HMI server, displays, alarms, and data connections to controllers. A PASS contains the following:

- FactoryTalk® Directory and Activation server
- FactoryTalk® View SE HMI server
- FactoryTalk® Alarms and Events server
- FactoryTalk® Linx Data server
- FactoryTalk® Historian node interface

A PASS is scalable from a single standalone server to multiple distributed servers. You can deploy a PASS directly to a host computer or run as a virtual guest on a host server.

The sizing recommendations help determine how to best deploy the software for your PlantPAx system:

- Smaller systems (typically less that 2000 I/O points) place all system software on a consolidated Process Automation System Server (PASS-C) with multiple operator workstations (OWS-ISO)

  Examples include skid, station, and distributed architectures where a single PASS-C supports the system.
- Larger systems use a Process Automation System Server (PASS), in addition to individual application servers (AppServ), engineering workstations (EWS), and operator workstations (OWS).

  Larger systems are typically distributed architectures with multiple PASS servers.

Consolidated Process Automation System Server (PASS-C)

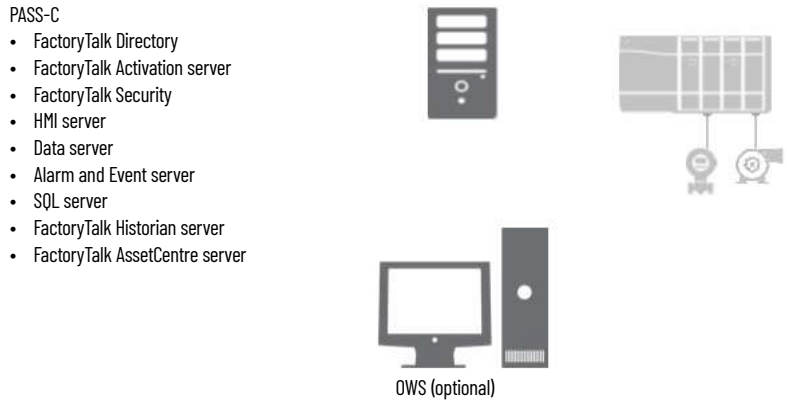
The consolidated Process Automation System Server (PASS-C) supports smaller systems, such as skids or stations, where the system software runs on only a few computers. The PASS-C offers reduced complexity and cost.

A PASS-C computer can be manually installed and configured or is available as a pre-configured virtual image. The virtual image includes a server-based Windows® operating system and contains pre-installed FactoryTalk server software. The PASS-C is intended to support up to 10 OWS clients.

Similar to the PASS-C, an operating workstation OWS virtual image is also available. This image includes a client-based Windows operating system that contains the required FactoryTalk client software.

Figure 1 illustrates a small PlantPAx system with a PASS-C that runs all FactoryTalk software and an OWS that provides a client interface.

Figure 1 - Smaller PlantPAx Systems with Single PASS-C Server



For more information, see the PASS-C chapter in the PlantPAx Template User Manual, publication 9528-UM001.

Process Automation System Server (PASS)

The Process Automation System Server (PASS) supports larger, distributed systems or customer-defined, critical processes. Whenever possible, use virtualization to provide greater computing efficiency, enhanced backup and recovery capability, and to offer high availability with server redundancy.

PlantPAx virtual images are available for PASS and application servers to run on server-based computer hardware with a hypervisor, such as VMware ESXi. The PlantPAx virtual images are deployed from templates and contain a Windows operating system along with pre-installed FactoryTalk software. The virtual images help:

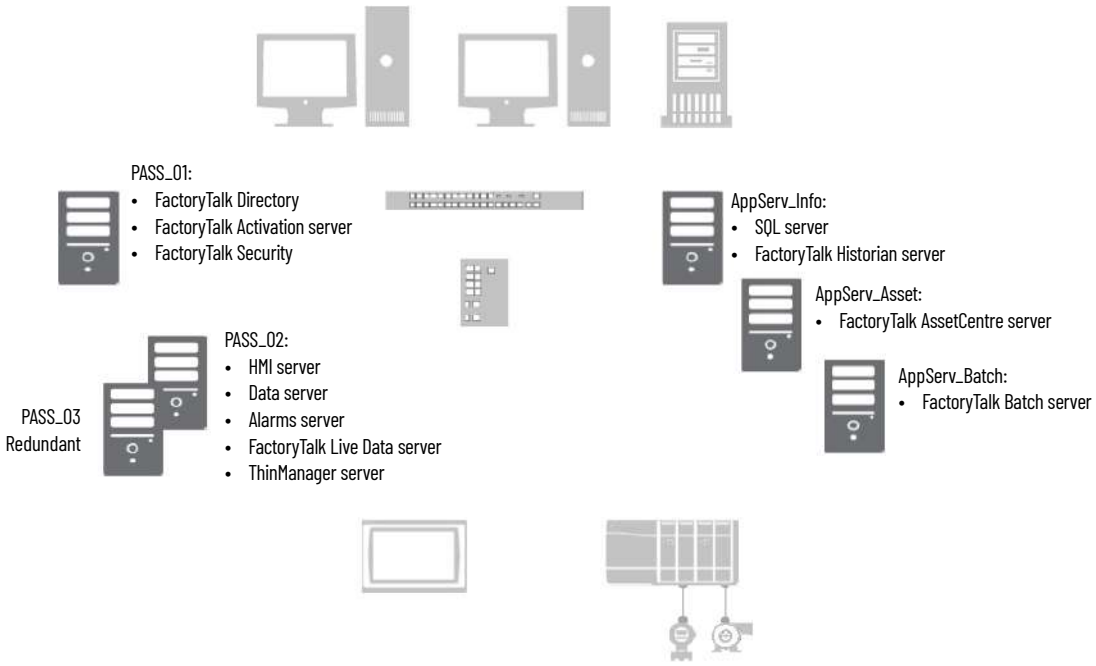
- Reduce installation time and increase consistency with drop-in virtual machines with pre-configured system elements
- Enable the consolidation of computing resources that multiple operating systems and applications can share a single physical server
- Support flexibility and portability across hardware platforms

For configuration details, see the PlantPAx Template User Manual, publication 9528-UM001.

Figure 2 illustrates a larger PlantPAx system, with two PASS computers and supporting application servers, in a network distributed architecture.

- **PASS_01** server contains the FactoryTalk Network Directory, Security configuration and often hosts FactoryTalk® Activation licenses.
- **PASS_02** server contains FactoryTalk® View SE (HMI server, data server, and alarms server) and optional ThinManager® server.
- An optional **PASS_03** server could be a secondary (HMI, data, and alarms server) that would switch over if PASS_02 was unreachable.
- **AppServ_Info** server contains a Factory Historian SE server and a local Historian database.
- An optional **AppServ_Info2** server could be a redundant FactoryTalk® Historian SE server, as part of a collective. In this configuration, the Historian database would be hosted on a separate computer that both could access.
- **AppServ_Asset** server contains FactoryTalk® AssetCentre for system tracking and verification.
- **AppServ_Batch** server contains FactoryTalk® Batch software to handle large batching processes.

Figure 2 - Large PlantPAx Systems with Multiple Servers



Next Steps

Once you have sized your system and decided on whether to use a PASS-C or PASS, complete the following:

1. Manage Servers and Security Policies

   A Domain Controller is recommended for most PlantPAx systems, however, in smaller systems a Workgroup can be sufficient.

   For more information, see Chapter 2, Domain or Workgroup
2. Configure the Process Automation System Server

   For more information, Chapter 3, Process Automation System Server
3. Design Network Topologies and Configure Switches

   The PlantPAx system supports several network topologies to meet various system requirements. Each topology is based on system characterization tests to help deliver system performance.

   For more information, see Chapter 4, Network Infrastructure
4. Develop Process Applications

   Process applications implement control strategies that encompass control logic and HMI displays.

   Execute control logic on Logix 5000® process controllers. The process controller comes with a default task model and embedded PlantPAx instructions that improve design and deployment efforts. The process controller is also conformal-coated for protection from dust and corrosive pollutants.

   Deploy HMI displays for operators and maintenance personnel so they can monitor and maintain the system.

   For more information, see Chapter 5 - Process Controller Features,

Chapter 6 - Bulk Configuration of a PlantPAx System, and Chapter 7 - Modifying an Existing PlantPAx System.

5. Add Application Servers

   PlantPAx application servers (AppServ) manage system software that is required for your application. There can be multiple servers depending on the size and structure of your application.

Table 2 - System Server Descriptions

AppServ Elements	Description
AppServ-Asset	The asset management server acts as a centralized tool for managing automation-related asset information (both Rockwell Automation and third-party assets). The asset management application server includes capabilities for source control, audits, change notifications, reporting, security, and backup/restore. For more information, see Chapter 8, Asset Management.
AppServ-Info (Historian, SQL)	Data management storage can include a Historian or SQL server. These two servers depend on the function that is being provided: FactoryTalk Historian software or a SQL server. For more information, see Chapter 9, Historical Data.
AppServ-Batch	The batch application server provides comprehensive batch management, including unit supervision, recipe management, process management, and material management. The batch application server can be linked with visualization elements on the OWS and configuration clients on the EWS. For more information, see Chapter 10, Batch Management.

Guidelines for Servers and Workstations

The following guidelines for servers and workstations are already implemented in the PlantPAx templates. If you create custom VMs, follow these guidelines to align with PlantPAx configurations.

- Install the latest software patches for all Rockwell Automation software.

  The Patch File Validator utility verifies software versions on your system and installs a patch roll-up. To download, see the Knowledgebase Technote Patch File Validator Utility.
- Disable power-saving for the Network Interface Card (NIC).

  The NIC card connects a workstation to other devices on the network. The power-saving feature turns off the network card when not in use, which can interfere with network throughput.
- Disable power-saving for the Windows operating system.

  The power-saving feature turns off Windows features when not in use, which can interfere with network throughput.
- Enable Remote Desktop Server (RDS) functionality on application servers that need remote access, such as the AppServ-EWS or AppServ-OWS (available via templates).

  RDS enables multiple instances of the OWS and EWS as thin clients from one server. Thin clients can run applications and process data on a remote computer to minimize the amount of information on a network.

  Enable Adjust for Best Performance so that Windows features that are not is use are turned off, which yields more memory and performance for the system.
- Make sure that the user is never notified by the User Account Control.
- Disable automatic Windows updates. This helps prevent updates that haven't been qualified by Rockwell Automation from being installed on the workstation or server.

The only exception is if your organization has a controlled patching process to verify updates on a non-production system, or when a facility is non-active, to reduce the chance of any unexpected results or side effects.

Antivirus

PlantPAx recommends the installation of antivirus software on servers and workstations running industrial automation software. Although all FactoryTalk software is expected to be compatible with the antivirus protections on the market, PlantPAx has tested Windows Defender and Crowdstrike antivirus packages. These antivirus packages had no adverse effect on the performance of the PlantPAx Distributed Control System when used with the default configurations.

- Proper configuration, management, and updating of antivirus software is required. Any antivirus protection can impact operation if the configuration of firewalls, network threat protections, and access controls is too restrictive.

PlantPAx System ID

The PlantPAx system ID is a unique identifier that helps simplify the management of your system over its lifecycle. The System ID creates a record of the installed products in your system and provides a dashboard that shows the hardware lifecycle status, notifications of updates and patches, and compatibility information. Use this information to:

- Plan spare and replacement parts to better size inventory
- Define the boundaries of the system
- Plan when and where to implement system upgrades

The system ID is **only** available if you purchase a PlantPAx catalog number for the software for the first PASS in your system. The catalog number determines an activation string for the software products on the bundle. This activation string (serial number) is the system ID.

The system integrator uses an Asset Inventory Agent in a FactoryTalk AssetCentre project to generate an inventory file (.raai file). The System ID is gathered via the license number of FactoryTalk AssetCentre via FactoryTalk Activation Manager. The System Integrator registers your System ID with Rockwell Automation and provides you directions on how to access your MyEquipment portal.

System Verification

A critical system attribute is a visible performance indicator of a system-wide characteristic. Critical system attributes do the following:

- Determine system limits
- Establish system rules
- Establish system recommendations
- Measure system element and system infrastructure performance

The following critical system attributes are used to verify PlantPAx system characterization.

Table 3 - CSA Performance Indicators

Critical System Attribute	Performance
Display callup (paint time)	A noncached display is called up by the operator and ready for operator use within 2 seconds.
Display update	The display updates control information within 1 second.
Steady state alarm time	Steady state alarms occurring at 20 per second are timestamped within 1 second.
Alarm burst time	All alarms in a burst of 2000 alarms are timestamped within 3 seconds.
Recovery	A system element returns to full operation within 5 minutes of the restoration after a failure or loss.
Operator-initiated control	Operator-initiated actions are loaded into the controller and the feedback for the operator action is within 2 seconds.
Batch server: operator action time	An operator batch command has been acted on by the controller in 1 second.
Batch server: server action time	A server batch command has been acted on by the controller in 1 second.
Batch server: controller action time	Batch status events display on the operator workstation within 1 second.

For a complete system verification, use the guidelines in Appendix C, PlantPAx Deployment Recommendations and Verification Tool.

Notes:

Domain or Workgroup

PlantPAx® systems require computer management, from either a domain controller or workgroup configuration, for secure interaction.

- A Windows® 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
- A Windows workgroup computer is independently configured. Workgroups are only suitable in smaller systems with 10 or fewer computers.

The following is the recommended workflow to configure a domain controller or workgroup. For experienced users, each step outlines requirements. For more detailed information, follow the referenced links.

Step 1: Configure the Domain Controller or a Workgroup

In larger systems, create a dedicated domain controller for the PlantPAx system. If your control system contains an existing domain controller, add the configuration that is recommended for a PlantPAx system. Domain controller components include:

- Microsoft Windows Server operation system
- Active Directory Domain Services, DHCP, and DNS Server Roles.
- Parent and child domains
- Reverse DNS Lookup Zone.
- Configure DHCP server options and authorize server.

For more information, see Primary Domain Controller.

Windows Workgroups are available for small systems that do not require complex security controls. Considerations when using a workgroup include:

- There are typically no more than 10 computers.
- All computers must be on the same local network or subnet.
- All computers are peers; no computer has control over another computer.
- Each computer has a set of user accounts. To log in to any computer in the workgroup, you must have an account on that computer.
- A workgroup isn't protected by a centrally managed password.

For more information, see Windows Workgroup.

Step 2: Configure a Redundant Domain Controller

If needed, create a redundant domain controller for high availability. Considerations for the redundant domain controller include:

- The redundant domain controller has a unique name and IPv4 address.
- Install the Active Directory Domain Services role and promote to domain controller.
- Add the Directory Services Restore Mode (DSRM) password.

For more information, see Additional Domain Controller.

Step 3: Create Roles, Areas, and Users

There are required roles for a PlantPAx system. Areas and users depend on your application. Assign users to Roles and Areas.

The PlantPAx Roles are:

- PlantPAx Administrator
- PlantPAx Engineering
- PlantPAx Maintenance
- PlantPAx Maintenance Supervisor
- PlantPAx Manager
- PlantPAx Operator
- PlantPAx Operator Supervisor
- PlantPAx View Only

Name areas based on access, for example:

- Area01_Advanced (engineering access)
- Area01_Basic (non-engineering access)

Replace 'Area01' with the name of your process area.

For more information, see Create Roles, Areas, and Users.

Step 4: Configure Group Policies

Configure recommended group policies for a PlantPAx system, such as:

- Windows NTP client
- Windows time service

For more information, see Configure Group Policy Management.

Configure recommended security policies, such as password strength, account lockout, Kerberos, and interactive login.

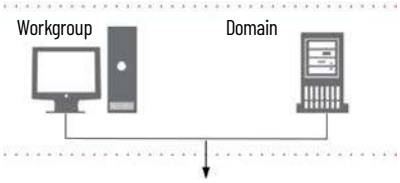
For more information, see Configure Group Policies.

Create a PlantPAx user policy that limits access to USB drives, portable devices, and other software.

For more information, see PlantPAx Users Policy Object.

Prerequisites

Following the System Workflow, configure a domain controller or a workgroup, depending on the size of your system.



The PlantPAx architecture assumes that there's a Microsoft Windows forest in place to host a supervisory and/or control domain network.

- You need at least one domain controller per each parent/root/child domain.
- The domain controllers are separate computers.
- You need at least two domain controllers for fault tolerance.
- Do not load any application software on a domain controller.
- The domain controllers must be local (within the firewall) to the PlantPAx system.

We recommend that PlantPAx servers and workstations be members of a Windows domain. However, workgroups are supported for systems with 10 or fewer workstations and servers.

Configuration	Details
Workgroup - decentralized administration (allowed if 10 or fewer computers)	Workgroup advantages: • No domain controller (Windows Server OS) to purchase or maintain. • Recommended for small PlantPAx applications only where user accounts do not change often Workgroup rules: • All workstation and server system elements in a single PlantPAx system must be members of the same workgroup • All users participating in the workgroup must be members of the Administrators group • Create the same set of user accounts and passwords on every computer in a FactoryTalk® View application
Domain - centralized administration (recommended)	Domain advantages: • Centralized administration of users, policies, and security • High availability, when both primary and secondary domain controllers are used. • Recommended for larger systems to provide the best system performance. Domain rules: • All workstation and server system elements in a single PlantPAx system must be members of the same domain • PlantPAx server system elements must not be used as domain controllers. • Required for systems with more than 10 computers • The domain controller must be its own independent computer with no other application software.

For more information, see this additional resource.

Resource	Description
Windows Operating System and domain references	Microsoft® online libraries, for example TechNet, provide detailed guidelines for all aspects of the Windows and Windows domains. Examples of detailed guidelines are design, deployment, maintenance, security, disaster recovery, and so on. PlantPAx documentation provides best practice critique to certain Windows roles, features, and such where a typical PlantPAx DCS is hosted.

Primary Domain Controller

The domain controller manages:

- IP address scheme for the computer network
- DNS and reverse lookup zone
- DHCP server
- Assigned roles, areas, and users
- Group policies

If your company has an existing domain infrastructure, in which the PlantPAx system interacts with, please consult with your local IT resources before continuing.

Create the Primary Domain Controller

Starting with a new installation of Windows Server 2019 operating system, login as local administrator. The computer is initially assigned a random 15-character computer name, which looks something like this: WIN-VPLC4SD9KWG.

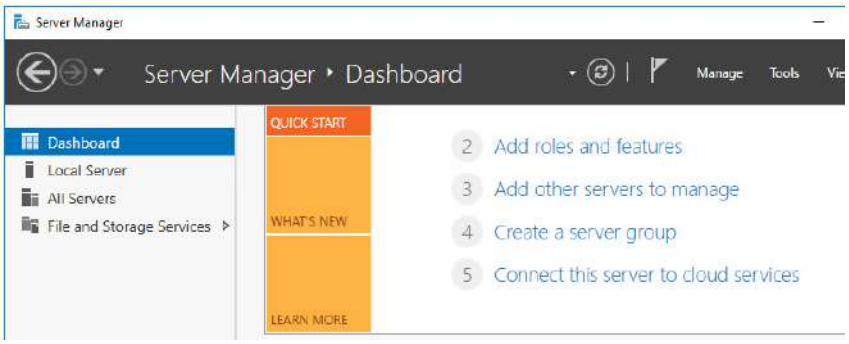
1. Change the computer name to comply with your company naming guidelines. Or, in this example, to reflect it as being a process automation domain controller (PADCA, PADCB, and so forth).
2. Next assign the Windows server a fixed IP address (TCP/IPv4), within the subnet designated for the given network architecture.

   For example: 172.18.1.10

Install Active Directory Services, DHCP, and DNS Roles

Before a Windows server can function as a domain controller, additional roles and features must be installed.

1. Launch the Server Manager.



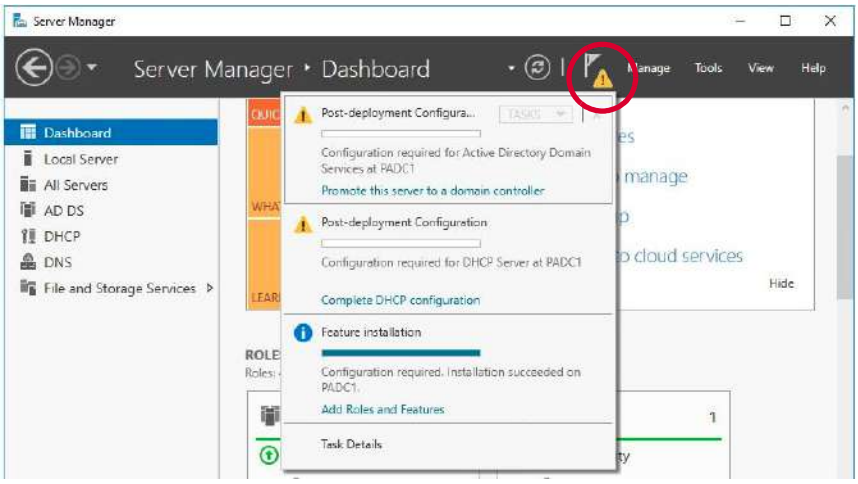
2. From the Dashboard, click the second option to 'Add roles and features'. Use the following table to complete the configuration.

Roles and Features Wizard	Configure
Before You Begin	Read and click next
Installation Type	Check 'Role-based or feature-based installation.'
Server Selection	Select a server from the server pool. Select the local computer PADCA in the Server Pool list
Server Roles	In the Roles dialog, select the following: • Active Directory Domain Services • DHCP Server • DNS Server
Pop up dialog. Add features that are required for Active Directory Domain Services.	Check the option to Include management tools (if applicable) and then select Add Features.
Features	Select the available .NET Framework features to be installed on the domain controller. Check 'Group Policy Management.'
AD DS	Active Directory Domain Services requires a DNS server. If selected for the Server Role, click Next.
Confirmation	Check 'Restart the destination server automatically if necessary', and select Install.
Results	Once the installation process completes, close the wizard and restart the server if necessary.

Promote the Primary Domain Controller

On the Server Manager management console, complete these steps for the active domain computer.

1. Select the Alert flag on the header.



2. Select 'Promote this server to a domain controller'.
3. Using the Active Directory Domain Services Configuration Wizard, use the following for guidance on your deployment.

IMPORTANT Take careful consideration when specifying a new root domain name.

- Understand domain naming conventions so they make sense given your system, owner, or location.
- Do not use any reserved words or characters, and use caution if adding a period, which must not be used in later versions of Windows.
- See Microsoft Support for more information on naming conventions in Active Directory for computers, domains, sites, and organizational units.

Topic	Configure
Deployment Configuration	Select to 'Add a new forest'. Specify the domain information for this operation. Enter a Root Domain Name. Examples: • PlantPAx.Company.Local • DCS.PlantPAxMfg.com • PlantPAx.RockwellAutomation.com
Domain Controller Options	Select Windows Server 2019 as the Forest functional level. Select Windows Server 2019 as the Domain functional level. Check 'Domain Name System (DNS).' Check 'Global Catalog (GC).' Enter a Directory Services Restore Mode password **IMPORTANT**: You use this password when you configure a redundant domain controller and for any subsequent DC recovery efforts. Record this password in a safe/secure place.
DNS Options	Do not specify 'DNS Delegation options.'
Additional Options	Make sure that the domain name is used for the NetBIOS Domain Name. Accept defaults for the remaining options.
Paths	Use the default folder locations.
Review Options	Review your selection options.
Prerequisites Check	Validate all prerequisites and Install if no errors. The server restarts.

Additional Domain Controller

IMPORTANT For each additional domain controller, you must have a fresh installation of Windows Server 2019 operating system before repeating the 'Create the Primary Domain Controller' procedure.

Create an Additional Domain Controller

To reduce disruptions during unplanned and planned downtime, add another Domain controller for backup as well as scalability later.

1. Change the computer name to comply with your company naming guidelines. Or, in this example, to reflect it as being a process automation domain controller (PADCB, and so forth).
2. Next assign the Windows Server a fixed IP address (TCP/IPv4), within the subnet designated for the given network architecture. For example, 172.20.1.11, and supply the DNS address from the initial domain controller: 172.20.1.10
3. Repeat Create the Primary Domain Controller steps. Name, address, and install Active Directory roles for the additional domain controller.
4. Install the 'Active Directory Domain Services' role.

Install Active Directory Services, DHCP, and DNS Roles

Just like creating the primary domain controller, repeat these steps.

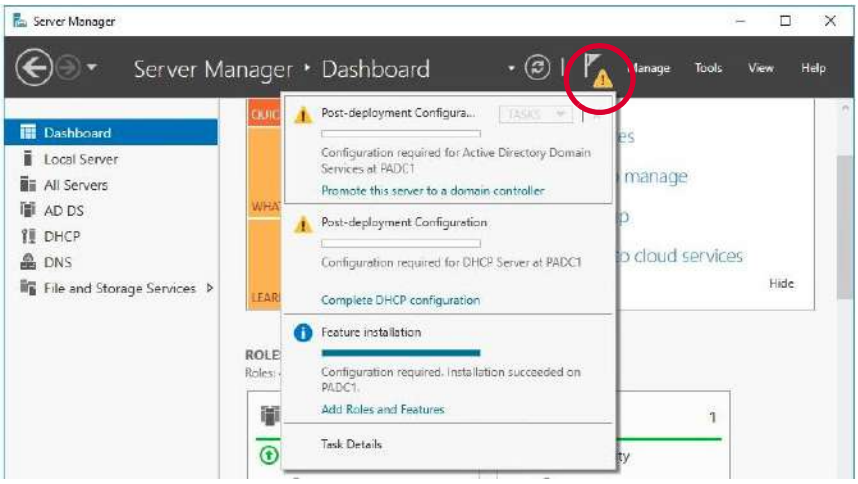
1. Install Active Directory, DHCP, and DNS roles used on creating the primary domain controller.
2. Install the 'Active Directory Domain Services' role.

See the primary domain controller instructions if you need help with using the roles wizard.

Promote the Additional Domain Controller

On the Server Manager management console, complete these steps for the standby domain computer.

1. Select the Alert flag on the header.



2. Select 'Promote this server to a domain controller'.
3. Using the Active Directory Domain Services Configuration Wizard, use the following for guidance on your deployment.

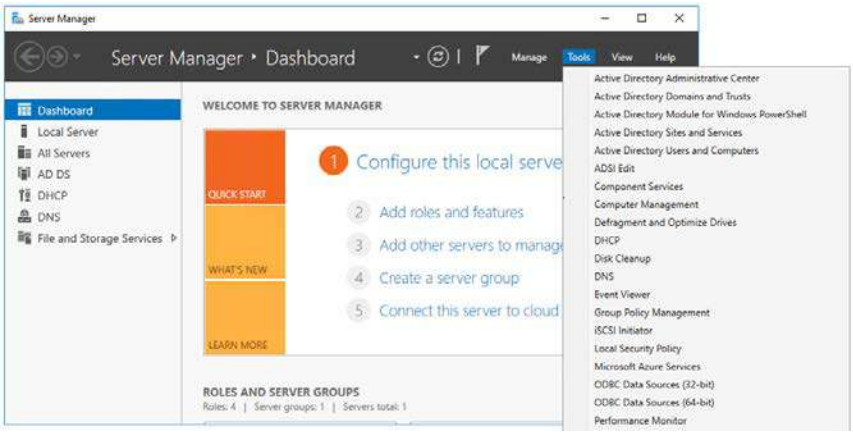
AD DS Configuration Wizard	Configure
Deployment Configuration	Select to 'Add a domain controller to an existing domain.' Select the Domain: Select the forest:
Domain Controller Options	Select Windows Server 2019 as the Forest functional level. Select Windows Server 2019 as the Domain functional level. Check 'Domain Name System (DNS).' Check 'Global Catalog (GC).' Enter a Directory Services Restore Mode password. **IMPORTANT**: You use this password when you configure a redundant domain controller and for any subsequent DC recovery efforts. Record this password in a safe/secure place.
DNS Options	Do not specify 'DNS Delegation options.'
Additional Options	Replicate from: 'your domain name'
Paths	Use the default folder locations.
Review Options	Review your selection options.
Prerequisites Check	Validate all prerequisites and Install if no errors. The server restarts.

Configure Domain Controllers

On the primary and additional domain controller, now you can implement and configure the new features and roles that were added, such as: Active Directory, DHCP, and DNS.

Server Manager Tools Menu

The Windows 'Server Manager' contains a Tools menu that provides quick access to many of the management consoles required for the following configurations.

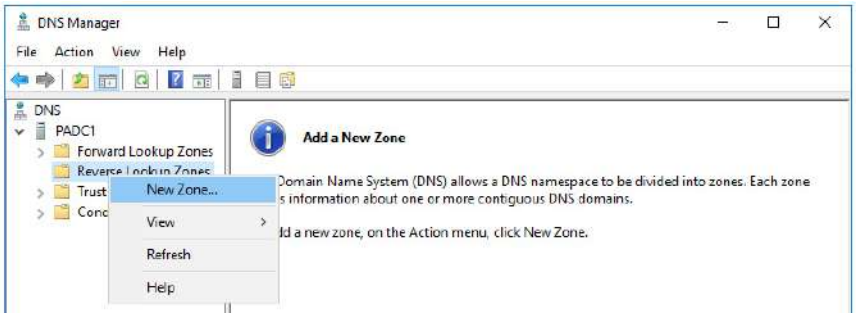


Create a Reverse DNS Lookup Zone

Reverse lookup zones are used to resolve IP addresses to host names, rather than host names to IP addresses, as is the case with forward lookup zones. You must program a special domain namespace (in-addr.arpa) as a reverse lookup zone.

On your initial domain controller, use the Server Manager to access the DNS Manager console window.

1. To access the DNS Manager, right-click Reverse Lookup Zone New Zone.



2. Configure the New Zone wizard as shown in the following table.

Basic Step	Configure
Zone Type	Select 'Primary zone.'
Active Directory Zone Replication Scope	Check 'To all DNS servers running on domain controllers in this domain <your target domain>'. For example: PlantPAx.MyCompany.Local.
Reverse Lookup Zone Name	Check 'IPv4 Reverse Lookup Zone.'
Network ID	Enter the network ID portion of the IP address of the domain controller (omit the last number). For example, enter 172.20.1.
Dynamic Update	Check 'Allow only secure dynamic updates (recommended for Active Directory).'

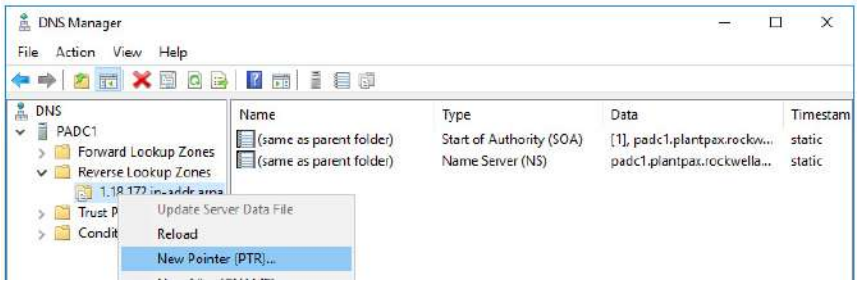
A successful configuration displays details of the lookup zone.

Map the Host Name to the IP Address

Create a pointer (PTR) record that associates the DNS name to the IP address. During a search, the IP address is reversed to find the associated DNS name.

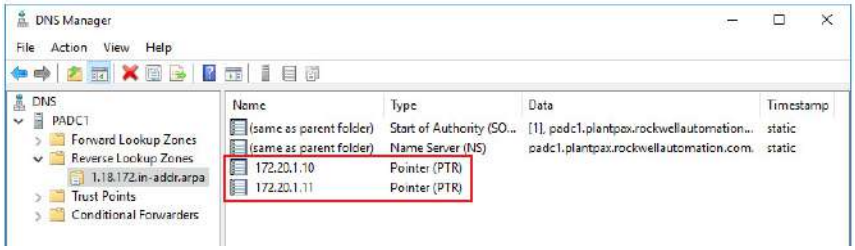
From the Server Manager, use the DNS Manager to create the New Pointer (PTR).

1. Go to Tools > DNS > Reverse Lookup Zone > Zone > New Pointer



2. Enter the IP address of the domain controller and browse for the host name.

   Successful configuration shows pointers for both a primary and secondary domain controller.

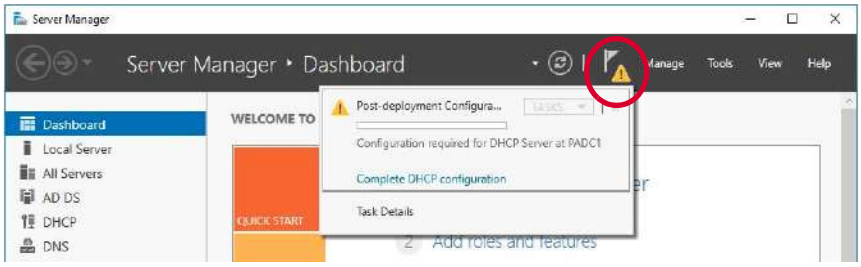


Add DHCP Features

A DHCP server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices that request the information.

On the Server Manager management console, complete these steps to add a DHCP server.

1. Select the Alert flag on the header.



2. Click to 'Complete DHCP configuration'
3. Open the DHCP management console and right click IPv4 > New Scope and configure the following for the control network.

Basic Step	Configure
Scope Name	Enter a name (such as Control Network) and a description (such as PlantPAx Control Network).
IP Address Range	Enter the start and end of the IP address range. Example: Start IP Address: 172.20.1.128 End IP Address: 172.20.1.254 Length: 24 Subnet Mask: 255.255.255.0
Add Exclusions and Delay	Optional: Exclusions are address or a range of addresses that aren't distributed by the server. A delay is the time duration by which the server delays the transmission of a DHCPOFFER message.
Lease Duration	The lease specifies how long a client can use and IP address from this scope. Default values: Days: 8 Hours: 0 Minutes: 0
Configure DHCP Options	You have to configure the most common DHCP options before clients can use the scope. Select: 'Yes, I want to configure these options now'.
Router (Default Gateway)	Enter the gateway IP address. Example: 172.20.1.1
Domain name and DNS servers	Parent Domain: 'your domain name' Server IP addresses. Example: 172.20.1.10 and 172.20.1.11
WINS	Optional: Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.
Activate Scope	Select 'Yes, I want to activate this scope now'.

Configure Failover

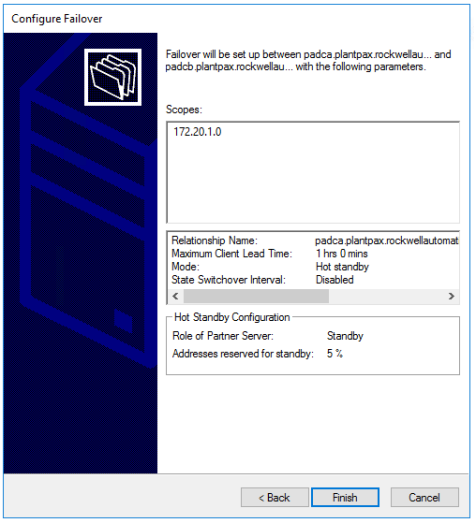
This DHCP option provides high availability by synchronizing IP address information between two DHCP servers.

1. Go to Tools > DHCP > primary domain > IPv4 > Configure Failover and configure the following.

Basic Step	Configure
Configure Failover	Click Add Server and locate the secondary domain controller. Example: PADCB
Create New Failover Relationship	Select 'Hot standby' for mode. You can also choose to require authentication (a shared secret password) to secure communications between failover partners. Enter a 'Shared Secret', which can be passwords, pass phrases, or random numbers.

2. Repeat step 1 to configure a second DHCP server.

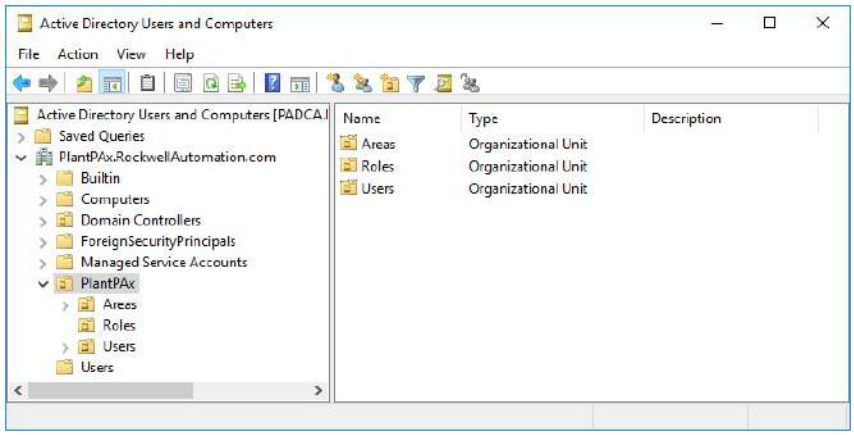
   A successful configuration displays details of the failover configuration.



Create Roles, Areas, and Users

From operators and maintenance personnel to engineers, the domain controller manages groups in the Active Directory. Use the Server Manager to configure the roles, areas, and users.

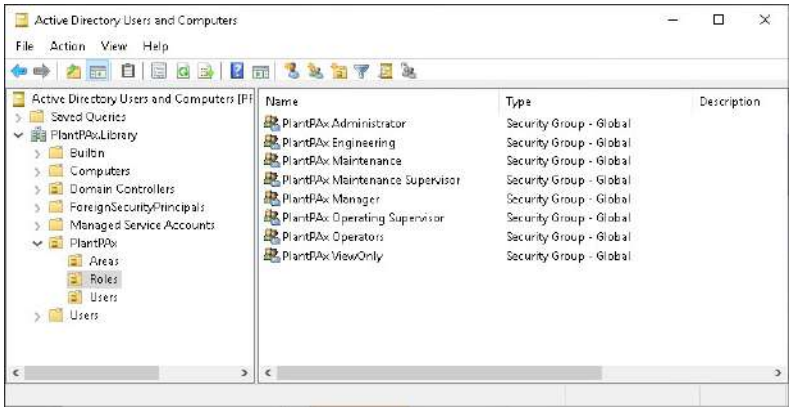
1. Use the Windows Server Manager Tools menu to launch the 'Active Directory Users and Computers' console.
2. From your domain, right-click, select New> Organizational Unit and type the name PlantPAx.
3. Under the PlantPAx group, right-click and select New > Organization Unit to create folders for Users, Areas, and Roles.



Add Groups for Role-Based Security

Roles define different security access for areas of a plant. We recommend the following roles:

- PlantPAx Operators
- PlantPAx Operating Supervisor
- PlantPAx Maintenance
- PlantPAx Maintenance Supervisor
- PlantPAx Manager
- PlantPAx Engineering
- PlantPAx Administrator
- PlantPAx View Only
- HMI Approver



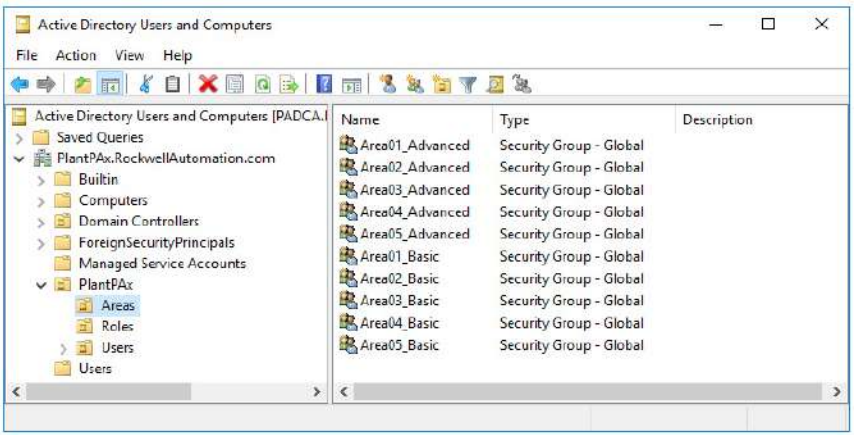
Add Groups for Area Based Security

We recommend the following areas that are based on a group:

- **Basic –** Allows access to non-engineer functions, such as Maintenance, Operator, on process library faceplates.
- **Advanced –** Allows access to engineering modifications on process library faceplates

IMPORTANT	Even though the examples show generic area names, such as Area01, we recommend that you use more specific names, such as Packaging, or Molding. And create two types for each area — Basic and Advanced—for each area.

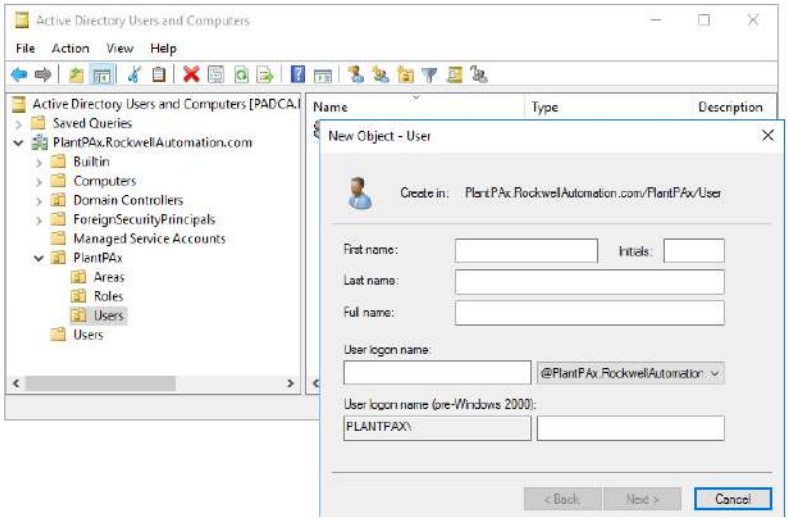
Create as many areas as needed for the system.



Assign Users

Users are unique to each system.

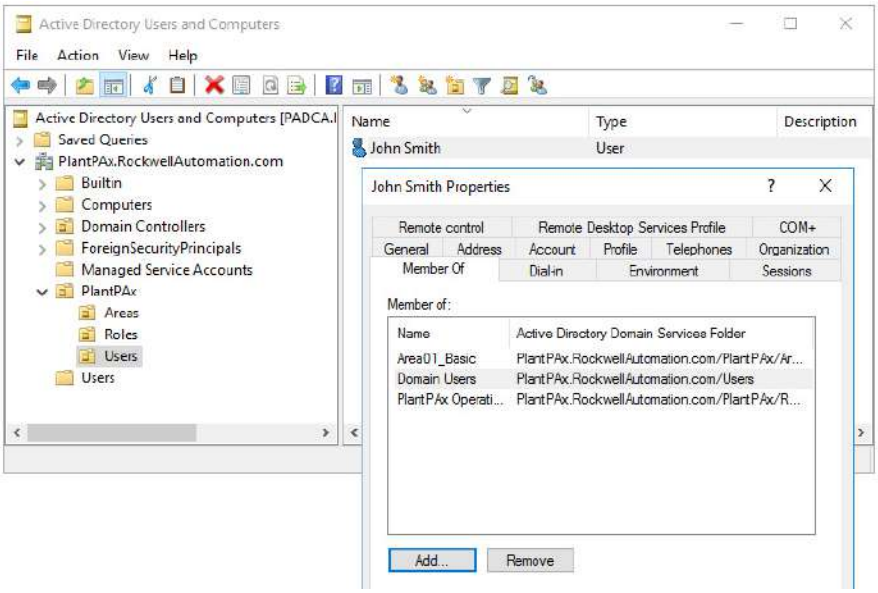
1. Create users and assign them to the Member tab on the Properties for the associated Role.



2. Once the user name and password are created, configure the following properties as shown in the table for each user.

On This Page	Configure
Properties	Select the domain on the 'Member of' tab
Select Groups	Type Area as the object name and select the appropriate Area

The successful configuration of a user shows both their domain and area.



Configure Group Policy Management

Group policies help reduce the maintenance and complexity when you add new users and computers into the PlantPAx system. The group policies determine what users can and can't do, such as password maintenance or to restrict folder access. The same approach applies for how to define server maintenance.

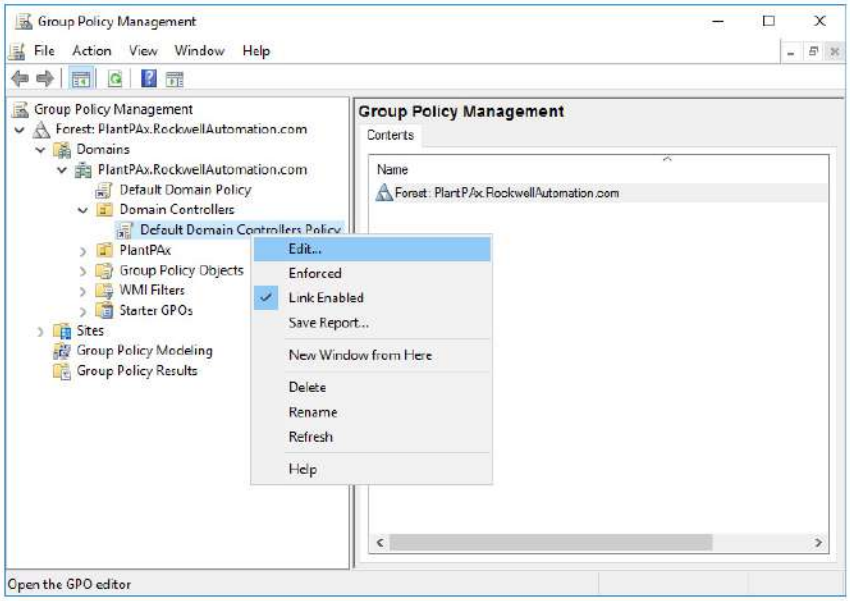
The settings that are outlined are baseline recommendations. Individual business, IT, and security requirements could require additional policies.

Configure the Windows NTP Client

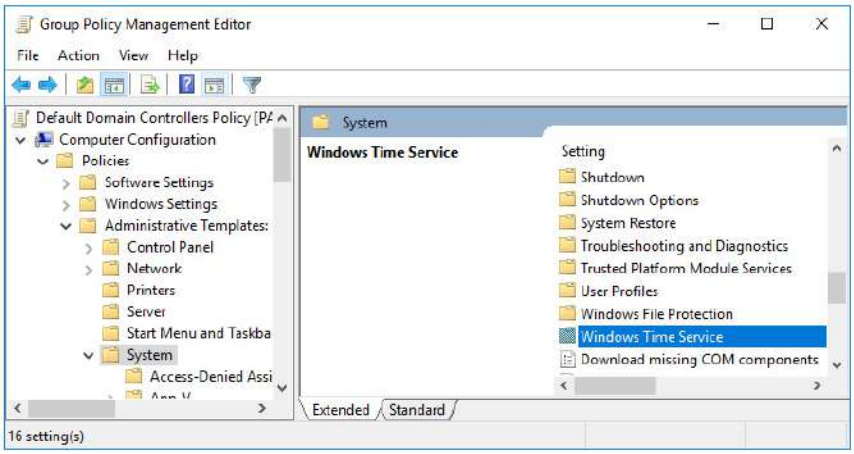
The domain is responsible to propagate and enforce the clock time to the domain computers. Use the Server Manager to configure the Windows NTP client so that the domain controller is in sync with the Windows NTP server.

1. Go to Tools > Group Policy Management.

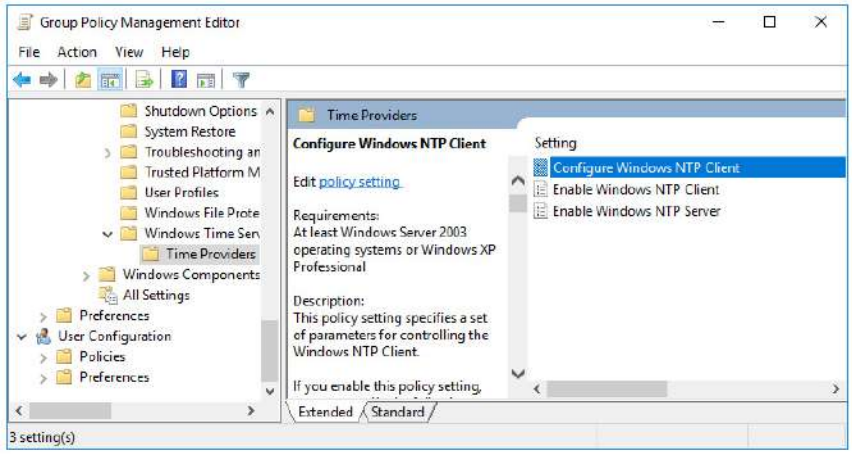
2. Select the Default Domain Controllers Policy to edit.



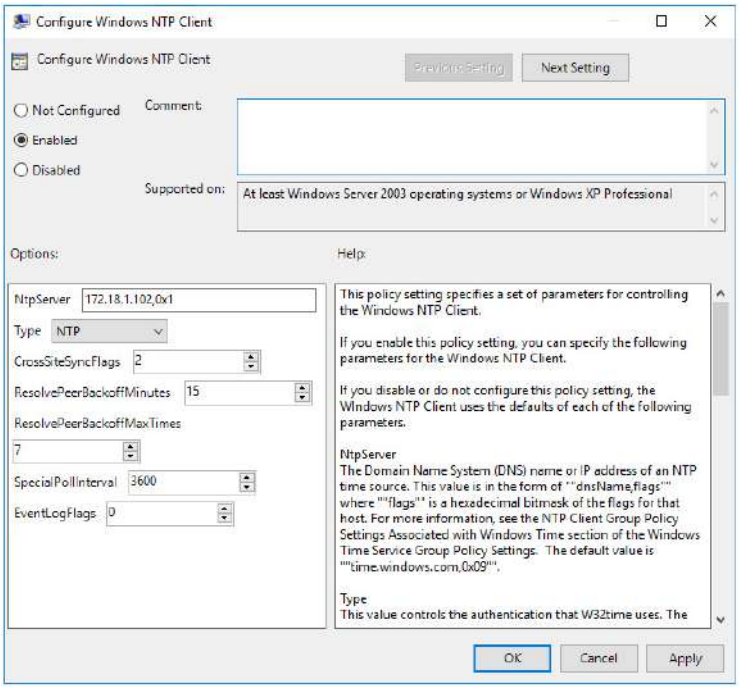
3. In the Group Policy Management Editor, select Policies > System > Windows Time Service.



4. Go to Time Providers > Configure Windows NTP Client.



5. Select 'Enable' and configure the 'Options' with your NtpServer: IP address and use Type: NTP.

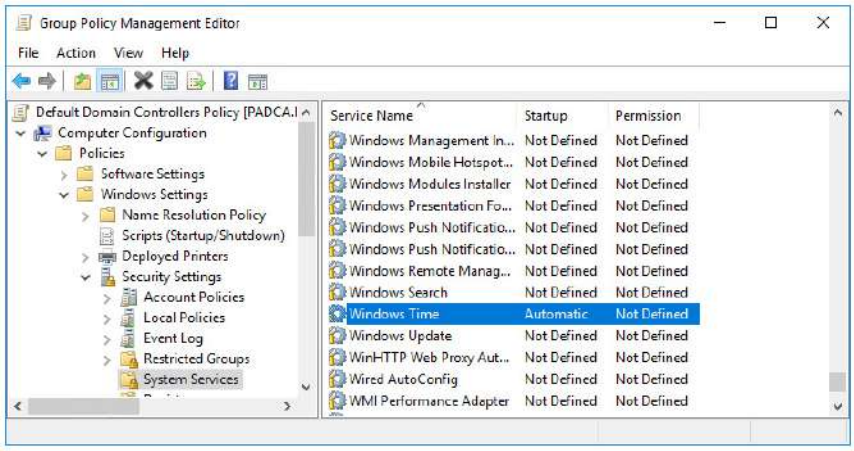


6. Go to Time Providers > Enable Windows NTP Client and check 'Enabled.'

Configure Windows Time Service

Enable the NTP server to initiate automatically upon startup.

1. In the Group Policy Management Editor, go to Policies > Windows Settings > Name Resolution Policy > System Services >Windows Time.

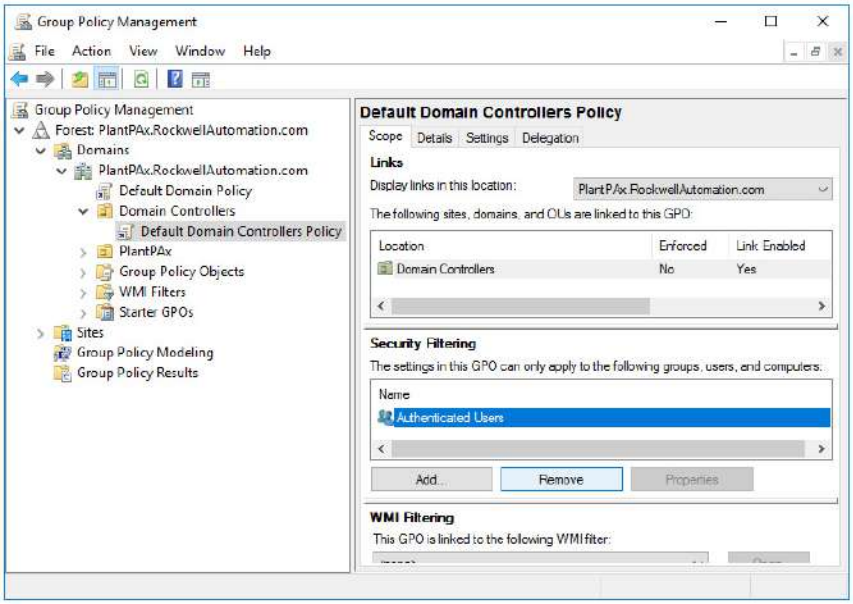


2. In the Windows Time Properties, select the following:
   - Check 'Define this policy setting.'
   - Check 'Automatic' for service startup mode.

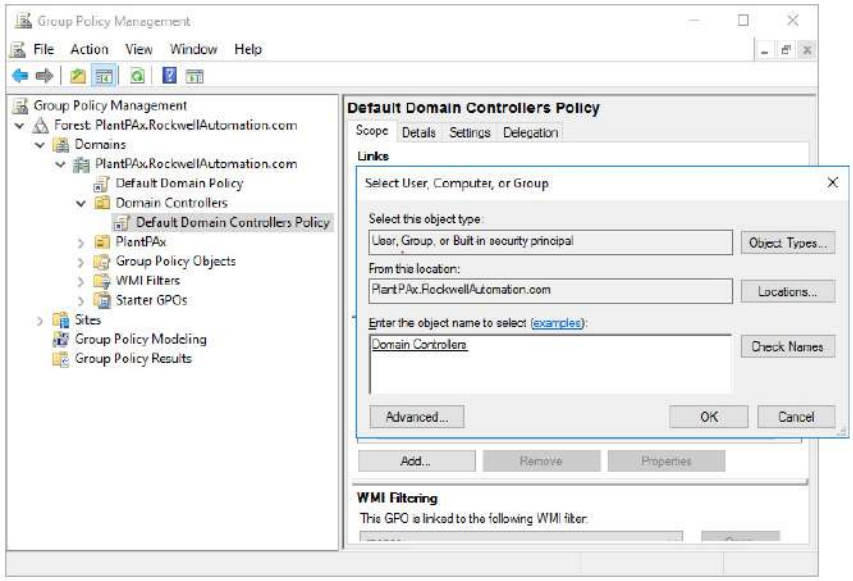
Enforcing the Domain Controller Policy

Policy enforces the domain controllers to use the NTP server settings.

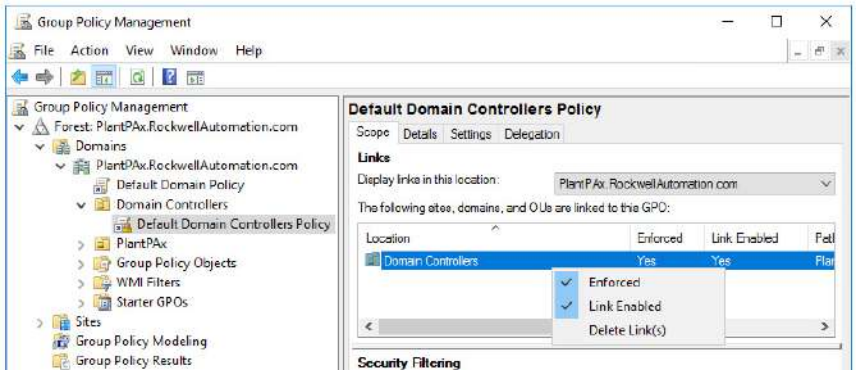
1. In the Group Policy Management Editor, select the Default Domain Controllers Policy and remove 'Authenticated Users' from Security Filtering.



2. Add Domain Controllers from the PlantPAx domain to Security Filtering.



3. Right-click Domain Controllers and select Enforced.



Configure Group Policies

These group policies are recommended:

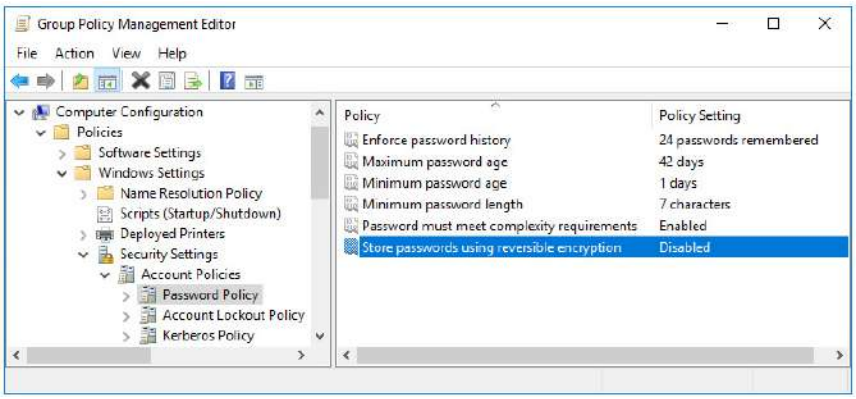
- Password strength
- Account lockout
- Kerberos
- Interactive login

Use the specifications for your PlantPAx system to set the values for these policies. If you configure any of these policies, you **must** enforce the policies on the domain controller for them to take effect.

Configure the Password Strength Policy

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

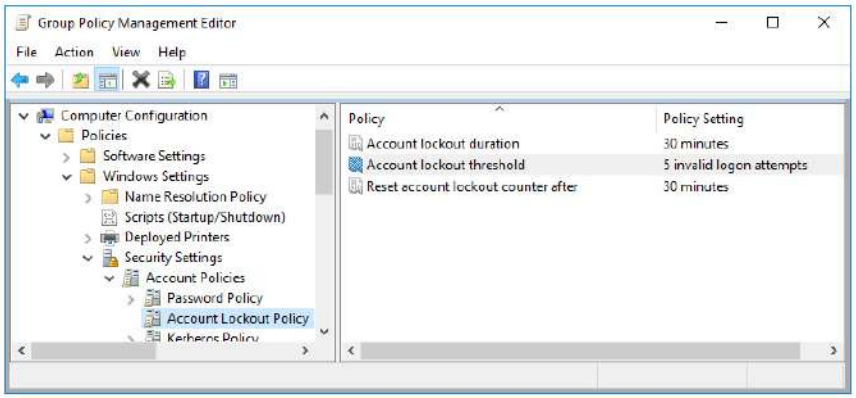
1. In the Group Policy Management Editor, select the Default Domain Policy to edit and select Password Policy.



Configure the Account Lockout Policy

This policy configures the number of password attempts and how an administrator resolves a user lockout situation.

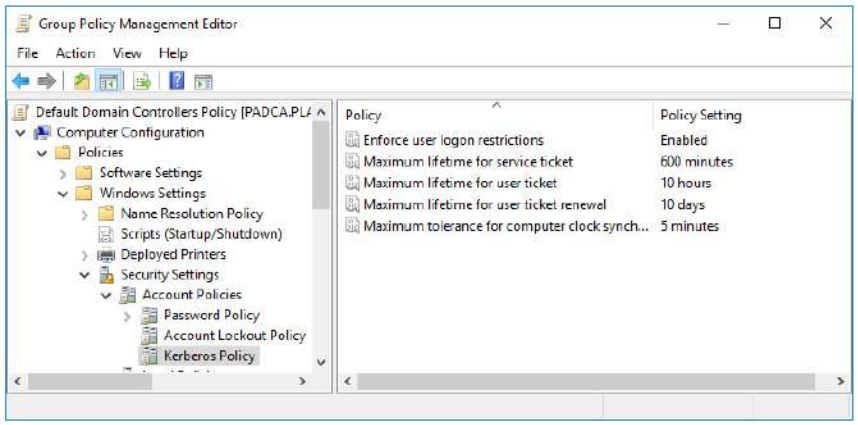
1. In the Group Policy Management Editor, select the Default Domain Policy to edit and select Account Lockout Policy.



Configure the Kerberos Policy

This policy helps administer network authentication.

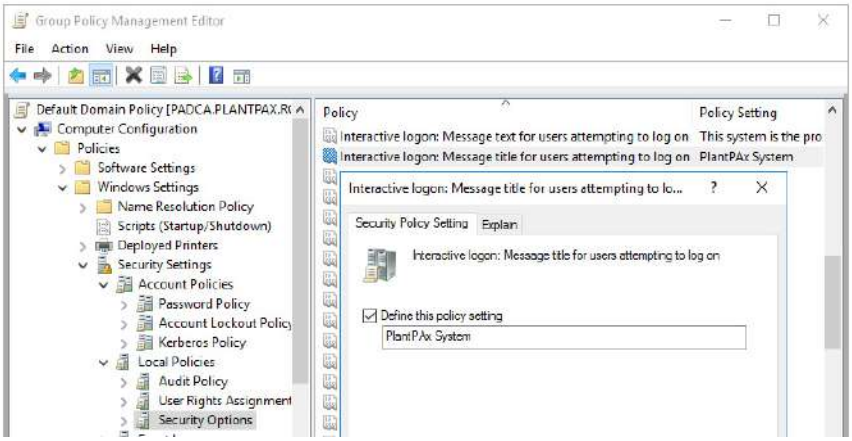
1. In the Group Policy Management Editor, select the Default Domain Policy to edit and select Kerberos Policy.
2. Enable the default options or modify if desired.



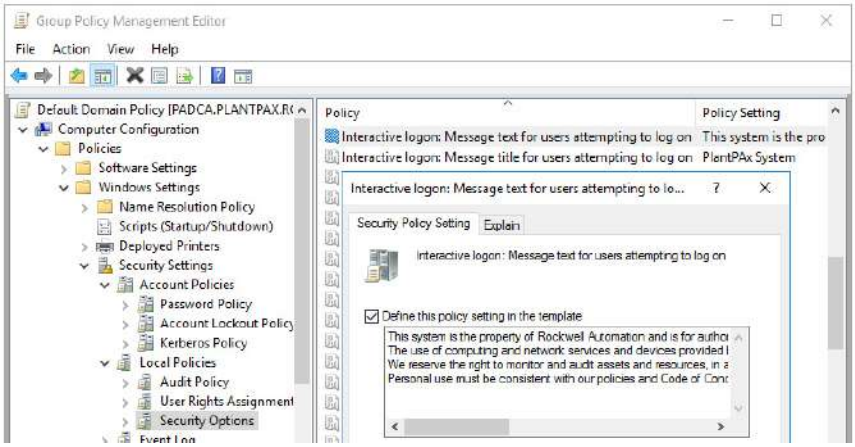
Configure the Interactive Logon Policy

This policy configures a warning message to users of the consequences for misusing company information.

1. In the Group Policy Management Editor, select the Default Domain Policy to edit and select Interactive Logon Policy.
2. In the tree configuration of the Group Policy Management Editor dialog box, Go to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies.
3. Select the Security Options folder and select the Interactive login: Message Title option. Enter the name of the group that receives the interactive message.



4. Select the Interactive Logon: Message text option. Enter the message that appears to users during login.



PlantPAx Users Policy Object

You can create a PlantPAx Users Policy to restrict privileges and site access. Recommended policies include access for the following:

- USB drive
- Portable device
- Software

Use the specifications for your PlantPAx system to set the values for these policies. If you configure any of these policies, you must enforce the policies on the domain controller for them to take effect.

For how to configure the recommended FactoryTalk® Security settings, see Configure System Security Features User Manual, publication SECURE-UM001.

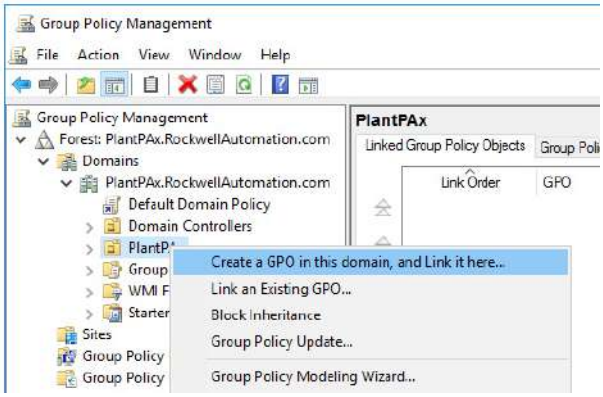
Knowledgebase Technote, *PlantPAx System Release 5.20 Configuration and Implementation Tools*, contains recommended FactoryTalk® Security policy settings for PlantPAx systems. Download the spreadsheet from this public article.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Create the PlantPAx Users Policy Object

You can select a group and set restrictions. For example, a group of users can't use USB drives as a layer of system security.

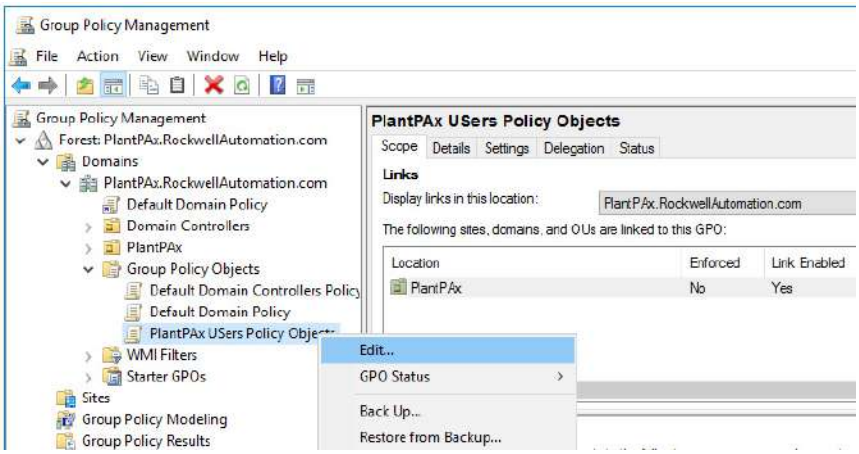
1. In the Group Policy Management Editor, select the PlantPAx Domain and select 'Create a GPO in this domain and link it here...'



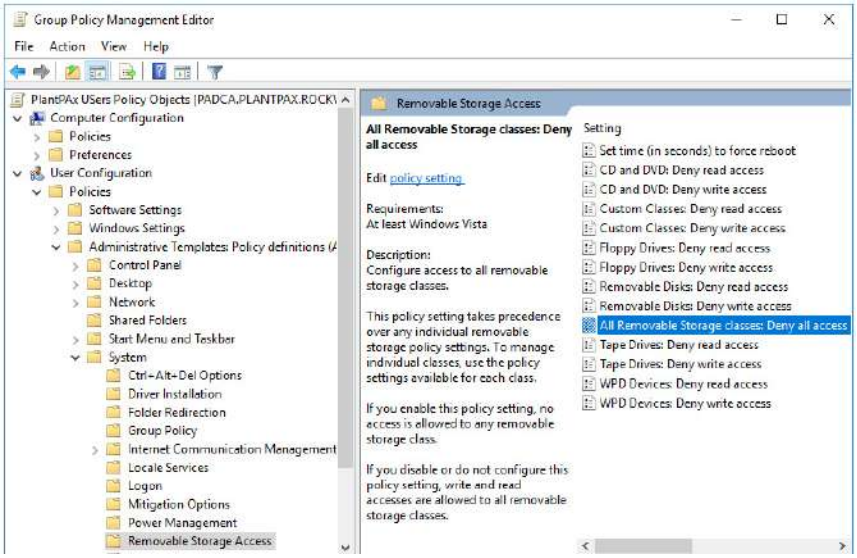
Configure the USB Drive Policy

A group of users can be restricted from using a USB drive.

1. In the Group Policy Management Editor, select the PlantPAx Users Policy Object to edit and select Removable Storage Access.



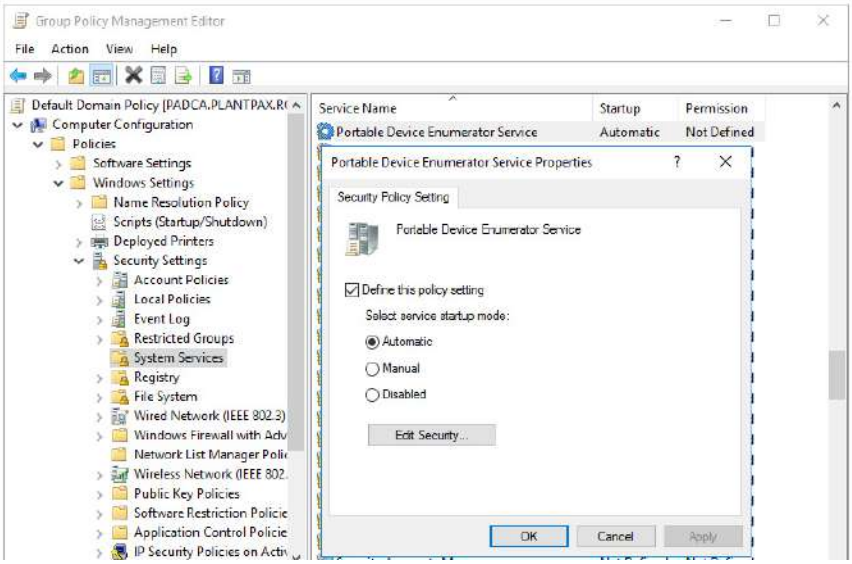
2. Go to Computer Configuration >User Configuration > Policies > Administrative Templates > System.
3. Select Removable Storage Access and choose All Removable Storage classes: Deny all access.
4. Select Enabled.



Configure the Portable Device Enumeration Policy

This policy enforces Group Policy Objects for connected mass storage devices.

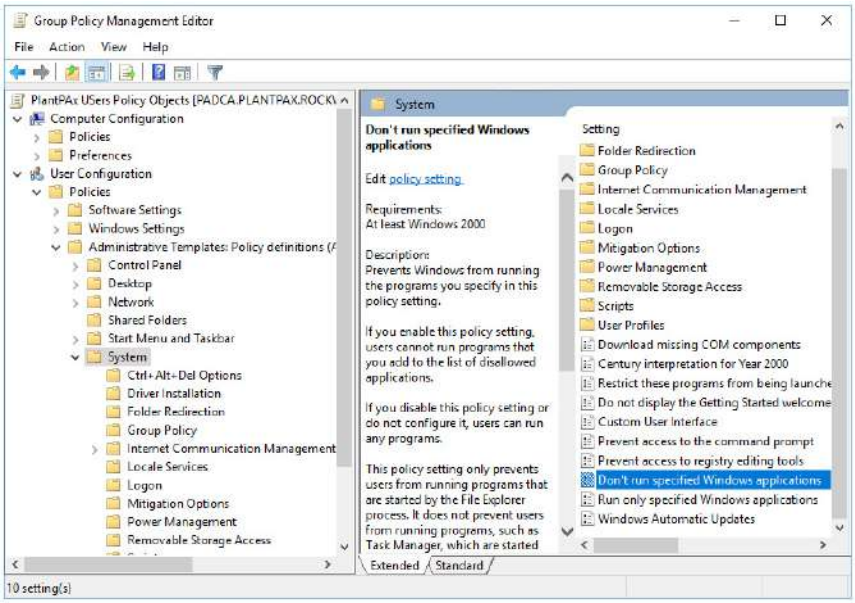
1. In the Group Policy Management Editor, select the PlantPAx Users Policy Object to edit and select Portable Device Enumeration Policy.



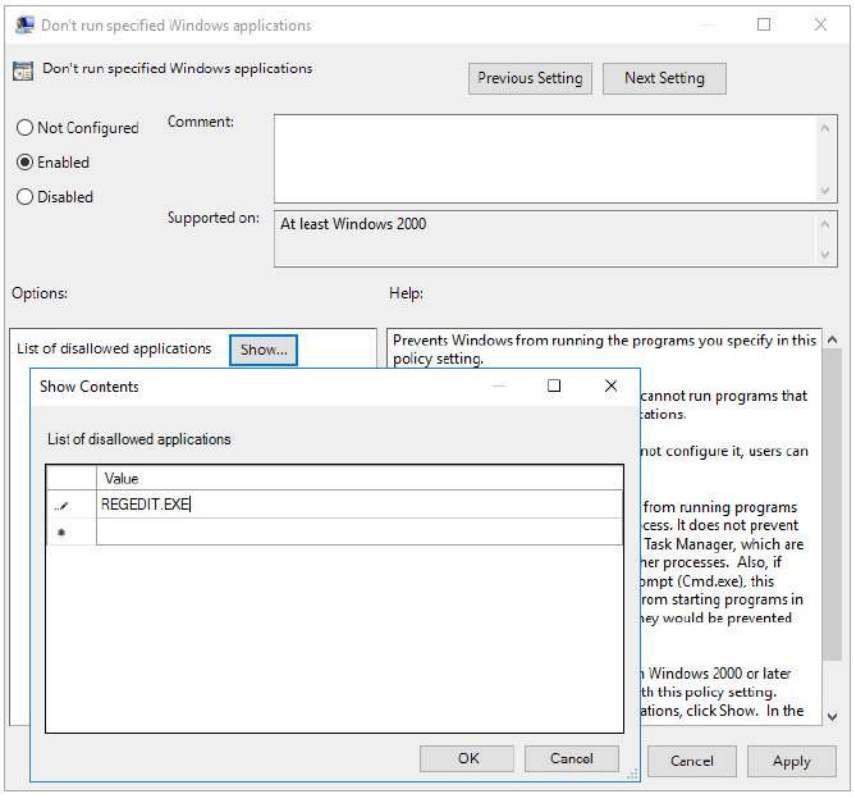
Configure the Software Access Policy

This policy helps protect against the use of non-approved system software.

1. In the Group Policy Management Editor, select the PlantPAx Users Policy Object to edit and select Software Access Policy.
2. Go to Computer Configuration > User Configuration > Policies > Administrative Templates.
3. In the System folder, select 'Don't run specified Windows applications.'



4. Select Enabled, Show, and then type any application software to create an access restriction. Example: Regedit.exe



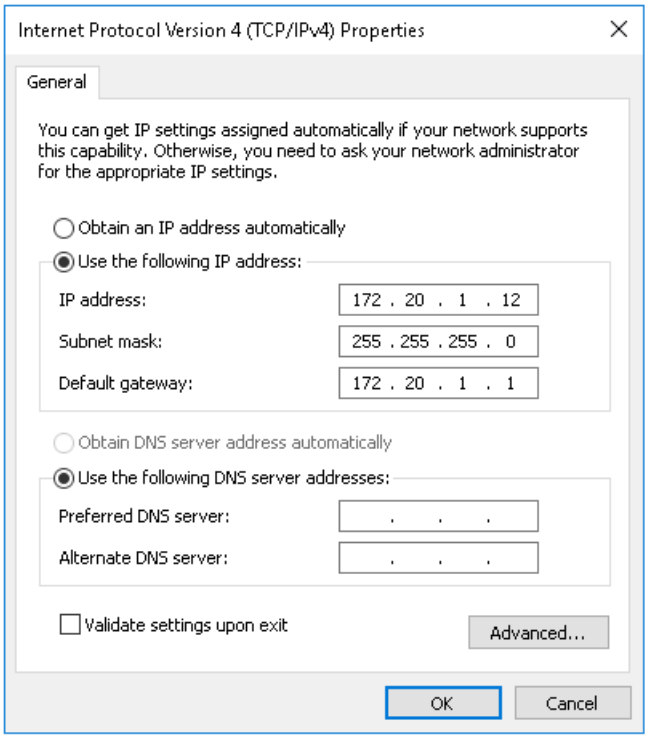
Windows Workgroup

For small PlantPAx systems, you can use a Windows Workgroup where complexity and security controls are kept to a minimum. An example might be a PASS-C server for a self-contained process unit or packaged equipment that is built by an Original Equipment Manufacturer (OEM); commonly called a process skid.

Assign Static IP Addresses

Without a domain controller, there's no DCHP server to assign IP addresses. The workgroup requires all workstations and servers to contain manually set (static) IP address assignments.

1. On each workstation, access the Network Adapter TCP/IPv4 properties and assign a unique IP address.

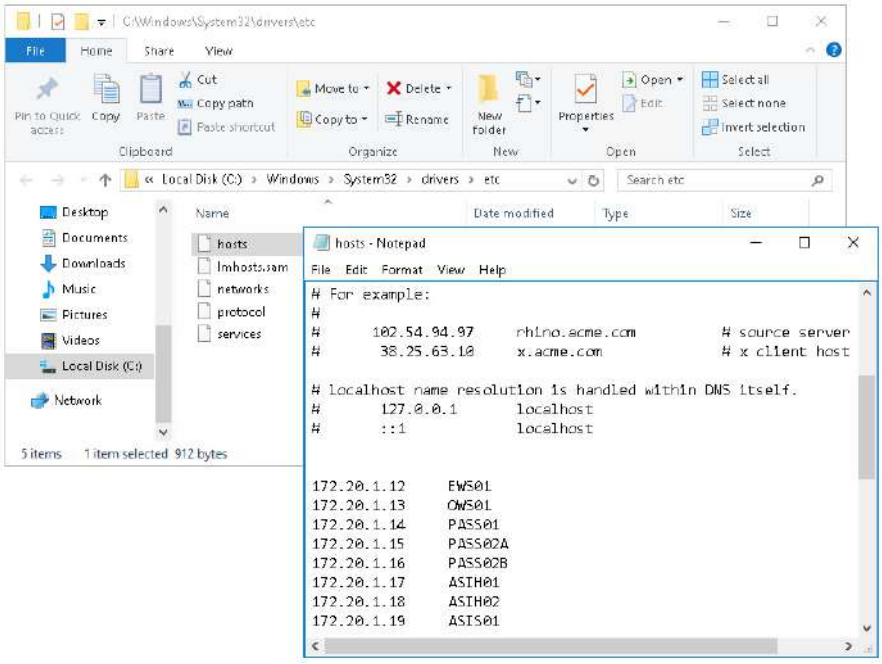


IMPORTANT Stratix® managed switches can be set to operate as a DHCP server and provide DHCP persistence. See the switch user manual if using DHCP for workgroup computers.

Map Computer IP Addresses

Without a domain controller, there's no DNS server to provide name resolution, meaning the computers can only communicate by IP address. To communicate by using a computer host name, mapping is required. All Windows computers contain a HOSTS plaintext file that maps IP addresses to host names.

1. Locate the HOSTS file in C:\Windows\System32\Drivers\etc directory and specify to open with Notepad.
2. Create a list of your workgroup computers, starting with each IP address followed by the corresponding computer name. Use a tab to delimit space between each mapping.



3. Copy the HOSTS file to all other computers in the workgroup.

IMPORTANT Anytime a change or new computer is added, all workgroup computers must receive the updated HOSTS file.

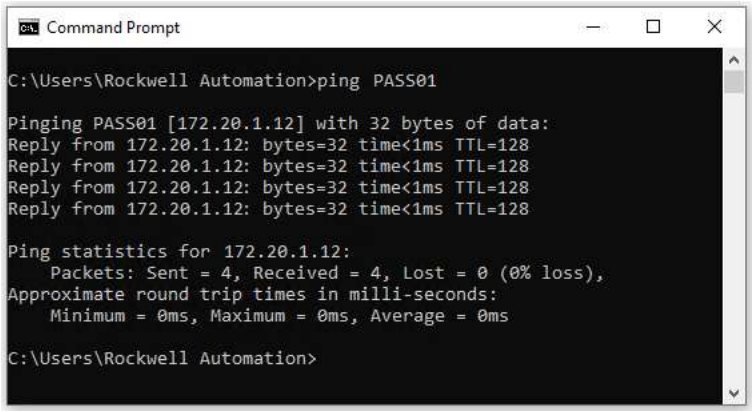
Test Communication by Host Name

You can verify that each workgroup computer responds to a PING command from another workgroup computer, referencing the remote computers host name.

1. Open a Command Prompt and type PING followed by a host name.

   For example: CMD: PING PASS01

2. Verify that a reply from the remote computer is returned with the correct IP address.



Create Local Users

While not required, increased security is achieved when using local user accounts of varying privilege.

Use the most restrictive account to help protect from security threats that could otherwise use elevated privileges to exploit the operating system. Only log into an administrative account as needed.

1. Open Computer Management. (Run > compmgmt.msc)
2. Select Local Users and Groups in the left window pane.
3. Right-click the Users folder and select New User.
4. Enter a user name, password, and select 'password never expires'.
5. After the user is created, right-click user and select Properties.
6. Go to the Member Of tab and Add the local group as desired.

Local Users and Groups Example

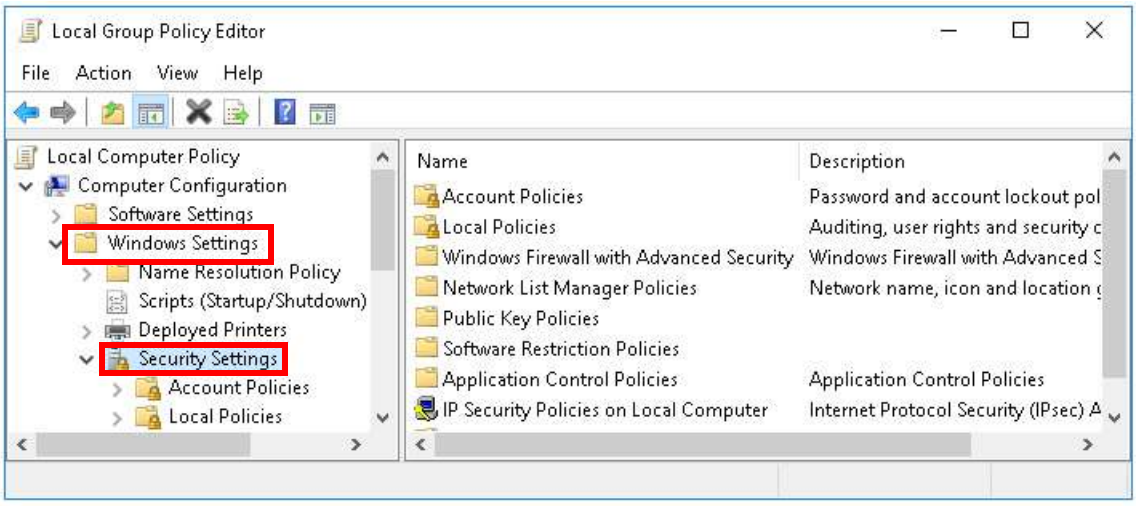
User Name	Local Group
PlantPAx Engineering	Administrators
PlantPAx Operators	Power users

IMPORTANT Local user accounts must be duplicated on all workstations with shared credentials for seamless access.

Create Local Security Policies

While not required, if you have various levels of local users you can set local security policies that the more restricted accounts will not be able to modify.

1. Login to the highest privilege local account with administrator access.
2. Open the Local Group Policy Editor (Run > gpedit.msc).
3. Expand Computer Configuration and go to Windows Settings > Security Settings.



4. Expand Computer Configuration and go to Windows Settings > Security Settings > Account Policies.

   You can configure a lockout policy for several failed login attempts of unauthorized users.

5. Expand Computer Configuration and go to Windows Settings > Security Settings > Local Policies.

   You can configure User Rights Assignment and Security Options. You can limit actions such as who can shut down the computer, change the system time, access the computer from a network, and so on.

IMPORTANT Local Policies must be duplicated on all workstations for seamless operation. This can be tedious and is why a domain controller with the ability to push domain policies is recommended over a workgroup.

FactoryTalk DeskLock Utility (Optional)

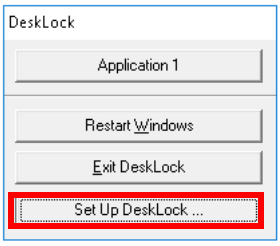
DeskLock is a FactoryTalk® View tool for the Windows operating system. DeskLock provides control options for smaller systems that do not use policy or domain management.

Use the DeskLock tool to:

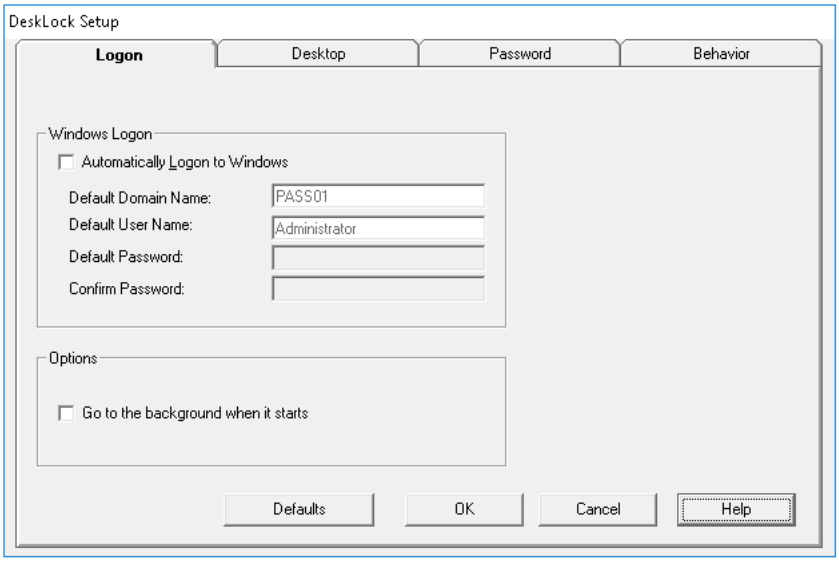
- Choose setting so that an operator using FactoryTalk View can't gain access to functionality not expressly configured by the system administrator.
- Hide items on the Windows Explorer desktop, including the Taskbar and Start menu.
- Disable key combinations that are used to perform specific Windows actions, such as accessing the Task Manager.

Launch the DeskLock tool on computers with FactoryTalk View SE, FactoryTalk® Studio, server, or client components.

1. Go to Rockwell Software > FactoryTalk View > Tools > DeskLock
2. Select Set Up DeskLock.



3. Explore each of the four tabs (Logon, Desktop, Password, Behavior).



4. Use the Help button for information on how to configure and use the DeskLock utility.

Notes:

Process Automation System Server

The Process Automation System Server (PASS) can be configured after joining an active domain or workgroup. The configuration steps described here cover larger system implementations.

This is the recommended workflow to configure a Process Automation System Server. For experienced users, each step outlines requirements. For more detailed information, follow the referenced links.

Step 1: Determine FactoryTalk Components

The PASS hosts the FactoryTalk® Services Platform that provides a set of common services (such as diagnostic messages, health monitoring services, and access to real-time data).

- FactoryTalk® Administration Console
- FactoryTalk® Directory
- FactoryTalk® Activation
- FactoryTalk® Security
- FactoryTalk® Diagnostics
- FactoryTalk® Alarms and Events

For more information, see FactoryTalk Components.

Step 2: Configure the PASS

Configure the PASS for standalone or distributed connectivity.

- Specify FactoryTalk Directory
- Configure the FactoryTalk Directory
- Run the Windows® Firewall Configuration Utility
- Configure FactoryTalk Activation servers

For more information, see Configure the PASS

For redundant PASS considerations, see Redundant Server Considerations

Step 3: Configure Servers on the PASS

A FactoryTalk® View SE application is required to create the three major server components that run on 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
- Tag Alarm and Event server – Provides alarm information from the controllers and servers to each OWS upon request

Large distributed systems may require multiple servers running remotely in a more elaborate architecture.

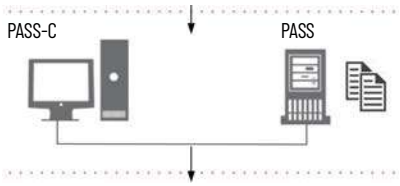
For more information, see Configure Servers on the PASS.

Step 4: Configure the Runtime Security

Runtime security must be configured 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.

For more information, see Configure Runtime Security With Control power present, set the desired EtherNet/IP™ address.

Prerequisites



Following the System Workflow, configure a PASS or PASS-C, depending on the size of your system. Your results from the PSE determine the size of the system.

- 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 Template User Manual, publication 9528-UM001.
- PASS servers can be configured as redundant for HMI servers, data servers, and/or alarm servers.

FactoryTalk Components

The PASS hosts the FactoryTalk® Services Platform that provides a set of common services (such as diagnostic messages, health monitoring services, and access to real-time data). FactoryTalk software products and applications depend on these services in a PlantPAx system.

FactoryTalk Service Platform components for the PASS include:

Component	Description
FactoryTalk Administration Console	FactoryTalk Administration Console is a standalone tool for developing, managing, and securing multiple FactoryTalk View applications. On the Administration Console, delete old computer names from the FactoryTalk Directory. By deleting old computer names, the FactoryTalk Directory contains current computer names only. Deletions also make sure that applications do not attempt to communicate with computers that are no longer in the FactoryTalk Directory. **Required:** Yes; a prerequisite on every PlantPAx® computer containing FactoryTalk software.
FactoryTalk Directory	FactoryTalk Directory provides a central lookup service for a PlantPAx system so all definitions do not have to exist in a single physical project file. References that are saved by FactoryTalk Directory are used by FactoryTalk-enabled products and FactoryTalk services to locate definitions when they're needed. It allows clients to locate key configuration information such as system organization, server locations, and policy information. FactoryTalk Directory provides a common address or phone book of factory resources that are shared among FactoryTalk-enabled applications in a distributed system. **Required:** Yes
FactoryTalk Activation	FactoryTalk Activation services provide a secure, software-based system for activating Rockwell Software® products and managing software activation files. **Required:** Yes; a prerequisite on every PlantPAx computer containing FactoryTalk software. Activation file access is required for continuous use of FactoryTalk software otherwise a 7-day grace period is started. **Placement:** A PASS is recommended location to bind and place the license files. Other servers and workstations can refer to the PASS location for floating or time borrowed activations. For more robust applications, activate each server locally to remove the dependency of remote license access.
FactoryTalk® Security	FactoryTalk Security centralizes user authentication and authorization at the FactoryTalk Directory. The users and groups are very similar in their management to Active Directory and can be linked to the Active Directory. This centralized authentication and access control allows for a 'single user sign-in' experience when using FactoryTalk enabled products. **Required:** Yes **Placement:** Same server that is hosting the FactoryTalk Directory.
FactoryTalk® Diagnostics	FactoryTalk Diagnostics collects and provides access to activity, status, warning, and error messages generated throughout a FactoryTalk system. **Required:** Yes **Placement:** Yes; a prerequisite on every PlantPAx computer containing FactoryTalk software.
FactoryTalk Alarms and Events	FactoryTalk Alarms and Events provides system-wide alarm monitoring and control centralized at the FactoryTalk Directory. **Required**: Yes **Placement:** Alarm and Events Server on the PASS

System SQL Server Deployment

Before configuring the PASS server, confirm that the SQL Server deployment has been completed and is accessible via the PASS server. This is required to ensure that Alarms and Events can be recorded in the SQL Database. Additionally, Batch server and Asset Management server will also create a DB in the SQL Server. PlantPAx requires the following SQL features to be enabled to ensure that data recording is possible.

Instance Features

- Database Engine Services
- SQL Server Replication
- Full Text and Semantic Extractions for Search
- Data Quality Service
- Analysis Services

Shared Features

- Data Quality Client
- Client Tools Connectivity
- Integration Services
- Client Tools Backwards Compatibility
- Client Tools SDK
- Documentation Components
- SQL Client Connectivity SDK

Configure the PASS

To configure the PASS:

- Specify the location of the FactoryTalk Directory
- Configure the FactoryTalk Directory
- Run the Windows® Firewall Configuration Utility
- Configure FactoryTalk Activation servers

Specify FactoryTalk Directory Location

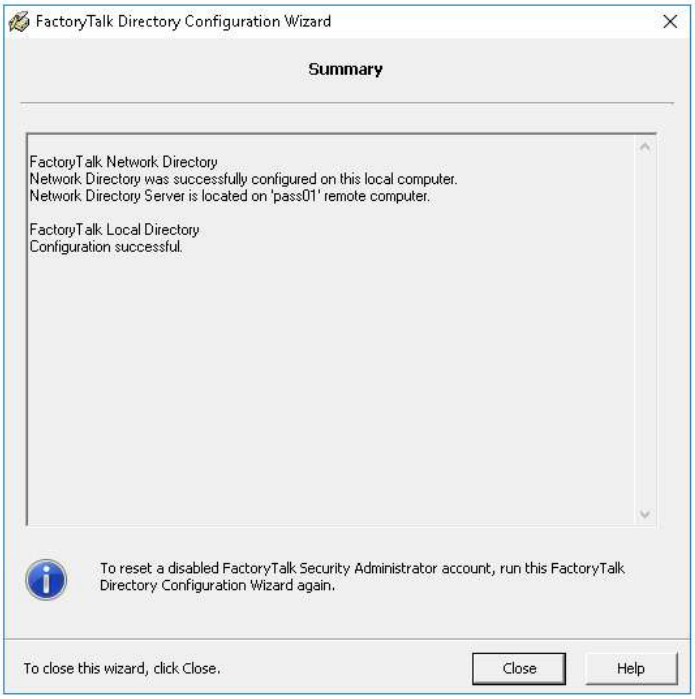
Every computer must know whether to use its own local directory or to use a network directory on a remote computer. Do the following for each computer in the system.

1. Go to Rockwell Software > FactoryTalk Tools > FactoryTalk Directory Server Location Utility and specify the location.
   - For a PASS-C, specify the LOCAL directory and for each OWS client specify the PASS-C directory.
   - For a distributed system, specify the server that will host the directory. Repeat for all other servers and workstations in the distributed system.
2. Restart each computer after specifying its directory location.

Configure the FactoryTalk Directory

Once you specify the FactoryTalk Directory location and restart the computer, configure the FactoryTalk Network Directory or Local Directory on each computer.

1. Go to Rockwell Software > FactoryTalk Tools > FactoryTalk Directory Configuration and select Network or Local or both, depending upon the perspective of the computer being configured.
2. Enter the Windows Administrative account user name and password.
3. In the Summary, verify that the configuration was successful.



Run Firewall Configuration Utility

The FactoryTalk Services Platform includes a Windows Firewall Configuration Utility (WFCU) to provide firewall port exceptions to incoming and outgoing processes that require remote access. Run this utility on every computer that has installed FactoryTalk software.

1. Go to Rockwell Software > FactoryTalk Tools > Windows Firewall Configuration Utility.

   And process-related exceptions are displayed at the bottom.
2. If needed, save a list of exceptions for future reference and the WFCU activity is logged to C:\ProgramData\WFCU\WFCULog.txt
3. If no exceptions are needed, click Exit.

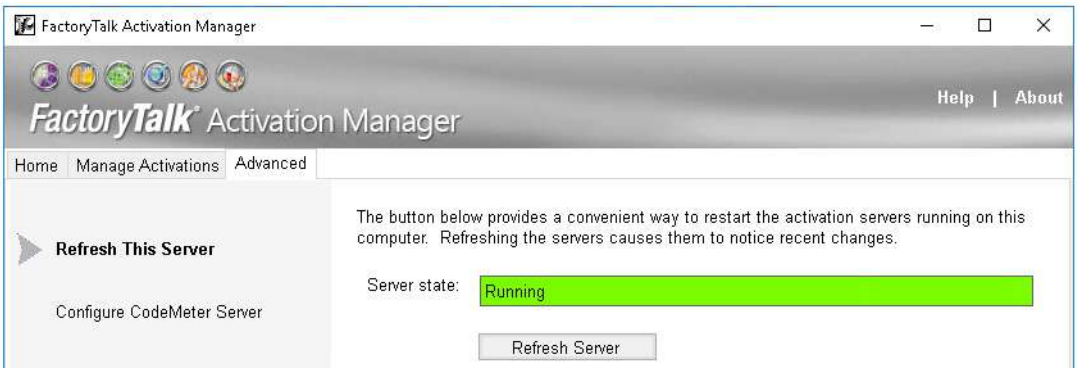
It's recommended to enable Windows Defender Firewall notifications to inform you of any additional applications that would be blocked.

Configure FactoryTalk Activation Servers

The FactoryTalk Activation Manager (FTAM) software is a prerequisite that is automatically installed on every PlantPAx computer that contains FactoryTalk software.

For a PlantPAx system, the computer that hosts the FactoryTalk Directory, such as the PASS, hosts the license files.

1. Go to Rockwell Software > FactoryTalk Activation > FactoryTalk Activation Manager and select new activations, as needed.
2. After all new activations are generated, go to the Advanced Tab and click 'Refresh Server'.

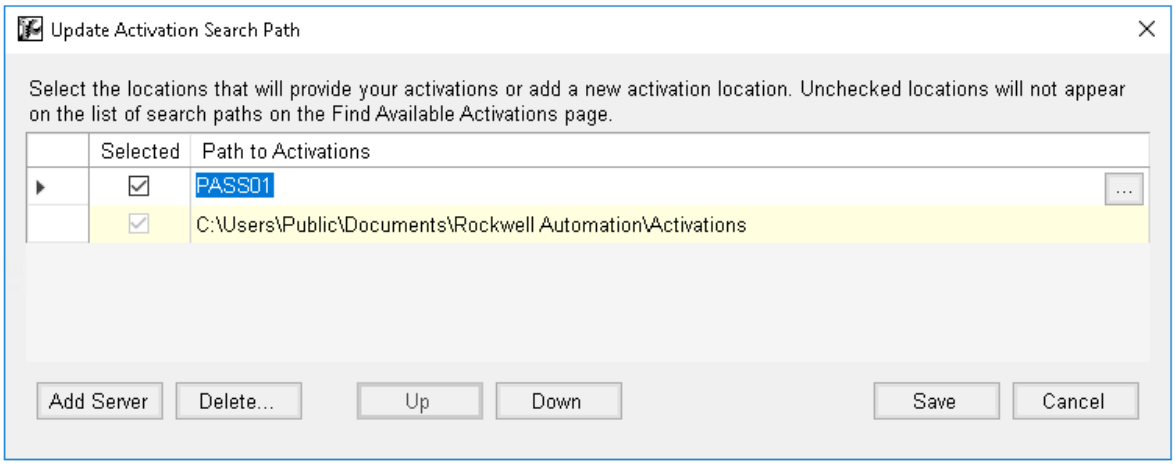


Configure all other computers to reference the PASS location.

1. Go to Rockwell Software > FactoryTalk Activation > FactoryTalk Activation Manager and select Update Activation Search Path.

2. Select Add a server and enter the name or IP address of the license server (PASS01).

3. If there are no local activations, move PASS01 to the top as the first location to search for activations.



4. Update the search path on all computers that require an activation.

Configure Servers on the PASS

A FactoryTalk View SE application is required to create the three major server components that run on 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.
- Tag Alarm and Event server – Provides alarm information from the controllers and servers to each OWS upon request.

The number of servers and how they're configured can impact the speed of system communication. Servers can be simplex or redundant.

- A single HMI server is sufficient for most PlantPAx systems.
- Multiple data servers are common. By locating each in separate areas, tag lookup performance is improved as an HMI server knows specifically which data server to browse and can ignore others.

The following steps provide basic server creation on a single PASS. Large distributed systems can require multiple servers running remotely in a more elaborate architecture.

Create a New HMI Project

This section provides a method to create your own project and then import the components from the PlantPAx Graphic Framework.

1. Go to FactoryTalk® View Studio software > New and select an application type of View Site Edition.

   The application types are Local Station, Network Station, or Network Distributed.

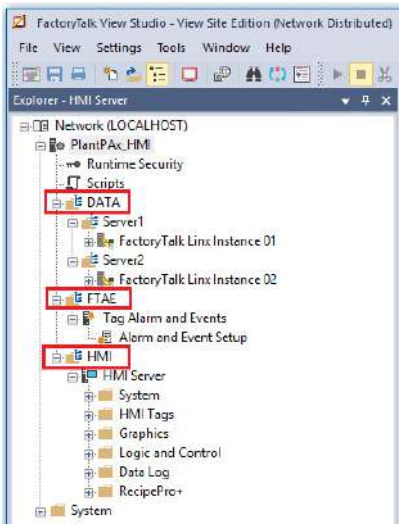
PlantPAx systems are Network Distributed applications, even when server components are consolidated on a standalone computer (PASS-C). The exception is a process skid, where a Local Station application provides sufficient functionality.

You now have a default application.

Define Areas

Areas organize and subdivide applications in a network directory into logical and physical divisions. Areas can be created for different processes within a manufacturing facility or to group each server type. This name hierarchy can be visible externally, such as in the historian or alarm database.

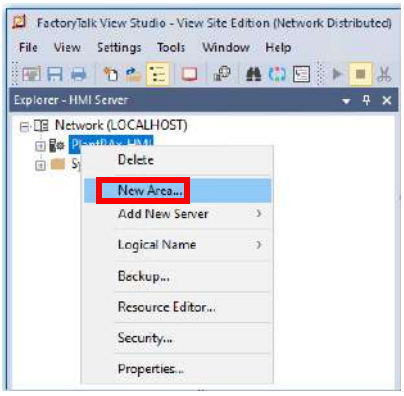
Server assignment helps optimize performance. To help prevent unpredictable search results, do **not** insert a server into the application root path. Each server must be in its own area.



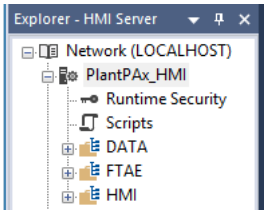
- Alarm area folder stores the Alarm and Event server.
- Data area folder contains the data server.
- HMI area folder stores FactoryTalk® View tags and displays.

Use the Explorer window in FactoryTalk View Studio to add areas.

1. Go to the application and select New Area.



2. Create three Areas, one for each of the three main server types (DATA, FTAE, and HMI).



IMPORTANT Once you create an area, you can't change the name. You must delete and recreate if you need to modify the name.

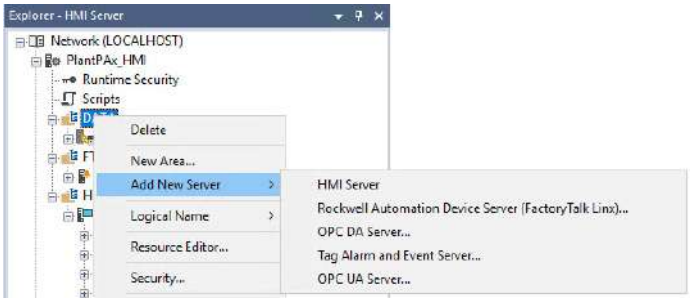
Do not use spaces in the Area name to achieve proper HMI functionality.

Do not put multiple servers in the root location of an area.

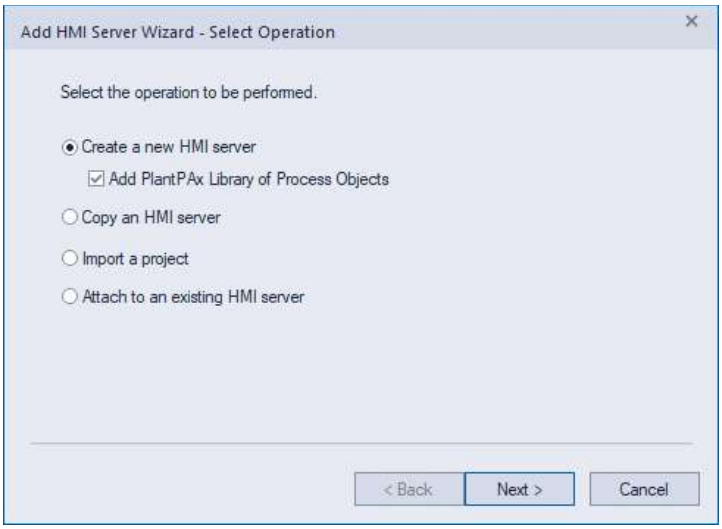
Add an HMI Server

All PlantPAx systems require an HMI server.

1. Go to the HMI area and select Add New Server> HMI Server. Each area can only contain one HMI server.

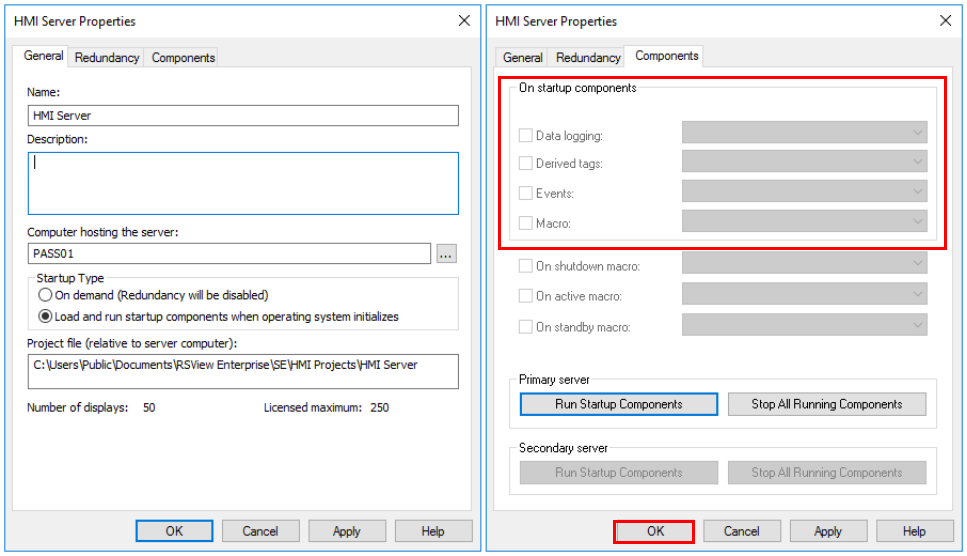


Starting with FactoryTalk View SE 13.0, developers have the ability to add all process library components to a new or existing HMI server.



2. Enter a name, startup type, and specify the computer that hosts the service (for example, PASS01).
3. (optional) Click the Redundancy tab to specify a secondary PASS.

4. Select startup items on the Components tab, such as data logging, derived tags, events, and macros.

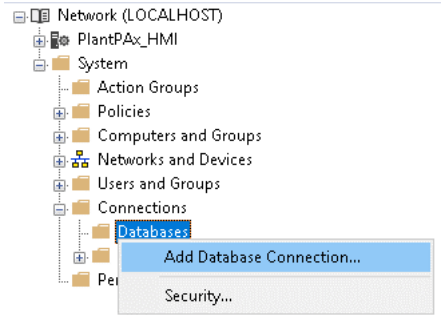


5. Click OK.

Add the Alarms and Events Database

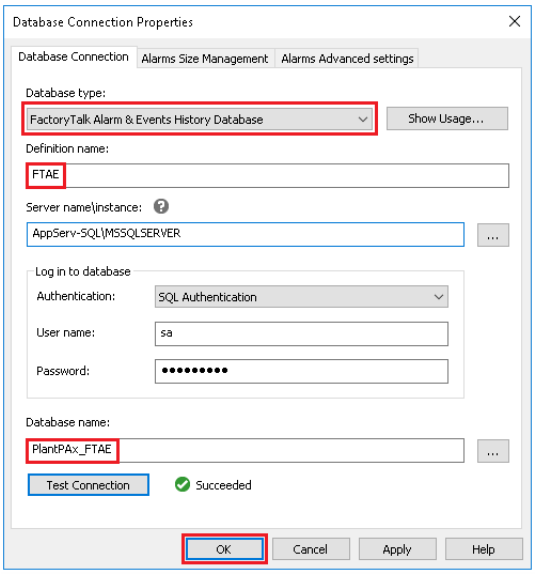
The data servers and the alarms and events servers can log alarm and event history to a SQL database. You must create this database before you can enable logging to the servers.

1. Use either FactoryTalk View SE Studio or the FactoryTalk Administrative Console to add a database connection.



2. Configure the database connection properties.
   - Type: FactoryTalk Alarm & Events History Database
   - Definition name: (new or existing)
   - Server that hosts your SQL database: (local or remote)
   - SQL database authentication

- Database name (new or existing)

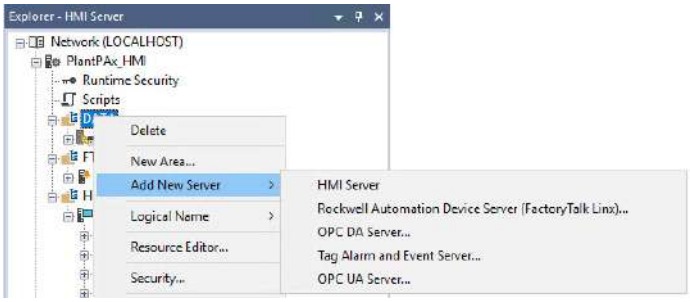


If the database does not exist, you get a prompt when you click OK. Click YES to create the database.

Add a Data Server (FactoryTalk Linx)

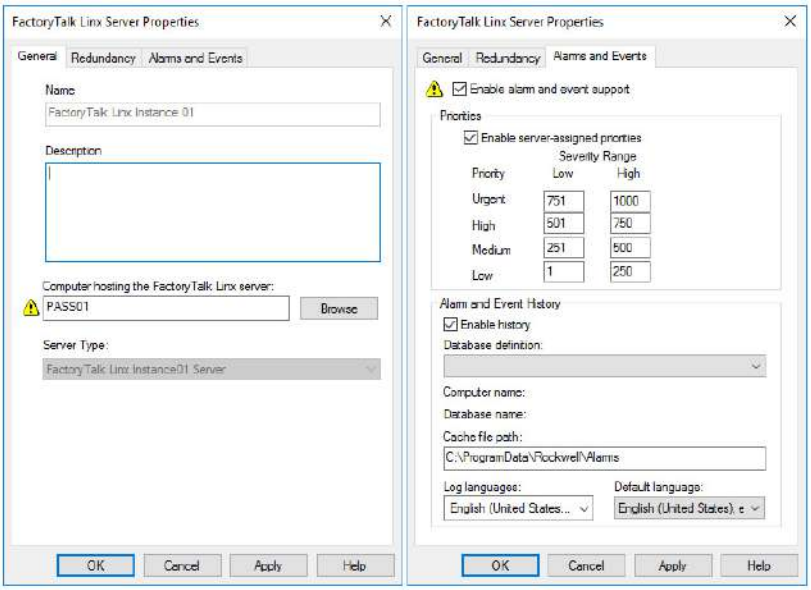
A FactoryTalk Linx data server is required to communicate to controllers.

1. Go to the Data area and select Add New Server > Rockwell Automation Device server (FactoryTalk® Linx).



2. Enter a name, startup type, and specify the computer that hosts the service (for example, PASS01).
3. Create a first or second instance Data server (FactoryTalk Linx), each in its own area.
4. Enter a name, startup type, and specify the computer that hosts the service (for example, PASS01).
5. (optional) Click the Redundancy tab to specify a secondary PASS.
6. On the Alarm and Events tab, enable alarm and event support and enable history.
7. Enable server-assigned priorities and configure as required.

8. Enable history to configure alarm and event logging.

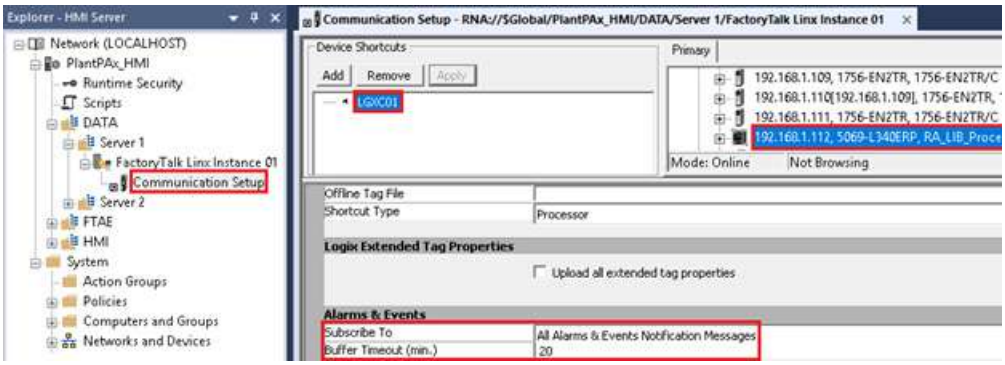


IMPORTANT FactoryTalk Linx Instance02 is an independent service on the Windows operating system that is designed to allow applications to increase tag, data, and client capacities without impacting the performance of the first instance (also an independent service).

Instance02 is not supported on FactoryTalk View SE local station and is limited to an Ethernet driver.

For information on verifying the data server, see Appendix C, PlantPAx Deployment Recommendations and Verification Tool.

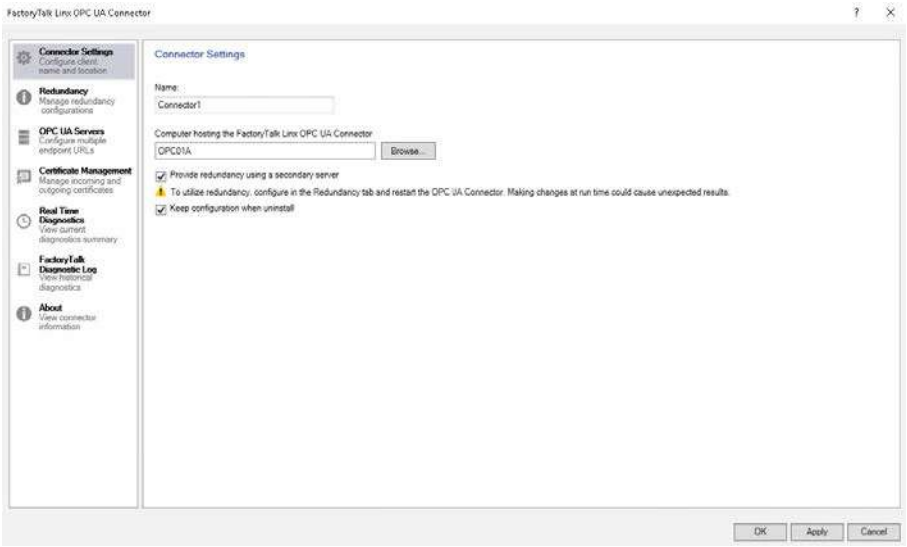
Once the data server is created, configure device shortcuts to controllers and subscribe to the data server. Select All Alarms & Events Notification Messages to support Logix tag-based alarms and automatic diagnostic messages.

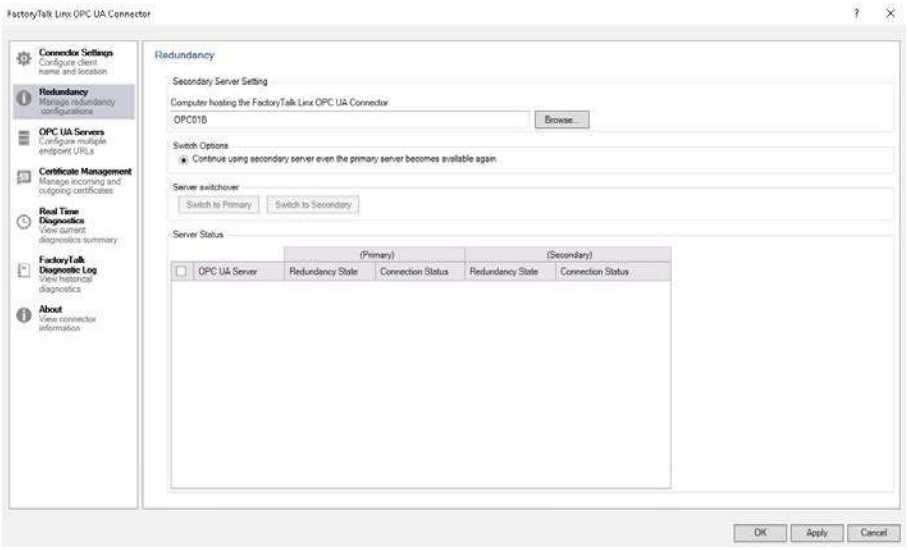


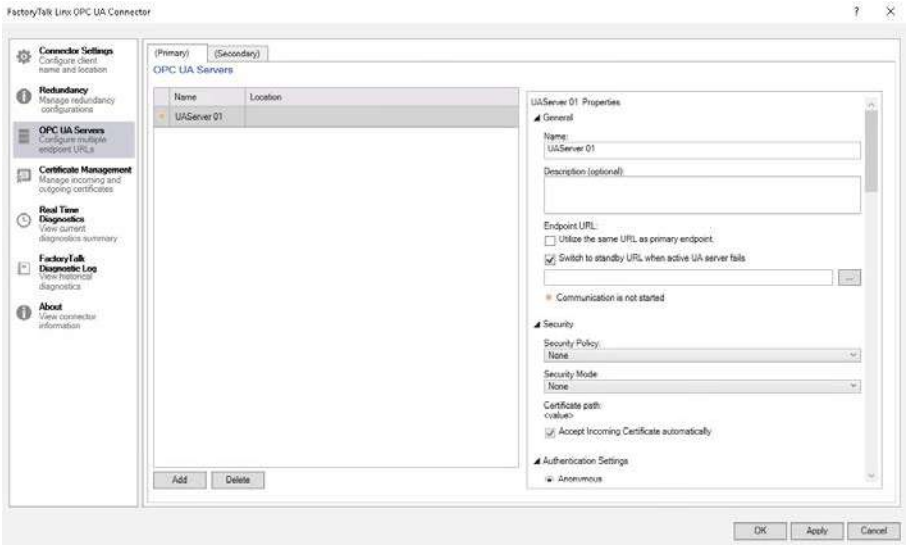
Add a Data Server (OPC UA)

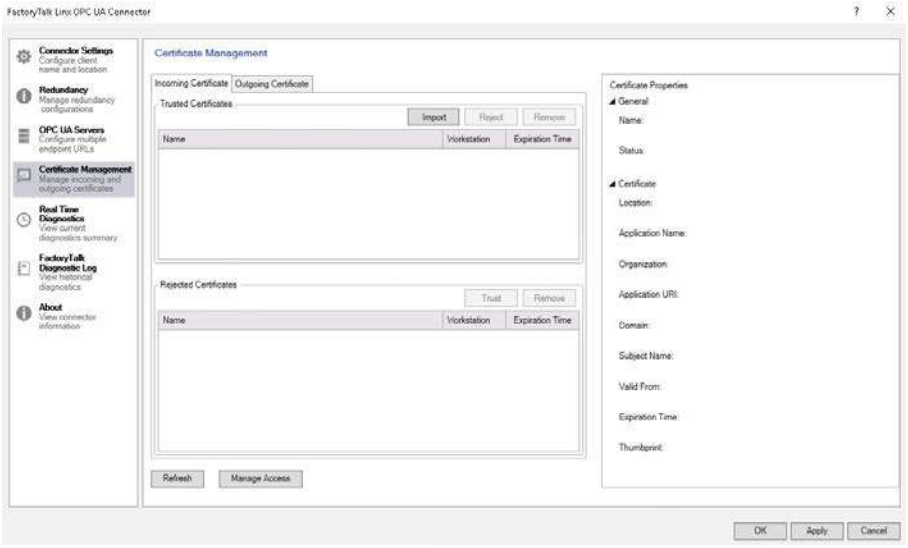
An OPC UA data server is required to communicate with OPC UA devices. This server type supports OPC UA data and OPC UA Alarms and Conditions.

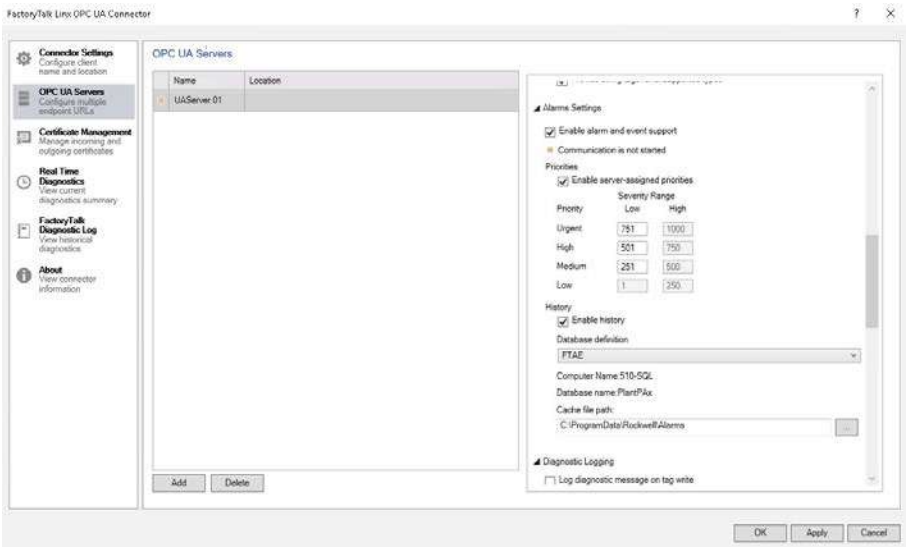
1. Use the Explorer window in FactoryTalk View Studio to add a new area for the OPC UA server.
2. Go to the new area and select Add New Server > OPC UA Server.
3. (optional) Click the Help button for more information about configuring the OPC UA server.
4. Enter a name and specify the computer that hosts the service. It's a best practice to host the OPC UA server on a dedicated computer with no other FactoryTalk servers.
5. (optional) Enable option to keep configuration when service is uninstalled.
6. (optional) Enable redundancy option if using a secondary server. Click the Redundancy tab and specify a secondary server.
7. Click the OPC UA Servers tab.
8. Enter a name for the OPC UA server. Specify an Endpoint URL for the server.
9. (optional) If Redundancy is enabled and using a different standby URL, click the (Secondary) tab and specify a standby URL. Otherwise, enable the option to utilize the same URL as primary.
10. Specify Security settings for the OPC UA server.
11. Specify Authentication Settings for the OPC UA server.
12. Specify Data Access settings for the OPC UA server.
13. (optional) Enable alarm support and History in the Alarms Settings.
14. Specify Diagnostic Logging settings for the OPC UA server.
15. (optional) Click Add and repeat previous steps for any additional OPC UA servers.
16. (optional) Click the Certificate Management tab to manage access and certificates for the OPC UA servers.




FactoryTalk Linx OPC UA Connector
Connector Settings
Configure client name and location
Redundancy
Manage redundancy configurations
OPC UA Servers
Configure multiple endpoint URLs
Certificate Management
Manage incoming and outgoing certificates
Real Time Diagnostics
View current diagnostics summary
FactoryTalk Diagnostic Log
View historical diagnostics
About
View connector information
Redundancy
Secondary Server Setting
Computer hosting the FactoryTalk Linx OPC UA Connector
OPC01B
Browse...
Switch Options
Continue using secondary server even the primary server becomes available again.
Server switchover
Switch to Primary
Switch to Secondary
Server Status
(Primary)
(Secondary)
OPC UA Server
Redundancy State
Connection Status
Redundancy State
Connection Status
OK
Apply
Cancel


FactoryTalk Linx OPC UA Connector
Connector Settings
Configure client name and location
Redundancy
Manage redundancy configurations
OPC UA Servers
Configure multiple endpoint URLs
Certificate Management
Manage incoming and outgoing certificates
Real Time Diagnostics
View current diagnostics summary
FactoryTalk Diagnostic Log
View historical diagnostics
About
View connector information
(Primary)
(Secondary)
OPC UA Servers
Name
Location
UAServer 01
UAServer 01 Properties
General
Name:
UAServer 01
Description (optional):
Endpoint URL
Utilize the same URL as primary endpoint
Switch to standby URL when active UA server fails
Communication is not started
Security
Security Policy:
None
Security Mode
None
Certificate path:
Accept Incoming Certificate automatically
Authentication Settings
Anonymous
Add
Delete
OK
Apply
Cancel



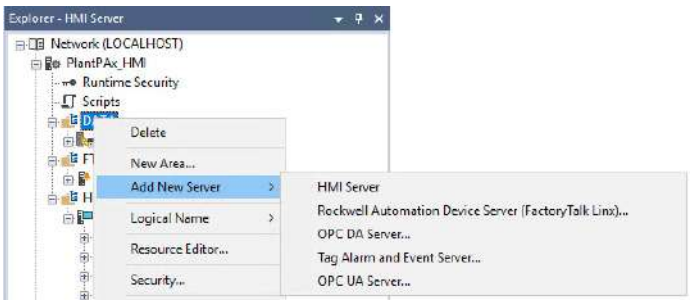


For information on verifying the data server (OPC UA), see Appendix C.

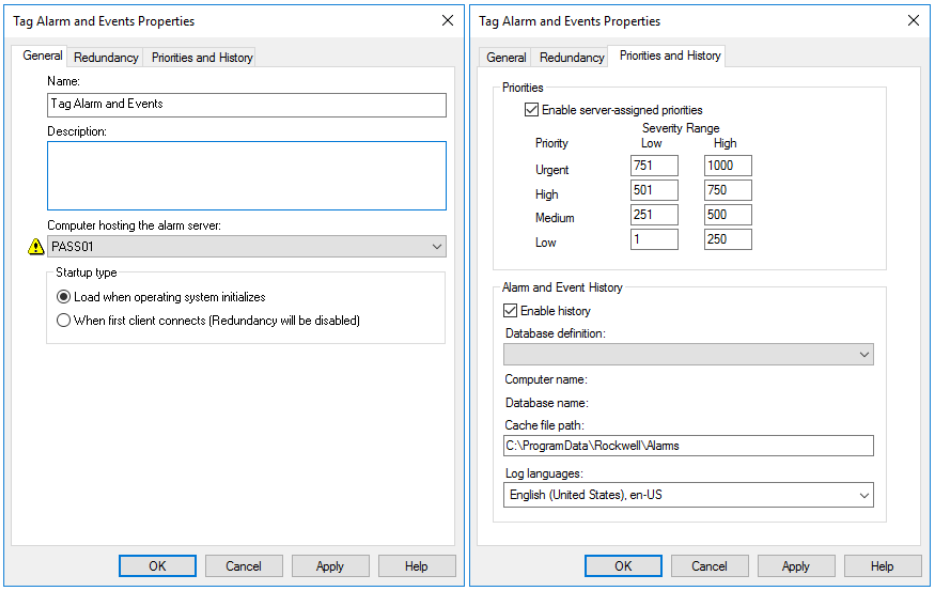
Add an Alarm and Events Server

An alarms and events server is required for server tag-based alarms.

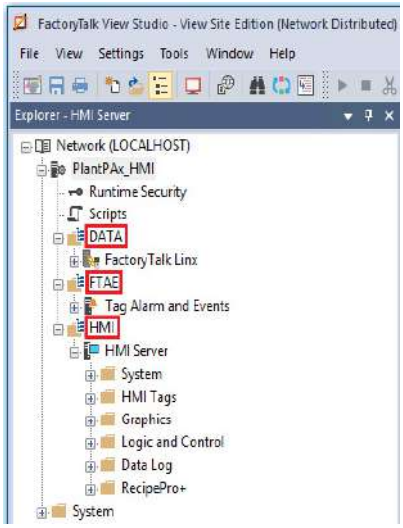
1. Go to the FTAE area and select Add New Server > Tag Alarm and Event Server.



2. Enter a name, startup type, and specify the computer that hosts the service (for example, PASS01).
3. (optional) Click the Redundancy tab to specify a secondary PASS.
4. Click the Priorities and History tab and enable server-assigned priorities.
5. Enable history to configure alarm and event logging.



Now that your servers are organized into areas, you're ready to start developing your HMI application.



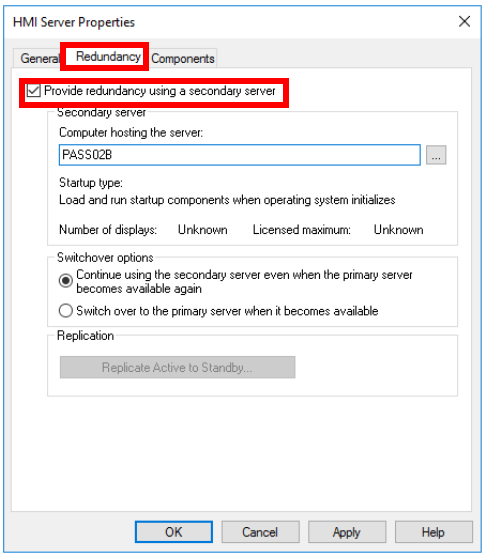
For details on building an HMI template, see the Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200.

Redundant Server Considerations

Redundant HMI, Data, and Alarm servers provide higher availability on a network distributed architecture. Primary and secondary servers are hosted on different PASS servers where control can be switched between them.

When implementing a primary and secondary server (PASS02A and PASS02B), we recommend that you use a single PASS01 (non-redundant) to host the FactoryTalk Network Directory and FactoryTalk Activations. By using the PASS01, these common components still are accessible in case one of the redundant servers is unreachable.

Access the Redundancy tab of each servers' properties to enable redundancy and specify the secondary server.



Configure Runtime Security

Runtime security can be configured for three different capabilities or a blending of those capabilities when deploying the HMI content provided in the Process Library.

- User role (that is, Operator, Engineer, and so on)
- Area
- Line-of-sight

Security by user role restricts users to the actions their role allows. The addition of area security can further restrict those allowed actions to specific areas of the plant. Finally, with the addition of line-of-sight security, the user can be further restricted from performing identified actions to the specific computer they are using. Not all these capabilities are required, you can deploy each security option individually or in any combination.

Refer to Security Example with Concurrent Implementation of all Three Security Methods on page 91 for an example implementation.

Role-Based Security

Knowledgebase Technote, *PlantPAx System Release 5.20 Configuration and Implementation Tools*, contains the security information spreadsheet. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

The images in this section depict a single application with both FactoryTalk User Groups and Domain User Groups together. However, it isn't recommended to use both types of user groups in a single application.

Runtime security must be configured 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.

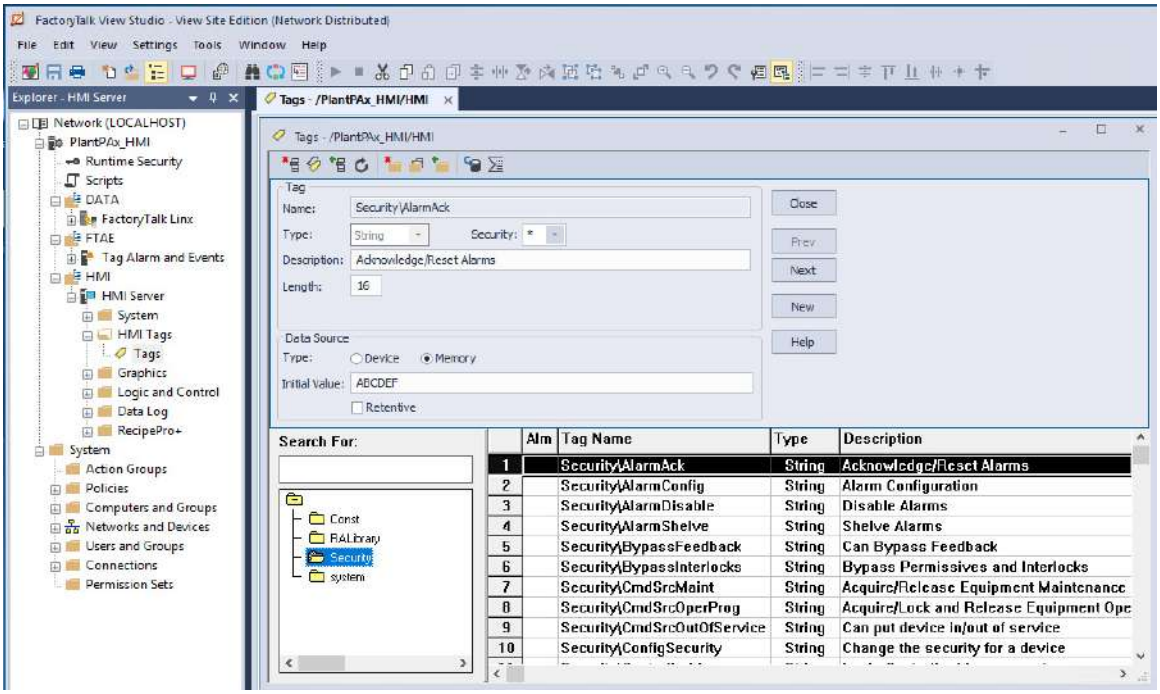
1. On the PASS, go to Rockwell Software > FactoryTalk View > Tools > Tag Import and Export Wizard.

Page	Action
Tag Import and Export Wizard Operations field	From the Operation pull-down menu, select Import FactoryTalk View tag CSV files and click Next.
	From the pull-down menu, select Site Edition and click Browse (ellipsis '...').
	Select the path of SE > HMI Projects > HMI Server.
	Select HMI Server.sed and click Open.
	Click Next and Browse (ellipsis '...') for the FTViewSE_ProcessLibrary_Tags_5_00_xx.CSV file; where xx = the service release number. This file is distributed with the PlantPAx Library of Process Objects Library.
	Click Open, click Next twice, and then Finish. The import results appear on the Database Import window.

To set security permissions to groups on the workstation, complete these steps.

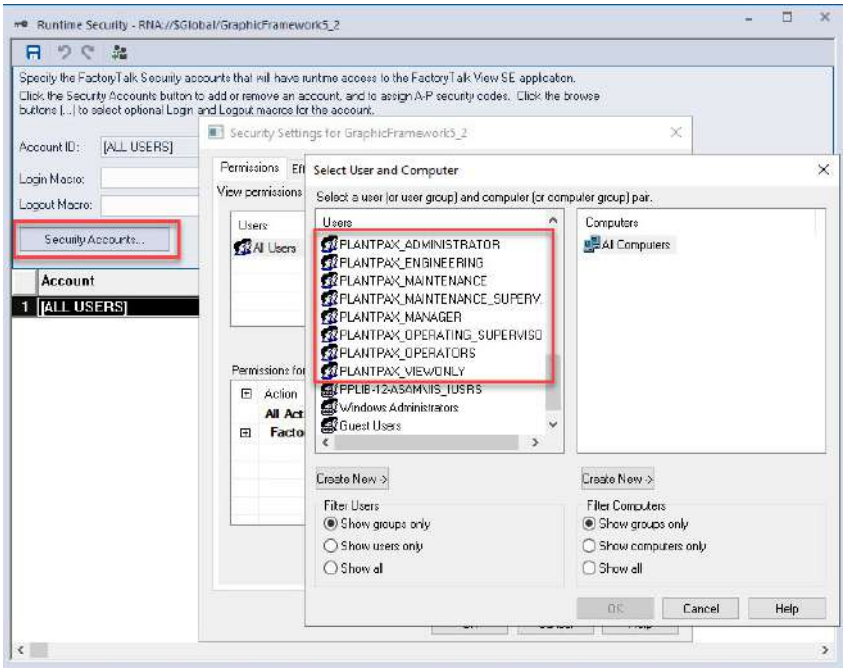
1. Open the HMI application with FactoryTalk View Studio software.

2. Verify that the security tags have been imported by expanding the HMI Area and viewing HMI Tags folders. (Const, RALibrary, and Security)

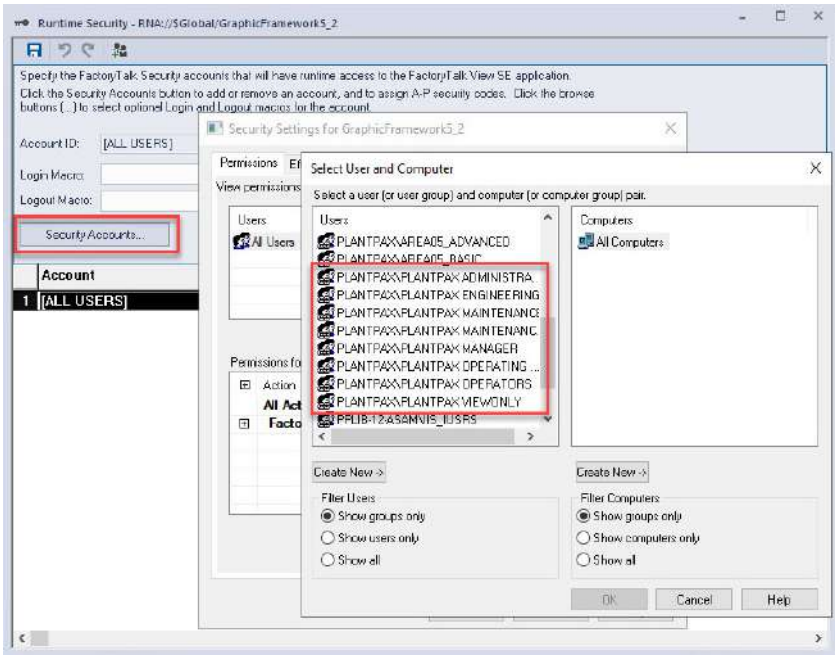


3. Select Runtime Security from the Explorer window or top menu bar under Settings.
4. Within Runtime Security, click the Security Accounts button.
5. From the Security Settings dialog box, select 'All Users' and click Remove.
6. Click Add.
7. From the Select Users and Computer dialog box, select a PlantPAx group and click OK.

For **FactoryTalk** user groups:



For **Domain** user groups:



8. Repeat adding users until all PlantPAx groups are selected.
9. You can assign security to each PlantPAx group based on letters (A...G, P).
10. If you're using e-signature with approval, add the group HMI_Approver. A-P codes aren't required for HMI_Approver.
11. Select a group from the Users list.

    The default is that all FactoryTalk View Security Codes are checked Allow.

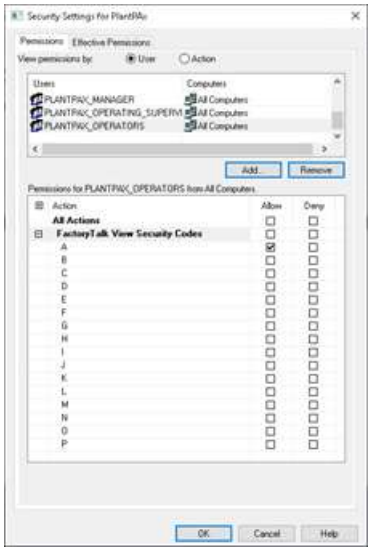
12. Click the Allow box beside each FactoryTalk View Security Code that you want to allow permission for the selected account.

For example, allow security of 'A' for an Operator.

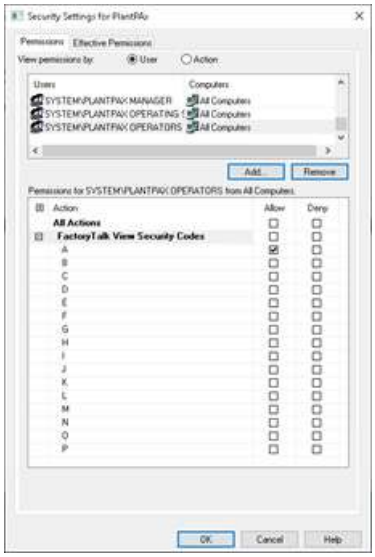
Table 4 - Recommended Group Security Codes

Group	Security Code
Operators	A
Operating Supervisor	B
Maintenance	C
Maintenance Supervisor	D
Engineering	E
Manager	F
Administrator	G
View Only	P

For **FactoryTalk** user groups:



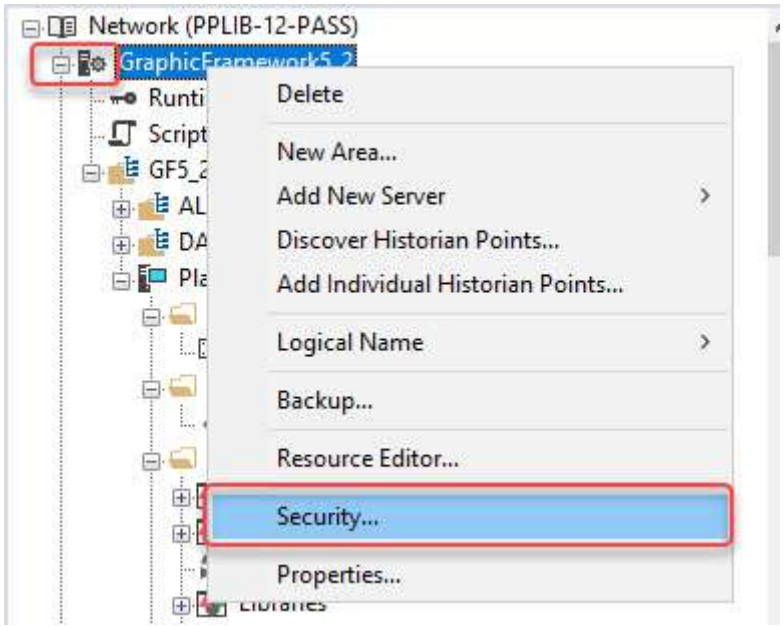
For **Domain** user groups:

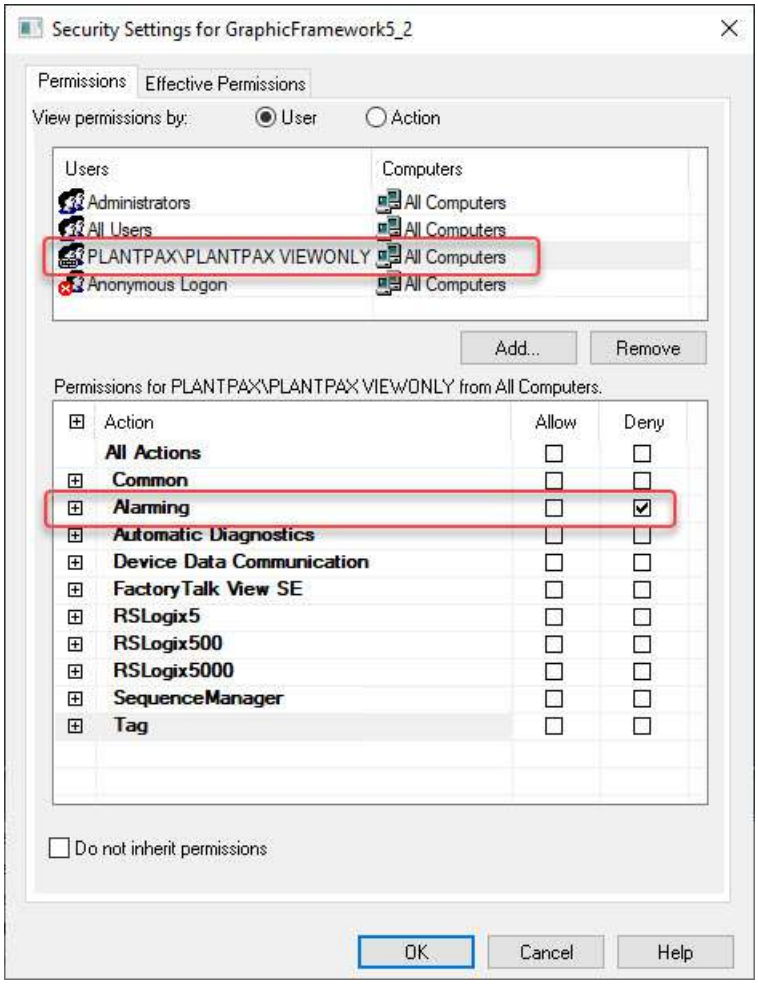


13. Repeat the steps for each user or group account that you want to configure with runtime security.

    For the View Only user group, it is recommended to “Deny” certain security privileges for the application. Right-click your application,

select “Security...”. Add the View Only user group and select “Deny” for applicable permissions.





Area-Based Security

Complete these steps to create area **FactoryTalk** user groups for each secure area of a production facility.

1. From the FactoryTalk Administration Console, click '+' to expand System and then click '+' to expand Users and Groups.

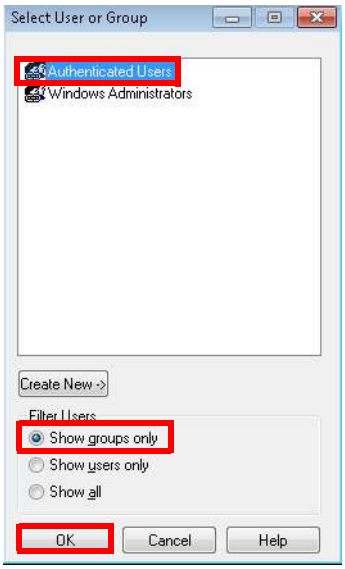
2. Right-click User Groups and choose New>User Group.

   On the New User Group dialog box, you must add two groups: 'area01_Advanced,' 'area01_Basic'. These groups define which Area01 Users have basic functions on the faceplate or advanced functions (engineering, maintenance).

The instructions default to Area01. You may modify the area name in the instruction and group names to meet your needs.

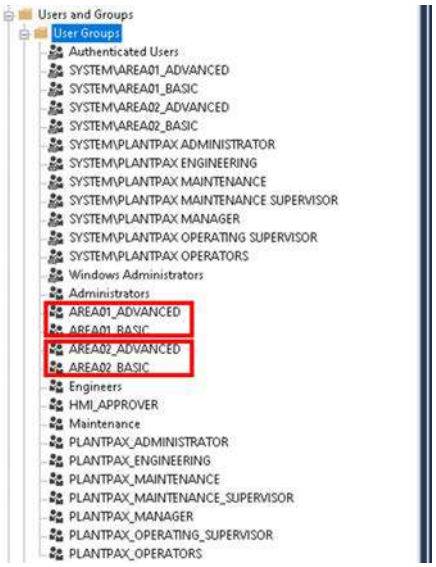
3. To add groups, type the name (example, AREA01_ADVANCED) and click Add.

4. Select Authenticated Users and use the default 'Show groups only' and click OK.



5. Click OK again.

Your two groups for AREA01 look like the example.



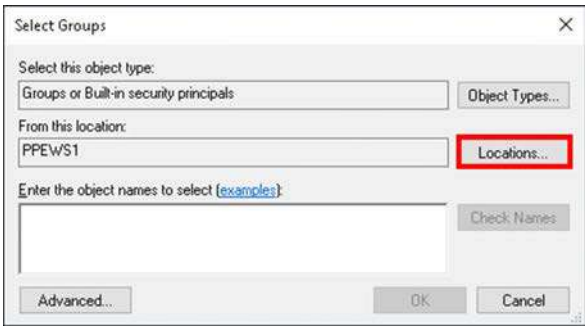
6. Repeat step 3 and step 4 to add groups for additional areas.

Complete these steps to import area **Domain** user groups for each secure area of a production facility.

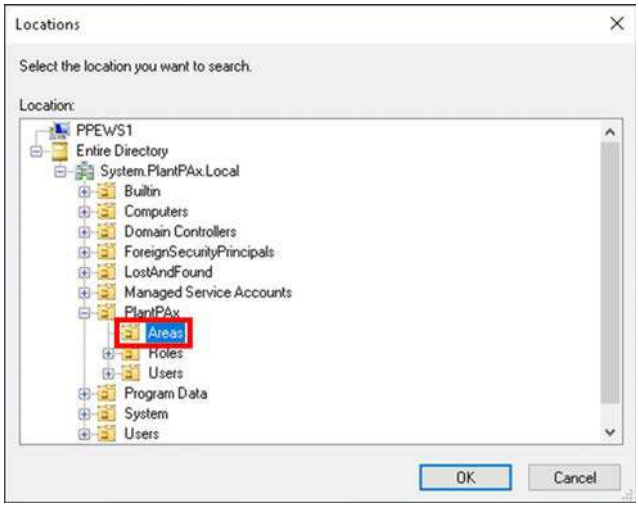
1. From the FactoryTalk Administration Console, click '+' to expand System and then click '+' to expand Users and Groups.
2. Right-click User Groups and choose New>Windows-Linked Group.

3. Select Add.

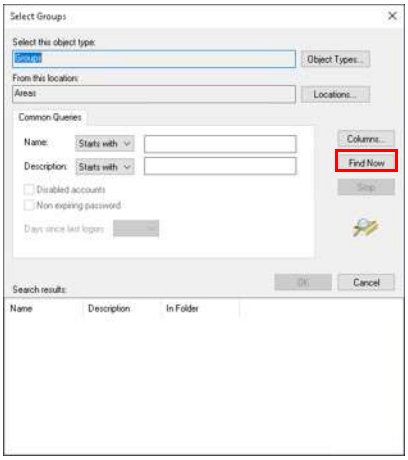
4. Select Locations.



5. Browse to your domain directory where you created areas. For this example System.PlantPAx.Local\PlantPAx\Areas

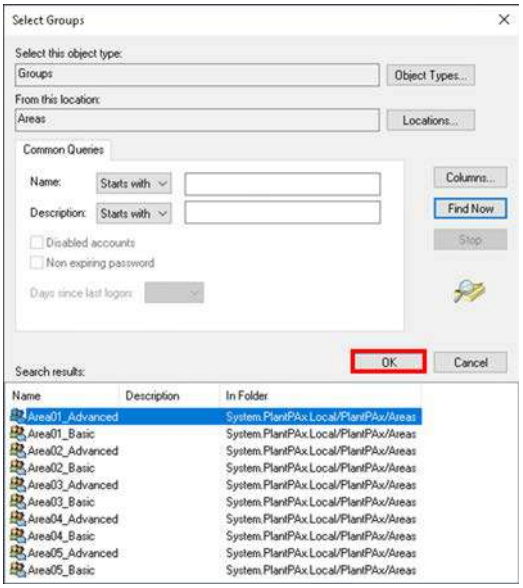


6. Select Find Now.

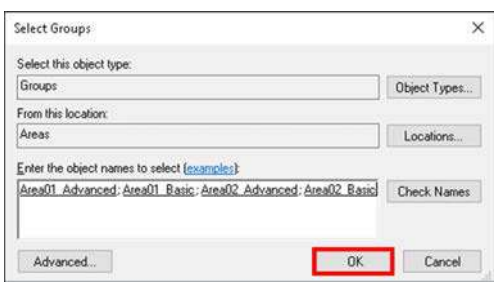


7. Select all areas from the search results that you want to import.

   For this example Area01_Basic, Area01_Advanced, Area02_Basic, Area02_Advanced. Click OK.



8. Select OK on the next two displays.



The domain areas are added to User Groups and look as follows:

Configure an Area

For each object instance in controller code, it's required to configure an area using the instruction dialog box (PlantPAx instructions) or extended tag property area (Add-On Instructions). Configuring each instruction with the specified area name will grant or deny permissions on the faceplates for these objects. The following displays use the default value "Area01".

To grant permission on faceplates, the Area name in the controller must match the area that is created within the HMI application (without _Basic \ _Advanced).

For **FactoryTalk** user groups:

Figure 3 - PlantPAx Instruction Dialog Box

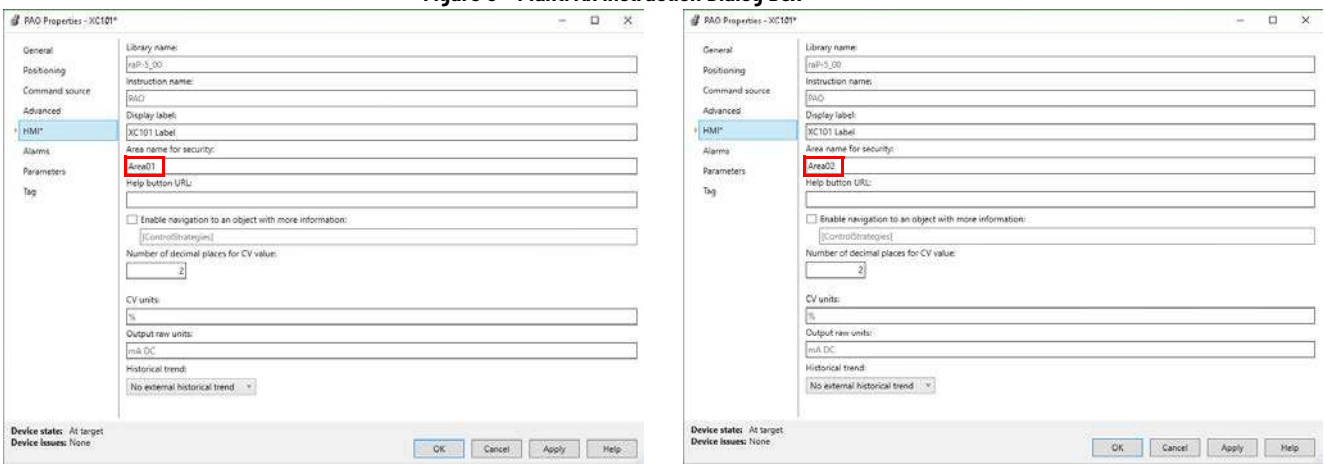
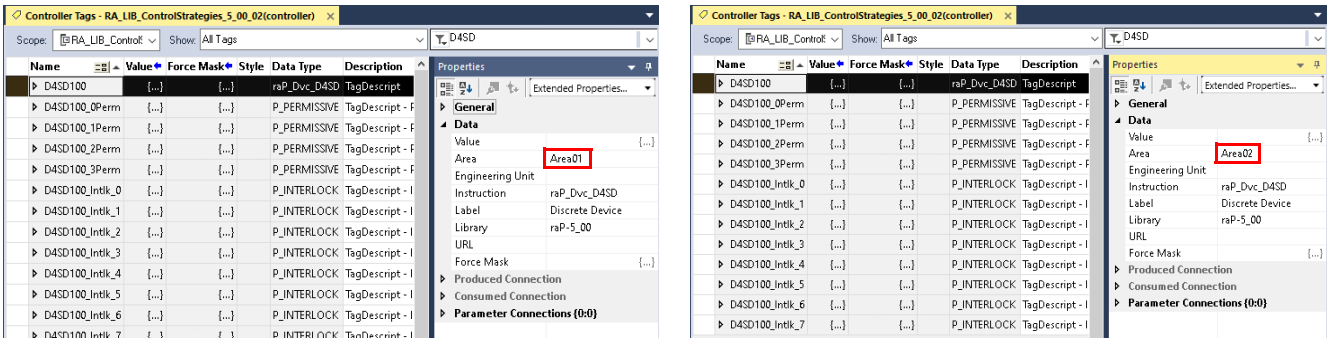


Figure 4 - Add-On Instruction Extended Tag Property



For **Domain** user groups:

Figure 5 - PlantPAx Instruction Dialog Box

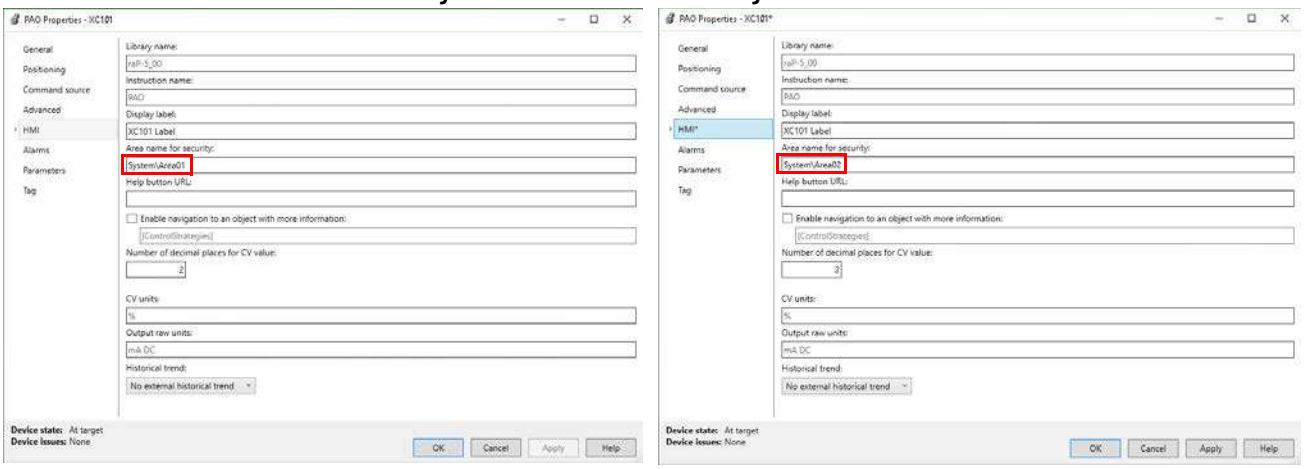
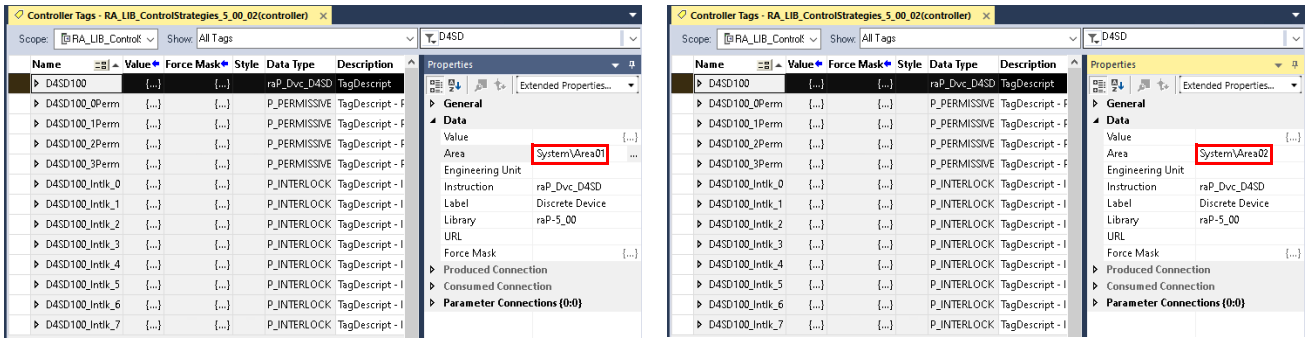


Figure 6 - Add-On Instruction Extended Tag Property



Adding Users to Groups

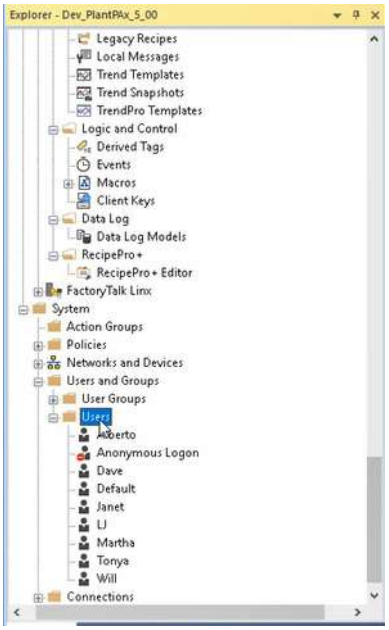
Assign each user to the appropriate user group. Only FactoryTalk users need to be added to Users. Windows-Linked Users are automatically added when Windows-Linked User Groups are added.

With multiple process areas defined (example Area01, Area02), note that each user needs to be assigned not only to the HMI_{group} (example HMI_Operator) but also the “area” group. Operators are assigned to the HMI_Operator group and then also to the Area01_Basic group. This limits operator access to only the faceplate operator controls for devices that are assigned to Area01. Engineers are assigned to the HMI_Engineering group and also to the Area01_Advanced and Area01_Basic groups. This allows the engineer access to also the advanced engineering features on the faceplates for devices that are assigned to Area_01.

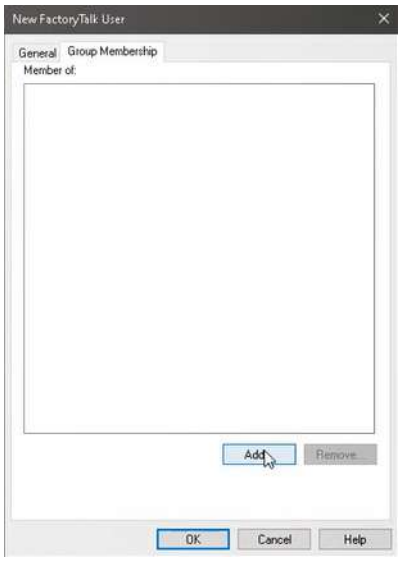
IMPORTANT Users assigned to “Advanced” groups must also be assigned to the corresponding “Basic” groups

1. Open the HMI application with FactoryTalk View Studio software.

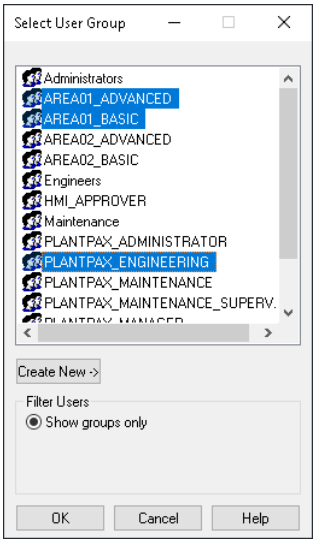
2. Select Users from the menu.



3. Right-click on a user to select that user's properties.
4. Select the Group Membership tab and select Add.

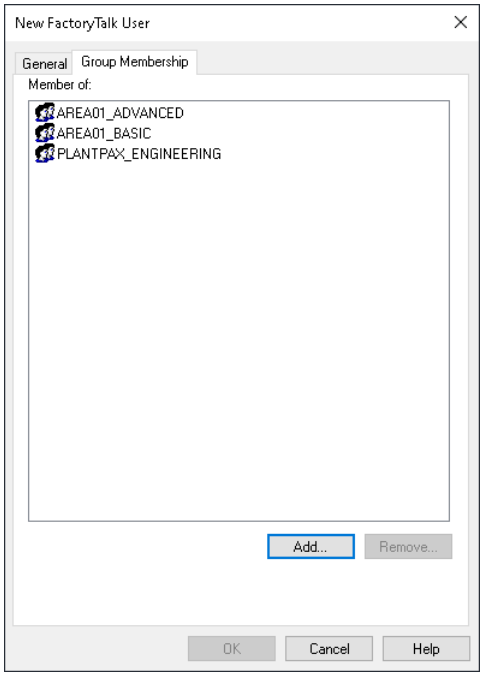


5. Select the groups to assign to the user. (Multiple groups can be selected by holding down the Ctrl key.)



It's recommended that users that belong to the HMI_Engineer and HMI_Maintenance_Supervisor group also be added to both the area01_Basic and area01_Advanced groups.

6. Once added, the groups appear assigned to the user.

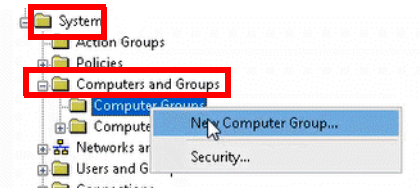


Line of Sight Based Security

The procedures for this functionality require a distributed system. This section describes how to add a desired computer to a group (‘Computer Group’) and to an area of the plant.

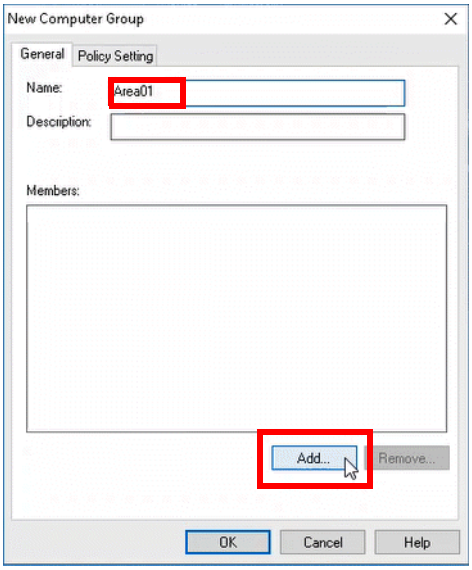
IMPORTANT The macro ‘NavToDisplay with line of sight’ must be added to the project and renamed ‘NavToDisplay’ to replace the existing ‘NavToDisplay’.

1. From the FactoryTalk View Distributed application, click ‘+’ to expand System and then click ‘+’ to expand Computers and Groups.

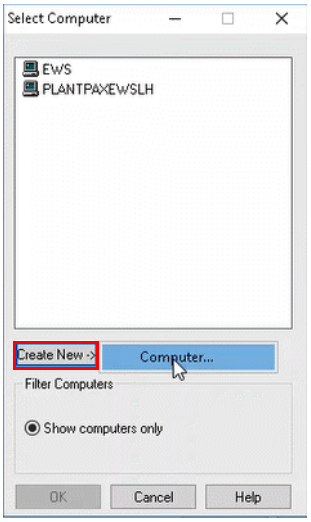


2. Right-click Computer Groups and choose New Computer Group.
3. Enter the area name and click Add.

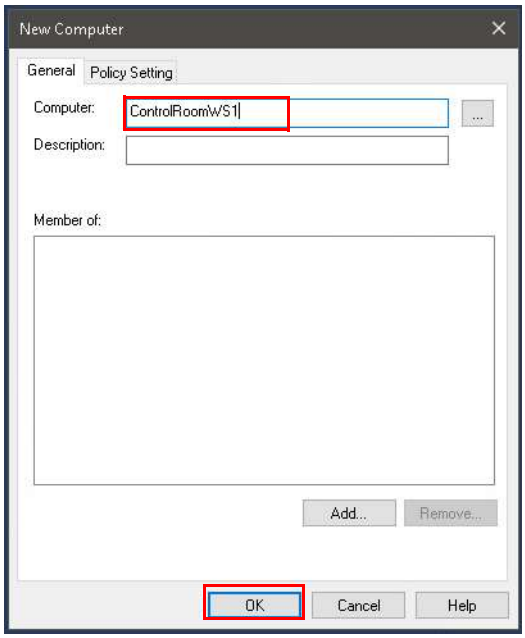
   The area name is the same name as the area name configured in the controller. The computer area name does not have the ‘Basic’ or ‘Advanced’ suffix.



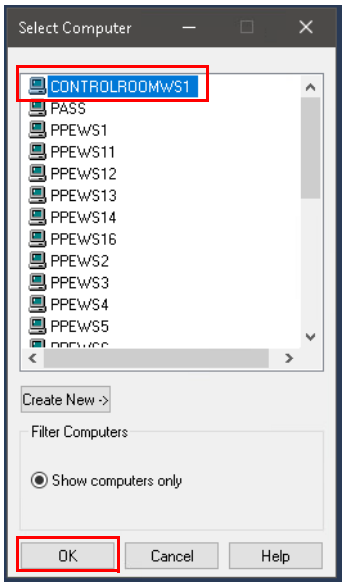
4. On the Select Computer window, select Create New and choose Computer.



5. Enter a desired computer name.



6. Select the name of the desired computer.



7. To add the computer group to the area, click OK.

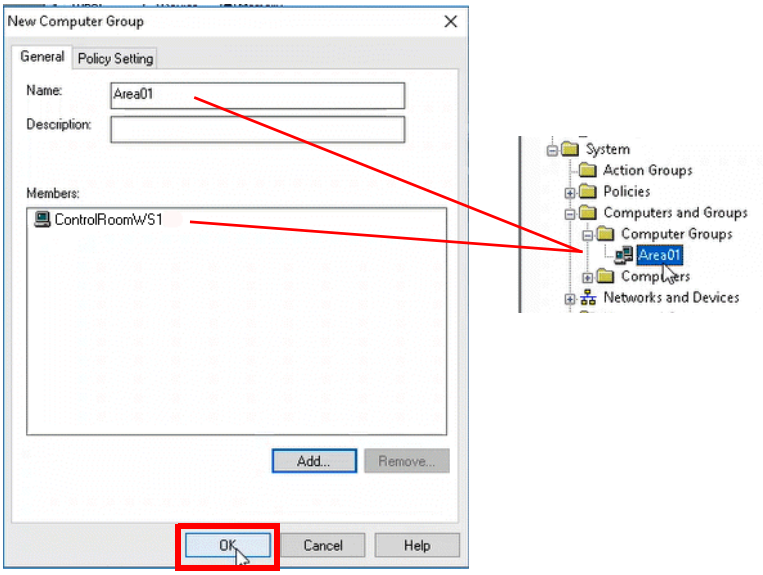
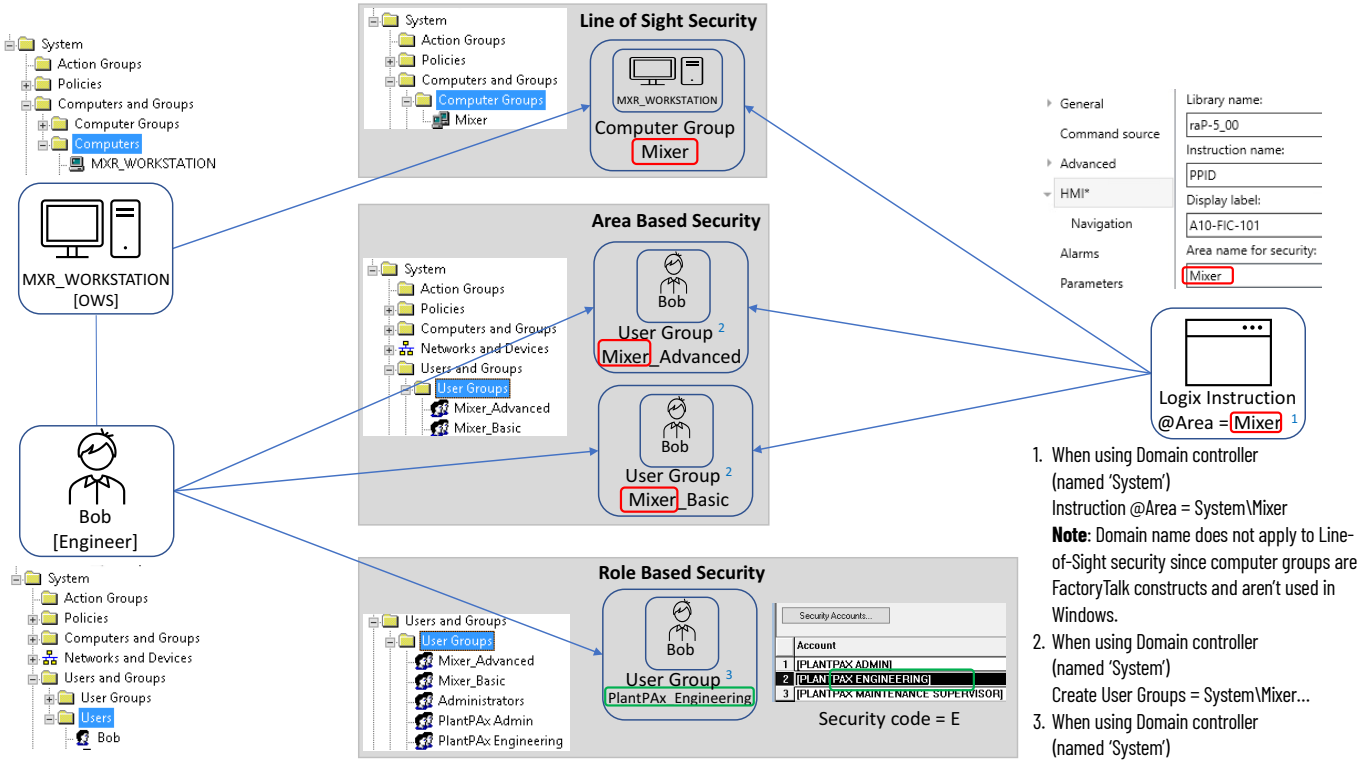


Figure 7 - Security Example with Concurrent Implementation of all Three Security Methods



1. When using Domain controller (named 'System')
   Instruction @Area = System\Mixer
   Note: Domain name does not apply to Line-of-Sight security since computer groups are FactoryTalk constructs and aren't used in Windows.
2. When using Domain controller (named 'System')
   Create User Groups = System\Mixer...
3. When using Domain controller (named 'System')
   Import user groups = System\PlantPAx...

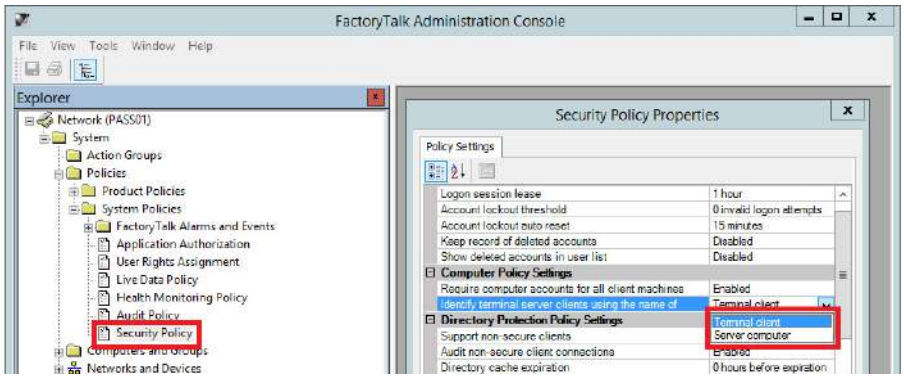
Remote Desktop Services

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

Use Default Terminal Client

You have two server options to specify how each remote terminal identifies itself to FactoryTalk Security: terminal client or server computer; terminal being the default.

1. Navigate to Rockwell Software>FactoryTalk Administration Console.
2. Under System>Policies>System Policies, double-click Security Policy.
3. On the Policy Settings dialog box under Computer Policy Settings, leave terminal client as the default for remote desktop services to be available and select OK.

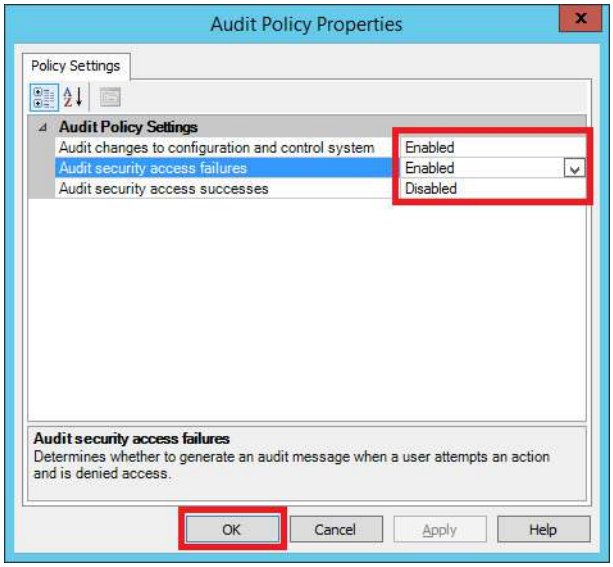


Select Server computer from the pull-down menu and click OK if you want external client computers to be able to log in to the FTD without any pre-configuration. This option, however, does not let you track specific actions from the terminal client.

Audit Security Actions

You can enable an audit to track configurations and security.

1. Navigate to Rockwell Software>FactoryTalk Administration Console.
2. Under System>Policies>System Policies, double-click Audit Policy.
3. Under Audit Policy Settings, select Enabled from the Audit security access failures pull-down menu and select OK.



Network Infrastructure

The PlantPAx® Distributed Control System supports several network topologies to meet specific needs. The following sections summarize the recommended network topology designs with more detail available by following the referenced links to the details provided later in this chapter.

Redundant PRP Topology

This topology provides high availability with the duplication of infrastructure for the most critical process operations:

- NIC teaming for dual connections between PASS servers and supervisory controllers
- EIGRP (Enhanced Interior Gateway Routing Protocol) provides Layer 3 routing capabilities
- HSRP provides redundant PRP 'RedBox' functionality
- PRP provides dual connectivity between two devices
- RedBox (redundancy box) connects devices without PRP technology to both LAN A and LAN B
- Cisco® Stackwise provides redundancy at core switches

For more information, see Redundant PRP Topology.

Resilient DLR Topology

This architecture provides a means to detect, manage, and recover from a single fault in a ring-based network. You can use redundant gateways to provide DLR network resiliency to the rest of the network. This architecture also includes the following:

- NIC teaming for dual connections between PASS servers and supervisory controllers
- EIGRP (Enhanced Interior Gateway Routing Protocol) provides Layer 3 routing capabilities
- Redundant DLR gateway functionality
- DLR is a ring topology that recovers after a single point of failure
- Cisco® Stackwise provides redundancy at core switches

For more information, see Resilient DLR Topology.

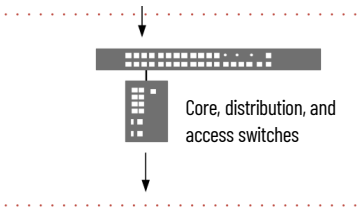
Simplex-Star Topology

This architecture provides a basic network configuration. This topology is effective when there is no requirement for high availability and network disruptions are tolerable.

- No disruptions to the network when you connect or remove devices.
- IMPORTANT: If a connecting network device fails, there's no redundancy and connected nodes can't communicate on the network.
- EtherNet/IP™ backbone between devices in a STAR topology
- NIC teaming is optional.

For more information, see Simplex - Star Topology.

Prerequisites



Following the System Workflow, design the network infrastructure. You need to know which of the following are in your system:

- Domain controller or workgroup
- PASS or PASS-C

Before you design and implement a PlantPAx network infrastructure, you should:

- Have experience with VLAN and IP schemes.
- Have a network design that defines the requirements for the supervisory and control networks in the PlantPAx system.
- Be familiar with how to use the Express Setup and Device Manager utilities to configure and configure Stratix® switches.
- Be familiar with the Cisco IOS® command-line interface (CLI).
- Verify that no fixed IP 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.

For more information, see these additional resources.

Resource	Description
Stratix Managed Switches User Manual, publication 1783-UM007	Describes how to build, configure, and troubleshoot Stratix switches.
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.
EtherNet I/P Parallel Redundancy Protocol Application Technique, publication ENET-AT006	Describes how you can configure a PRP network with a compatible device or switch.
EtherNet I/P Device Level Ring Application Technique, publication ENET-AT007	Describes DLR network operation, topologies, configuration considerations, and diagnostic methods.
Deploying a Resilient Converged Plantwide Ethernet Architecture, Publication ENET-TD010	Describes how to design and deploy a resilient plant-wide or site-wide LAN architectures for IACS applications.
Deploying Device Level Ring within a CPwE Architecture, publication ENET-TD015	Describes how to design and deploy DLR technology with IACS device-level, switch-level, and mixed device/switch-level ring topologies across OEM and plant-wide or site-wide IACS applications.
Scalable Time Distribution within a Converged Plantwide Ethernet Architecture, publication ENET-TD016	Describes how to design and deploy Scalable Time Distribution technology throughout a plant-wide Industrial Automation and Control System (IACS) network infrastructure.
Deploying Parallel Redundancy Protocol within a CPwE Architecture, publication ENET-TD021	Describes how to design and deploy PRP technology with redundant network infrastructure across plant-wide or site-wide IACS applications.

Network Configuration Preparation

Smart devices on PlantPAx system architectures communicate on the EtherNet/IP network via Stratix and Cisco switches. These managed switches provide a secure switching infrastructure for harsh environments. You can connect the switches to network devices such as servers, routers, and other switches. In industrial environments, you can connect Ethernet-enabled industrial communication devices, including controllers, human machine interfaces (HMIs), drives, sensors, and I/O.

The Ethernet network provides the communication backbone for the supervisory network for the workstations, servers, and the controllers:

- Configure all communication interfaces to operate at the fastest speed possible for your hardware configuration, full-duplex for 100/1000 network adapters. See Important for autonegotiate settings.

IMPORTANT Use of autonegotiate settings is recommended to reduce chance of mis-configuration and failures. However, it's desirable to operate at the fastest speed possible at full-duplex. We recommend verifying your switch settings during commissioning to make sure that the system was able to autonegotiate properly. The speed and duplex settings for the devices on the same Ethernet network must be the same to avoid transmission errors.

- Select the cable type based on environmental conditions.

Type	Details
Fiber-optic	• Long distances • Near high magnetic fields, such as induction-heating processes • For extreme high-noise environments • For poorly grounded systems • For outdoor applications
Shielded twisted-pair	• Use Category 5e, 6, or 6a cables and connectors • Use termination sequence 568A for industrial applications

Follow these guidelines for devices on the EtherNet/IP network:

- Make sure that an I/O module RPI is two times faster than the periodic task that you're using.
- The number of devices can affect the CIP™/TCP count differently. Never use more than 80% of the available connections for the communication modules.
- Consider packets per second for performance if you use many devices.
  - I/O packets per second (pps) describes an implicit message rate (Class 1). An I/O communication use approaching or above 80% can necessitate an adjustment to the RPI.
  - HMI packets per second (pps) describes an explicit message rate (Class 3). RSLinx® connections and message instructions generate CIP traffic. HMI traffic is TCP-based, not UDP-based.
  - The combination of implicit and explicit messaging provides the total use for a device. If you add implicit messaging (I/O), it takes bandwidth from the HMI because it has higher priority than HMI messaging. The combination of CIP implicit (highest priority) and CIP explicit (second priority) can't exceed 100% use.
- Use compatible keying on communication modules. Where required, such as in validated industries, you can use an exact match for keying.

Recommended VLANs

Subnets 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 following table of recommended VLANs segments the system and recommends IP address ranges. Use these recommendations with the topology worksheet to segment your system.

Knowledgebase Technote, *PlantPAx System Release 5.20 Configuration and Implementation Tools*, contains the recommended topology and switch settings. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Table 5 - Descriptions for VLANs and Ethernet Address Ranges(1)

VLAN ID (Name)	EtherNet/IP Address Range		Description
1	N/A	N/A	Not used
300 (Native VLAN)(2)	N/A		Not to have any assigned IP addresses Native for Control and Supervisory
500 (Control network management VLAN)	172.18.0.1		Default gateway
	172.18.0.2	172.18.0.9	VLAN routing – switch addresses (to be utilized for Layer 3 switches)
	172.18.0.10	172.18.0.253	Application – switch addresses
501 (Control network – Default)	172.18.1.1	N/A	Default gateway
	172.18.1.2	172.18.1.9	VLAN routing
	172.18.[2…].10	172.18.[…9].253	Ethernet interface between controllers and system applications.
502…509 (Additional Control network VLANs for IO and MCC)	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, I/O modules, and MCCs (fixed)
600 (HMI Control + Supervisory management VLAN)	172.20.0.1	N/A	Default gateway
	172.20.0.2	172.20.0.9	VLAN routing – switch addresses (to be used for Layer 3 switches)
	172.20.0.10	172.20.0.253	Application – switch addresses
601 (HMI Control network + Supervisory network – wired network)	172.20.1.1	N/A	Default gateway
	172.20.1.10	N/A	Domain/DNS primary server
	172.20.1.11	N/A	Domain/DNS secondary server
	172.20.1.12	172.20.1.99	Servers and workstations (DHCP)
	172.20.1.2	172.20.1.9	VLAN routing
	172.20.1.1	172.20.1.25	Workstation interface
602 (Supervisory network - wireless network)	172.20.2.1	N/A	Default gateway
	172.20.2.2	172.20.2.9	VLAN routing – switch addresses (to be used fro Layer 3 switches)
	172.20.2.10	172.20.2.253	Mobile interface
603 (External - untrusted network) **Note:** From IDMZ (industrial demilitarized zone)	172.20.3.1	N/A	Default gateway
	172.20.3.2	172.20.3.9	VLAN routing – switch address (to be used for Layer 3 switches)
	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 need to use a dedicated management VLAN, but it's a good practice. Many times, a supervisory VLAN is the same VLAN as the management VLAN.

Command-line Interface (CLI)

Along with Device Manager and Logix Designer applications, you can use the Cisco IOS® command-line interface (CLI) to manage the switch. This interface enables executes Cisco IOS commands by using a router console or terminal, or by using remote access methods. You can:

- Connect directly to the switch console port
- Enable Secure Shell (SSH) or Telnet in Device Manager

For more information about how to use the CLI, see https://www.cisco.com/.

Redundant PRP Topology

Parallel Redundancy Protocol (PRP) is defined in international standard IEC 62439-3 and provides high-availability in Ethernet networks. PRP technology creates seamless redundancy by sending duplicate frames to two independent network infrastructures, which are known as LAN A and LAN B.

A PRP network includes the following components.

Component	Description
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel.
Double attached node (DAN)	An end device with PRP technology that connects to both LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to either LAN A or LAN B. A SAN does not have PRP redundancy.
Redundancy box (RedBox)	A switch with PRP technology that connects devices without PRP technology to both LAN A and LAN B.
Virtual double attached node (VDAN)	An end device without PRP technology that connects to both LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.
Infrastructure switch	A switch that connects to either LAN A or LAN B and isn't configured as a RedBox.

Redundancy uses Hot Standby Router Protocol (HSRP). HSRP lets you configure two or more routers as standby routers, but only one router is active at a time.

Additional Resources for PRP Topology

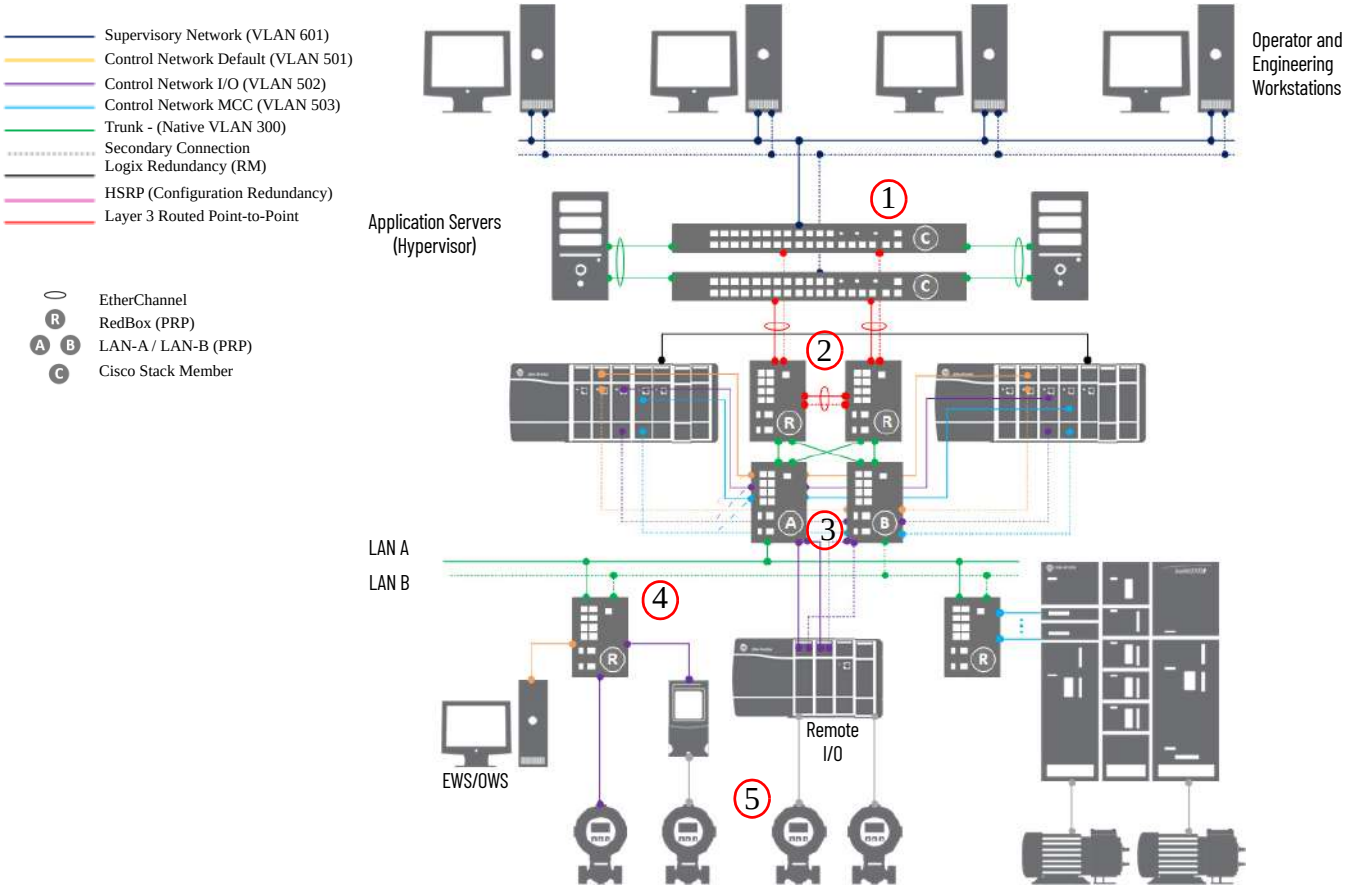
For more information, see these additional resources.

Resource	Description
Design Guide, Deploying Parallel Redundancy Protocol within a CPwE Architecture, publication ENET-TD021.	Highlights key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of PRP applications.
EtherNet/IP Parallel Redundancy Protocol, publication ENET-AT006	Describes how you can configure a Parallel Redundancy Protocol (PRP) network with a compatible device or switch.
EtherNet/IP Network Devices User Manual, publication ENET-UM006	Explains Logix 5000© tools that are used in EtherNet/IP topologies and network operation.
Cisco Catalyst© 9300 Series Switches	Describes the hardware installation.
	Describes how to update firmware.
	Lists the recommended firmware downloads.
	Describes how to configure the switch.

Switch Configuration in a Redundant PRP Topology

The following figure shows an example PRP topology. The numbers circled in red match the sequential instructions below the example.

Figure 8 - Redundant PRP Topology Example



Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the recommended topology and switch settings. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

WARNING: Do not connect switches together before the network is fully configured.

1. Configure the Cisco stack switches.

   See the '1 PRP Cisco Stack Switch' tab in the topology worksheet.xlsx.

   a. Connect to distribution switches
   b. Connect to application servers

   For stacking guidelines and cabling considerations, see Cisco user documentation.

2. Configure the HSRP distribution switches.

   See the '2 PRP HSRP Switch' tab in the topology worksheet.xlsx.

   a. Connect distribution switches to the core stack
   b. Configure PRP

3. Configure the LAN A/B access switches.

   See the '3 PRP LAN A B' tab in the topology worksheet.xlsx.

4. Configure the RedBox switches.

   See the '4 PRP RedBox Infrastructure' tab in the topology worksheet.xlsx.

5. Add PRP devices or skids.

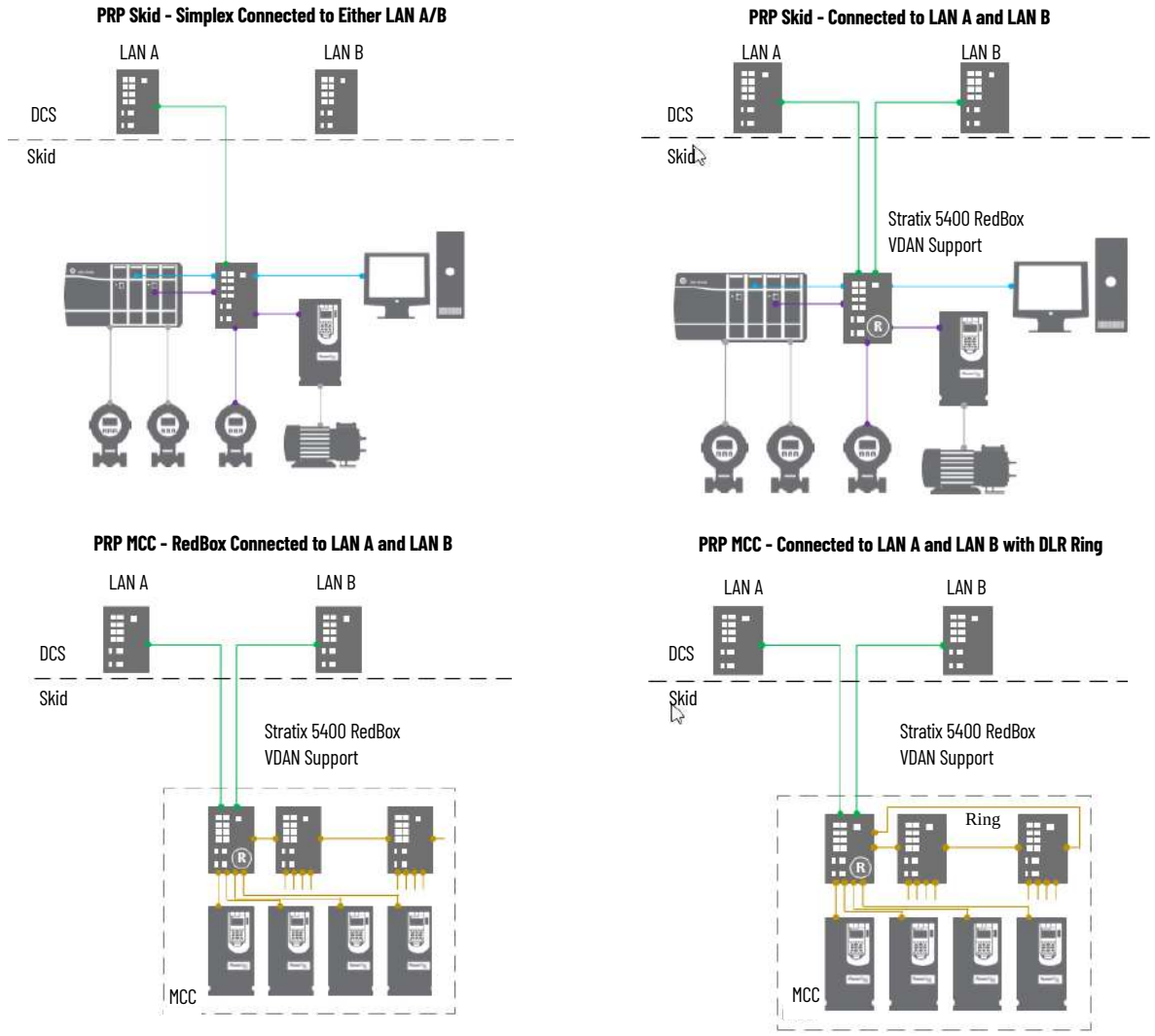
   See the user documentation for your devices on how to configure PRP settings.

   For examples, see Figure 9.

6. Verify the PRP configuration.

   See the '5 PRP Verification' tab in the topology worksheet.xlsx.

Figure 9 - PRP Skid and MCC Lineup



Resilient DLR Topology

Device Level Ring (DLR) is an EtherNet/IP protocol that is defined by the Open DeviceNet® Vendors' Association (ODVA). DLR provides a means to detect, manage, and recover from single faults in a ring-based network.

A DLR network includes the following types of ring nodes.

Node	Description
Ring supervisor	A ring supervisor provides these functions: • Manages traffic on the DLR network • Collects diagnostic information for the network A DLR network requires at least one node to be configured as ring supervisor. By default, the supervisor function is disabled on supervisor-capable devices.
Ring participants	Ring participants provide these functions: • Process data that is transmitted over the network. • Pass on the data to the next node on the network. • Report fault locations to the active ring supervisor. When a fault occurs on the DLR network, ring participants reconfigure themselves and relearn the network topology.
Redundant gateways (optional)	Redundant gateways are multiple switches that are connected to a single DLR network and also connected together through the rest of the network. Redundant gateways provide DLR network resiliency to the rest of the network.

Consider the following if you choose this topology:

- Depending on firmware capabilities, both devices and switches can operate as supervisors or ring nodes on a DLR network. Only switches can operate as redundant gateways.
- Multiport EtherNet/IP devices that are 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 that are built into DLR-enabled products identify the point of failure, helping to speed maintenance and reduce mean time to restoration.
- The DLR ring supervisor maintains a loop-free topology by blocking port 2 of the embedded-switch device. If the supervisor detects a fault in the network, it unblocks port 2 until the fault is corrected. It's important to remember to enable a ring supervisor before closing the DLR ring. If the ring closed before the supervisor is enabled, a bridge loop results, which generates a broadcast storm.

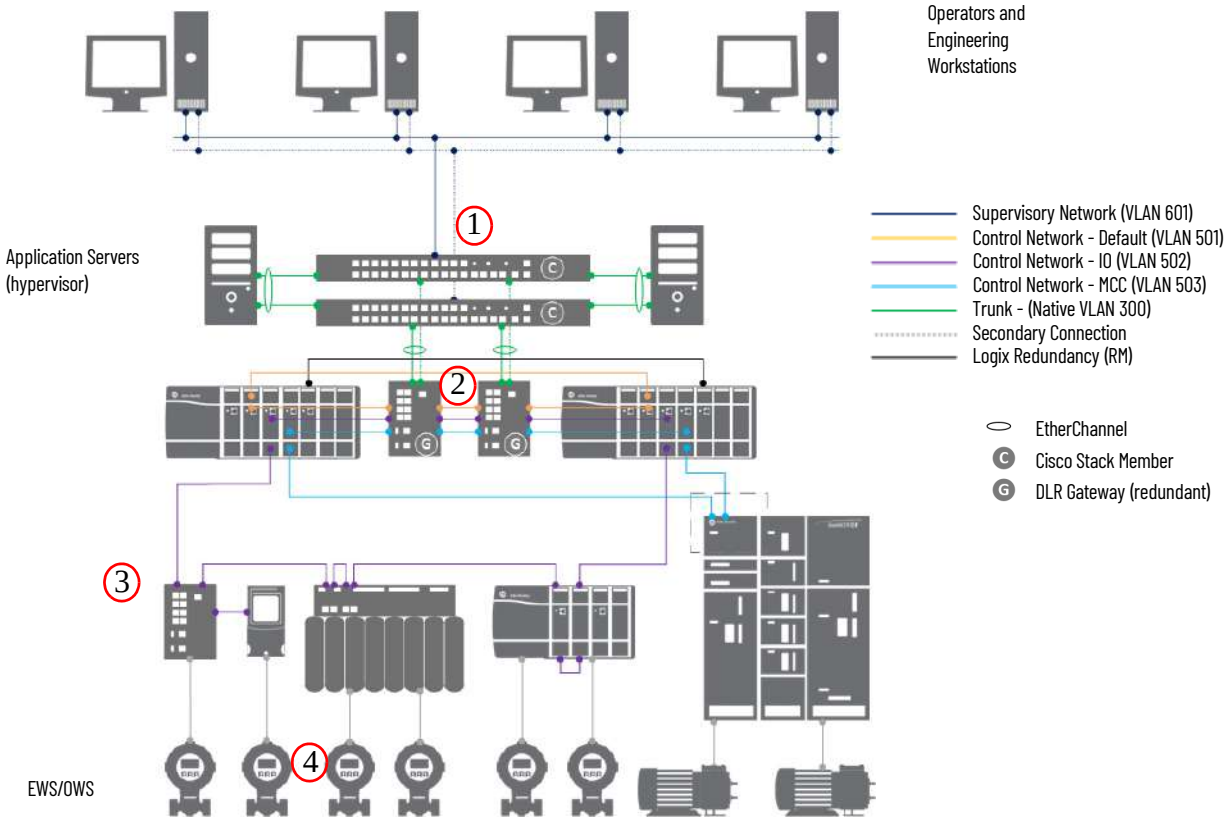
Additional Resources for DLR Topology

For more information, see these additional resources.

Resource	Description
EtherNet/IP Device Level Ring, publication ENET-AT007	Describes DLR network operation, topologies, configuration considerations, and diagnostic methods
EtherNet/IP Network Devices User Manual, publication ENET-UM006	Explains Logix 5000 tools that are used in EtherNet/IP topologies and network operation.

Figure 10 shows an example DLR topology. The numbers circled in red match the sequential instructions below the example.

Figure 10 - Resilient DLR Topology Example



Switch Configuration in a Resilient DLR Topology

Switch configuration in a DLR topology follows the workflow that is shown in Figure 10.

Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the recommended topology and switch settings. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

WARNING: Do not connect switches together before the network is fully configured.

1. Configure the Cisco stack switches.

   See the '1 DLR Cisco Stack Switch' tab in the topology worksheet.xlsx.

   a. Connect to distribution switches
   b. Connect to application servers

   For stacking guidelines and cabling considerations, see the Cisco user documentation.

2. Configure the gateways.

   See the '2 DLR Gateway Switch' tab in the topology worksheet.xlsx.

3. Configure the ring access switches.

   See the '3 DLR Ring Switch' tab in the topology worksheet.xlsx.

4. Add DLR devices or skids.

   See the user documentation for your devices on how to configure DLR settings.

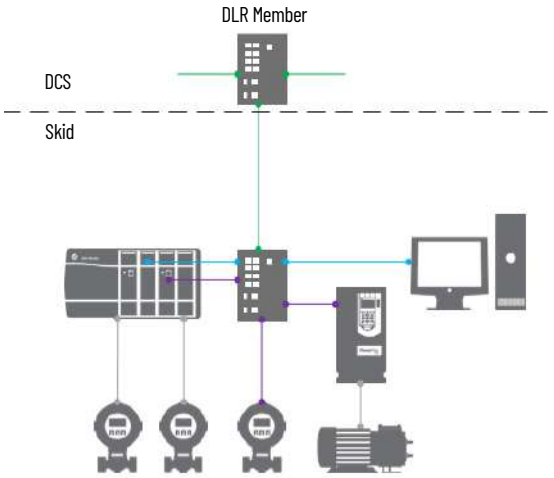
   For examples, see Figure 11.

5. Verify the DLR configuration.

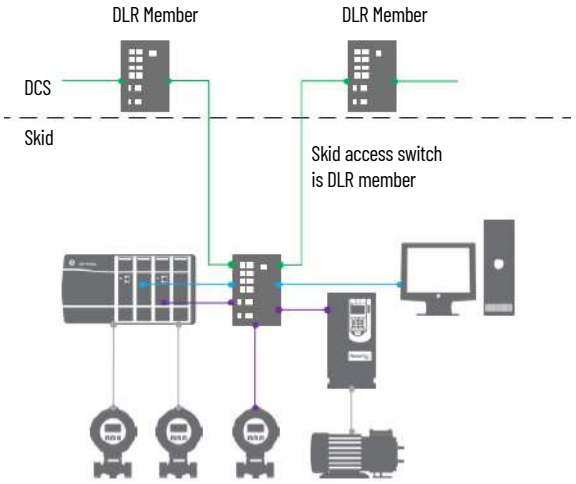
   See the '4 DLR Verification' tab in the topology worksheet.xlsx.

Figure 11 - DLR Skid and MCC Lineup

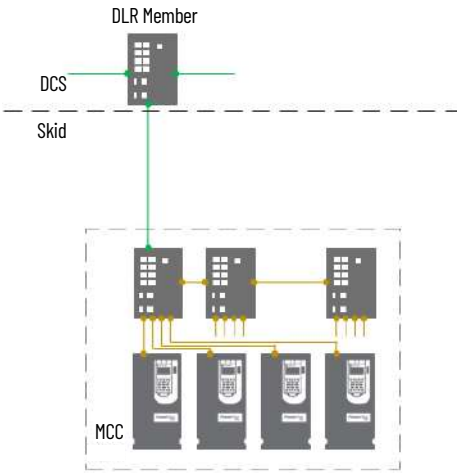
DLR Skid - Simplex Connected to DLR Ring



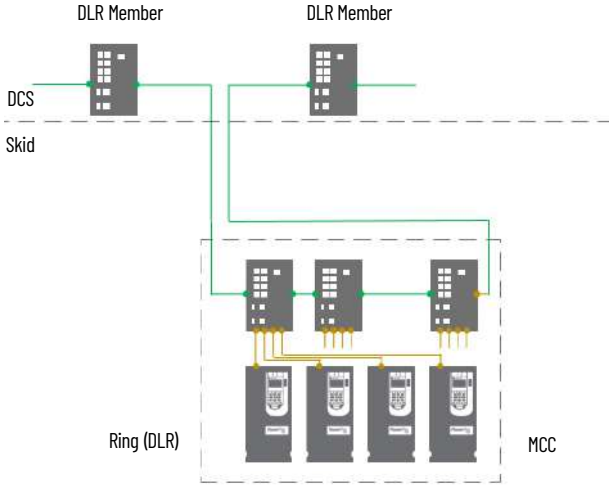
DLR Skid - DCS Integration



DLR MCC - Simplex Connected to DLR Ring



DLR MCC - DCS Integration

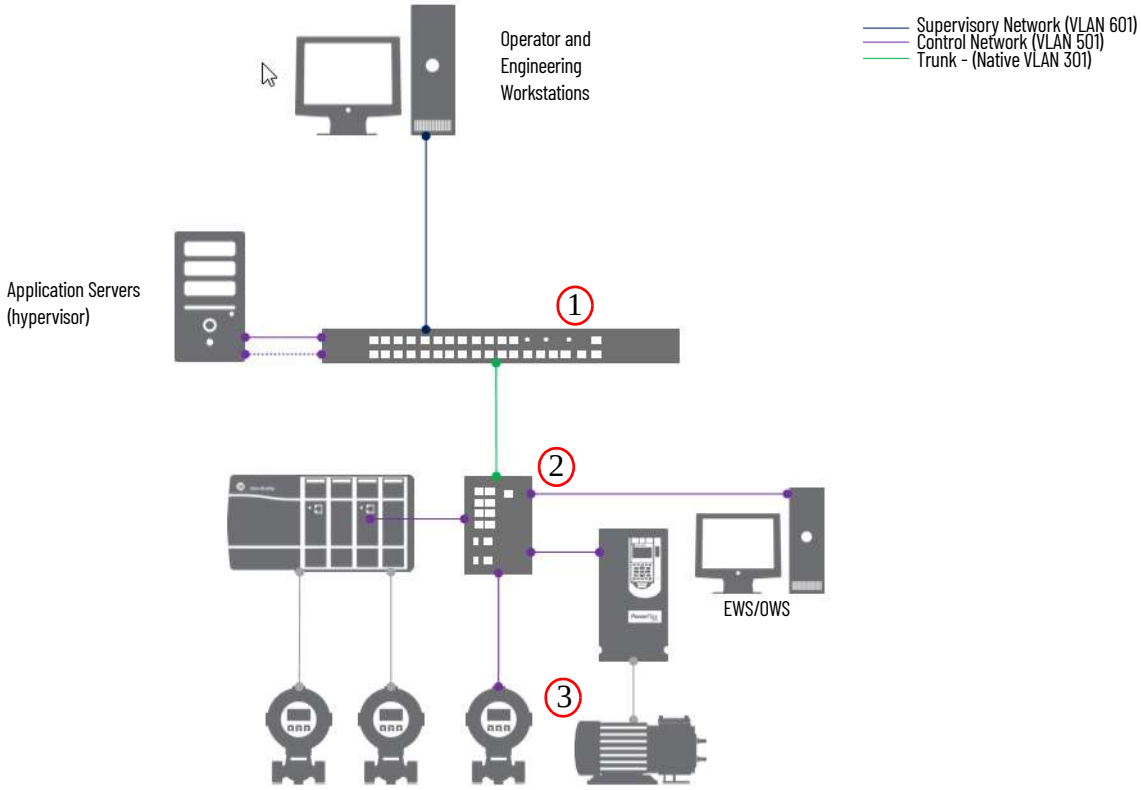


Simplex - Star Topology

In a star topology, access switches serve as an uplink from the servers to the workstations. Layer 2 switches also send information 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.

Figure 12 shows an example simplex star topology. The numbers circled in red match the sequential instructions below the example.

Figure 12 - Simplex - Star Topology Example



Consider the following if you choose this topology:

- The first switch that Rockwell Automation equipment touches must have IGMP snooping enabled. IGMP snooping enables switches to forward multicast packets to ports that are only part of a particular multicast group.

Additional Resources for Simplex Star Topology

For more information, see these additional resources.

Resource	Description
Stratix Managed Switches User Manual, publication 1783-UM007	Describes the embedded software features and tools for configuring and managing the Stratix 5410, Stratix 5400, and the Stratix 5700 Ethernet managed switches.
Stratix Infrastructure Product Family Quick Reference Drawing, publication IASIMP-QR029	Illustration that shows options for connecting your plant network by using standard Ethernet technology.

Switch Configuration in a Simplex Topology

Switch configuration in a simplex topology follows the workflow that is shown in Figure 12.

WARNING: Do not connect switches together before the network is fully configured.

Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the recommended topology and switch settings. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

1. Configure the Cisco stack switch.

   See the '1 Simplex Cisco Stack Switch' tab in the topology worksheet.xlsx.

   For stacking guidelines and cabling considerations, see the Cisco user documentation.
2. Configure the access switches.

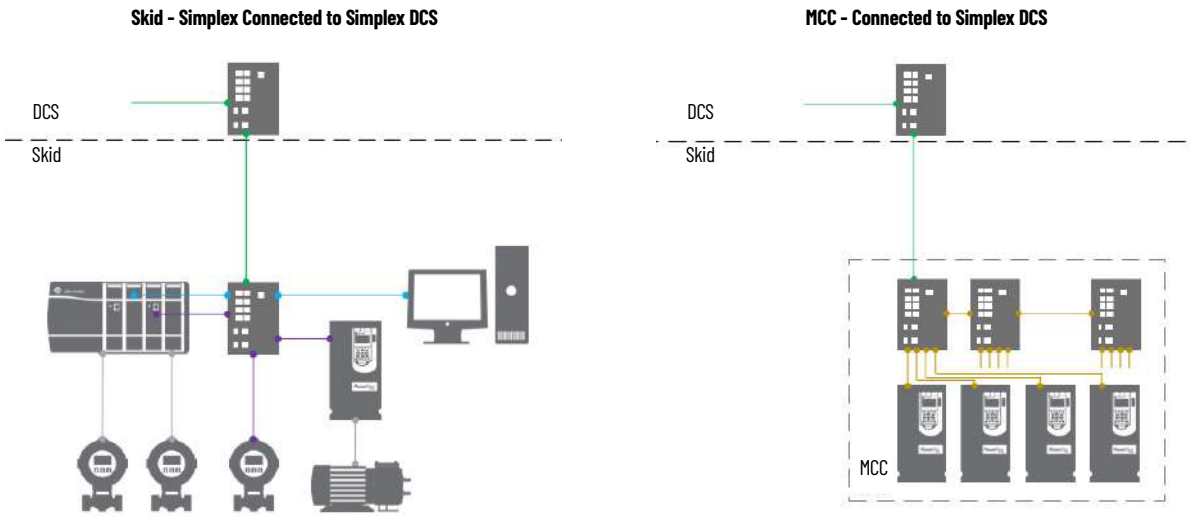
   See the '2 Simplex Access Switch' tab Simplex Switches tab in the topology worksheet.xlsx.
3. Add simplex devices.

   See the user documentation for your devices on how to configure network settings.

   For examples, see Figure 13.
4. Verify the Simplex configuration.

   See the '3 Simplex Verification' tab in the topology worksheet.xlsx.

Figure 13 - Simplex Skid and MCC Lineup



Perimeter Network Considerations

The Perimeter Network (Microsoft®) is a buffer that enforces data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone).

For secure data sharing, the Perimeter Network contains assets that act as brokers between the zones. Consider these methods:

- Use an application mirror, such as a PI-to-PI interface for FactoryTalk® Historian
- Use Microsoft Remote Desktop Gateway services
- Use a reverse proxy server

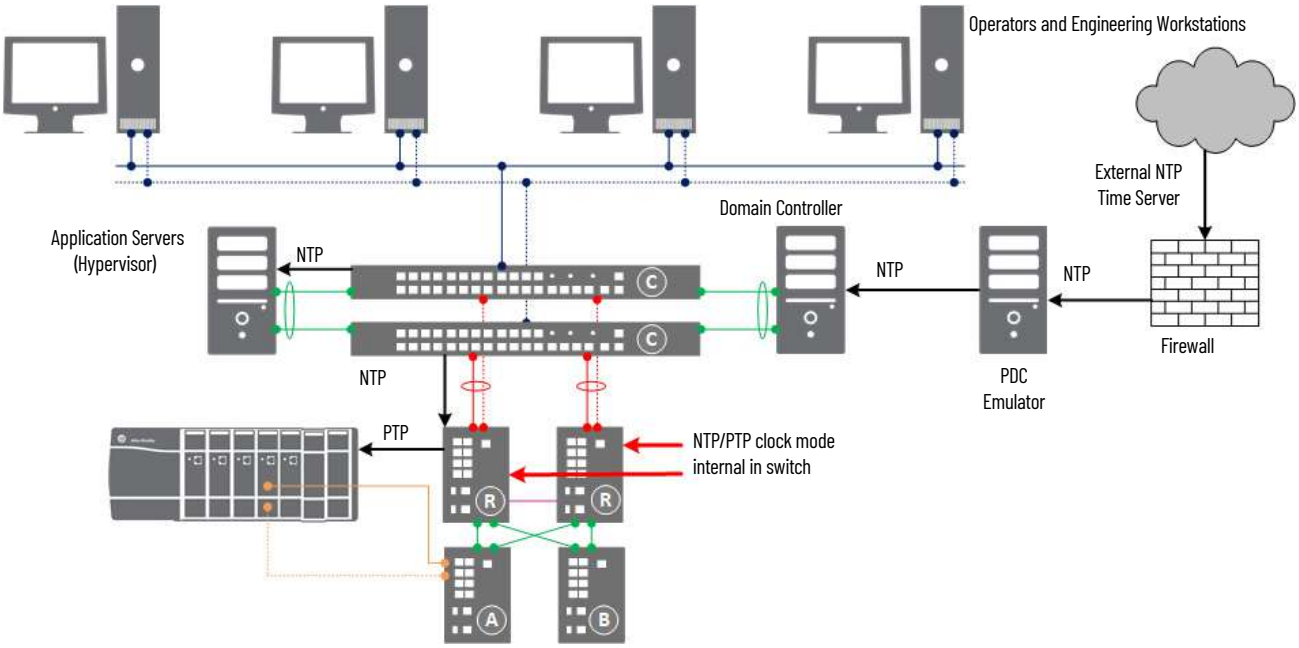
Time Synchronization

System time synchronization is important so that the internal clocks in the controllers, workstations, and servers reference the same time for any event or alarm that occurs. Configure the PASS, application servers, OWS, and EWS to use a single server (for example, a domain controller) as their time reference and keep their clocks synced to it.

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 the following figure. 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.



Two methods are described to use UTC time in your domain:

- Via your local network (intranet) or the Internet (previous diagram)
- Via GPS

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.

For more information on time synchronization and CIP Sync™, see the Integrated Architecture® and CIP Sync Configuration manual, publication IA-AT003.

Considerations

Consider the following suggestions before starting this chapter:

- Decide which network time source, external NTP or GPS reference, that you're going to use.
- To enable CIP Sync functionality in a ControlLogix® controller, select Time Synchronization in Ethernet adapters by using Studio 5000 Logix Designer application.

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.

Configure Internet Time Synchronization

Use a domain controller

PADC

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 can't access the Internet, those URLs could be of your parent domain controller. You can research UTC sources for your proximity, the following table has examples that work for the U.S.

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

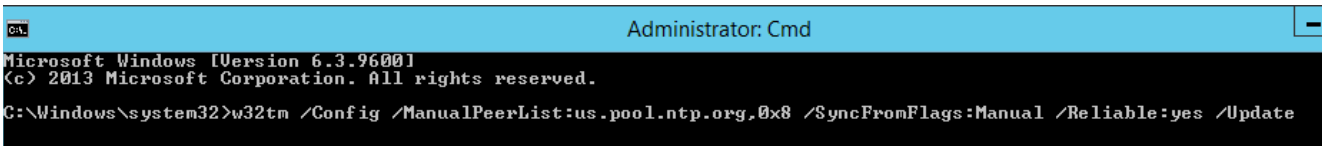
There are (at least) four server pools of pool.ntp.org. But, the preferred assignment for <pool> is the first one (us.pool.ntp.org,0x8). Windows Event Viewer can log errors for URLs that do not respond.

The 0x8 qualifier specifies Client Mode packets for server communication. For more information, See Microsoft Knowledgebase article 875424, Time

synchronization may not succeed when you try to synchronize with a non-Windows NTP server.

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 the previous table. For example, 0x8 (client mode).

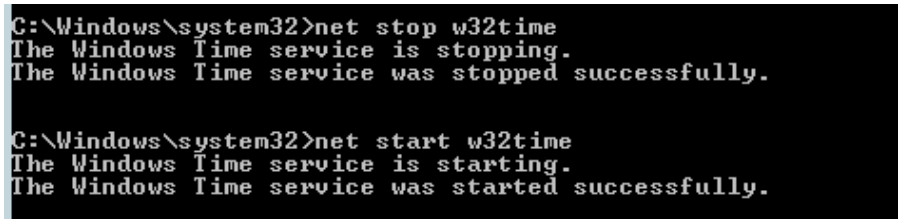
The illustration shows an example that sources the U.S. pool.



If your system can't 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.

Example	Purpose
.	Uses the current computer (PADCA) as the time source
PADCA	Specifies a network time server on your local network

4. After you've 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.



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.

Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the recommended topology and switch settings. Download the spreadsheet from this public article and use the tab that is referenced in each step.

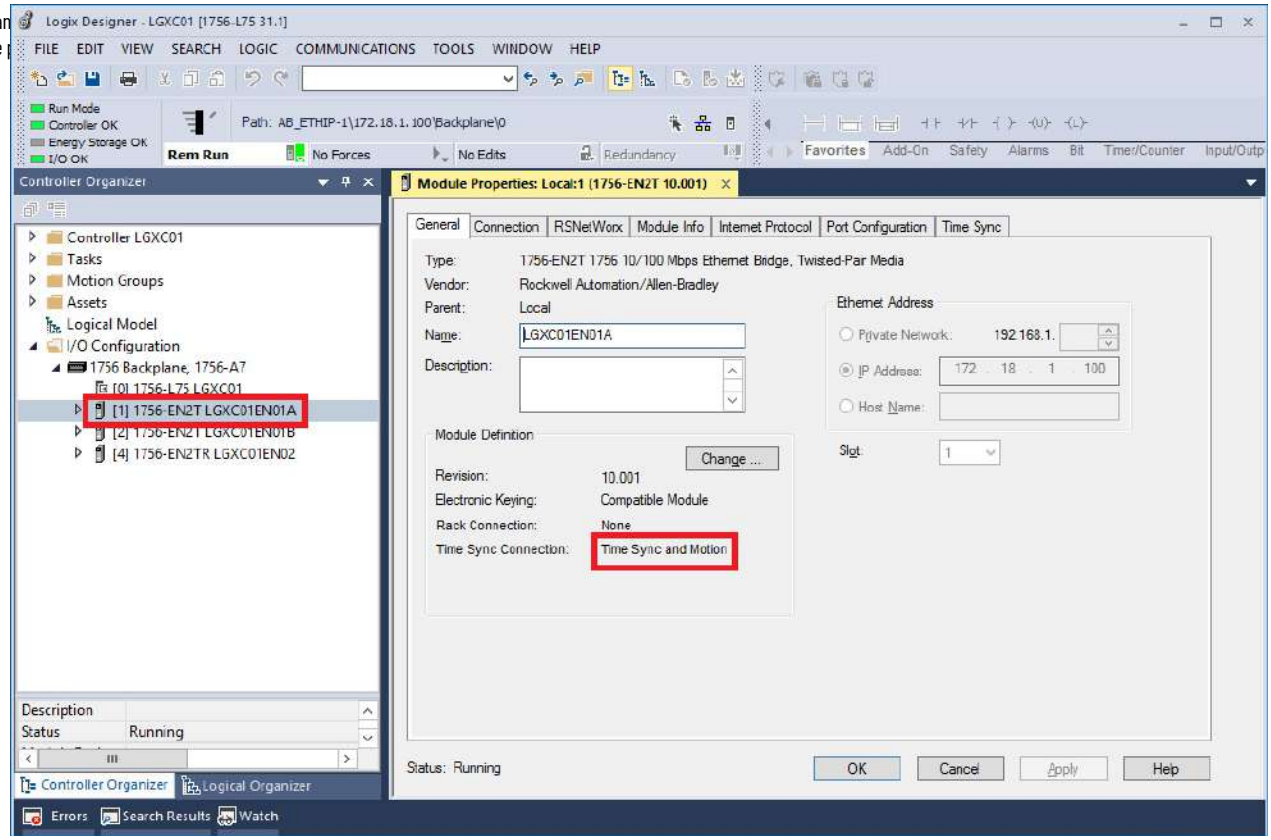
You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Configure PTP Time Synchronization for Ethernet Bridges

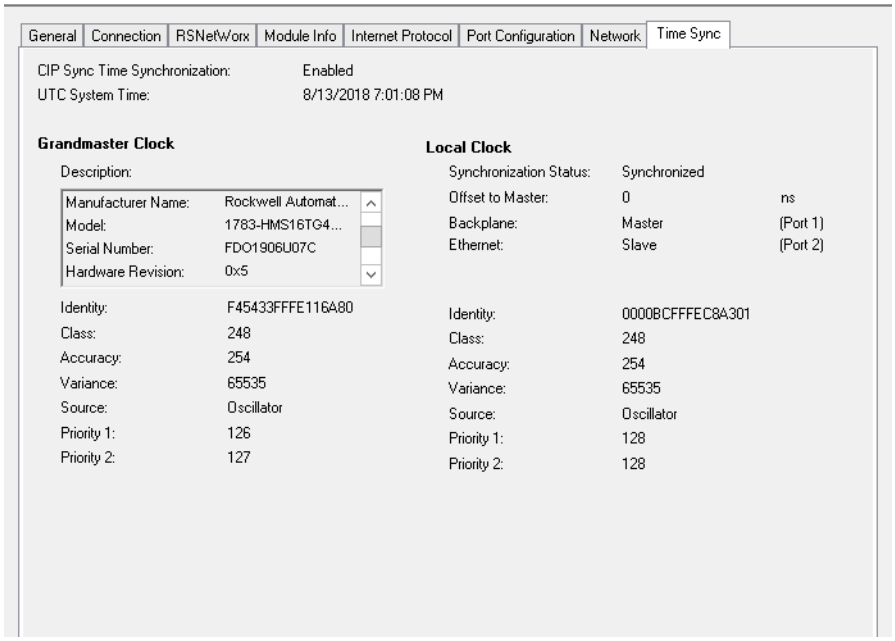
Precision Time Protocol (PTP) enables precise synchronization of clocks in measurement and control systems. PTP generates a Master-Slave relationship among the clocks in the system. Clocks, which are synchronized over the EtherNet/IP network, derive their time from a clock that is selected as the Grandmaster clock. The Time Sync and Motion option **must** be enabled for Ethernet bridge modules to propagate time through the network via switches.

1. Open your project in Logix Designer. On the General tab of the Module Properties dialog box, make sure that 'Time Sync and Motion' is selected for the connection.

Use an
these



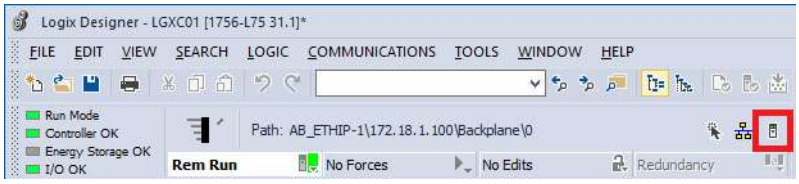
2. If online, select the Time Sync tab to confirm Grandmaster clock settings.



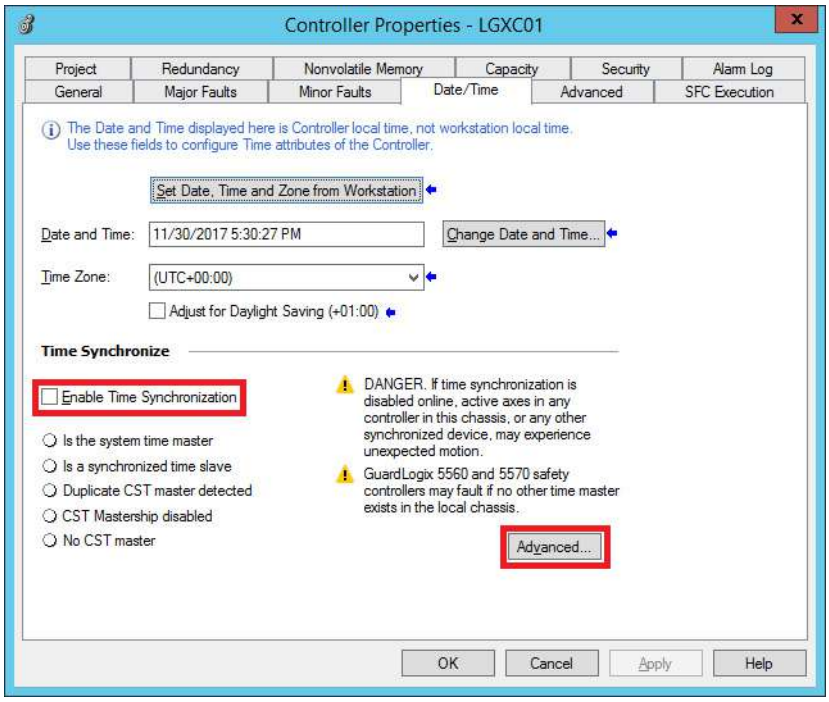
Configure PTP Time Synchronization for Controllers

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.



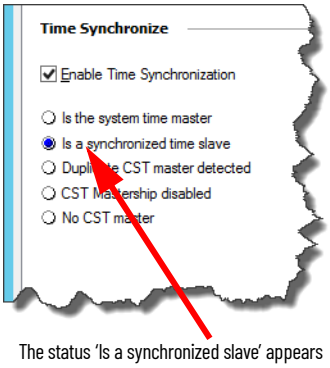
The Controller Properties dialog box appears.



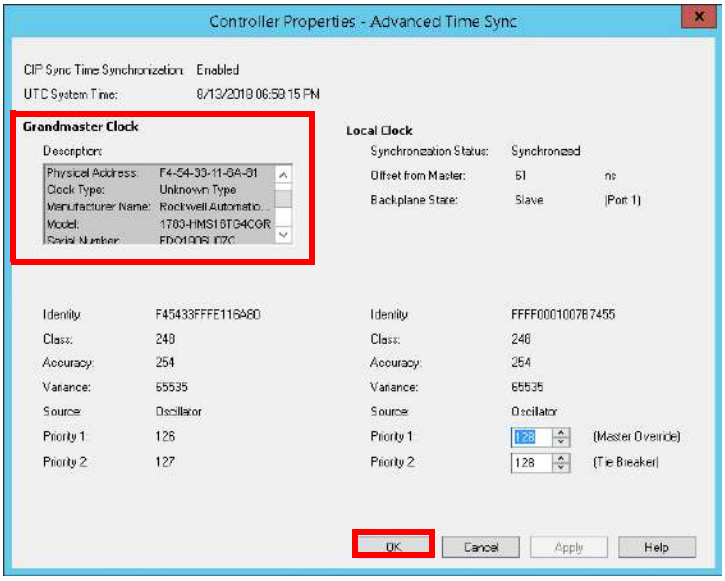
2. On the Date/Time tab, select Enable Time Synchronization.

IMPORTANT Use your local time to configure the Time Zone and Adjust for Daylight Saving.

3. Select Advanced.
4. Select 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.

Notes:

Process Controller Features

The process controller is a member of the Logix 5000® family that provides out-of-box process functionality. Embedded PlantPAx® instructions, graphical workflows, and tag-based alarms streamline code development for your system.

This chapter explains the process controller features that are central to a PlantPAx application. If you create a new application, see Bulk Configuration of a PlantPAx System If you want to edit an existing application see Modifying an Existing PlantPAx System.

Configure Controller Properties

- Controller-to-controller communication
- Produced and consumed tags
- Message instructions

Integrate Field Devices

- HART devices
- Electrical protection devices

Configure Alarms

- Tag-based alarms
- Server tag-based alarms
- Instruction-based alarms

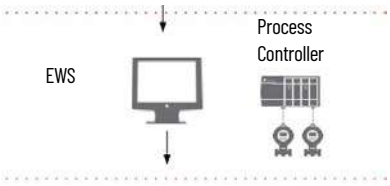
Security Considerations

- Controller security options
- Runtime security
- System security (domain controller, FactoryTalk® Security)
- IEC 62443-3-3 System Security Requirement

HMI Displays

- Optimize runtime performance
- Optimize HMI redundancy

Prerequisites



PlantPAx system release 5.0 added process controllers to the Logix 5000 family of controllers. The process controllers offer additional capabilities that are targeted for DCS applications.

Controller	Catalog Numbers
ControlLogix® 5580 process controller	• 1756-L81EP • 1756-L83EP • 1756-L85EP
CompactLogix™ 5380 process controller	• 5069-L320ERP • 5069-L340ERP

For standard use information, see:

- ControlLogix 5580 and GuardLogix® 5580 Controllers, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 Controllers, publication 5069-UM001

To best use controller resources:

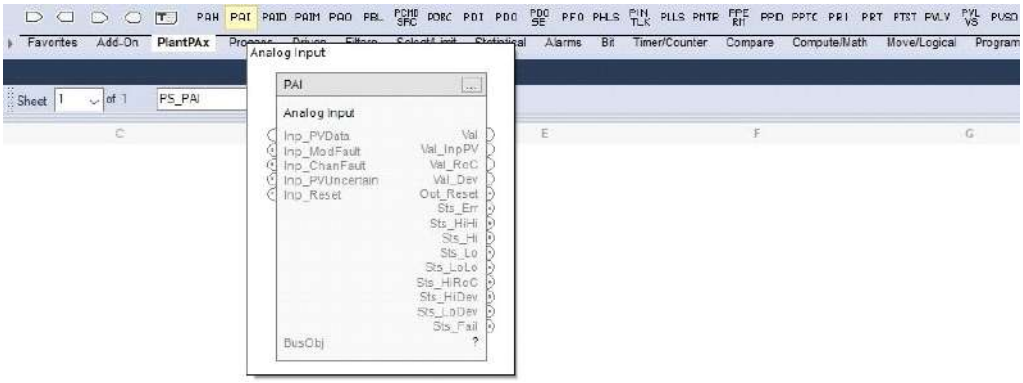
- Use periodic tasks **only**, with minimum number of tasks that are used to define execution speed, faster tasks getting higher priority (lower number).
- Use the L_CPU Add-On Instruction to monitor controller use.

For more information, see these additional resources.

Resource	Description
High Availability Systems Reference Manual, HIGHAV-RM002	Provides guidelines for high availability systems, including redundant system components, networks, and other hardware and software considerations.
Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200	Describes how to build and use library components that comprise the Rockwell Automation Library of Process Objects.
Logix 5000 Controllers Produced and Consumed Tags, publication 1756-PM011	Details how, with a Logix 5000 controller, to produce and consume standard tags and produce a large array.
Logix 5000 Controllers Import/Export Programming Manual, publication 1756-PM019	Describes how to import and export logic components to and from a controller project.

PlantPAx Process Objects

Process controllers support an exclusive set of embedded PlantPAx instructions.

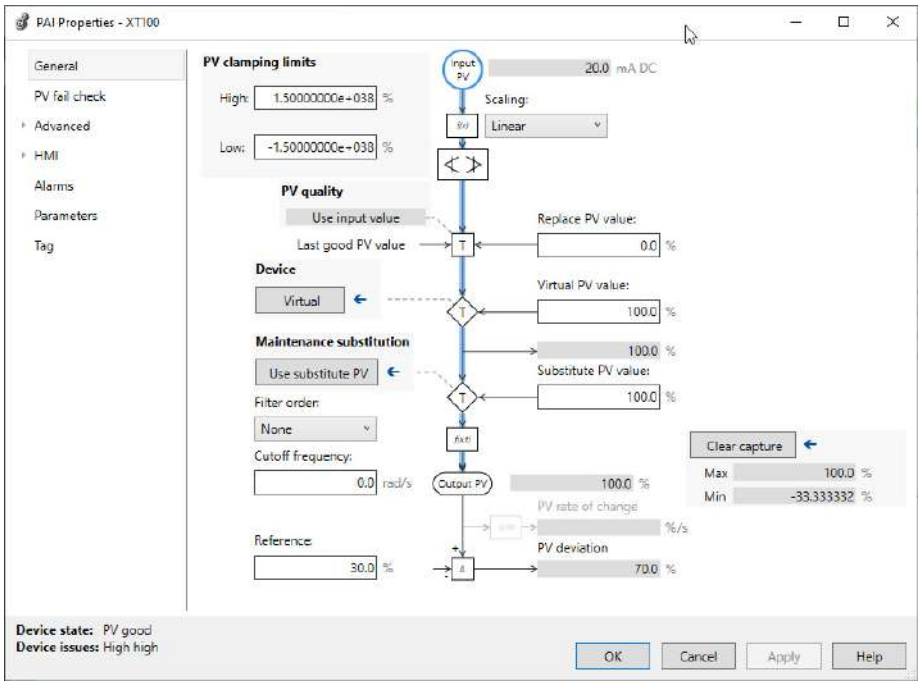


The PlantPAx instructions offer enhanced functionality, including tag-based alarms, that can reduce the number of steps to configure control strategies. For more information about the instructions, see:

- Studio 5000 Logix Designer® online help
- Logix 5000 Advanced Process Control and Drives and Equipment Phase and Sequence Instructions Reference Manual, 1756-RM006

Each PlantPAx instruction features an intuitive design-time configuration interface. It's based on the SAMA (Scientific Apparatus Makers Association) diagram interface, which focuses on the flow of information.

The example shows the PAI - Process Analog Input Object.



This interface improves upon prior releases of the process library, in where the underlying elements of an Add-On Instruction can be viewed but do not illustrate how it functions.

The blue animation line adjusts depending on the instruction execution. In the previous example, see the Maintenance substitution option. If you select 'Use substitute PV,' the blue animation line shows a new execution path.

Import Add-On Instructions

There are additional libraries of Add-On Instructions that you can use to supplement the PlantPAx embedded instructions. Studio 5000 Logix Designer can import a single Add-On Instruction or a Program/Routine containing multiple Add-On Instructions, such as a control strategy generated with ACM software.

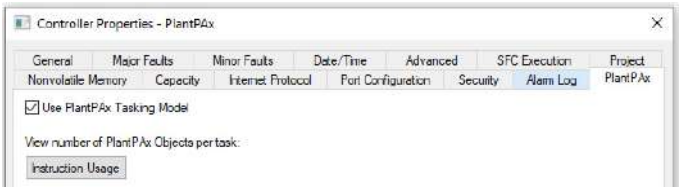
Add-On Instructions are used when the following functionality is required:

Feature	Description
Organization, ownership, and arbitration	• Allows the organization of devices into groups from HMI • Manages and prioritizes ownership of equipment groups • Propagates command and status through equipment groups
Process Instructions from prior libraries	Non-process controllers use the Add-On Instructions from the process library, release 4.1 or earlier
Device Add-On Instructions for supported network devices	The purpose of device Add-On Instructions is to reshape the data structure of similar but disparate equipment to a common structure that can be used by a single common PlantPAx instruction. For example, a device Add-On Instruction for a Variable Speed Drive (VSD) is used to reshape the disparate VSD source data so that a common PlantPAx instruction (PVSD) can also mean that a common control strategy can be used to control all those same VSDs

Configure Controller Properties

Use Studio5000 Logix Designer application to configure the controller.

1. From the Controller Properties dialog box, click the PlantPAx tab.

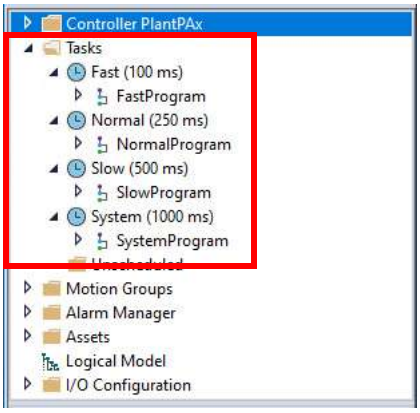


2. If you're using a process controller, leave the check for Use PlantPAx Tasking Model box (checked by default).
3. Click the Date/Time tab and check the Enable Time Synchronization box.
4. Enable Automatic Diagnostics on the Advanced tab.

   Automatic Diagnostics is a mechanism to detect and present device descriptive events with no programming required. Diagnostics based on the device definition (such as fault or open wire) are sent to the HMI and displayed on the Automatic Diagnostic Event Summary object.

PlantPAx Task Model

The Task folder contains a project structure that consists of four pre-defined periodic tasks.



Logic is placed in the appropriate task to verify that it meets the process requirements. These tasks are:

- **Fast (100 ms) –** For control fast loops, such as liquid pressure with related transmitters and pump drives
- **Normal (250 ms) –** For discrete control, such as motors, pumps, and valves
- **Slow (500 ms) –** For level, temperature, analysis loops, phases, and batch sequencing
- **System (1000 ms) –** For slow change temperature control and general controller operations, such as messaging or status

The ControlLogix 5580 and CompactLogix 5380 controllers (including the process controllers) have simplified task management from previous controllers. The controller runs control, communication, and packet processing on separate cores within the controller. You no longer have to reserve CPU time for communication or overhead.

Create the Logical Organizer

The Logical Organizer is a graphical representation of the organization of the configuration logic that is aligned to the process being controlled, called the logic model. It enables you to create and organize hierarchies of the programs and folders in your project, independent of the execution model.

A process controller contains tasks that execute at various rates. Each task contains programs of code that is required to execute at the selected task's rate of execution. The Logical Organizer helps create an understandable organization, based on process functional requirements.

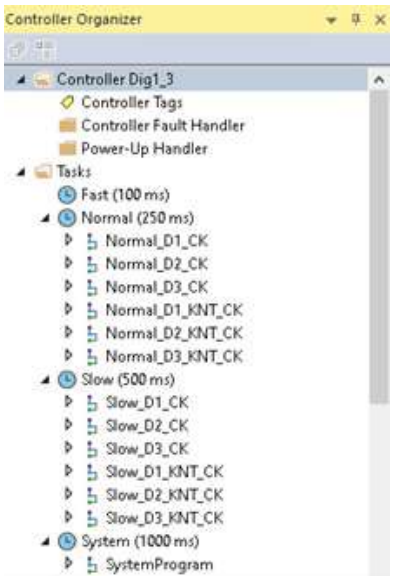
- Server-based alarms and Logix tag-based alarms are often based on area organization within the Logical Organizer and built using the PlantPAx configuration tool.

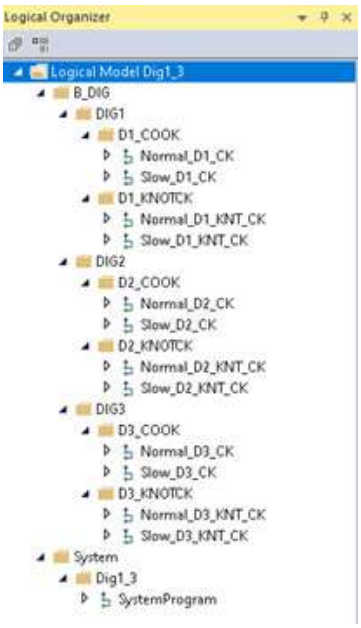
- Organize batch applications following the ISA-S88 physical model.

IMPORTANT Several components in a PlantPAx system depend on the organization and hierarchy of the system:

- HMI application
- Alarms
- User roles and responsibility
- Security

This example shows the same controller project that is viewed from the Controller Organizer and its associated Logical Organizer. The Controller Organizer is used to ensure that the logic is executed at a rate suitable for the process. The Logical Organizer can be used to create folders aligned with the application (a folder for each HMI display) and allows dragging the associated programs into the appropriate folders. This enables accurate alarm rollups and breadcrumbs on the Navigation bars to assist the operator in troubleshooting abnormal conditions. (See PROCES-RM200 Chapters 2 and 3 for more detail).





Add Modules and Devices to the Controller Organizer

All Logix 5000 controllers require module connections (analog, communication, digital, specialty) to be defined in the I/O Configuration list.

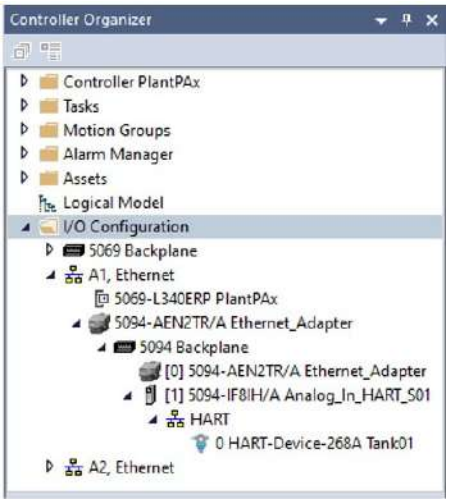
Follow these guidelines for I/O module properties in a PlantPAx system.

Table 6 - Guidelines for Module Configuration

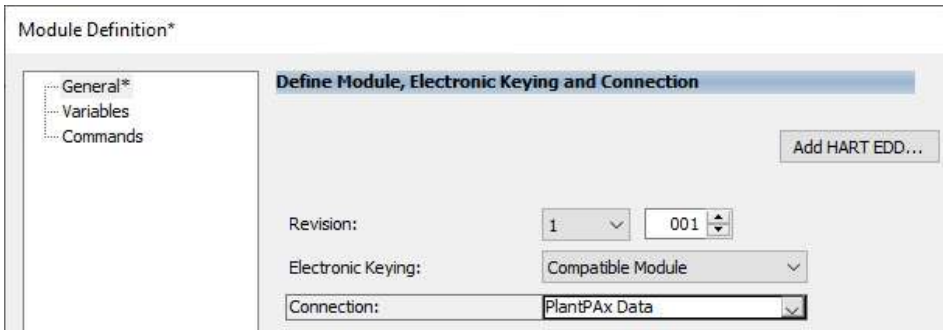
Item	Description
Electronic keying	Electronic Keying reduces the possibility that you use the wrong device in a control system. It compares the device that is defined in your project to the installed device. If keying fails, a fault occurs. • Use Exact Match for keying in a validated environment. This makes sure that only the same series and revision device can be used. • Use Compatible Module for keying in environments where a newer series or revision device can be used without requiring changes to the definition. For more detailed information on Electronic Keying, see Electronic Keying in Logix 5000 Control Systems Application Technique, publication LOGIXAT001.
Requested Packet Interval (RPI)	The RPI value is the rate at which the controller attempts to communicate with the module. RPI is often defined by the inherent properties of the signal being measured. For example, a temperature measurement changes slower than pressure, so a larger RPI could be used to a device that measures the temperature. We recommend that you specify an RPI that is two times faster than task period. For example: • A device that is used within a 250 ms task requires a 125 ms RPI. • A device that is used within a 100 ms task requires a 50 ms RPI. Use NONE for the Connection Format to remote communication modules used as bridged adapters. For modules that support Precision Time Protocol (PTP) synchronization, it's recommended to use Time Sync and Motion.
Connection tab options	• If inhibited, the controller does not attempt to make a connection. This is used as placeholder for a device that is not yet implemented or installed. • Major Fault On Controller If Connection Fails While in Run Mode. This is used on critical connections, where controller execution can't continue if a problem is detected.
Integrated HART device connection	FLEX 5000® and FLEXHA 5000™ I/O with 5094 HART modules support two device connections types. The PlantPAx data format is recommended and is pre-defined for the PAH instruction. • PlantPAx Data: Input data includes basic input from the HART device that is used by PlantPAx for the four dynamic variables and semi static data. Also includes the configured device variables and commands. • Data: Input data includes basic input from the HART device for the dynamic and device variables that are configured plus the configured commands.
Concurrent Communications with FLEXHA 5000 I/O	Concurrent communications require a dedicated 1756-EN4TR.

Integrated HART Configuration

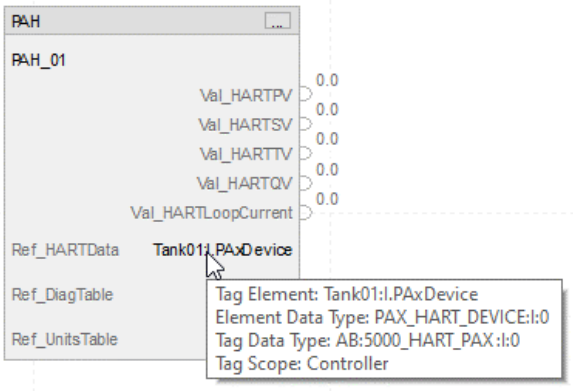
HART integration lets you directly add field devices to the I/O Configuration list.



Configure the variables and commands for the HART devices within the Module Definition. You can add HART EDD files if additional device descriptions are required. See the appropriate manufacturer for these files.

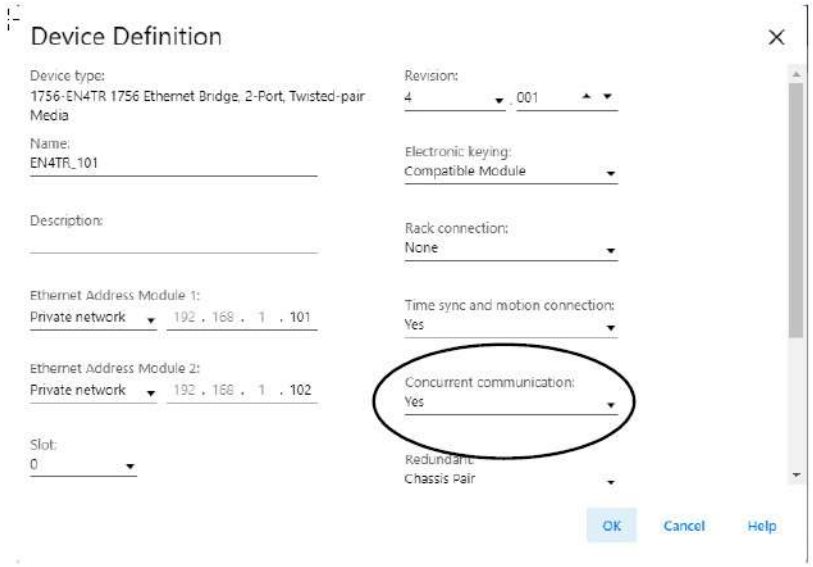


The PlantPAx Data connection creates a PAX_HART_DEVICE:I:0 structure that is formatted for direct use in the Process Analog HART (PAH) instruction.



Concurrent Communication Module Configuration

FLEXHA 5000 I/O requires concurrent communications. To use concurrent communication with FLEXHA 5000 I/O modules, you must configure the 1756-EN4TR EtherNet/IP™ communication module on the Device Definition dialog box in your Studio 5000 Logix Designer application project to use concurrent communication.



IMPORTANT You can configure the 1756-EN4TR EtherNet/IP communication module for concurrent communications, to use with I/O modules such as FLEXHA 5000 I/O modules. Or you can configure the 1756-EN4TR EtherNet/IP communication module for standard I/O, for example, remote 1756 ControlLogix I/O modules. You can only configure the module for one or the other.

If the 1756-EN4TR EtherNet/IP communication module is configured for concurrent communication, you can still use it for class 3 communications, for example, HMI, program upload/download/monitor.

Controller-to-Controller Communication

There are two main options to communicate among controllers:

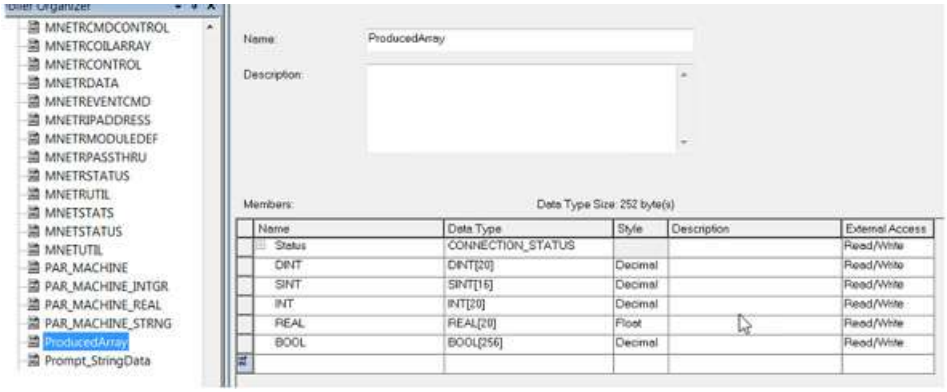
Produced and Consumed Tag	Message (MSG) Instruction
Consumed tag data is automatically received from a producer controller, at a requested packet interval (RPI), without the need for logic programming.	Read or Write messages are programmatically initiated on condition (False to True transition).
Ideal for exchanging critical data that changes frequently; use for higher priority communication.	Ideal for exchanging non-critical data that changes less frequently; use for lower priority communication.
Data is constantly sent regardless of change of state. This does not impact the scan of the controller, but it can impact network bandwidth.	Communication and network resources that are used when needed only, however, a delay can occur if controller resources aren't available when needed.
Tag size is limited to 500 bytes over the backplane and 480 bytes over a network.	Supports larger data payloads, up to 32,767 elements, using multiple data packets.
Supports tags of mixed data types (UDT).	CIP™ Generic messages to third-party devices.
You can't modify or create produced/consumed tags online in Run mode.	You can modify and create MSG instruction online in Run mode.
Routing of traffic across subnets depends upon the transmission type (Unicast or Multicast).	Message traffic can be routed across subnets and across slots of a 1756 chassis.

For more information on controller communication options, see Logix 5000 Controllers Design Considerations Manual, publication 1756-RM094.

Configure Produced and Consumed Tags

Group produced and consumed tags as members in user-defined structures. This technique helps monitor connection status between controllers without increasing execution time, such as using a GSV instruction to detect status.

1. In the Logix Designer application, define a user-defined structure of a tag to be used in all controllers.



2. Name the first member Status and a data type of CONNECTION_STATUS.

   This data type provides two BOOL bits (RunMode & ConnectionFaulted) in the Status member for each controller consuming the tag.

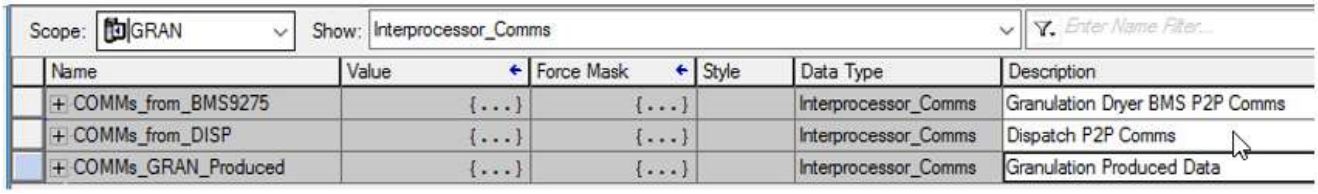
   MyTag.Connection_Status.RunMode

   - Value of 1 when Producer is in Run mode.
   - Value of 0 when Producer is in Program mode.

   MyTag.Connection_Status.ConnectionFaulted

   - Value of 0 when Producer connection is good, regardless of mode.
   - Value of 1 when Producer Connection is broken.

3. Once the UDT is finished, create a tag of that UDT type to be either Produced or Consumed.
4. It's recommended to add a common prefix to each tag instance of the UDT, so you more easily search for those tags.



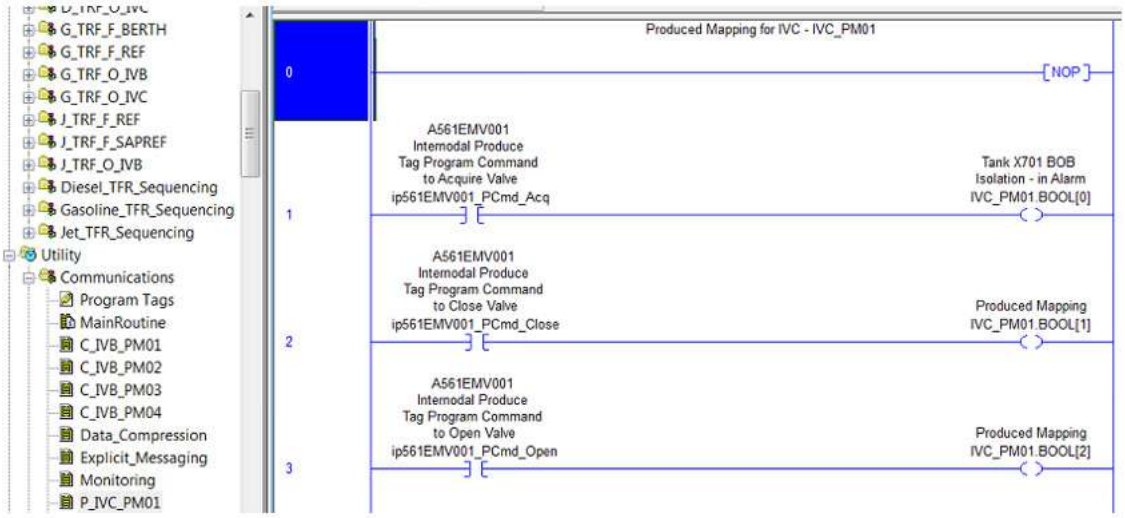
5. Create a Produced tag by simply changing the tag property from base to produced and setting the max number of consumers.
6. Create a Consumed tag by changing the tag property from base to consumed. The Producer controller is selected from the I/O configuration list and the remote data (exact name of produced tag) is entered.
7. Select the RPI rate in which the produce tag is consumed.

For bidirectional P/C tags between two controllers, both consuming controllers have each producer controller in its I/O configuration list. Multiple consumers can receive the same data from a single producer.

IMPORTANT When adding the Producer controller to the I/O configuration list of the Consumer controller, the firmware revision does not have to match. However, the rack size and slot number must be correct.

Data arrives asynchronous to program scan. Some applications may require a programmatic handshake. Buffering data to or from P/C tags helps to make sure that the user logic executes on that same data before it changes.

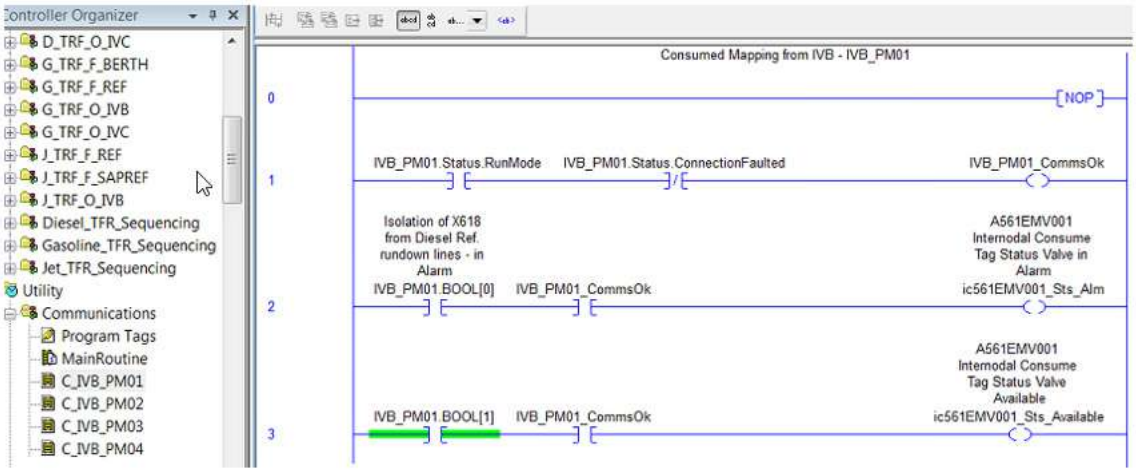
8. Create logic that writes values to the Produce tag elements.



9. Add corresponding consume tags to each controller that consumes the data.

   Note that UDT structures can be exported to. L5X format and imported into the other controllers.

10. Use Consume tag elements to write to variables in the Consuming controller.



PlantPAx Guidelines for Produced and Consumed Tags

- Produced and consumed (P/C) tags can be a single tag structure or a user-defined structure (UDT) of mixed data types. For example, a UDT tag can contain members up to 120 REALs or 100 REALs and 640 BOOLs.
- Group data in produced and consumed tags into a UDT to reduce the total number of connections.
- Make the first member of the UDT a data type of CONNECTION_STATUS for connection status.
- Export/Import the same P/C UDT data type among controllers to confirm they match exactly.
- Make sure the number of consumers configured, for a produced tag, is the actual number of controllers consuming it to reduce the number of connections to the controller.
- Always use a handshake when transferring data between controllers through health data or manually configured diagnostic.
- We recommend unicast traffic when possible, because it transmits only to an intended destination, which reduces bandwidth. However, redundant controllers require multicast traffic to consume data.

PlantPAx Guidelines for Message Instructions

The MSG instruction asynchronously reads or writes a block of data to another module on a network.

- ControlLogix 5580 and CompactLogix 5380 support up to 256 connections. If you want to enable more than 256 MSGs at one time, use some type of management strategy.
- Use the cached option when the message connection needs to be maintained.
- Use message Reads, instead of Writes. This makes it easier to troubleshoot code by knowing where the incoming data is coming from.
- When messaging between Logix 5000 controllers, use a DINT data type where possible for maximum efficiency.
- Use MSG status flags, such as the. DN and .ER bits for handling fault conditions.
- Data arrives asynchronous to program scan (use a programmatic handshake or insert between a UID/UIE instruction pair for higher priority)
- Use the unconnected option for CIP Generic messages

Integrate Field Devices

PlantPAx systems use specialized field devices that operate on various communication protocols, such as HART, EtherNet/IP™, PROFIBUS PA, and Foundation Fieldbus.

Depending on the controller type and process library version, you need different elements to integrate a field device. These elements use the Logix Designer application for device control to the corresponding object in FactoryTalk® View SE for HMI faceplates.

Most field device integrations require that you instantiate one Add-On module Profile (AOP) and two Add-On Instructions (AOI) per device for end-to-end control and monitoring.

- Module or Device-specific AOP for the Logix Designer application to create the item or device tags in the I/O Configuration list.

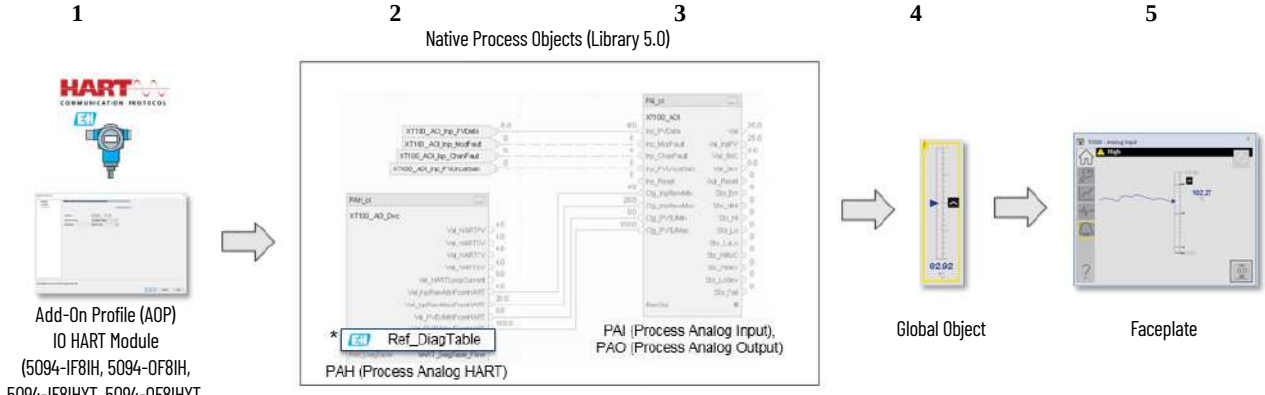
- Device-specific Add-On Instruction to access device tags and prepare the data for use within the controller project.
- Generic Add-On Instruction to access device data, along with custom-made device diagnostics and unit tables, to enable visibility on an HMI faceplate within the PlantPAx system.

HART Integration

Highly integrated HART provides a PlantPAx data type in the process controller:

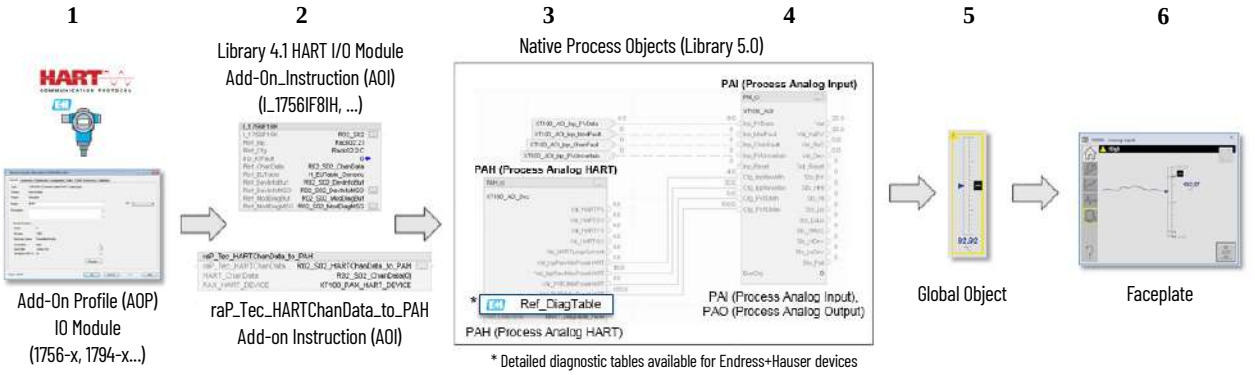
- Configuration of devices within the I/O Configuration tree (no Add-On Instruction needed)
- Device diagnostics automatically propagate to the controller project

Figure 14 - PlantPAx 5.0 Library and Highly Integrated HART I/O Modules



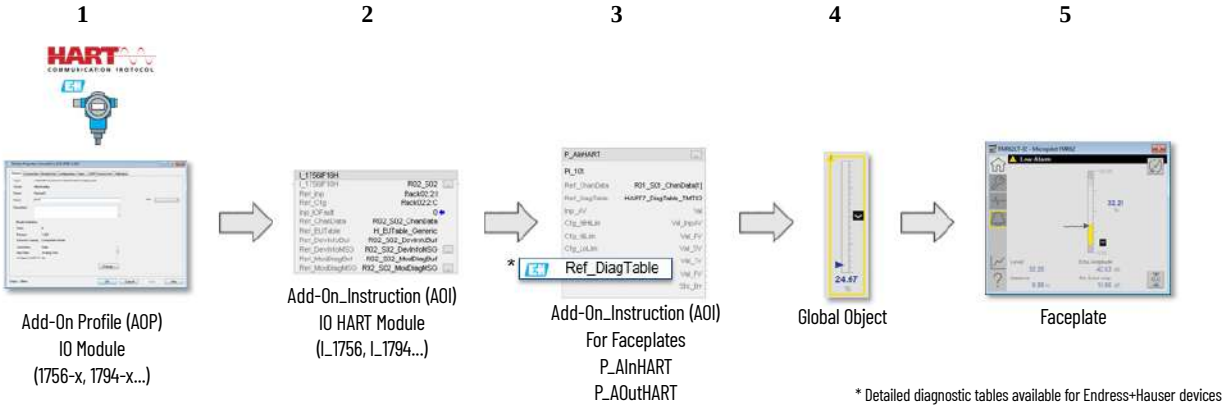
Element	Description
1	The HART I/O module is added to the I/O Configuration. If necessary, import the Add-On Profile for the module being used. Then the HART device is added to the I/O Configuration on the "HART" network under the module.
2	Use the PAH instruction to process HART data, from the module input assembly.
3	Use the PAI instruction to process the analog input, from the module input assembly.
4	Use the HMI global object for the analog input on HMI displays.
5	Clicking the global object calls up the PAI faceplate, which has navigation to the PAH faceplate for HART data.

Figure 15 - PlantPAx 5.0 Library and 1756, 1794, 1718, 1719, 1734, 1769 or 1715 HART I/O Modules



Element	Description
1	The HART I/O module is added to the I/O Configuration. If necessary, import the Add-On Profile for the module being used.
2	Use a PlantPAx Library 4.1 HART module Add-On Instruction to retrieve HART data from the module. Then use the raP_Tec_HARTChanData_to_PAH Add-On Instruction from PlantPAx Library 5.0 to take the HART data from the HARTChanData (Library 4.1) structure into the new structure used by the Library 5.0 PAH instruction.
3	Use the PAH instruction to process HART data associated with the analog input
4	Use the PAI instruction to process the analog input.
5	Use the HMI global object for the analog input on HMI displays.
6	Clicking the global object calls up the PAI faceplate, which has navigation to the PAH faceplate for HART data.

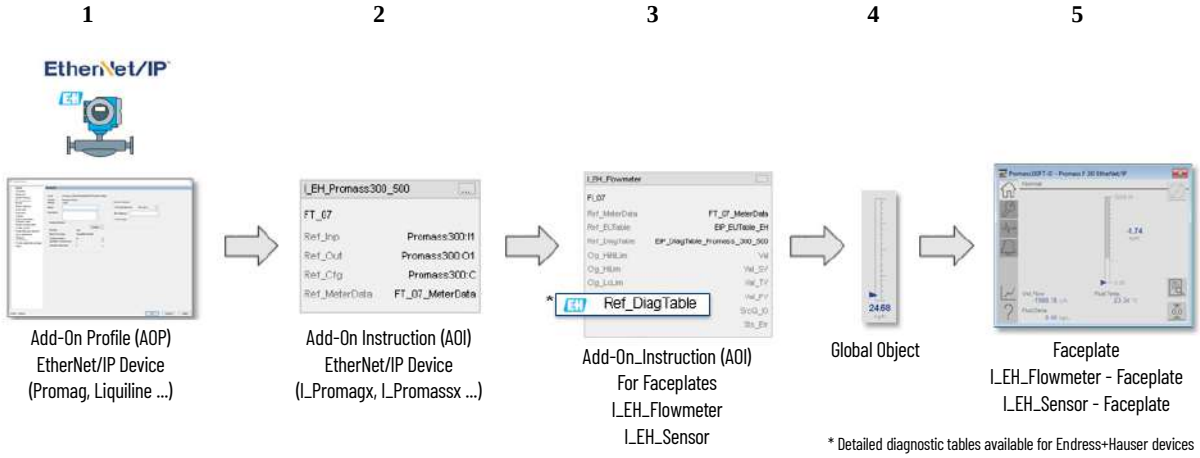
Figure 16 - PlantPAx Library 4.1 and 1756, 1794, 1718, 1719, 1734, 1769 or 1715 HART I/O Module



Element	Description
1	The HART I/O module is added to the I/O Configuration. If necessary, import the Add-On Profile for the module being used.
2	Use a PlantPAx Library 4.1 HART module Add-On Instruction to retrieve HART data from all the channels on the module.
3	Use the PlantPAx Library 4.1 P_AInHART Add-On Instruction to process the analog input and HART data for one channel.
4	Use the HMI global object for the analog input on HMI displays.
5	Clicking the global object calls up the P_AInHART faceplate, which displays the analog and HART data.

Ethernet/IP Integration via Custom Add-On Profile

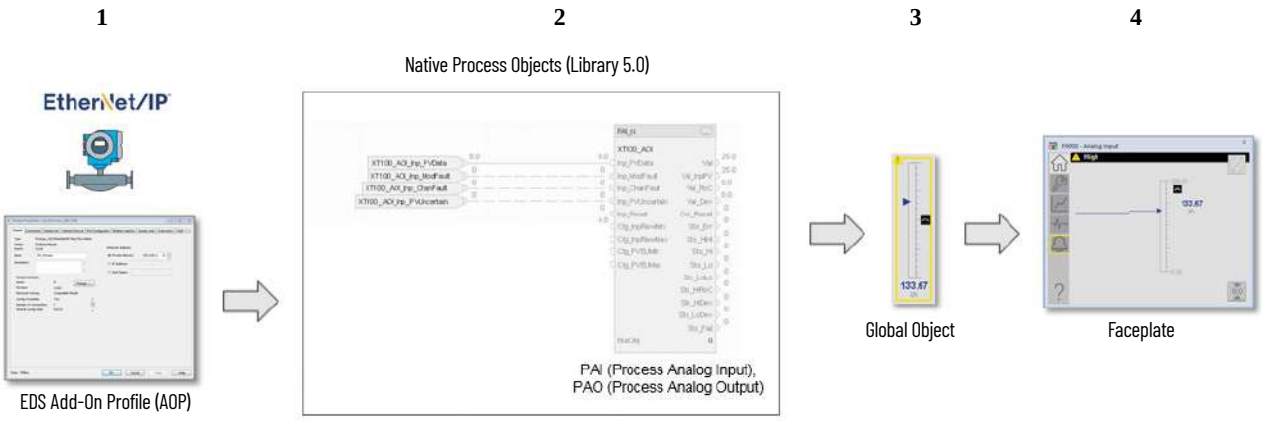
Figure 17 - PlantPAx Library 4.1 or 5.0 and EtherNet/IP device with Custom AOP (For Example, Endress+Hauser)



Element	Description
1	Endress+Hauser EtherNet/IP device is added to the I/O Configuration tree Add-on Profile for device creation and configuration, such as ProMag or Liquiline
2	Add-on Instruction accesses device tags, such as I_Promagx or I_Promassx for use with application logic / control strategies
3	Add-on Instruction for diagnostics and control to the HMI global object
4	Process library HMI global object supports faceplates
5	Process library I_EH_FlowMeter and I_EH_Sensor faceplates

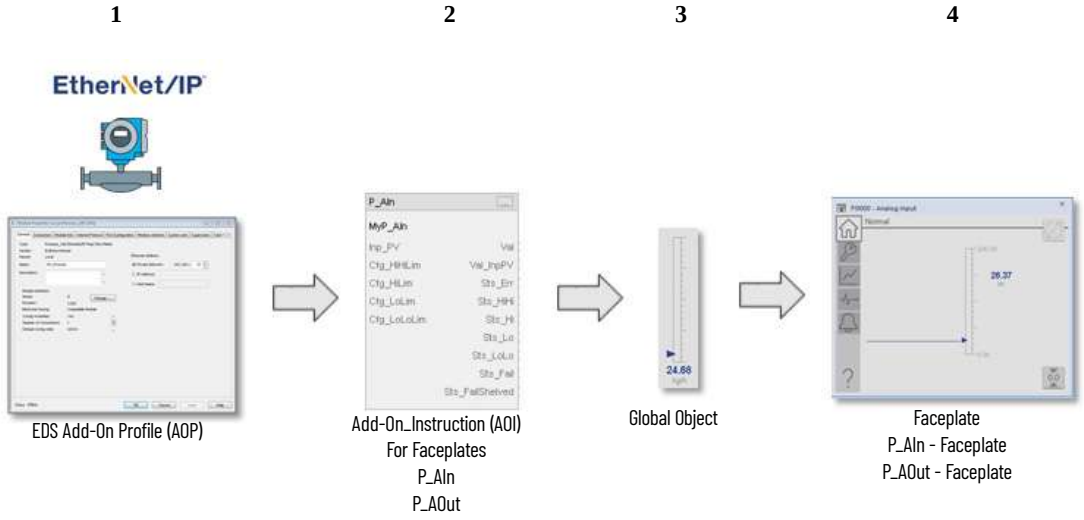
Ethernet/IP Integration via Electronic Data Sheet Add-On Profile

Figure 18 - PlantPAx Library 5.0 and EtherNet/IP device with EDS AOP



Element	Description
1	EtherNet/IP device is added to the I/O Configuration tree Add-on Profile, created via Electronic Data Sheet (EDS) file, for device creation and configuration
2	PlantPAx instructions for application logic/control strategies/alarms
3	Process library HMI global object supports faceplates
4	Process library PAI faceplate

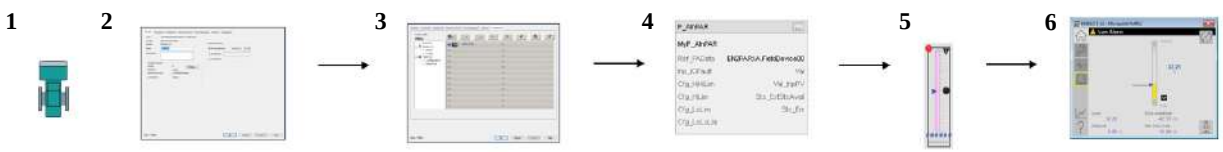
Figure 19 - PlantPAx Library Release 4.1 and EtherNet/IP device with EDS AOP



Element	Description
1	EtherNet/IP device is added to the I/O Configuration tree Add-on Profile, created via Electronic Data Sheet (EDS) file, for device creation and configuration
2	Add-on Profile for HMI faceplates, such as P_AIn and P_AOut
3	Process library HMI global object supports faceplates
4	Process library P_AIn and P_AOut faceplates

PROFIBUS PA Integration (1788-EN2PAR Linking Device)

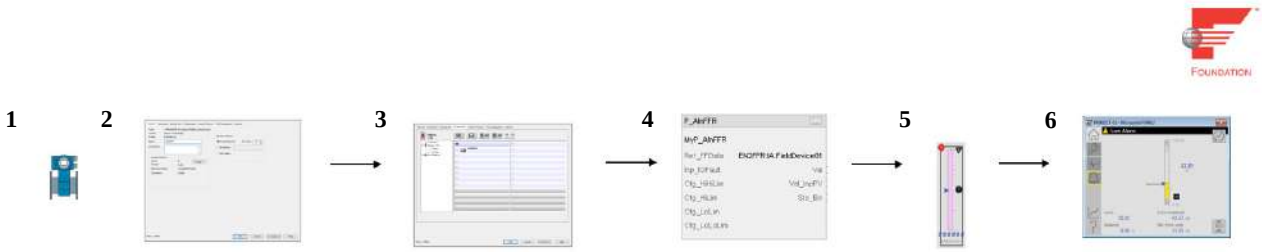
Figure 20 - PlantPAx Library 4.1 or 5.0 and 1788-EN2PAR Linking Device



Element	Description
1	Device is not added to the I/O Configuration tree
2	Add-on Profile for 1788 linking device
3	PROFIBUS PA network configuration
4	Add-on Instruction for HMI Faceplates, such as P_AInPAR
5	Process library HMI global object supports faceplates
6	Process library P_AInPAR faceplate

Foundation Fieldbus Integration (1788-ENFFR Linking Device)

Figure 21 - PlantPAx Library 4.1 or 5.0 and 1788-ENFR Linking Device



Element	Description
1	Device is not added to the I/O Configuration tree
2	Add-on Profile for 1788 linking device
3	Foundation Fieldbus network configuration
4	Add-on Instruction for HMI Faceplates, such as P_AInFFR
5	Process library HMI global object supports faceplates
6	Process library P_AInFFR faceplate

Electrical Protection Devices Integration (IEC 61850)

See Rockwell Automation Library of Electrical Protection Devices, publication PROCES-RM011 for more information about integrating electrical protection devices (IEC 61850).

Alarm Types

Alarms are a critical function of a distributed control system. Alarms monitor conditions that need response, such as a temperature or pressure signal out of range, or device failures such as drives and motors.

The FactoryTalk® Alarms and Events server provides a common, consistent view of alarms and events throughout a PlantPAx system. Language-switching alarm messages are also available. When an alarm condition is received, the FTAE server publishes the information to a subscribing Operator workstation via FactoryTalk Alarm and Event services.

- For information on how to configure the FTAE server on a PASS, see Chapter 3, Process Automation System Server.

- For information on how to configure and monitor FTAE alarm components, see the FactoryTalk Alarms and Events System Configuration Guide, publication FTAE-RM001.

The Alarm Banner resides on the Header display.

An effective alarm system directs the attention of an operator to improve the productivity, safety, and environment of a process plant.

- A PlantPAx system can use device-level and server-level alarm methods.
- Recommendations are based on the controller type and supported functionality.

Table 7 - Alarm Types Based on Instructions and Add-On Instructions

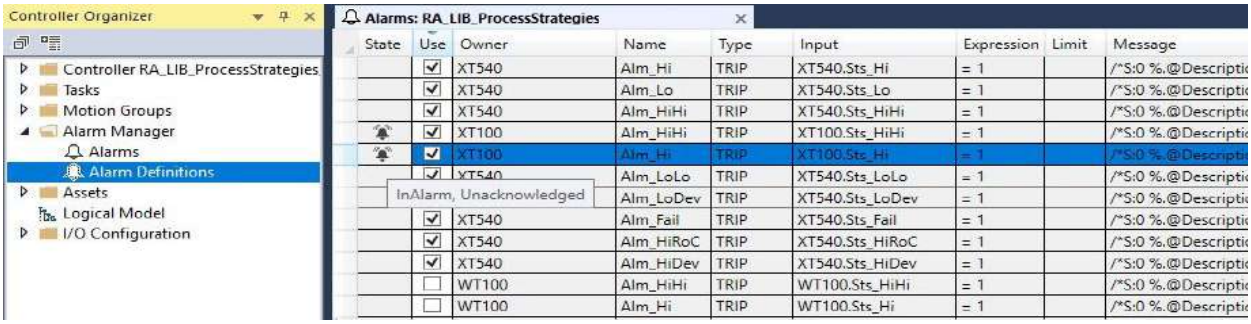
If You Have	You Have This Alarm Type	Description
PlantPAx 5.0 library	Logix Tag-based	Device level, tag-based alarms monitor a tag value to determine the alarm condition. Tag-based alarms aren't part of the logic program and do not increase the scan time for a project. The controller caches information, such as time stamps, alarm states, and associated tag values in a 1000 KB buffer. The controller transmits the information to subscribing FactoryTalk® Alarms and Event servers. **Recommended:** PlantPAx system release 5.0 or later. Requires: ControlLogix 5580 controller, CompactLogix 5380 controller.
PlantPAx 4.1 library or earlier	Server Tag-based	A FactoryTalk Alarm and Event server monitors controllers for alarm conditions through data servers and publishes event information that can be displayed and logged. **Recommended:** PlantPAx system release 4.6 and earlier. Server-based alarm monitoring offers the equivalent of HMI tag alarm monitoring, but with an expanded feature set of the FactoryTalk Alarm and Event server.
ALMA or ALMD controller instructions	Logix Instruction-based	These device-level alarm instructions can consume a larger portion of controller memory and increase scan time when executed. When an alarm is detected, it's time stamped and buffered until it's transmitted to subscribing FactoryTalk Alarms and Events servers. **Not Recommended** in large deployments due to added controller overhead. Requires: ControlLogix 5570, CompactLogix 5370, ControlLogix 5580, CompactLogix 5380 controller. Device level, Logix instruction-based alarms are programmed within the controller program and integrated to the FactoryTalk Alarm and Event server. • The Digital Alarm (ALMD) instruction detects alarms that are based on Boolean (true/false) conditions. • The Analog Alarm (ALMA) instruction detects alarms that are based on the level or rate of change of analog values.

Guidelines for Logix Tag-based Alarms

In a PlantPAx 5.0 or later system, we recommend no more than 7500 in-use Logix tag-based alarms per controller.

Create Logix tag-based alarms to send alerts about specific events or conditions. A tag-based alarm is similar to a digital alarm because both monitor a tag value to determine an alarm condition. However, a tag-based

alarm isn't part of the logic program and does not increase the scan time for a project.



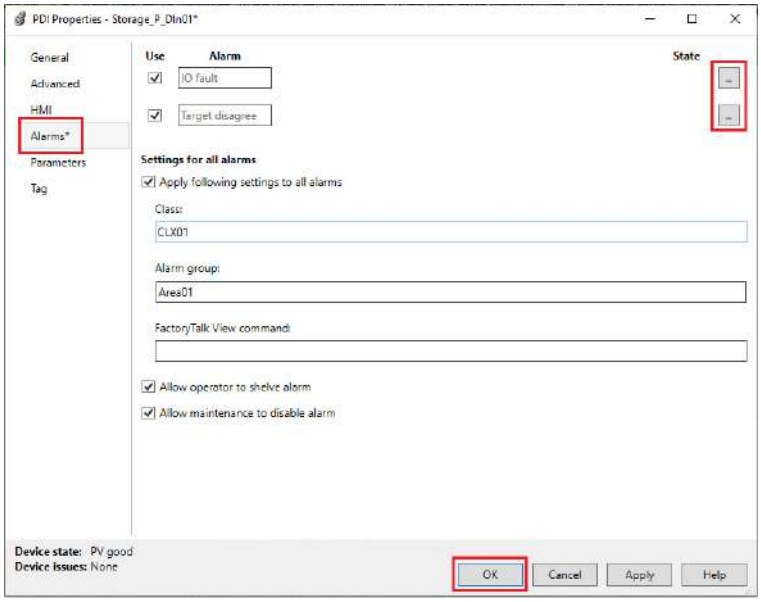
Tag-based alarms do not require an FTAE server. A controller's subscription to the HMI can be serviced using a FactoryTalk® Linx data server. See Add a Data Server (FactoryTalk Linx) on page 67 to confirm that FactoryTalk® Linx is configured for Logix Tag-based alarms. PlantPAx recommends a limit of 15,000 Logix Tag-based alarms per instance of FactoryTalk Linx. A PASS can host up to two instances of FactoryTalk Linx for a total of 30,000 Logix Tag-based alarms per PASS.

An alarm definition is associated with an Add-On Instruction (AOI) or a defined data type. When a tag is created using a data type or an AOI that has alarm definitions, alarms are created automatically based on the alarm definitions.

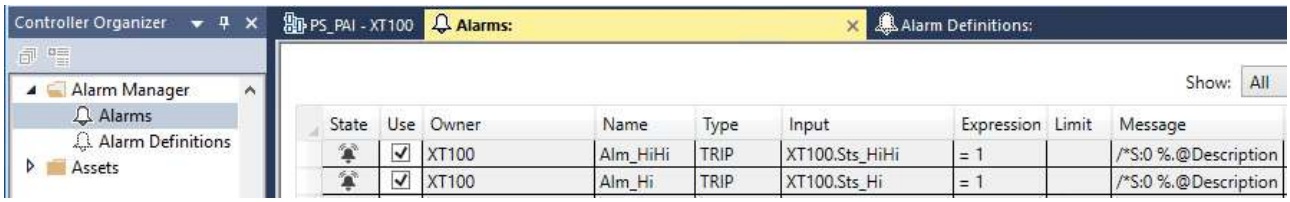
Embedded Tag-based Alarms in PlantPAx Instructions

The PlantPAx instructions have embedded tag-based alarms. Configure the states as needed and simply enable the alarms that you want to use.

Use the Alarms tab on the instruction properties to assign settings to all pre-defined alarms. There's an option to propagate specified Class/Group settings to all alarms in the instruction.



Alarm settings are also accessible via the Alarm Manager.



Guidelines for Server Tag-based Alarms (FactoryTalk Alarms and Events)

An FTAE server is required for server tag-based alarms. The server puts these alarm tags on scan, just as it does all other tags it polls for the HMI and Historian. In a PlantPAx 5.0 or later system, we recommend you limit the number of server tag-based alarms to 20,000 per FTAE Server. A PASS can host a single instance of the FTAE server for Server tag-based alarms. There are no hard-coded limitations, however you could experience longer recovery time during system restoration if you exceed the recommendation.

Use the PlantPAx System Estimator (PSE) for sizing the number of alarm instructions for a more accurate limit that is based on your specific configuration. Be sure to add additional memory that is required to maintain the alarm subscription as it isn't accounted for in the PSE memory calculations.

- Use alarm groups to organize alarms by operator role.
- Use alarm expressions against user groups to provide rolled up indication of alarms by role or display. For example, AE_InAlmUnackCount('T1*') returns a count of unacknowledged alarms within groups that start with T1.

  For more information on alarm expressions, see the FactoryTalk View Site Edition User's Guide, publication VIEWSE-UM006.
- Use an alarm class to identify alarms that share common management requirements (for example, testing, training, monitoring, and audit requirements). Do not use alarm class to identify alarms by operator role or display because you can't retrieve an alarm count by class by using alarm expressions in FactoryTalk® View software. However, you can filter by class on the alarm displays.
- Use the alarm builder feature in the PlantPAx Configuration Tool to help build server tag-based alarms.

Guidelines for Logix Instruction-based Alarms

The process library does not provide support for Logix instruction-based alarms. Note that the instruction-based alarms can impact controller performance.

Controller scan time and memory usage are variable with the use of the ALMA or ALMD instructions, depending on the states of the controller. Large alarm bursts can have a significant impact on controller CPU utilization. For example: Controller memory used for buffering by each subscriber (topic in the data server) = 100 KB.

Example execution times:

- ALMD in a 1756-L73 controller with no alarm state changes: 7 µs
- ALMD in a 1756-L73 controller with alarm state changes: 16 µs

In redundant controller configurations, cross loading of redundancy can add up to 70 µs per ALMD instruction.

Reserve the use of ALMA and ALMD instructions for the most critical alarms. Although there are no hard-coded limitations, we recommend limiting the number of instructions to the following:

- 250 per redundant controller
- 2000 per simplex controller

Monitor Alarms

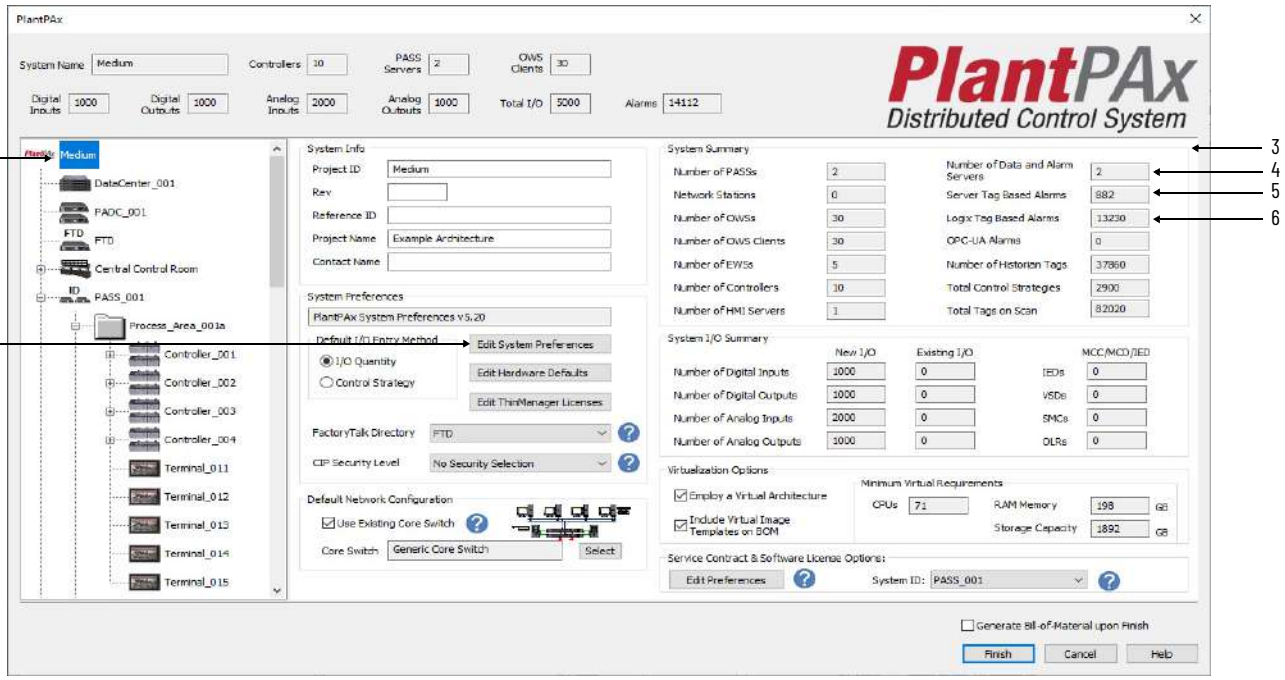
You can use the alarm status explorer in FactoryTalk View SE to browse all of your configured alarms on a server or the entire system. Alarms also are filtered by the Shelved, Suppressed, and Disabled options. The alarm explorer can be preconfigured as a Shelved alarm display to let operators view a list of shelved alarms.

ANSI/ISA-18.2 provides alarm performance metrics and recommended target values. Some key metrics include the following:

- Alarm rates: annunciated alarms per operator console:
  - Average of 6...12 per hour
  - Average 1...2 per 10 minutes
- Contribution of the top 10 most frequent alarms to the overall alarm load: ~<1...5% maximum, with action plans to address deficiencies
- Less than 5 stale alarms (remains annunciated for an extended period, such as 24 hours) present on any day with action plans to address

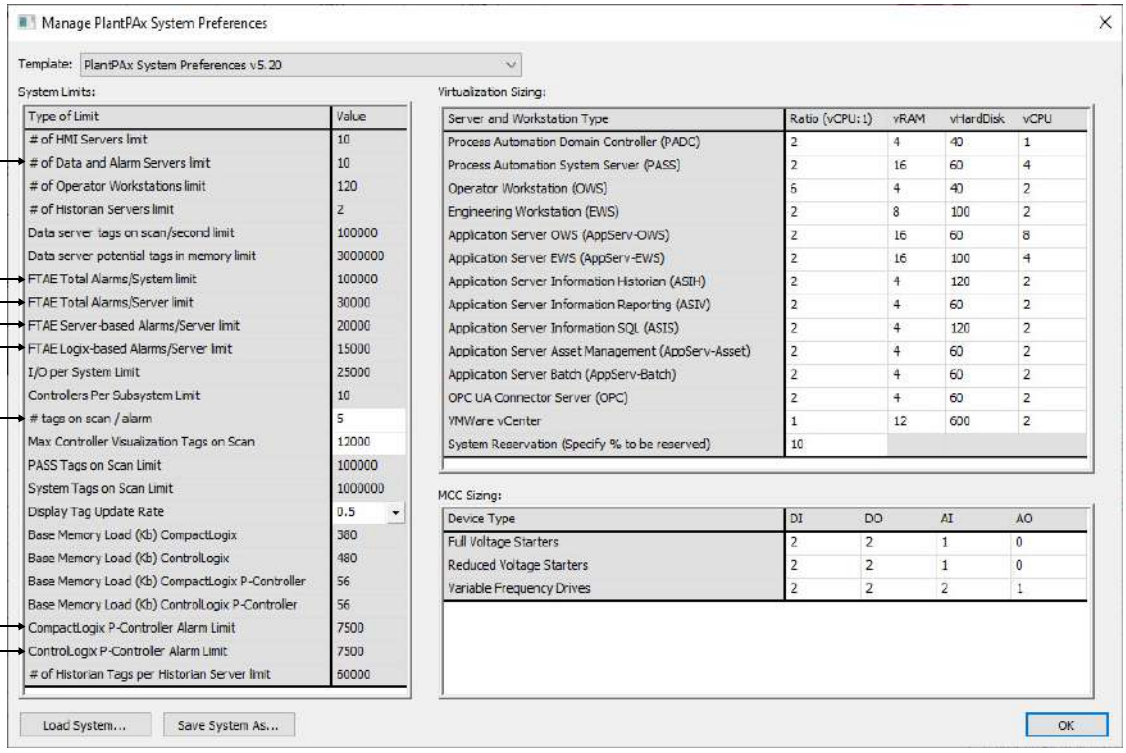
Use the Process System Estimator to Plan Alarms

Process System Estimator - Summary



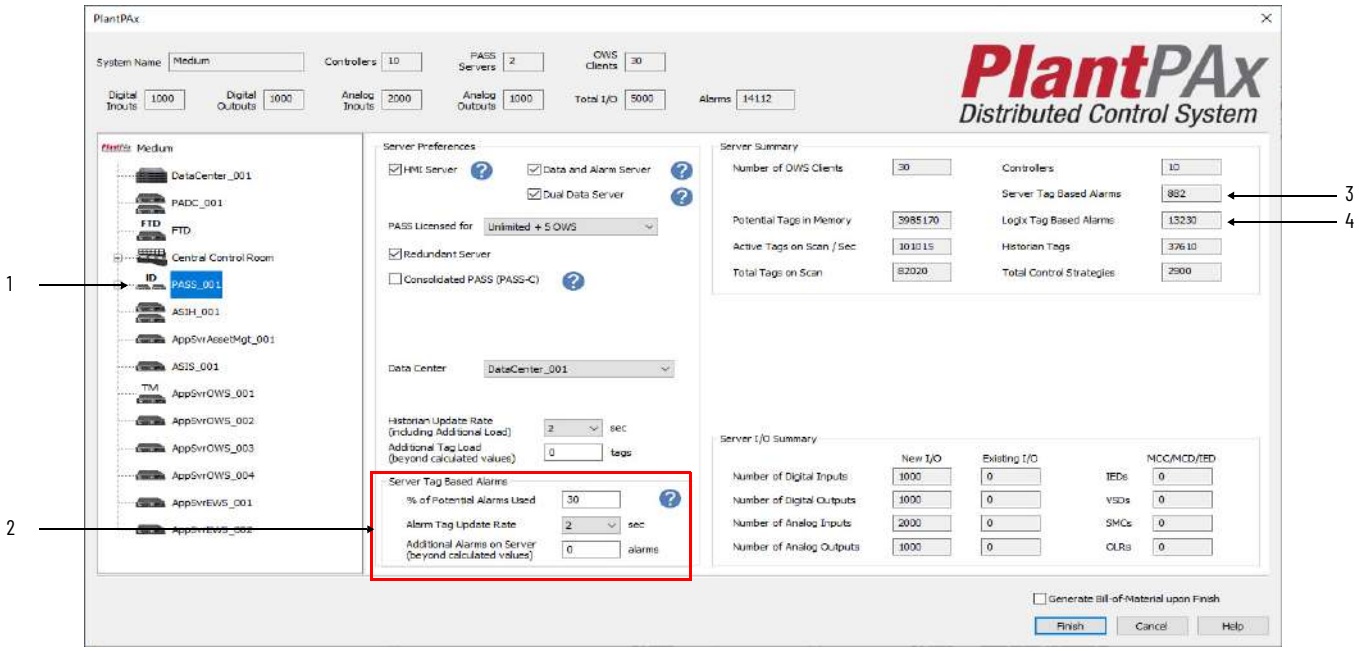
Item	Description
1	Select the top of the project tree to view the system summary.
2	Select to view some of the system limits.
3	System Summary
4	Total number of Server Tag-Based FactoryTalk Alarm and Event servers. **Note**: These servers support controllers that utilize the PlantPAx Process Object Library 4.1 and earlier.
5	The total number of Server Tag-Based Alarms.
6	The total number of Logix Tag-Based Alarms.

Process System Estimator - FactoryTalk Alarms and Events Limits



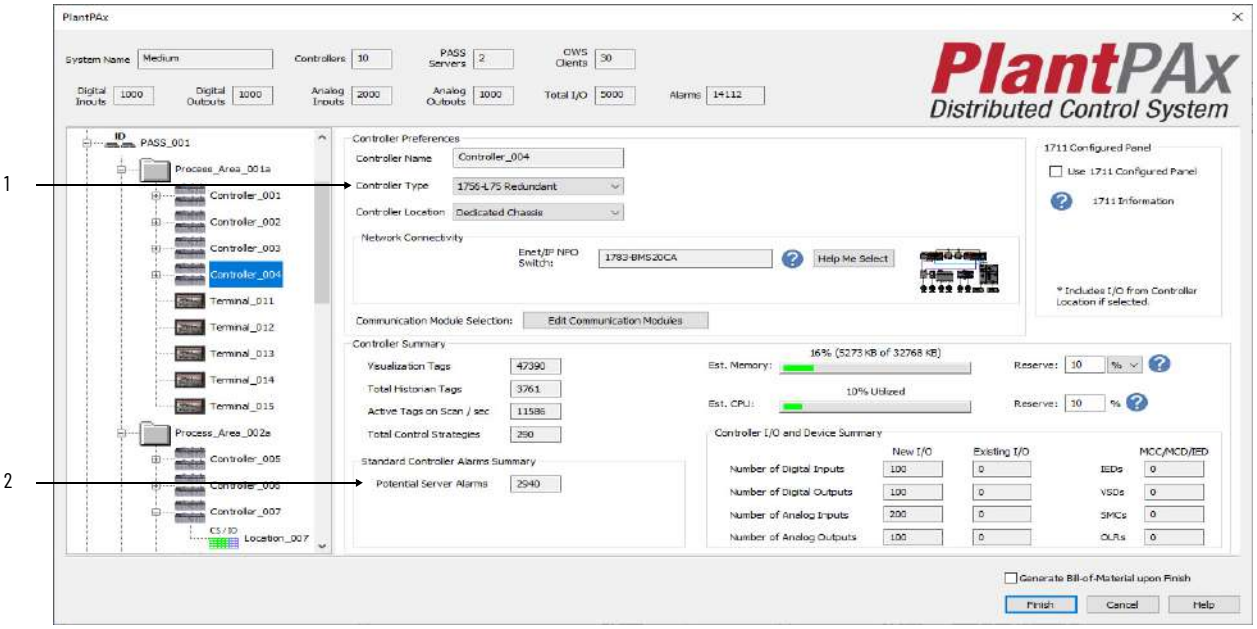
Item	Description
1	The maximum number of Data and Alarm Servers (Server Tag-Based) in the project.
2	Total number of FTAE Alarms allowed in the system. **Note**: The total **Server** Tag-Based Alarms plus the total **Logix** Tag-Based Alarms must be less than this value.
3	Total number of FTAE Alarms allowed in per PASS server. **Note**: The total **Server** Tag-Based Alarms plus the total **Logix** Tag-Based Alarms supported by any individual PASS must be less than this value.
4	The maximum **Server** Tag-Based Alarms that an individual PASS can support.
5	The maximum **Logix** Tag-Based Alarms that an instance of FactoryTalk Linx data server can support. A single PASS can host up to two data servers.
6	The average number of backing taqgs that are configured for **Server** Tag-Based Alarms. This field only applies to **Server** Tag-Based Alarms.
7	Maximum number of Logix Tag-Based Alarms. (CompactLogix)
8	Maximum number of Logix Tag-Based Alarms. (ControlLogix)

Process System Estimator - PASS Alarms



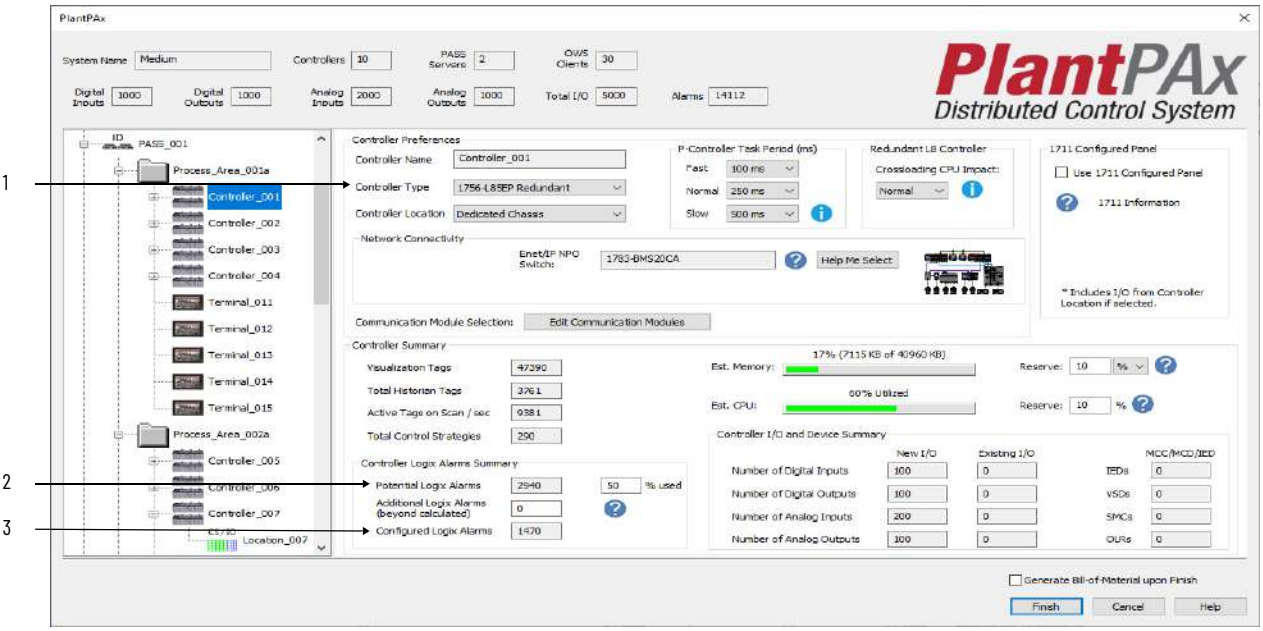
Item	Description
1	Select to view the alarm information for the PASS.
2	PASS-specific configuration information for the **Server** Tag-Based Alarm server. This is the configurable percent of **Server** Tag-Based Alarms that will be used for each controller under this PASS. **Note**: You can also add additional alarms in the server that are beyond what is calculated. The default is zero. When using the latest library and Process Controllers, the section in the red box does not appear as it does not apply.
3	Total number of **Server** Tag-Based Alarms for this PASS.
4	Total number of **Logix** Tag-Based Alarms for this PASS.

Process System Estimator - Non-Process Controller



Item	Description
1	This non-Process controller uses PlantPAx Process Object Library 4.1. **Note**: Since this controller is using Process Object Library 4.1, it uses Server Tag-Based alarms.
2	Potential Server Tag-Based Alarms. We know that 30 percent of these alarms are used (See Process System Estimator - PASS Alarms on page 142.) therefore, the actual load on the server for this specific controller will be: 2940 alarms x 30% = 882 alarms.

Process System Estimator - Process Controller



Item	Description
1	This Process controller uses PlantPAx Process Object Library 5.0 and later.
2	The calculated Potential Logix Alarms in the controller based on the configured I/O or control strategy counts.
3	Configured Logix alarms once multiplied by the user indicated percentage. In this example, 50%.

Security Considerations

PlantPAx provides options you can use to make your controller more secure. For controller security options, see:

- ControlLogix 5580 and GuardLogix 5580 Controllers, publication 1756-UM543
- CompactLogix 5380 and Compact GuardLogix 5380 Controllers, publication 5069-UM001

For runtime security, See Configure Runtime Security on page 73

For general system security (domain controller, FT Security), See Domain or Workgroup on page 23

A PlantPAx reference architecture has been certified for the IEC-62443-3-3 SL1 requirements. When certification is necessary, designing and implementing a similar architecture can improve the certification process timing.
See PlantPAx Security Certification on page 273.

Create HMI Displays

The Process Automation System Server (PASS) is a required system element for the PlantPAx system. The PASS hosts the HMI server, which stores the HMI project components, such as graphic displays, and provides these components to an Operator Workstations (OWS) client upon request.

For more information on how to configure these servers, see Chapter 3, Process Automation System Server.

Follow these guidelines:

- Use FactoryTalk® View Studio software on the EWS to access the application.
- Configure the FactoryTalk View SE servers to start automatically on startup on the PASS. Let the servers fully start up before starting the client computers.
- FactoryTalk View SE displays contain expressions for each customized animation that holds simple or complex calculations to accomplish the animations. Each expression consumes memory and requires processing time to execute. Too many expressions can make the screen animate sluggishly and affect system performance.
- Use global objects to display the status of a control module or device when the information to be displayed is stored in a tag structure within Logix (for example, UDT or Add-On Instruction) and there are many identical instances. A global object is a display element that is created once and can be referenced multiple times on multiple displays in an application. When changes are made to the original (base) object, the instantiated copies (reference objects) are automatically updated.
  - Base global objects are stored in FactoryTalk View in displays (.ggfx files). If you have a large number of base global objects defined, do not put them all in a single display. Limit the number of global object instances on a single display to 60 or less.
  - As global objects can be instantiated multiple times, the performance impact of their design is amplified by their number of instances. Therefore, design global objects carefully to reduce the number of objects, expressions, and animations that are used within the base object.
- Use ‘Replace’ display types. This display type closes the currently displayed screen when a new screen opens. ‘Overlay’ display types must be managed because multiple screens open at once consumes memory and CPU resources.

- Only use Cache After Displaying and Always Updating for displays frequently accessed by the operator and not applied generally. Used sparingly on these displays, these settings improve display call-up time for important displays. When displays are cached and always updating, the additional memory load of this display on the view client is persistent after call-up regardless of whether the display remains visible. This action affects system load and can affect system performance.
- We do not recommend the use of data logs. If necessary, use data logs for short-term data retention only.
- Do not create derived tags that depend on the results of other derived tags. Derived tag processing is not sequential.
- Avoid use of VBA when possible. VBA runs as a single-threaded process so it's possible the application that is written in VB does not allow the HMI to perform predictably.

Use FactoryTalk View Studio software to create or import any system-specific graphic displays that your PlantPAx system requires.

For PlantPAx common graphics, you can use ACM-generated displays or graphic framework displays (from the process library).

Graphic Framework Displays

The process library download contains the following files to use as a starting point to utilize the PlantPAx Graphic Framework:

- FTVSE_12_0_Template_{version}.APB
- FTVSE_13_0_Template_{version}.APB

  Restore the provided Local Station project templates (.APA) by using the FactoryTalk View SE Application Manager.

- FTVSE_12_0_Template_{version}.zip
- FTVSE_13_0_Template_{version}.zip

  Create your own project and import the HMI server or individual files as needed.

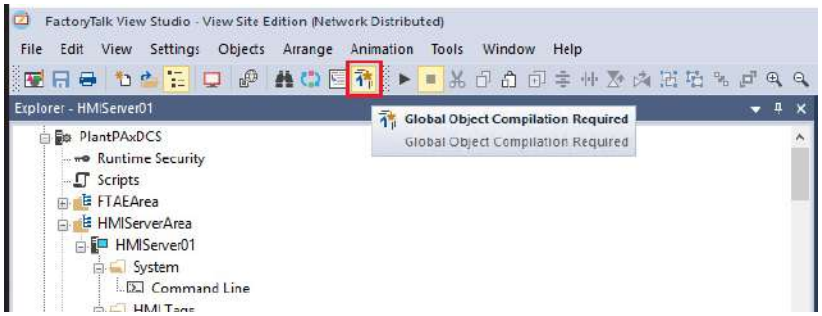
For more information on how to develop displays, see the Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200.

Optimize Runtime Performance

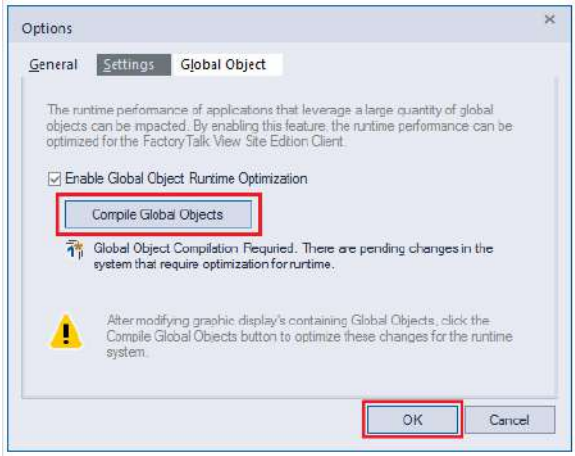
PlantPAx guidelines recommend using global objects to display the status of a control module or device when there are multiple, identical instances. Global objects offer consistency; and changes to a global object propagate to all the affected displays.

FactoryTalk View Studio has an Enable Global Object Runtime Optimization feature that improves runtime performance.

1. After you modify graphics that contain global objects, select Global Object Compilation Required



2. Select Compile Global Objects to optimize the changes for the runtime system.



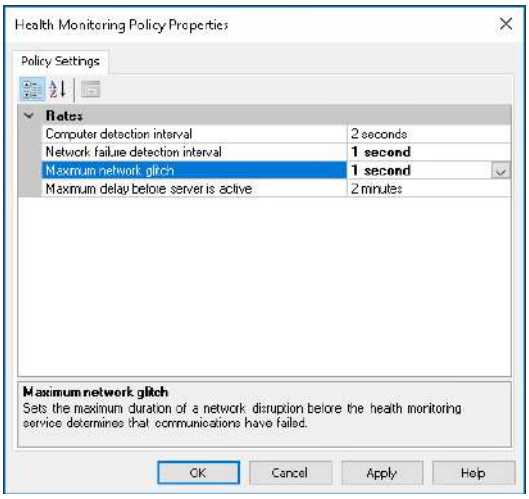
The first time that you compile global objects, the process can take an extended amount of time, depending on the number of displays in the application. Subsequent compiles require less time as they only process changes to displays.

Optimize HMI Redundancy

For HMI redundancy, change these settings to optimize the failover speed to achieve proper visibility on the HMI clients.

1. In FactoryTalk View Studio, go to System > Policies > System Policies and select Health Monitoring Policy.

2. Change the following settings:
   - Network failure detection interval: From 2 seconds to 1
   - Maximum network glitch: From 5 seconds to 1 second



Bulk Configuration of a PlantPAx System

ACM can reduce the development time for PlantPAx® applications. The process library provides components to help create process controller projects, HMI content for FactoryTalk® View SE displays, and tags for FactoryTalk® Historian SE applications.

For more information, see Application Code Manager User Manual, publication LOGIX-UM003.

New	Application Code Manager software	Application Code Manager (ACM) software is an optional, productivity tool you can use to manage multiple libraries and build these components for your control strategies. • HMI components • Alarms • I/O assignments ACM is best suited for new process applications or when wanting to generate or reuse modular project components from standard and custom libraries. ACM can use the process library to generate: • Controller project .ACD files • Controller program and routine .L5X files • HMI display and alarm .XML files • Historian point type and tag .CSV files

Step 1: Develop a Project Plan

Based on the system requirements and PSE results, plan the scope of the process application. Use a spreadsheet or other tracking tool to define the details for each controller in the project.

Determine when and which tools to use to help with project development

- Application Code Manager software
- Studio 5000® Design software
- PlantPAx Configuration Tool for Tags, Alarms, and Historian

For more information, see Develop a Project Plan.

Step 2: Use Application Code Manager

- Create a project
- Add control strategies
- Map I/O

Step 3: Add Alarm Groups

- Add an FTAlarmEvent object from the library.
- Add groups for your areas and assign the Parent Alarm Group ID
- Enable the alarms that you need

Step 4: Add HMI Displays

- Add an FTViewSE object from the process library.
- Generate HMI Displays

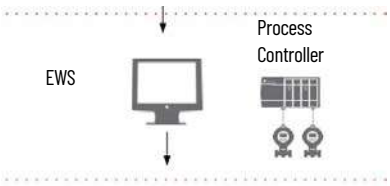
Step 5: Develop Historian Tags

- Add a Historian object to your ACM project.
- Generate Historian Tags

Step 6: Import Displays

- Import ACM-generated displays into your HMI application

Prerequisites



Following the System Workflow, develop your process application, including graphical displays and controller logic. To develop your controller program, you must be familiar with how to do the following:

1. Gather system requirements, such as:
   - User requirement specifications
   - Instrument index or database
   - P&ID diagrams
   - Network architecture requirements
   - I/O requirements
   - Produced/consume and message requirements
   - Product specifications
2. Use the PlantPAx System Estimator tool that comes with Integrated Architecture® Builder utility, to:
   - Size your PlantPAx system
   - Generate a bill of materials
3. Build your PlantPAx system:
   - Use the Virtual Image Templates to build system elements (recommended)
   - Install and configure process controllers (recommended)
   - Make sure the HMI server and requirements are configured (required)

For more information, see these additional resources.

Resource	Description
Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200	Describes how to build and use library components that comprise the Rockwell Automation Library of Process Objects.
Application Code Manager User Manual, publication LOGIX-UM003	Provides details on a modular, object-based approach to the creation of ACD controller code, FactoryTalk® View SE /ME display content, FactoryTalk® Historian Tag and FactoryTalk® Alarms and Events (FTAE) import configuration.

Develop a Project Plan

Based on the system requirements and PSE results, start by planning the scope of the process application. Use a spreadsheet or other tracking tool to define the details for each controller in the project, such as:

- Controller name
- Task name
- Program name
- Description
- I/O type
- Control strategy name
- Minimum and maximum values and units of measure
- Alarm values (LoLo, Low, High, and HiHi)
- HMI display name

This level of detail helps you organize the actual programs and tasks in the application. For example:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	NAME	CONTROLLER	TASK	PROGRAM	DESCRIPTION	I/O	Control Strategy	Min	Max	Unit	LOLO	LOW	HIGH	HIHI
11	FT0120	Water	Task_D_500ms	Polymer_TaskD	Flow to Large Storage #2	AI	P_AIn	0	10000	GPM	-1.50E+38	-1.50E+38	1.50E+38	1.50E+38
12	FT200	Water	Task_D_500ms	Canals_TaskD	Flow Offsite #1	AI	P_AIn	0	100	GPM	5	10	90	99
13	FT201	Water	Task_D_500ms	Canals_TaskD	Flow Offsite #2	AI	P_AIn	0	100	GPM	5	10	90	99

Determine Which Libraries to Use

Rockwell Automation provides libraries to simplify application development.

Table 8 - Library Descriptions

Item	Description
Process Library	Rockwell Automation Library of Process Objects provides sample projects, application templates, Endress + Hauser library objects, Application Code Manager library objects, and tools and utilities. Includes the following: • Graphics for built-in instructions • HMI images and Help files • Logix diagnostic objects • Process objects • Control strategies • Sequencer object • PlantPAx Configuration Tools for Tags, Alarms, and Historian • Color Change utility • Historian -- Asset Framework template and objects
I/O Device Library	Provides objects for Rockwell Automation 1756, 1769, 1734, 1794, 1738, 1732E, 1719, 5069, 5094 I/O modules. Provides preconfigured status and diagnostic faceplates sets for Rockwell Automation digital and analog I/O devices. You can use these objects with Machine Builder, Process, and Packaged Libraries, or as standalone components.
IO-Link Device Library	Provides IO-Link master and sensor objects. Provides preconfigured status and diagnostic faceplates.
Electrical Protection Device Library	Provides a standard to represent protection devices within your electrical distribution system
Machine Builder Libraries	Library objects for use with Application Code Manager. • Independent Cart Technology Libraries, includes ICT Libraries for iTRAK® and MagneMotion® • Studio 5000® Application Code Manager • Power Device Library, including objects for E300, ArmorStart®, PowerFlex®, and Kinetix®
Network Device Library	Provides objects for Stratix® switch and Device Level Ring network objects.
Power Device Library	Provides objects for E300, ArmorStart, SMC™-50, PowerFlex, and Kinetix.

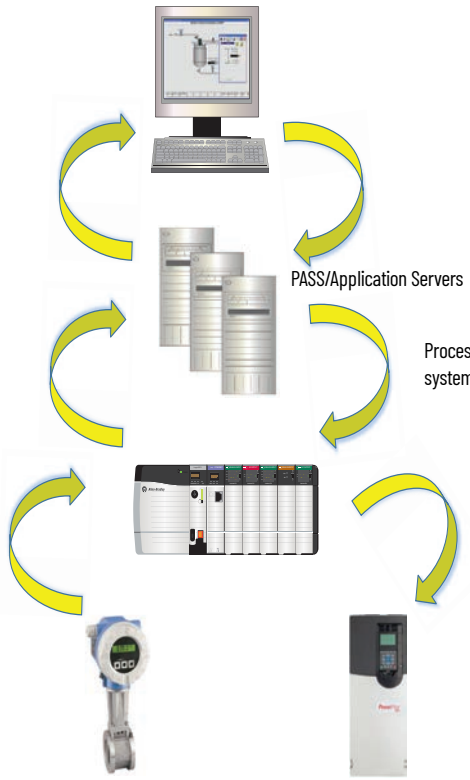
Build Application Content

A control strategy encompasses all application code that is required to implement a specific control function. The application code includes the I/O, controller code, display elements, and faceplates. The process library contains example control strategies for I/O processing, device control, and regulatory control.

By using the control strategy model, you can estimate the following:

- Potential alarms
- Visualization tags (affecting controller and server memory)
- Controller memory usage
- Controller execution time

Operator interface presents system information to the user.

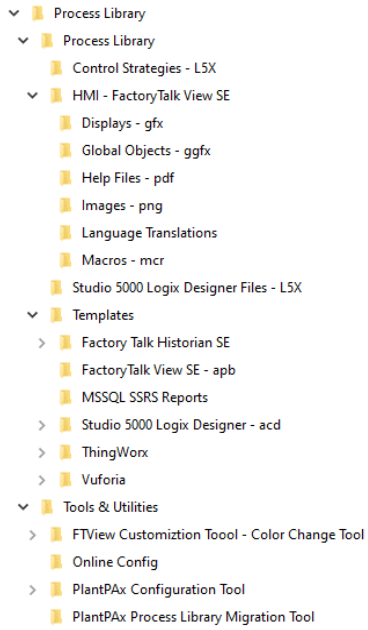


PASS/Application Servers

Process Information servers collect the process and system data for use in managing the process.

Controllers execute application code to control the process and communicate with the supervisory level.

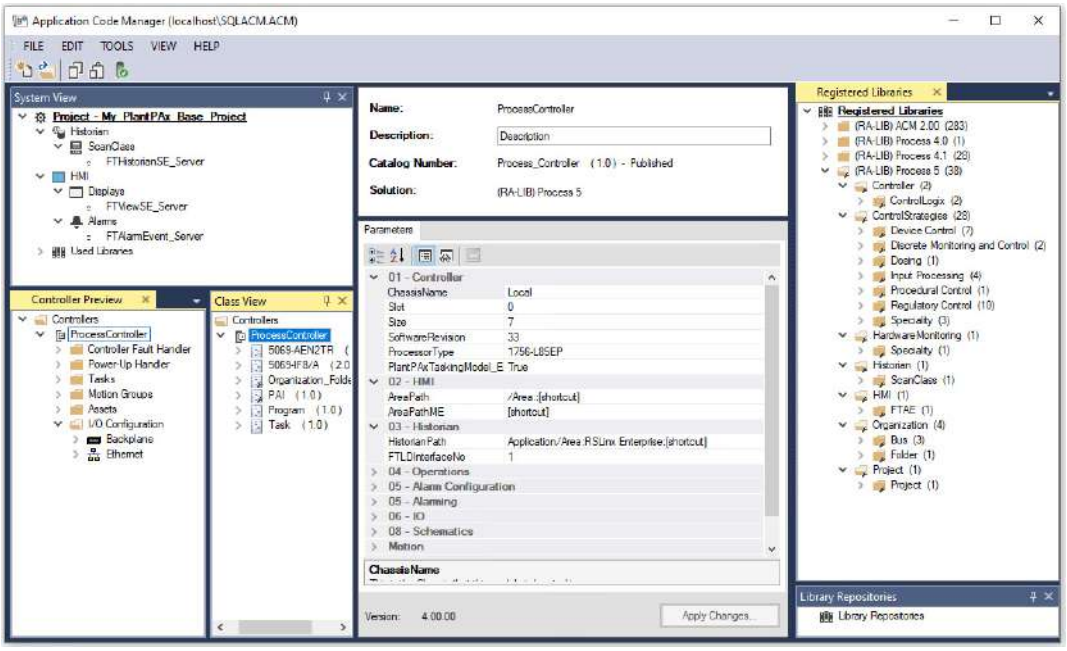
The Process library is key to building your process application content. In addition to the PlantPAx instructions embedded in the process controller, the library provides additional elements in both export and library formats.



Create a Project

Before you begin, download the libraries that you want to use and register them in ACM software.

1. Create a new ACM project and add a process controller object from the library.



2. Configure the controller parameters:
   - Set Controller properties and enable PlantPAx Tasking Model
   - Add HMI and Historian communication paths
   - Operations – specify if Redundant, has Change Detection, has Event Logging, or uses Organization Ownership Arbitration Propagation.

- Choose Alarm Configuration and Alarming Type
- Configure IO – HWBus size, Skip I/O references or Generate I/O references
- Schematics - Main Panel
- Ethernet Port1 enabled (non-redundant controllers)
- Enable and prioritize Time Synchronization

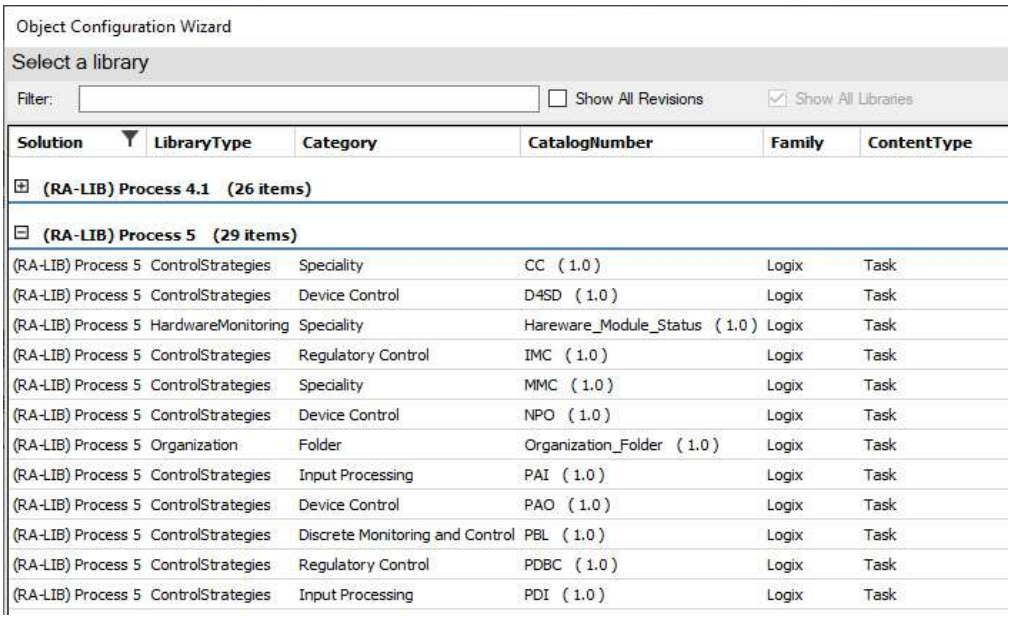
3. Select an I/O Map Strategy base on your preference.

Value	I/O Map Strategy	Description
0	Standard Mapping in ACM	Physical I/O address tied to object
1	Use Aliases for I/O	Tag to Alias I/O tied to the object
2	Use I/O Mapping tags in Mapping Routines	Input and Output routines connect the alias to the physical I/O
3	Use I/O Mapping Tags and Diagnostics in Mapping Routines	Input and Output routines connect the alias to the physical I/O plus fault detection mapping
4	Map I/O Directly in Mapping Routines	Input and Output routines connect to the physical I/O (no alias)
5	Use Program Connections (recommended)	Program-scoped tags connect to the physical I/O (binding can be done now or later when online with a controller)

For each IO map strategy, you can generate a different .ACD file and preview the output in the Studio 5000 Logix Designer® application.

Add Control Strategies

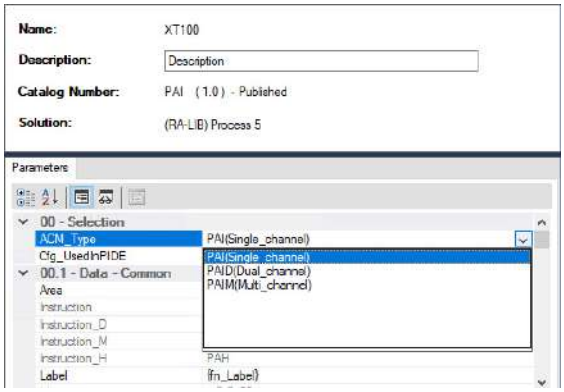
The ACM process library includes a comprehensive set of control strategies for you to use in your controller projects. Follow your project plan (the spreadsheet with your devices and tags) as you add control strategies for devices (that is motors, valves, drives, and so on) to the ACM project.



As you add objects to the project, enter unique names for each instance so you do not overwrite the original files.

Review all options on the parameter tab to complete the configuration of the control strategy.

- A True or False option means that the item is enabled when True and ACM modifies the code and tags to reflect your choice.
- Many of the control strategies have different types to choose. For example, the PAI strategy has Single, Dual, and Multi-channel types, under the 00 – Selection category.



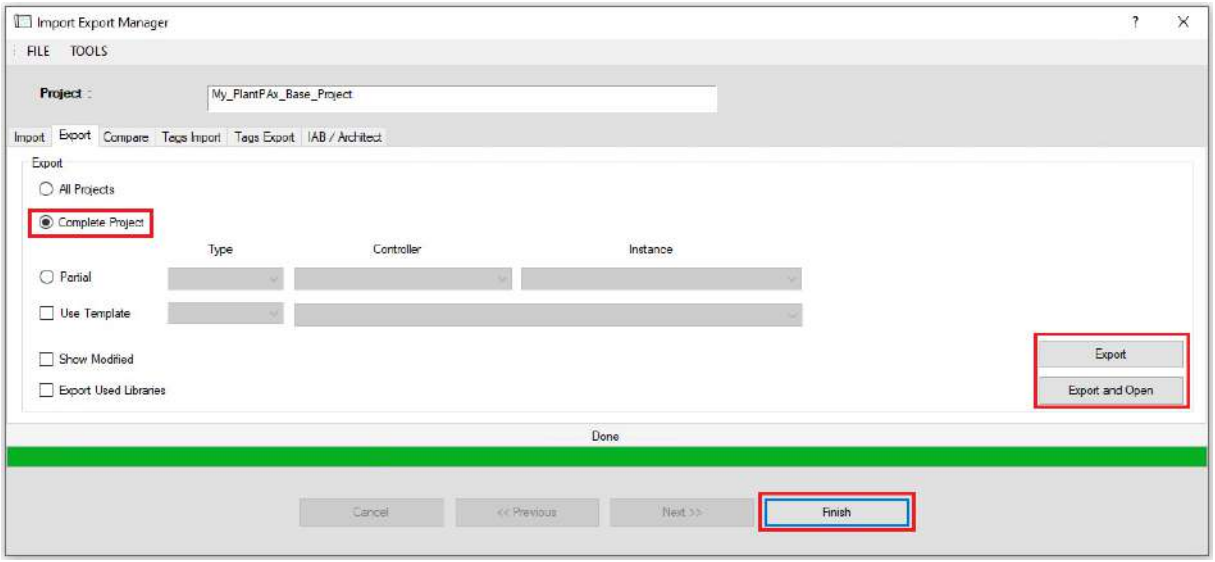
Create one control strategy for each type and export those control strategies to an Excel® file. Open the export with Excel and copy/paste additional control strategies as needed. Then import the Excel back into ACM.

Import/Export Manager

Use the Tools > Import/Export Manager to create additional devices (for motors, valves, drives) with your configured strategies. You export the control strategy to a .xlsx file, add additional devices to the file, and then import the modified .xlsx file back into the control strategy.

This example creates additional Process Analog Input objects.

1. Export a configured control strategy.

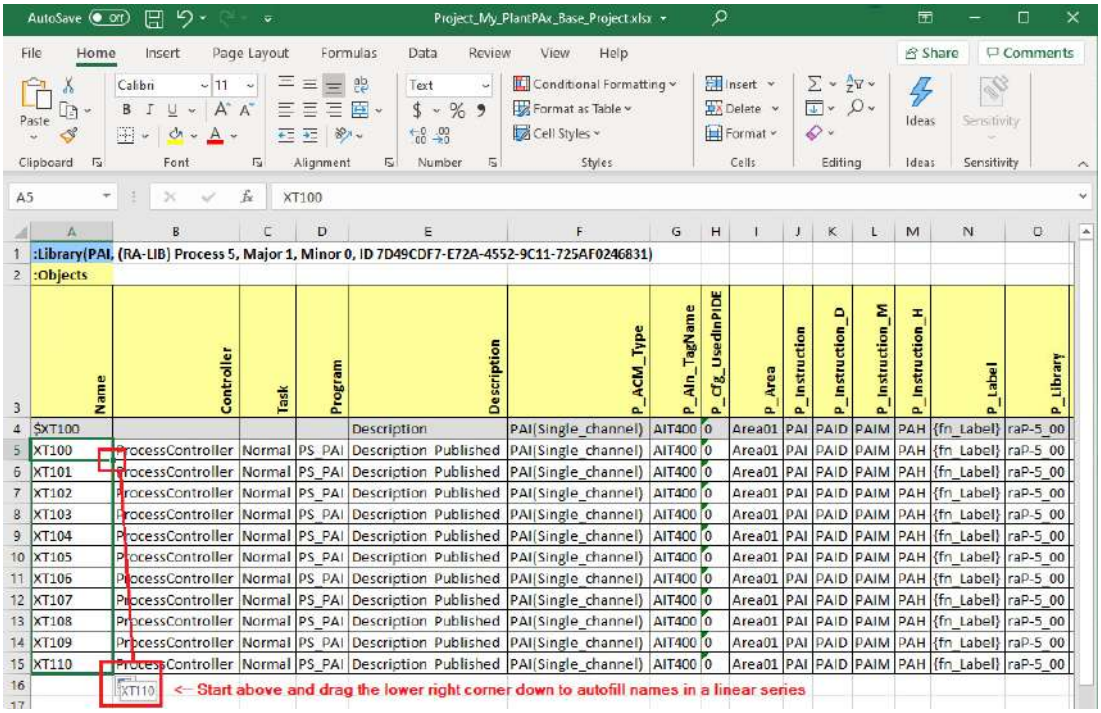


2. Open the .XLSX export file in Excel and find the tab of the object you want to duplicate.

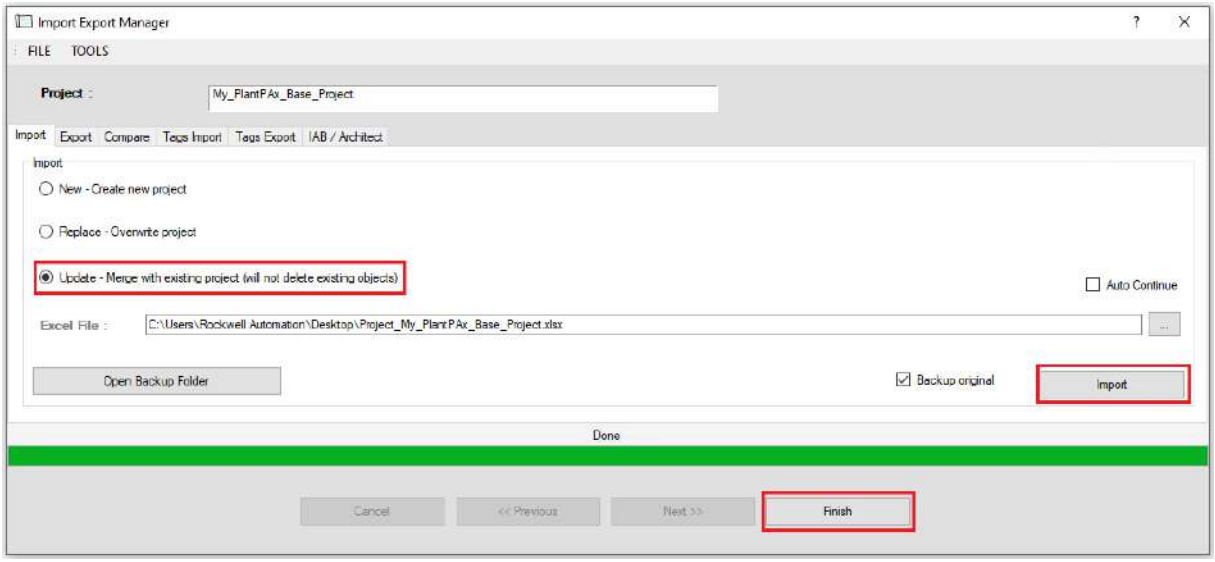
   A complete project .XLSX file can contain many tabs of various project components, which you can also modify.

3. To duplicate an object, locate the row and insert empty rows below for however many new objects you need.

4. Copy the original row and select the empty rows and paste.
5. The new objects require unique names. (such as, XT100 – XT110)
6. Select the cell of the first row, where the names start, and hover the lower right corner.
7. Click the + and drag it down the column to the bottom of the new row. Excel's auto fill feature renames all selected names in a linear series.



8. Modify names in other columns as needed, such as the column for program connections or the column to specify the I/O module channel.
9. Save the file import it back into the control strategy.



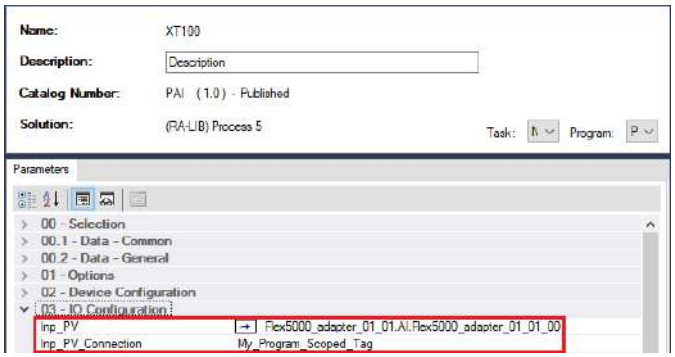
Your ACM project now contains several objects, with the same control strategy, to use throughout your project.

Map I/O

ACM supports several I/O map strategies. PlantPAx recommends that you use Program Connections, where program-scoped tags are linked to I/O modules physical addresses. Program connections are similar to alias tags, but have the advantage of being modifiable when online with a controller.

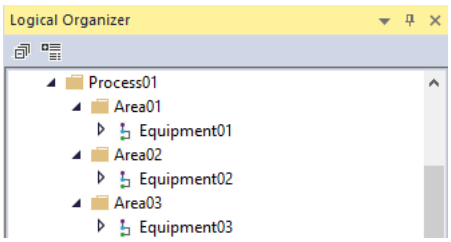
Define the I/O module physical address in ACM, in Excel®, or in Studio5000 Logix Designer.

- Enter the I/O module channel address, or leave it blank.
- Enter a name for a program-scoped tag that connects to the physical address. ACM generates this tag.



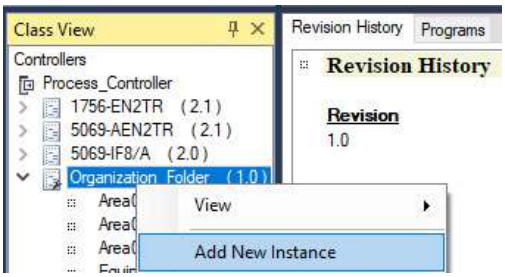
Develop a Logical Organization

The ACM process library contains an Organization Folder object that is designed to create a Logical Organizer within a Studio5000 Logix Designer project. ACM generates the Logical Organizer based on folder and program parent/child assignments.



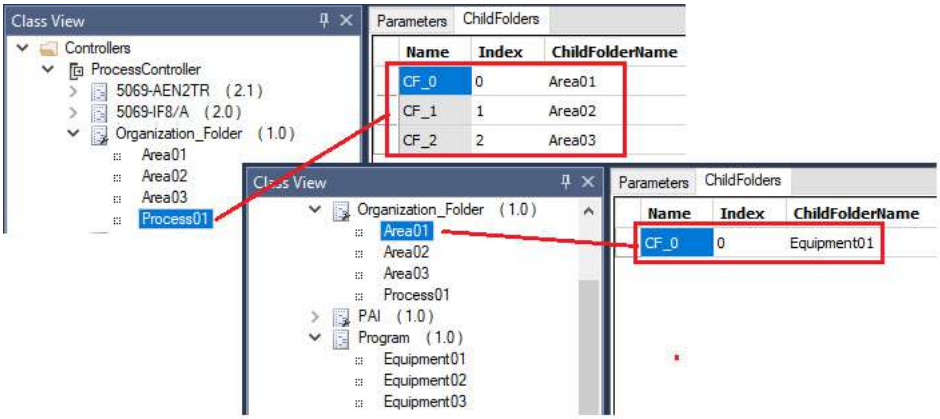
For more information about the Logical Organizer, see PlantPAx Process Objects.

1. Add the Organization Folders object to your project to build levels of areas, as required.
2. To create additional folders, select the Organization Folder object and select Add New Instance



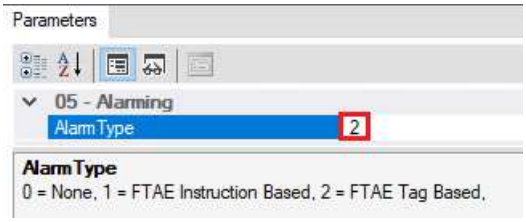
3. Build your folder hierarchy by assigning child folders.
4. Assign programs to the child folders.

   For example:



Add Alarm Groups

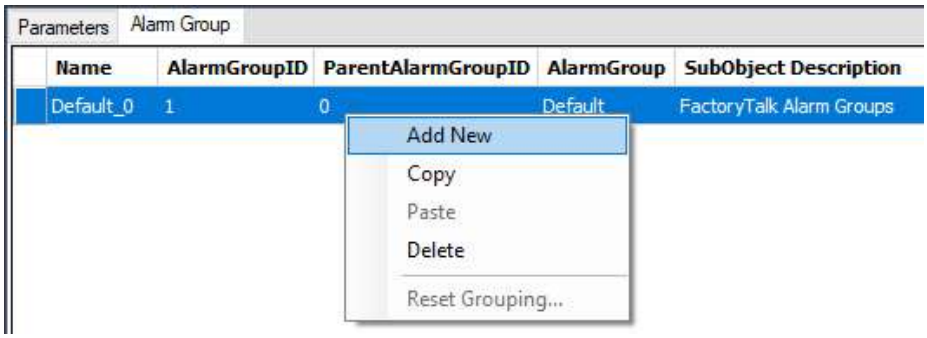
ACM can create alarm groups and you can assign alarms within control strategies to those groups based on organization. Specify the type of alarms that ACM generates in the controller parameters.



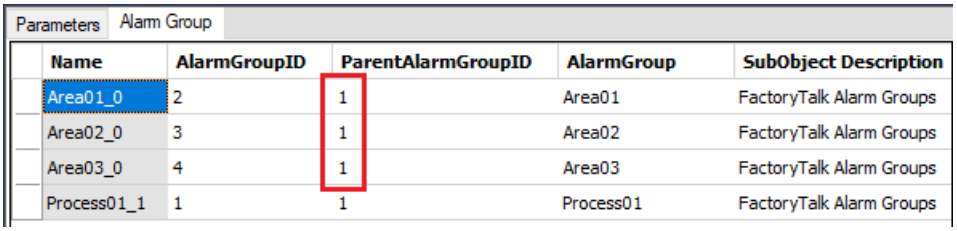
1. Go to ACM System View > HMI > Alarms and add an FTAlarmEvent object from the library.

   The default name is FTAlarmEvent_Server.

2. Select the FTAlarmEvent_Server object to access the Alarm Group Tab and select Add New.



3. Add groups for your areas and assign the Parent Alarm Group ID to represent the parent/child hierarchy.



Name	AlarmGroupID	ParentAlarmGroupID	AlarmGroup	SubObject Description
Area01_0	2	1	Area01	FactoryTalk Alarm Groups
Area02_0	3	1	Area02	FactoryTalk Alarm Groups
Area03_0	4	1	Area03	FactoryTalk Alarm Groups
Process01_1	1	1	Process01	FactoryTalk Alarm Groups

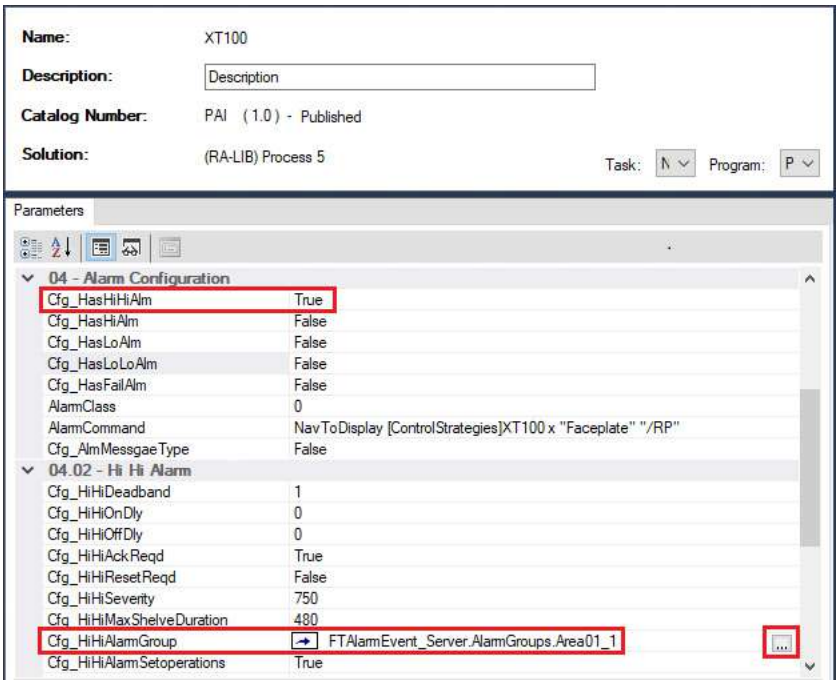
Once you have alarm groups, you can enable alarms in your control strategies and link each alarm to the desired group.

4. For each control strategy, access the parameters tab and expand 04 - Alarm Configuration. Enable the alarms that you need (such as, Hi Hi, Hi, Lo, or Lo Lo).

Ideally an alarm design has been performed to assure that only those alarms that uniquely identify an abnormal situation and require action by the operator are enabled. Configuring alarms without a proper design effort will create nuisance alarms that will make the operator less effective and create mistrust in the alarm system

5. Expand an enabled alarm (such as, Hi Hi Alarm) and select the Group parameter (such as, Cfg_HiHiAlarmGroup).

6. Click the ellipse button and use the Select a Reference dialog to choose the alarm group.



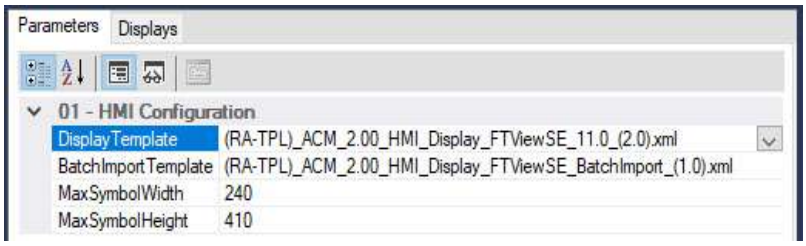
Add HMI Graphic Displays

ACM software can create graphic displays for control strategies. They're generated in .XML format that you can import into to a FactoryTalk View SE application.

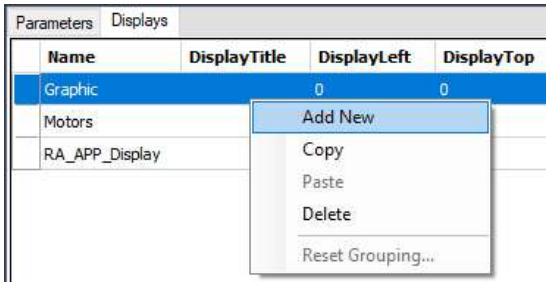
1. Go to ACM System View > HMI > Displays and add an FTViewSE object from the process library.

   The default name is FTViewSE_Server.

2. On the parameters tab, select a Display Template and a Batch Import Template from the library.

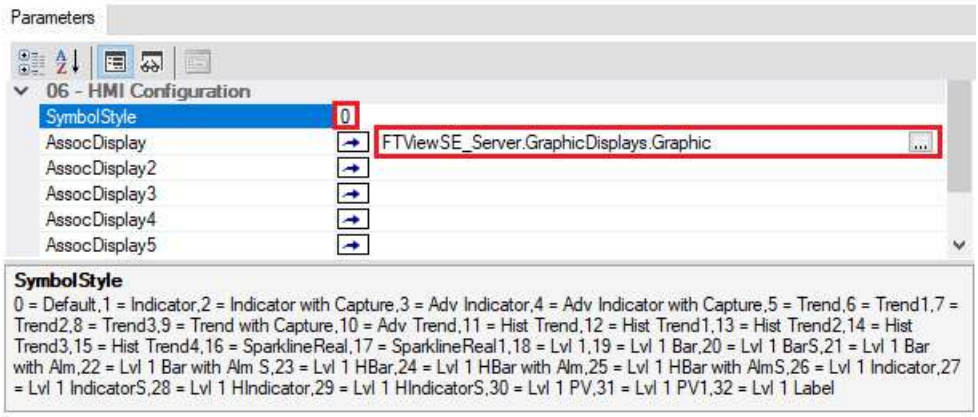


3. On the Display tab, add new graphics.



Now add your associated displays to your control strategies.

4. For each control strategy, access the parameters tab and expand 06 - HMI Configuration category.
5. Choose the desired symbol style, as described in the caption.
6. Choose the associated displays where the object is placed.



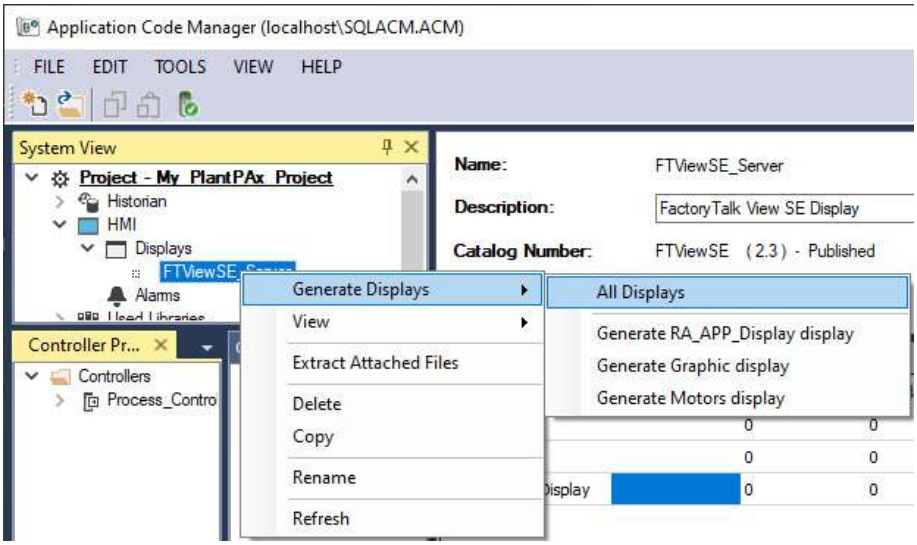
Generate HMI Displays

When the control strategies and displays are configured and associated, you can generate the displays.

1. Verify that the controller parameters contain the correct communication path of your HMI server and device shortcut.

   You create device shortcuts on the PASS using a FactoryTalk View SE application or the FactoryTalk® Administration Console.

2. Select HMI > Displays > FTViewSE_Server and select Generate Displays > All Displays



3. Browse to where you want to save the generated.XML file.

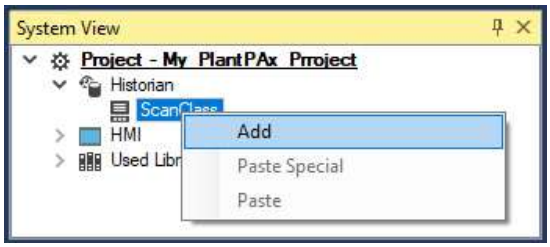
   ACM generates one batch import .XML file and all individual displays .XML files.

The graphic displays are now ready to be imported into a FactoryTalk View SE application.

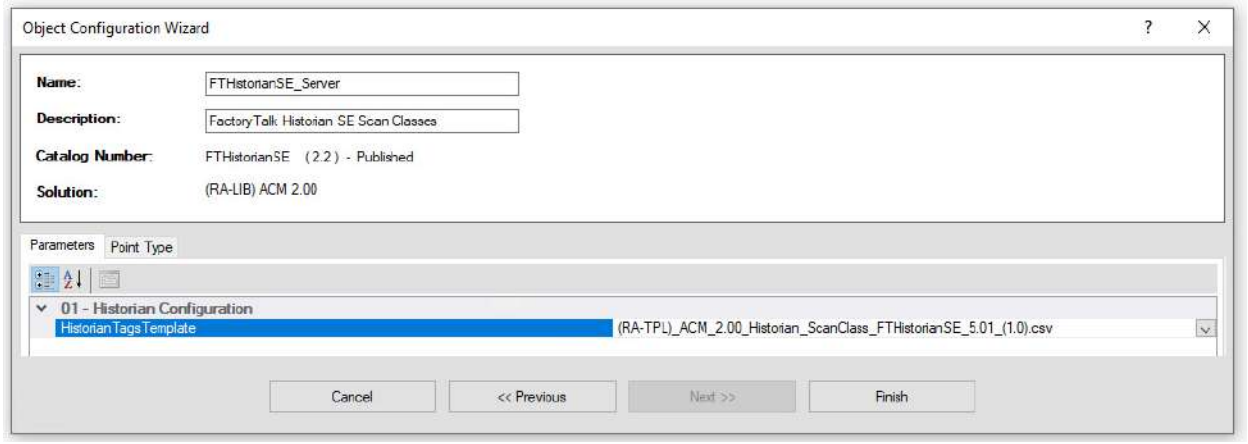
Develop Historian Tags

The process library objects reference multiple Historian digital sets. Digital points can be used to enumerate the process states, thus creating a relationship between the value and the text state name. For example: 1 = Good.

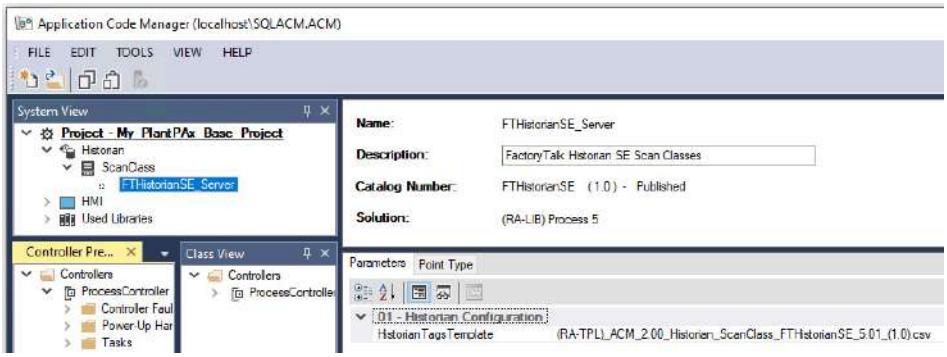
1. Add a Historian object to your ACM project.
2. Got to Historian > ScanClass and select Add.



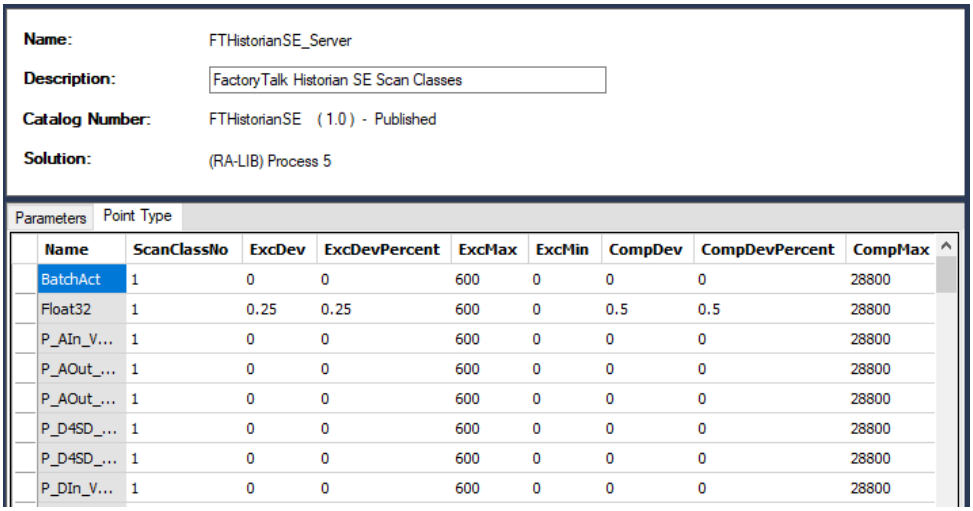
3. Use the Object Configuration Wizard to select and create the desired Historian digital sets.



The ScanClass now contains the FTHistorianSE_Server object.



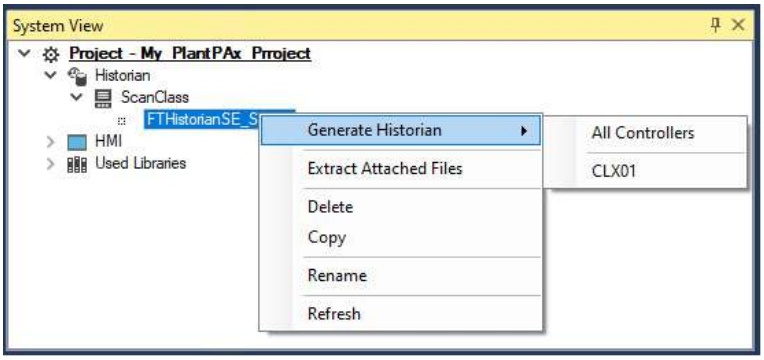
4. Select the Point Type tab to view the available digital sets.



Generate Historian Tags

Use ACM to generate the Historian tags to a .CSV file that corresponds to the configured control strategy.

1. Go to ACM System View > Historian > Scan Class > FTHistorianSE_Server and select to Generate Historian



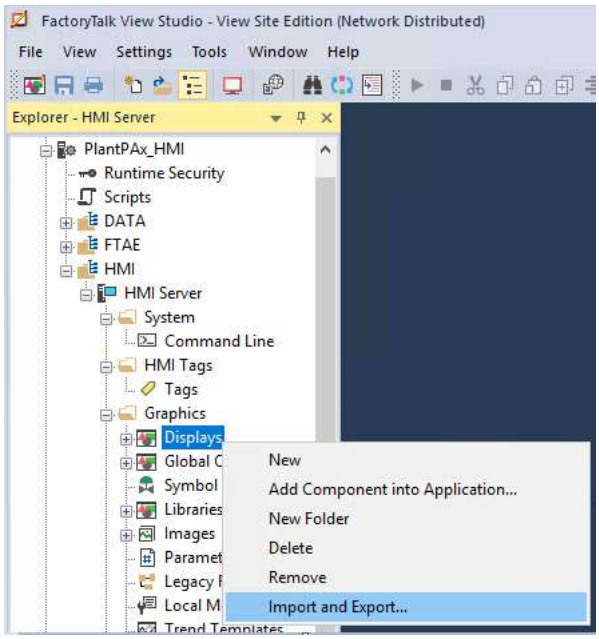
2. Save the Historian tags .CSV file to the computer that has the PI Builder Add-in for Microsoft® Excel.

ACM-Generated Displays

IMPORTANT The process library uses Global Objects. They must be imported into the FactoryTalk View SE application before the displays.

ACM-generated displays can be imported into your HMI application by using FactoryTalk View Studio software.

1. In FactoryTalk View SE Studio, import the ACM-generated graphics (.XML).

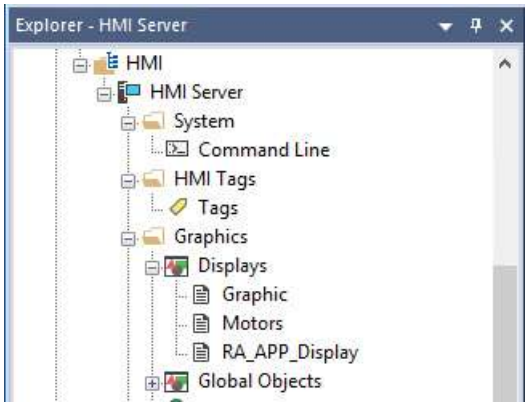


2. Use the Graphics Import Export Wizard to import either a single global object or batch of multiple global objects from an .XML file.

Page	Selection
Select the operation to perform	Import graphic information into displays
Do you want to backup the displays that will be modified by the import?	No

Page	Selection
Select the type of file to import	Multiple displays batch import file
Select the multiple display batch import file	Browse to your batch import file (Example: My_PlantPAx_Project_FTViewSE_Server_BatchImport.xml)
When importing	Create new objects on the display

3. Verify that the displays were created successfully.



Notes:

Modifying an Existing PlantPAx System

The process library includes templates of controller and HMI applications to get you started If you are not using ACM or have an existing project. The process library also includes the PlantPAx® Configuration Tool for Tags, Alarms, and FactoryTalk® Historian which can be used to edit existing projects. See the following table for software and tool usage and explanation.

New or existing	Studio 5000 Logix Designer® and FactoryTalk® View SE software	Studio 5000 Logix Designer and FactoryTalk® View SE software can open templates to start new projects or import library elements directly into existing projects. Both software products are required throughout the application development process, Open and import library elements: • Controller project template .ACD files • Controller Add-On Instruction and rung .L5X files • HMI project template .APA files • HMI global object and graphic display .GFX files • HMI image .PNG files
Existing	PlantPAx Configuration Tool for Tags, Alarms, and Historian	The PlantPAx Configuration Tool for Tags, Alarms, and Historian helps define controller .ACD files with associated HMI applications. The PlantPAx Configuration Tool for Tags, Alarms, and Historian is best suited for modifying the output from an ACM project, an existing controller project, or a template project from the process library. Use the PlantPAx Configuration Tool for Tags, Alarms, and Historian to: • Organize parameter files for use the code, tags, and HMI displays into a process tree (builds the Logical Organizer) • Create FactoryTalk® Alarms and Events alarm groups • Create Historian Asset Framework elements • Edit controller tag data with import and export • Build HMI parameters for use with tag search and navigation graphics

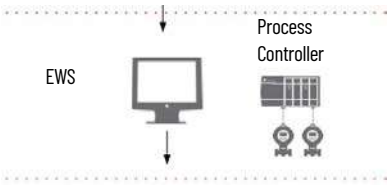
Step 1: Use Studio 5000 Logix Designer for Individual Edits

- Logix Designer application templates
- FactoryTalk View SE templates

Step 2: Use the PlantPAx Configuration Tool for Tags, Alarms, and Historian for Bulk Edits

- Tag data
- Alarm
- Historian points
- HMI displays

Prerequisites



Which library elements to use depends on whether you:

- Modify an existing application
- Create a new application based on a sample template
- Import library elements into a project
- Generate library elements into code by tools

For more information about the process library, see the Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200.

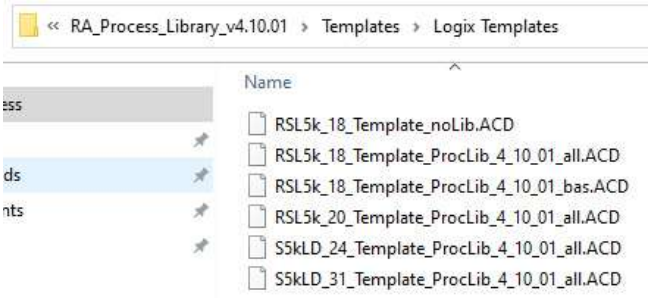
Resource	Description
Rockwell Automation Library of Process Objects Reference Manual, publication PROCES-RM200	Describes how to build and use library components that comprise the Rockwell Automation Library of Process Objects.

Studio 5000 Logix Designer and FactoryTalk View SE Software

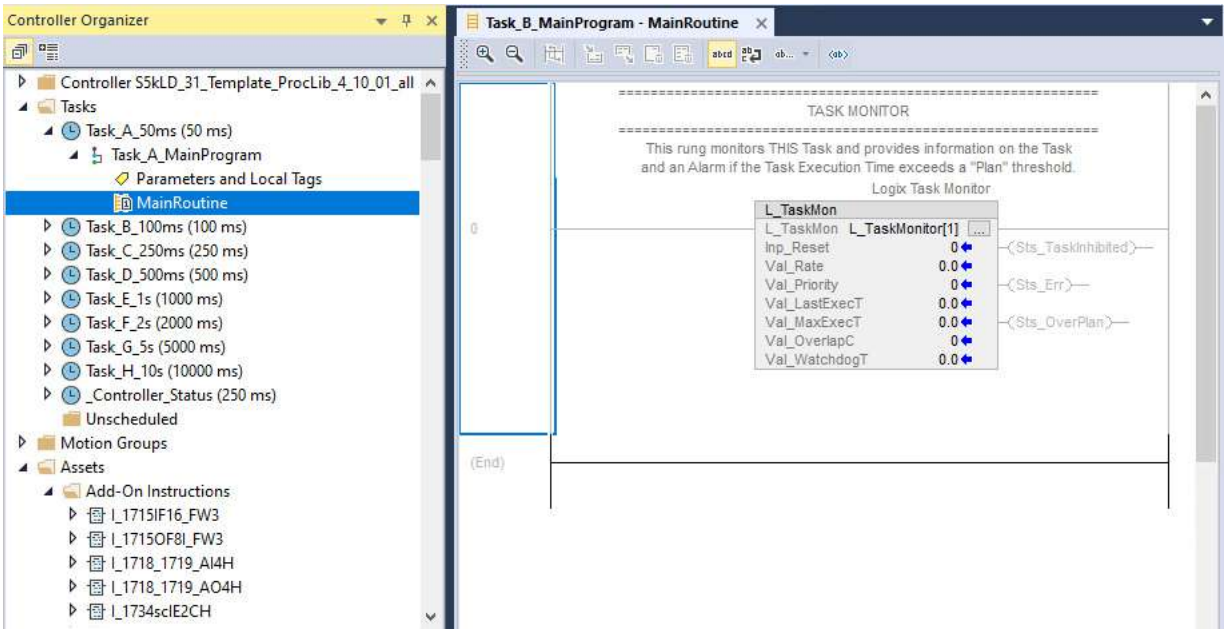
The process library includes templates of controller and HMI applications. These templates are designed to get you started if you aren't using ACM software or do not have an existing project.

Logix Designer Application Templates

Controller templates have the library instructions and task model already defined. They also have a basic IO configuration that you can modify according to your project plan.



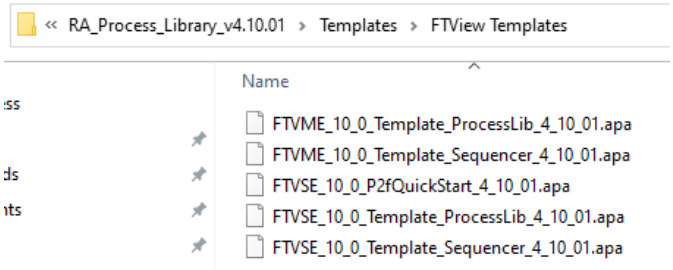
Open a Logix Designer application project and browse to the template directory and select the template to open.



For more information, see PlantPAx Process Objects.

FactoryTalk View SE templates

HMI templates contain pre-defined components such as, Displays, Global Objects, Libraries, Images, Macros, and basic configurations for FactoryTalk View SE applications.



If you already have an HMI project, on your PASS, you can:

- Use the template application as a new HMI, then recreate your Areas, HMI server, data server and alarms and events server, such as you do when you configure a PASS.
- Use the existing HMI application, on the PASS, and add library components into the application.

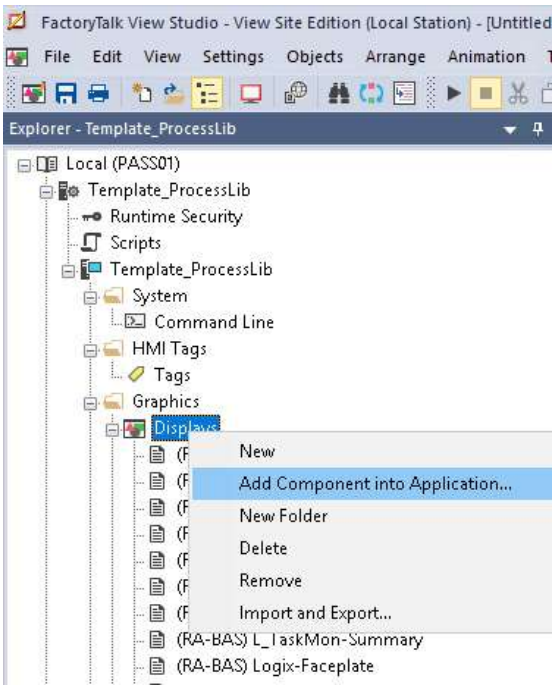
You need to restore the template so you can access the application and its components.

1. Go to the FactoryTalk View SE Application Manager and select to restore a local station archive.
2. Browse to the .APB file in the templates folder in the process library and open the application.

- If you choose to make this template your new HMI application, see Chapter 3, Process Automation System Server for how to create areas and servers.
- If you choose to maintain your existing HMI application, export the Displays, Global Objects, Libraries, Images, Macros from the template and import them into your application.

You can use the Add Components in Application method to add Displays, Global Objects, Libraries, Images, directly from the library.

1. In your application, select the component (such as Displays) and select Add Component in Application.



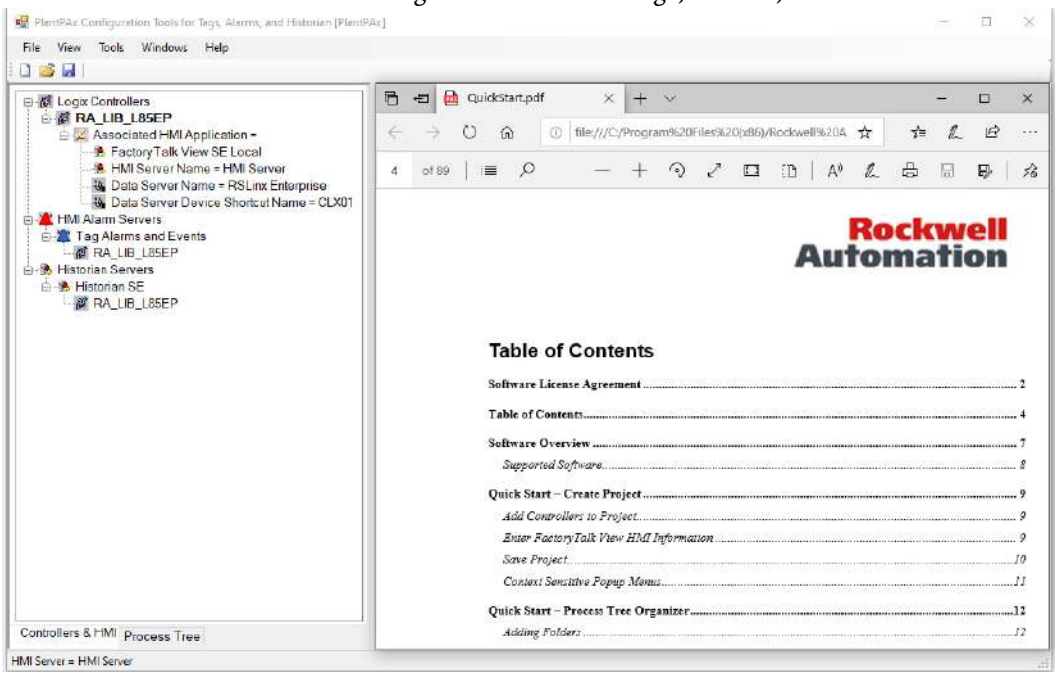
2. Browse to the .GFX files in the library folders and select those to open.

Edit a Project via the PlantPAx Configuration Tool for Tags, Alarms, and Historian

The process library includes the PlantPAx Configuration Tool for Tags, Alarms, and Historian. This tool performs various functions to help you create or modify an existing PlantPAx project. To use this tool, you must have a controller project (.ACD) file, which can be:

- Generated from ACM
- Existing controller project
- Sample controller project from the process library

For more information, see the quick start guide that comes with the tool. The Quick Start guide automatically launches when you open the PlantPAx Configuration Tool for Tags, Alarms, and Historian.



With the PlantPAx Configuration Tool for Tags, Alarms, and Historian, you can:

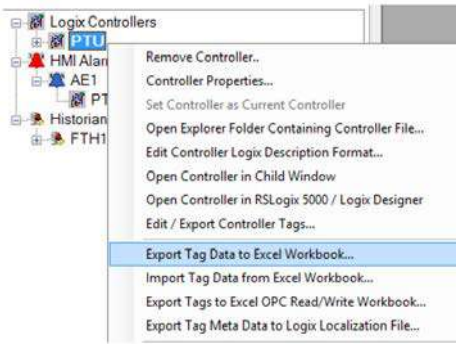
- Define a project that has multiple controller .ACD files and associated FactoryTalk® View HMI applications.
- Organize controller logic, tags, and HMI displays in a Process Tree organizer. You can then use the tree structure to create FactoryTalk Alarms and Events alarm groups and Historian Asset Framework elements.

Edit Tag Data

- Edit tags and data in offline controller .ACD files.
- Export and import tag data to and from text files.
- Create Microsoft® Excel® workbooks for online OPC tag data reads and writes.

1. Add controllers to the project or load existing project.

2. Launch the bulk data editing function from the controllers project tree by right-mouse clicking a project controller and selecting one of the four export/import tools:

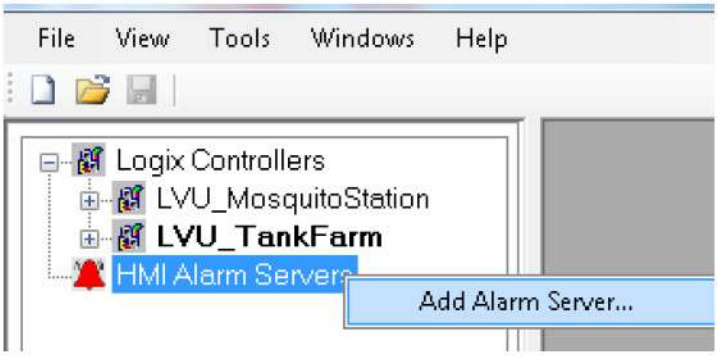


3. This launches a dialog window for each of the tools. Click the “Help” button in the dialog window for additional instructions.

Edit Alarms

- Create FactoryTalk Alarms and Events. XML import files using tag data from controller files.

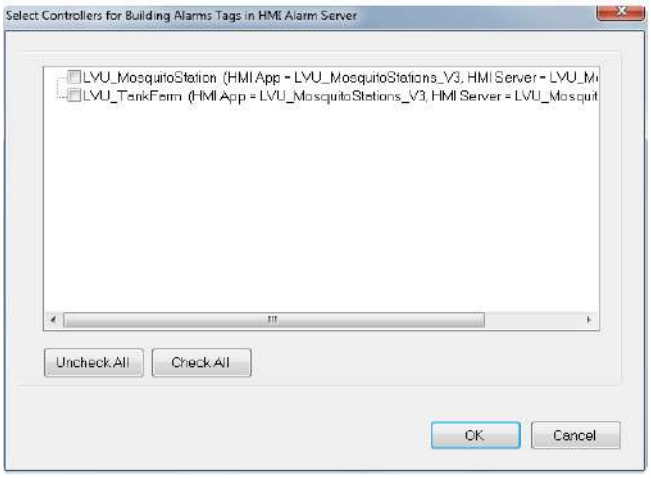
1. Multiple AE alarm servers can be used in FactoryTalk applications. Each AE alarm server can provide alarms from multiple Logix controllers. The project can contain multiple controllers. Select the controllers to use for each AE alarm server XML import file you want to create. Right-mouse click on “HMI Alarm Servers” and “Add Alarm Server”:



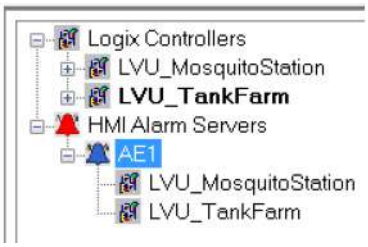
2. Enter alarm server name and description. It is recommended that the FactoryTalk AE server name be used.

IMPORTANT The software does not have the capability of accessing the FactoryTalk AE server. The alarm server created here is merely used for organizing the controllers associated with the server. Any name can be used. However, it is recommended to use the actual AE server name to avoid confusion.

3. Select the controllers to associate with the alarm server. Only Logix tags from the selected controllers will be used.

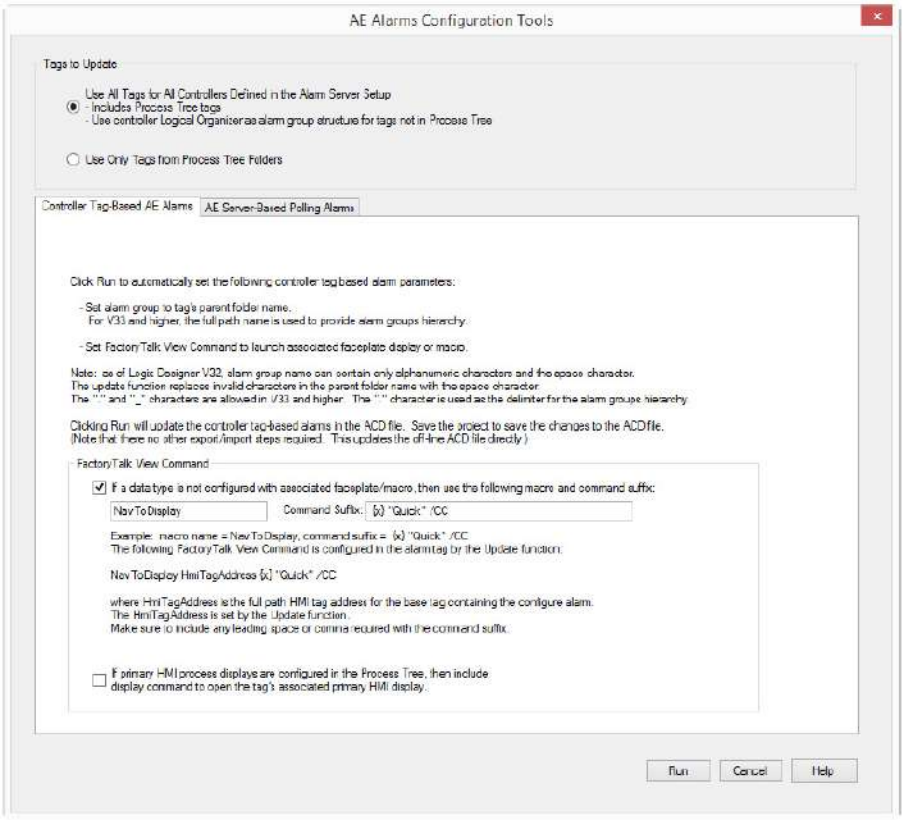


The alarm server and associated controllers are added to the project tree.



Launch AE Alarm Configuration Tools

The tool can be used for controller tag-based alarms and AE server-based alarms. Click Help for details.



Edit Historian Points

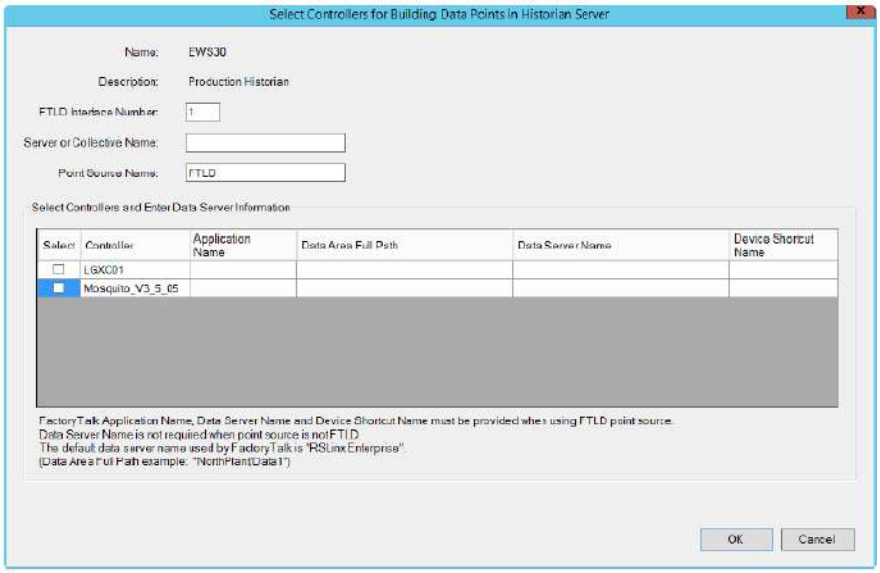
- Bulk configure OSI PI Asset Framework (AF) databases with Logix tag AF elements. This includes automatic configuration of related PI points in the FactoryTalk® Historian data server (PI data server).
- For systems without Asset Framework, a separate utility provides bulk configuration of PI points in the Historian data server. The utility provides the option of generating a bulk import file, or adding the PI points directly if a Historian data server connection is available. The bulk import file can be used with the PI Point Builder Excel AddIn to create points in the data server.

For more information about Historian tags, see Chapter 7, Historical Data

1. Create project with Logix controller files.

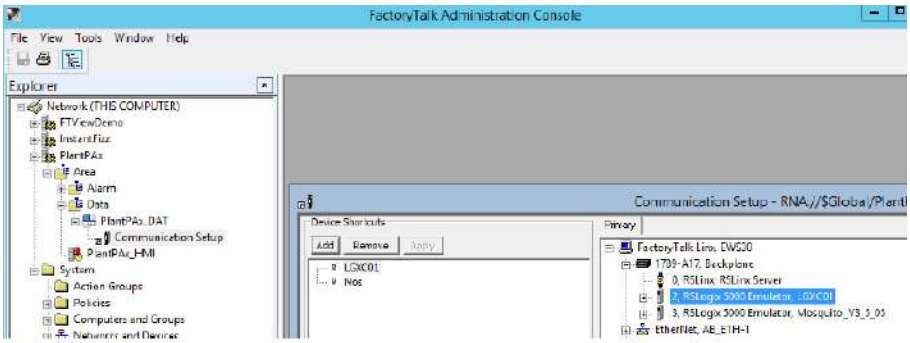
2. Right-mouse click on the Historian Servers tree node and add a historian server. Any names and description can be used as the name is used as a project placeholder.

3. Select the controllers to use and fill in the information in the window. For FTH, the point source name is “FTLD”. Contact your PI administrator for the point source name if not using FTH. Note the data server name is not required when the point source is not FTLD.

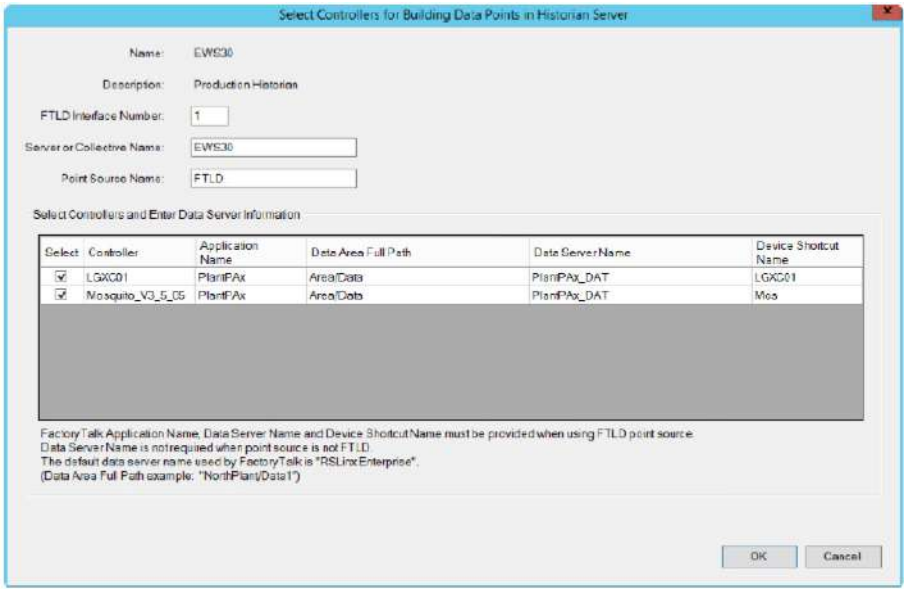


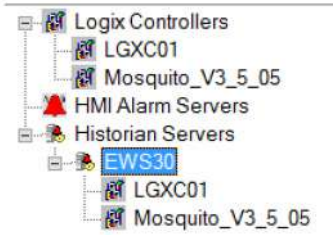
If the controllers are already configured for a project Alarm Server (refer to the Alarm Builder user manual), then the application and data server information are automatically filled in – it’s assumed that the same data servers from the HMI application are used. Make any changes if necessary.

Use FactoryTalk Administration Console to find the data server information:

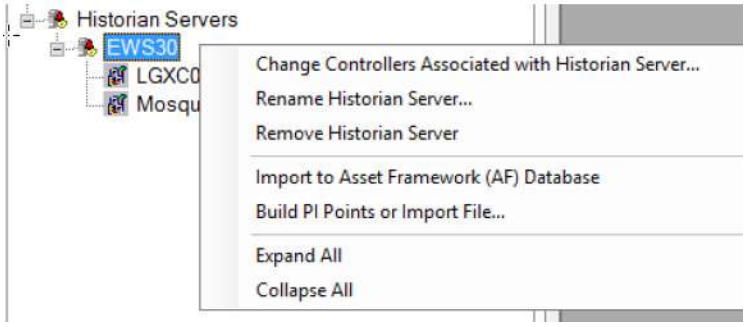


4. Click OK when the information has been entered. A new Historian Server tree node should appear in the project tree.

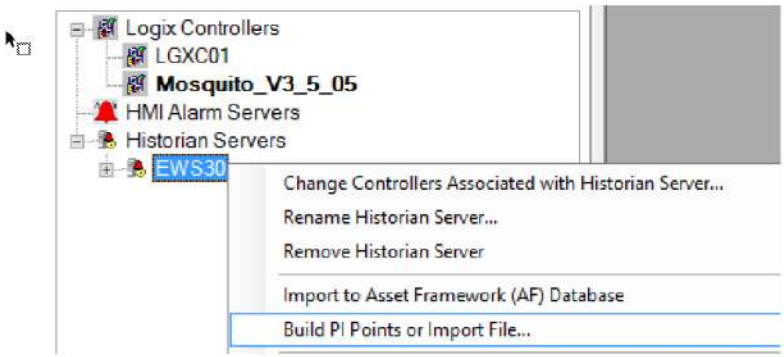


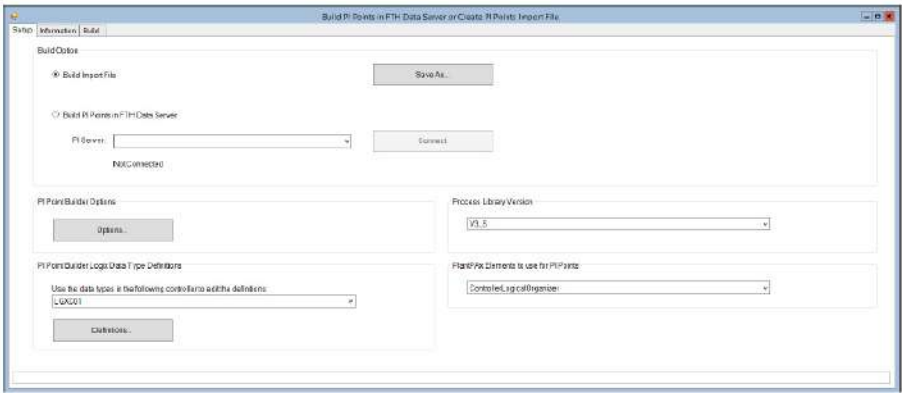


5. Right-mouse click the historian server node to make changes.



6. Right-mouse click the project historian server tree node and select “Build PI Points or Import File”:





7. Select the Build Option to create an import file or add PI points directly to an FTH Data Server. An OSI PI client must be installed to add PI points directly. See OSI PI documentation for instructions.

8. If the “Build PI Points in FTH Data Server” option is selected, then use the pull-down list box to select the data server and click Connect.

The connection status is displayed under the pull-down list box after clicking Connect:

9. Since different Process Library versions can have the same data type names containing different parameter names, separate sets of historian

library definitions and templates are used. Select the library version using the pull-down list box:

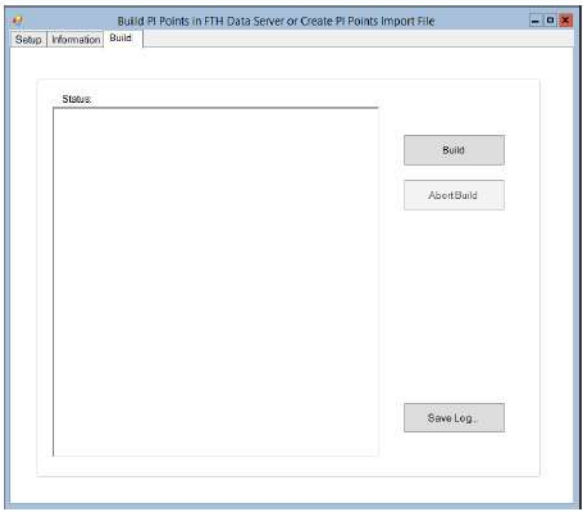
10. Use the “PlantPAx Elements to use for PI Points” pull-down box to select the project elements to use.

    a. “ControllerLogicalOrganizer”. All tags from the historian controllers list are added (same as ControllerTagsInFlatStructure option).

    b. “ProcessTree”. The contents of the project Process Tree are used. See the “Process Tree Organizer” user manual for configuration instructions.

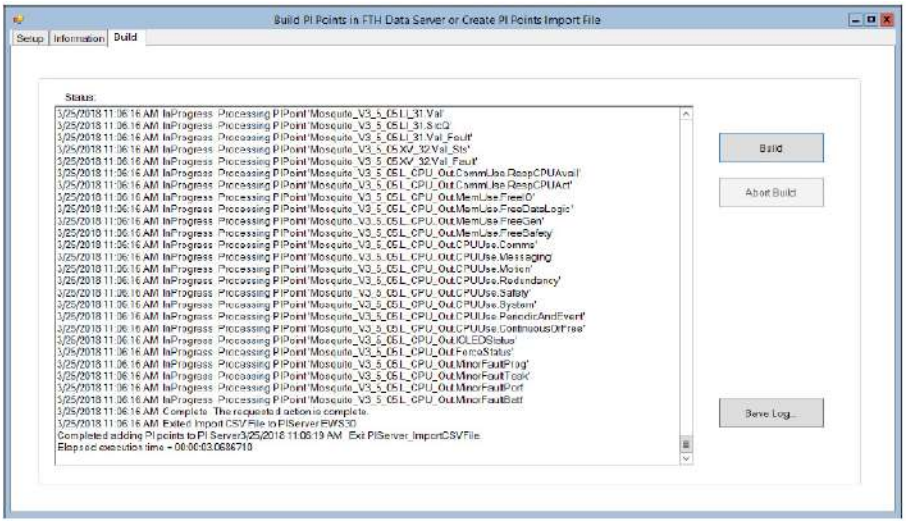
    c. “ControllerTagsInFlatStructure”. All tags from the historian controllers list are added (same as ControllerLogicalOrganizer option).

11. Click the Build button to create the import file or add PI points to the PI data server.

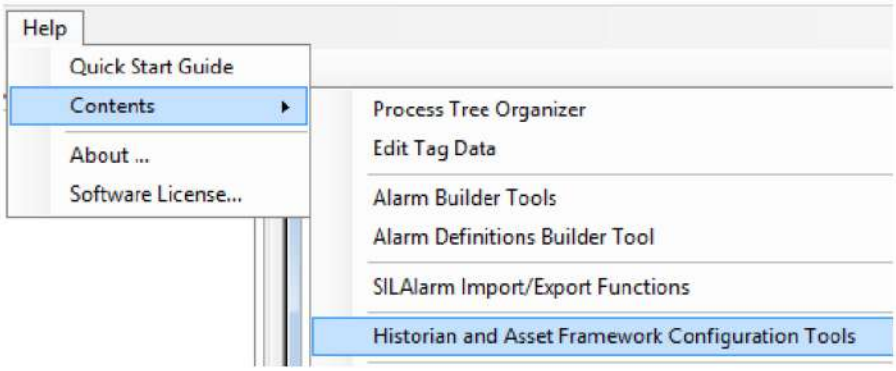


If the build import file setup option was selected, then a text file with PI points configuration generated. Use PI Builder Excel add-in to import the points to the PI data server.

If the PI points in FTH data server setup option was selected, then the build function updates the connected data server with library digital states sets and PI points.



See the help user manual for additional details:



Edit HMI Displays

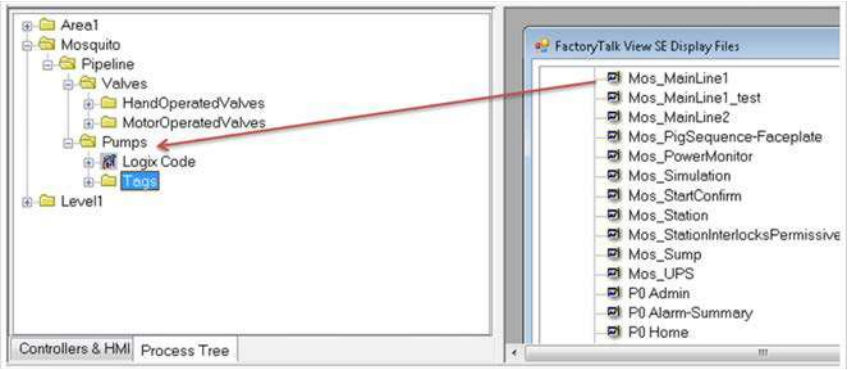
Two utilities help build specially formatted FactoryTalk View SE parameter files.

- One utility builds a parameter file containing a list of controller tags with associated HMI faceplate displays. Users can search for tags using tag names and tag descriptions. The user can open tag faceplates from the returned search results.
- The other utility creates a navigation tree from the project Process Tree structure.

Organize the FactoryTalk View SE HMI displays under process tree folders.

1. Go to Logix Controllers > Open FactoryTalk View SE Displays List... and select the Process Tree tab.

2. Drag a display file from the SE display files window and drop it into the Process Tree folder.



Asset Management

FactoryTalk® AssetCentre software is a centralized tool that helps:

- Maintain inventory assets in the system
- Manage version control to track program changes
- Collect audit logs to track user and system activity
- Schedule backups and verify program integrity

This is the recommended workflow to configure and implement a FactoryTalk AssetCentre application. Each step outlines requirements. For more detailed information, follow the referenced links.

Step 1: Inventory Plant Assets

FactoryTalk AssetCentre software provides a centralized tool to manage and track asset information as well as protect assets. You can:

- Scan the network for existing devices to create an inventory.
- Manually add individual assets.

Regardless of method, we recommend that you add asset types for controller project, HMI, engineering workstation, and servers.

For more information, see Inventory Plant Assets.

Step 2: Configure Audit Logs

There are multiple logs that can be generated to capture asset data. Select the one that you want:

- Audit Log monitors FactoryTalk-enabled software products and logs user actions. For example, who was the last user to change a program.
- Diagnostic Log to monitor system health.
- Event Log to track FactoryTalk AssetCentre events, such as when a backup starts and who generates a report.

Audit data is stored in the SQL server and displayed in the FactoryTalk AssetCentre logs. Information that is collected includes:

- User actions
- Program changes
- Security events

For more information, see Configure Audit Logs.

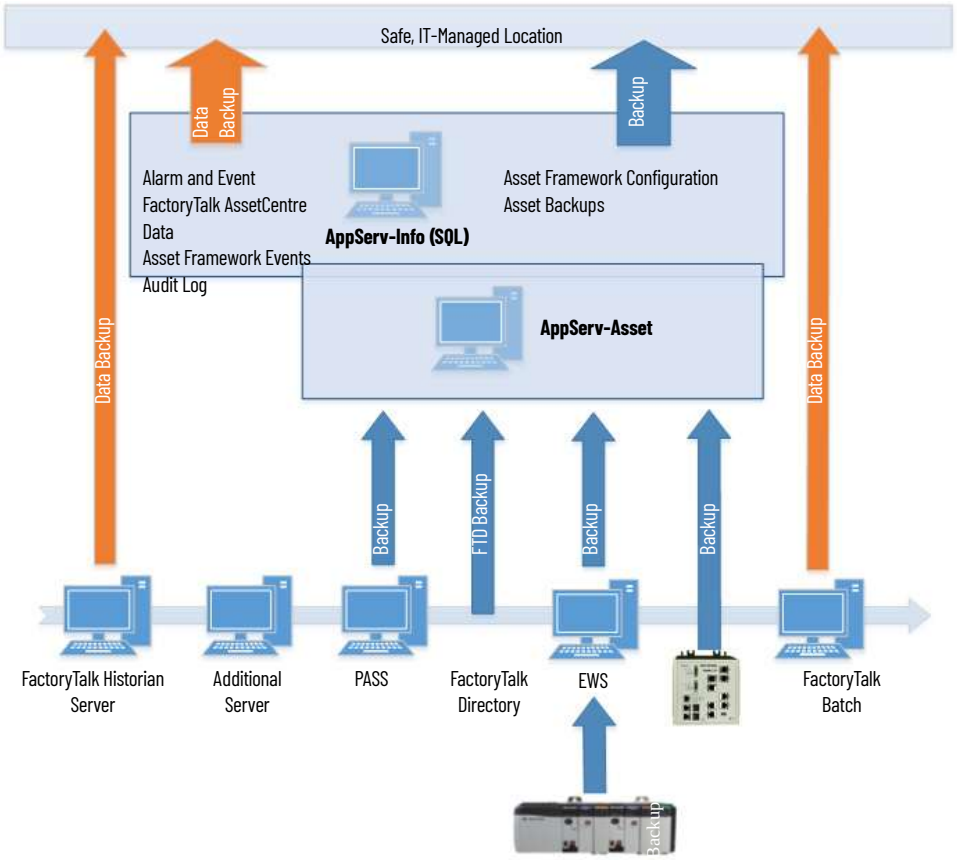
Step 3: Schedule System Backups

FactoryTalk AssetCentre software stores backup data on an SQL server.

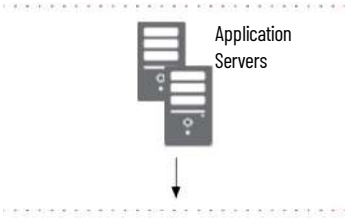
The Disaster Recovery function creates backup files from the running asset on the plant floor. The backup file is compared to the original and archived to a Master version. The Agent service performs these comparisons and can be scheduled to operate at specific times and intervals

For more information, see Schedule System Backups.

Example Asset Data Flow



Prerequisites



Following the System Workflow, configure application servers.

An asset management server (AppServ-Asset) supports maintenance and plant operations to the system with FactoryTalk AssetCentre software.

In most PlantPAx® systems, the AppServ-Asset server is on a separate computer and requires these components local or distributed on remote servers:

- FactoryTalk® Directory
- FactoryTalk® Activation server
- FactoryTalk® SQL server (can be on the same computer as the AppServ-Asset server or on its own computer)

Install FactoryTalk AssetCentre Client software on the FactoryTalk AssetCentre server, the EWS, and the OWS.

If you plan to use the FactoryTalk AssetCentre virtual images, see configuration procedures in 9528-UM001.

For more information, see these additional resources.

Resource	Description
FactoryTalk AssetCentre Installation Guide, publication FTAC-IN005.	How to install the FactoryTalk AssetCentre system.
FactoryTalk AssetCentre Getting Results Guide publication FTAC-GR002	How to get started with the FactoryTalk AssetCentre system.
FactoryTalk AssetCentre Utilities User Manual, publication FTAC-UM001	How to use FactoryTalk AssetCentre utilities.

For Rockwell Automation tutorials, see these YouTube videos.

- Introduction to Asset Management
- Using the Inventory Agent in FactoryTalk AssetCentre
- Getting Started with FactoryTalk AssetCentre
- Introduction to FactoryTalk AssetCentre Disaster Recovery
- FactoryTalk AssetCentre Disaster Recovery to Backup and Compare a FactoryTalk® View SE Application

FactoryTalk AssetCentre

FactoryTalk AssetCentre provides a centralized tool to manage and track asset information and protect assets.

To help protect your automated control system, we recommend that you develop a strategy for archiving application data and determine recovery plans. For a tutorial, see the YouTube video 'Introduction to Asset Management'.

If you plan to configure the FactoryTalk AssetCentre virtual image, see the procedures in the Template User Manual, publication 9528-UM001.

Inventory Plant Assets

An asset inventory lists the connected devices and computers on the network and stores unique identification information about the hardware, firmware, and software in the system.

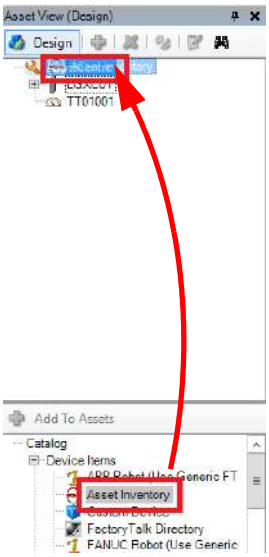
There are multiple ways to build your inventory list of assets with FactoryTalk AssetCentre software tools.

Scan the System for Assets

Drag-and-drop an Asset Inventory asset type into the FactoryTalk AssetCentre tree and scan for device information.

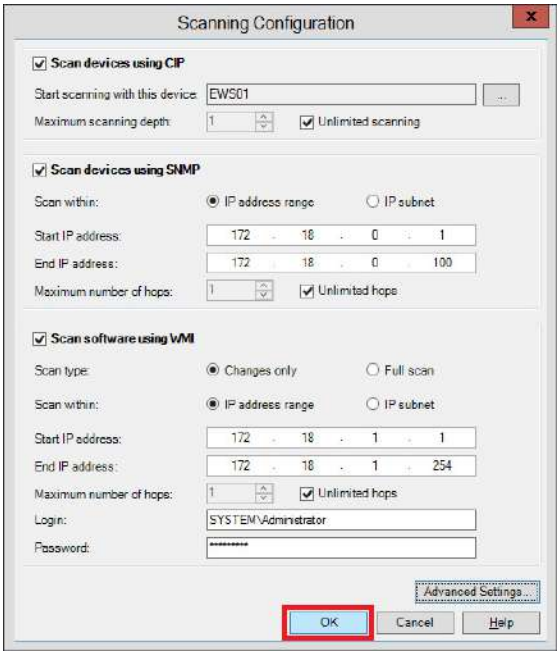
For a tutorial, see the YouTube video 'Using the Inventory Agent in FactoryTalk AssetCentre'.

1. In the FactoryTalk AssetCentre window in Design mode, move the Asset Inventory item into your asset tree.



2. Open the Asset Inventory Properties and select Scanning Configuration to define how to scan the system.

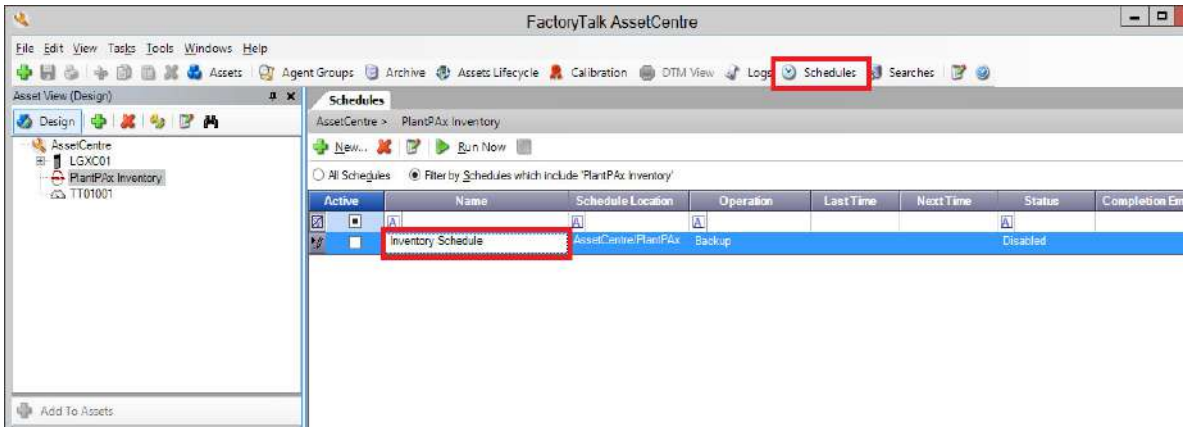
Dialog Box	Action
Scanning Configuration	Select a type of scan from the following options: **Scan devices using CIP™:** Common Industrial Protocol (CIP) scanning browses the network by using FactoryTalk® Linx drivers to return Rockwell Automation® Asset Management Program™. **Scan devices using SNMP:** Simple Network Management Protocol (SNMP) scanning browses the network for SNMP-enabled devices with a specified IP address range or IP subnet. If a device responds, the FactoryTalk AssetCentre service requests available SNMP information. **Scan software using WMI**: Windows® Management Instrumentation (WMI) scanning browses the network within the specified IP address range or IP subnet, and returns software installed on a Windows host. When you've selected a scan type, select Advanced Settings. **IMPORTANT:** Leave the default Unlimited scanning box checked to scan the entire network.
Advanced Settings	Select Community String.



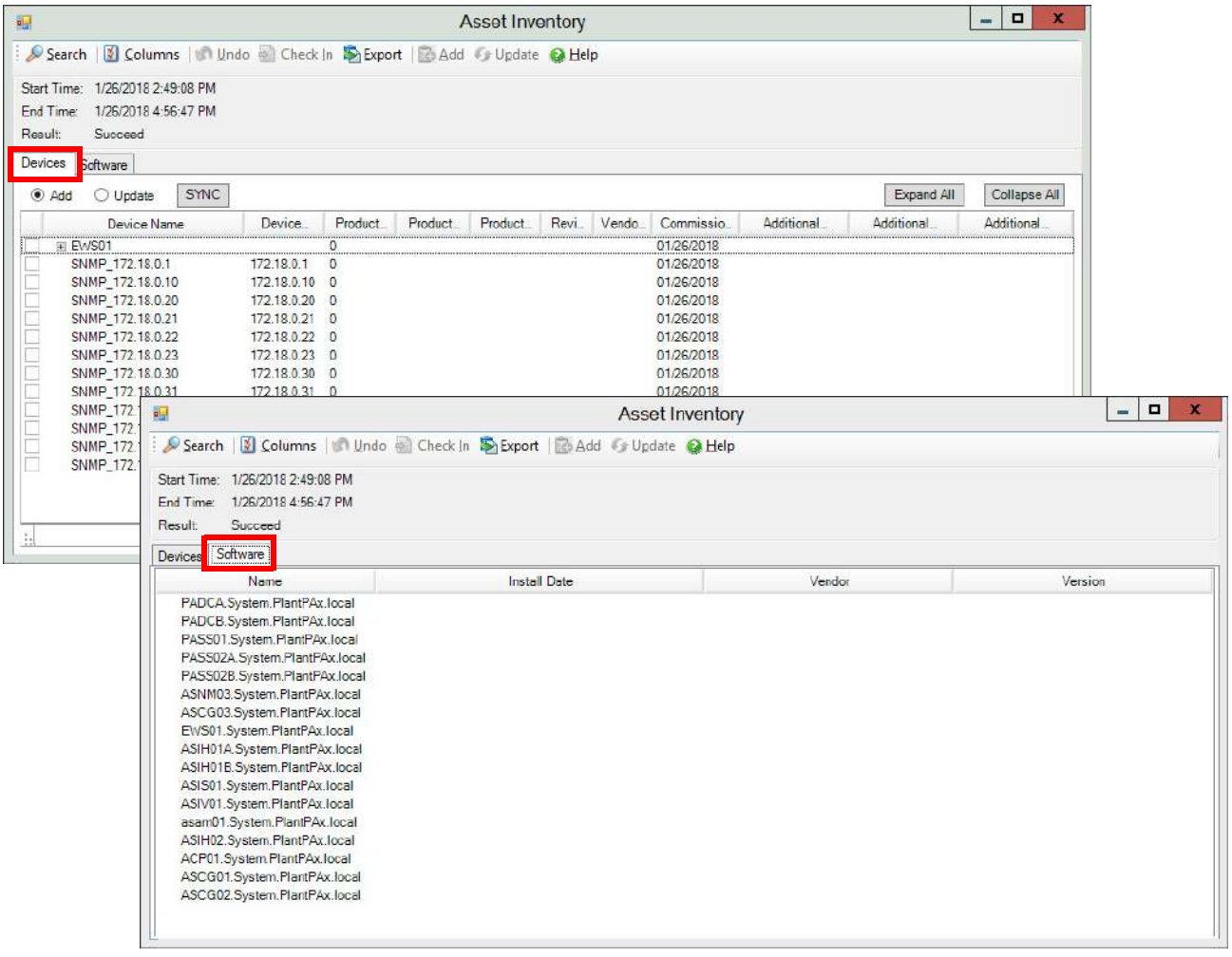
3. Select a device.

The device must have communication paths to any devices that you want to return when the Inventory Agent runs.

4. Select Schedules and create a schedule for the Asset Inventory item. When the schedule runs, an inventory list is generated.



An inventory has a list of devices and a list of software.

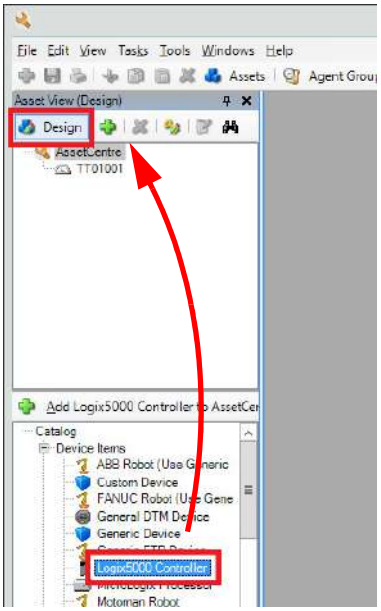


Manually Add Individual Assets

You can manually add assets.

For a tutorial, see the YouTube video 'Getting Started with FactoryTalk® AssetCentre'.

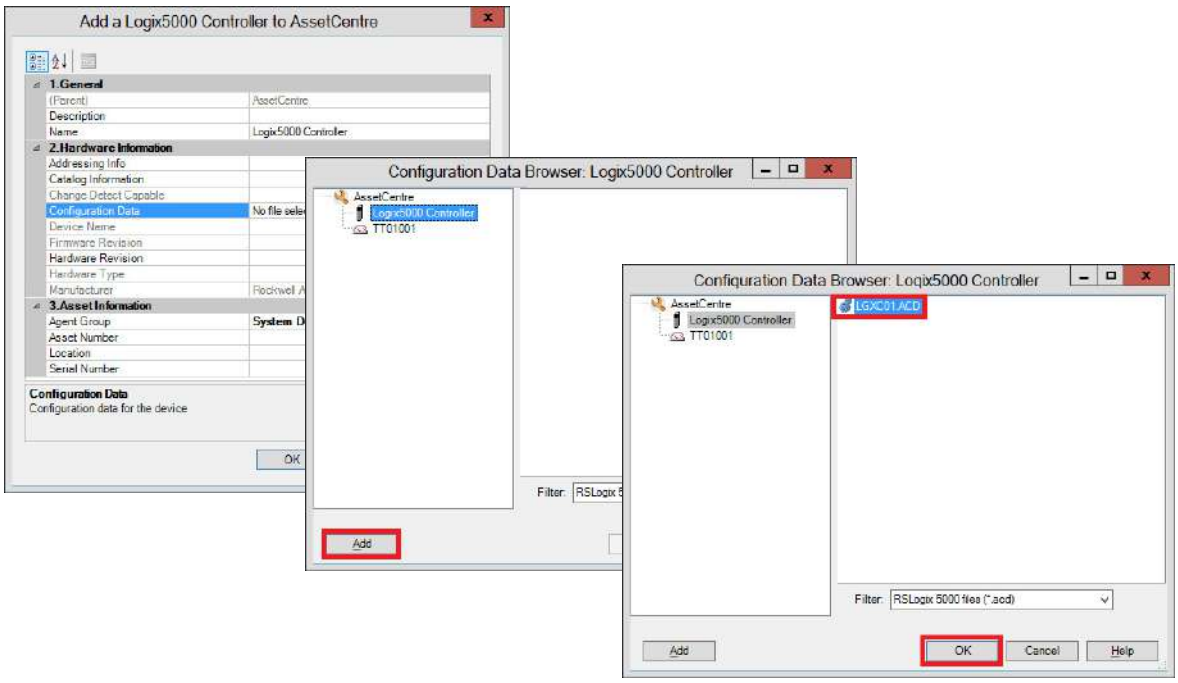
1. While in Design mode, drag-and-drop the asset into your FactoryTalk AssetCentre project.



An FactoryTalk AssetCentre dialog box appears for the asset that you are adding.

2. Select the asset to configure details.

For example, add an .ACD file for a controller.



3. For a controller, select a path to the controller by using the Addressing Info Browser ('...' ellipsis) button.

4. Name the asset.

   We recommend that you use the steps to add each of these asset types from the catalog to your inventory:

   - Controller project
   - HMI
   - Engineering workstation
   - Servers

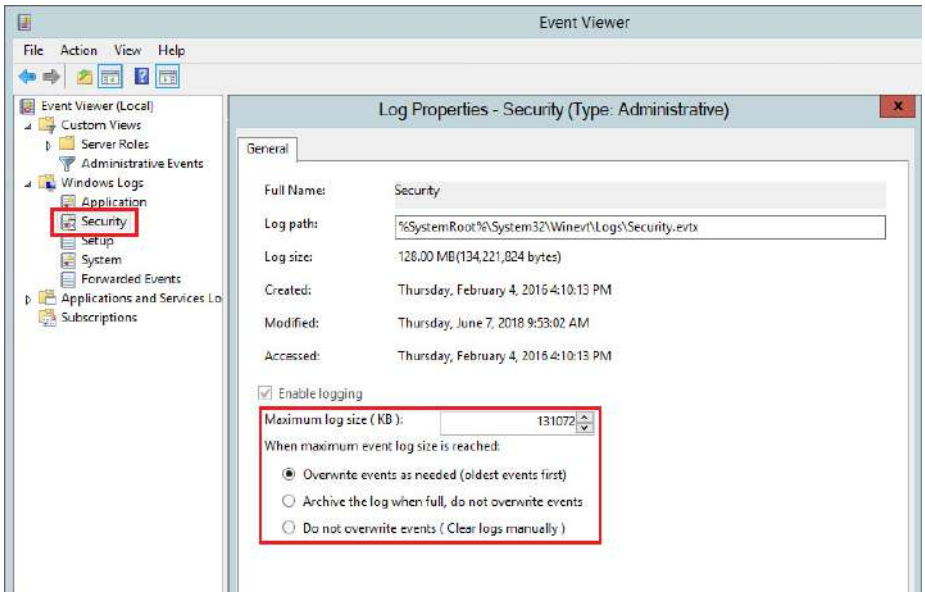
Configure Audit Logs

There are multiple logs that can be generated to capture asset data.

- Audit Log monitors FactoryTalk-enabled software products and logs user actions. For example, who was the last user to change a program.
- Diagnostic Log to monitor system health.
- Event Log to track FactoryTalk AssetCentre events, such as when a backup starts and who generates a report.

Security Audit Logs

Microsoft Windows® OS captures security audit records locally for every PlantPAx server and workstation. We recommend that you make sure the log is sized adequately to capture sufficient records to satisfy your retention policy. In Windows Event Viewer adjust the configuration of the security log according to your system requirements.

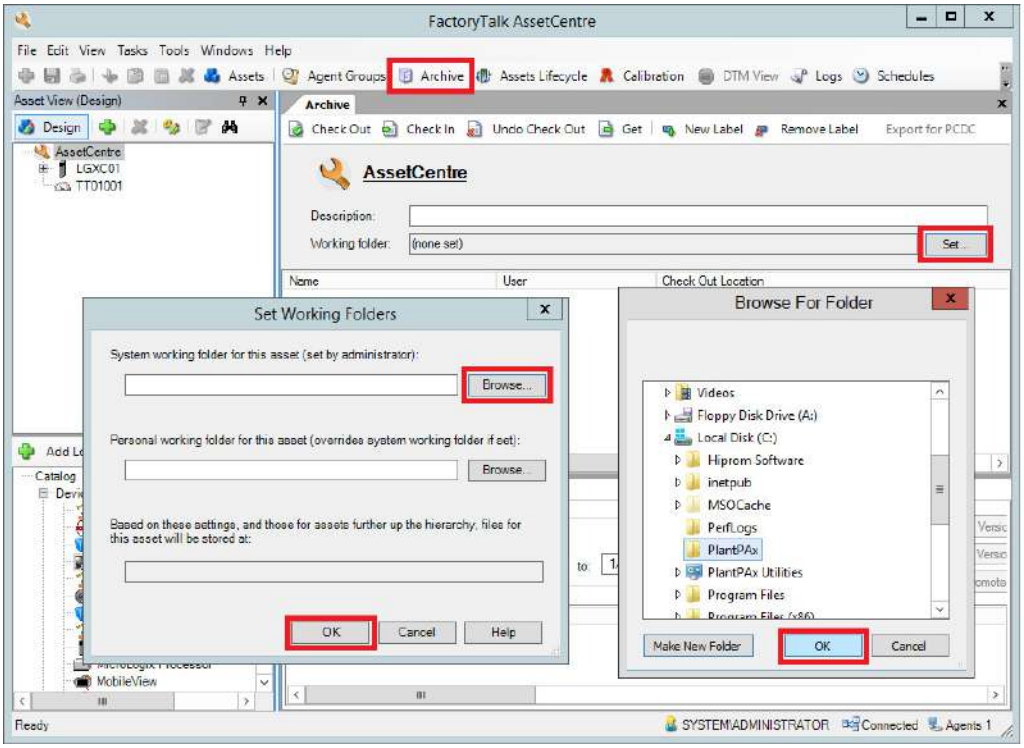


For information about how to configure secure audit logs, see Configure System Security Features User Manual, publication SECURE-UM001.

Schedule System Backups

Once assets have been added to your system, the assets can be configured from the Archive tab. From the Archive view, you can do the following:

- View the archive of current and previous versions of programs and assets.
- Set a personal working folder to hold Checked-Out files.
- Promote a specific program version to be the master.



Create a Backup Schedule

1. From the main menu of the FactoryTalk AssetCentre client dialog box, select Schedules.
2. Select New and follow the Wizard instructions at the top of the dialog boxes.

Configure Disaster Recovery

The Disaster Recovery function creates backup files from the running asset on the plant floor. The backup file is compared to the original and archived to a Master version. The Agent service performs these comparisons and can be scheduled to operate at specific times and intervals.

The Agent service can be co-located with the FactoryTalk AssetCentre server, or it can be located with another server. The Agent service performs the background actions of uploading and comparing program files and versions.

For more information about FactoryTalk AssetCentre Agents, see the resources that are listed in the table on page 183.

For a tutorial, see the YouTube video 'Introduction to FactoryTalk AssetCentre Disaster Recovery'.

Maintenance Strategy Recommendations

We suggest that you develop a plan to back up your control system configuration and process data on a regular schedule. Consider involving your IT department to develop this plan. An effective backup plan can help protect you from loss of resources and revenue.

IMPORTANT We recommend that you verify operating system or software updates on a non-production system or when the affected system components are not-active. These precautions help to prevent unexpected results.

For equipment monitoring and safety, we recommend that you follow the procedures of the manufacturer

The following table summarizes the types of backups and updates for routine and annual maintenance. The time frames are examples and can be modified based on the attributes and risk factors in your plant.

Maintenance Type Recommendations

Backups	Why?	When?	What?
Application configuration - See page 191	Roll back or file protection	Periodic	Controllers PASS servers • FactoryTalk Directory • HMI, FactoryTalk® Linx data servers • FactoryTalk® Alarms and Events servers Network switches
Data - See page 192	Archive or project protection	Periodic and on-demand	FactoryTalk® Historian FactoryTalk® Batch FactoryTalk AssetCentre

The PlantPAx system can be configured to back up control system configuration data automatically. FactoryTalk AssetCentre software stores data in a SQL server. The server stores an Archived copy of both the master files and previous file revisions in a protected database. The Archived files are available if there's a failure.

Database backups for FactoryTalk software packages (Historian, FactoryTalk AssetCentre) can occur anytime without system operation impact. We recommend that process backups be routinely scheduled so that data loss is minimized if computer issues occur.

FactoryTalk® Batch uses a SQL server for archiving journal data, storing master recipes, and material database.

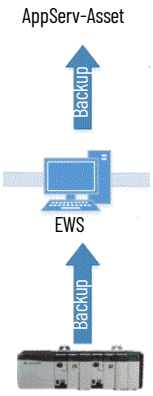
Application configurations for PlantPAx system servers and workstations are to be backed up separately and more regularly. The frequent backups mitigate the risk of configuration and application information loss between PlantPAx system backups. Frequent backups simplify the process of restoring only a portion of your application, if needed.

The following table shows examples of project files that are to be backed up regularly. Some files contain configuration scripts and collected data.

Recommended Configuration Backup

Configuration	Host Environment	Tool	Files Backed Up
Controller project file	Studio 5000® application	FactoryTalk AssetCentre Disaster Recovery	.ACD
FactoryTalk Directory	FactoryTalk® Administration Console	Distributed Application Manager	.APB
PASS servers	FactoryTalk® View Studio software		
Network switches	System network	User choice	.TXT (based)

Controller Project File

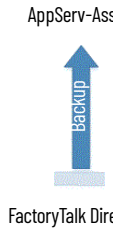


Use FactoryTalk AssetCentre software on your AppServ-Asset server to back up Logix 5000® software and Studio 5000 Logix Designer® application project files (.ACD). Logix 5000 assets are created in the FactoryTalk AssetCentre project tree for each controller and project files can be associated with those assets and checked into FactoryTalk AssetCentre software.

A schedule can be created to back up the project files at regular intervals. Use an EWS to perform check-out and check-in features to make modifications to the project file.

FactoryTalk AssetCentre software is integrated with the Logix Designer application to let you access files in the Archive without leaving the design environment. Use change tracking on project files to audit modifications.

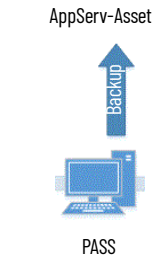
FactoryTalk Directory



Our recommendation is to back up the FactoryTalk® Directory regularly. The backup includes any FactoryTalk® Security, users, and computers, among other configurations.

The backup is contained in the output .APB file of the Distributed Application Manager, which is installed on the PASS with the FactoryTalk® View software, version 8.1 and later.

PASS Servers

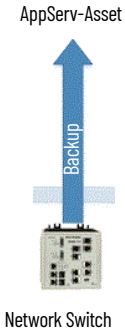


The core servers in the FactoryTalk View application need to be backed up regularly whenever changes are made. The core servers on the PASS consist of the HMI, Data, and Alarm and Event servers.

IMPORTANT FactoryTalk AssetCentre software, version 9, includes an asset for FactoryTalk View SE version 11 and later. This new asset can be created to support disaster recovery for a FactoryTalk View SE application. For details see the YouTube video 'Use FactoryTalk AssetCentre Disaster Recovery to Backup & Compare a FactoryTalk View SE application'.

A FactoryTalk AssetCentre custom asset can be created by following the procedure in Knowledgebase Answer ID 818741 'Building Custom Device assets for FactoryTalk Distributed Application Disaster Recovery'. The project servers store the output .APB file to the FactoryTalk AssetCentre server. Schedule the custom asset to run regularly.

Network Switches



If using an older version of FactoryTalk AssetCentre software, back up the network switch configuration to retain the network architecture by using a custom asset. An export of the switch configuration can be generated by using various tools, including the following:

- Studio 5000 Logix Designer application software
- Third-party applications, for example the Cisco® Network Assistant Tool
- Command-line interface
- Other desired methods of your IT department

The custom asset pulls the contents of the backup into the FactoryTalk AssetCentre server. You specify the file location in the custom asset configuration. Schedule the FactoryTalk AssetCentre software to back up the exported switch configuration regularly.

For more details about the custom device plug-in for FactoryTalk AssetCentre, see the Knowledgebase Answer ID 634595 Building Custom Devices for use with FactoryTalk AssetCentre Disaster Recovery.

Server Back up and System Restore

FactoryTalk® Historian and FactoryTalk® Batch servers produce process system data to document historical production data. The software configurations, which create the system data, must be protected along with the data.

Recommended Data Backup

Configuration	Host Environment	Tool	Files Backed Up
Historian configuration and data	FactoryTalk® Historian software	Pibackup.bat	Backup folder contents
Batch configuration and data	FactoryTalk® Batch software	Batch system files	System folder contents
FactoryTalk AssetCentre data	SQL server	SQL Management Studio	AssetCentre.BAK
SQL server data			[DBName].BAK

Consider the following when using FactoryTalk AssetCentre software:

- No single asset (verification or custom asset) is to exceed 1 GB.
- The system is not to exceed 100 assets that are scheduled in a 12-hour period for one Agent only. Increasing the number of Agents can increase the load capacity of your system.

Historian Configuration and Data

The FactoryTalk® Historian server contains historian points, configurations, and data that need to be regularly backed up. As a part of the Historian standard installation, a script file pibackup.bat is installed on the Historian server. This script is used to back up the Historian server.

The output of this tool is a folder hierarchy that contains all components necessary to back up and recover the Historian server. We suggest that you consider separating the historical data from the configuration for scheduling purposes.

The historical backup data, which is generated by FactoryTalk Historian, is stored on the Historian server. Consult with your IT department to determine the appropriate location to move and store these files outside of the AppServ-Info (Historian) server.

Batch Configuration and Data

There are multiple components of a FactoryTalk® Batch system that require a backup plan depending on the implementation of your system. See Knowledgebase Answer ID 538578 'FactoryTalk Batch: How to backup and restore a Batch configuration to a new computer'. Included are files that are to be backed up for each of the following components of a batch system:

- Batch server files
- Batch client files
- eProcedure® files
- Material manager files

The file contents of the various Batch system components need to be separated into two groups: (1) configuration or system files and (2) data files.

The configuration files are all files that comprise the Batch project, such as area models and recipes. The data files are the batch journals that are constantly created by a running Batch server.

The configuration files and data can be backed up at different intervals to a safe, IT-managed location outside of your AppServ-Batch server.

FactoryTalk AssetCentre Data

FactoryTalk AssetCentre software manages the information that is produced by each of its assets and processes the data into a SQL server. When performing a backup of FactoryTalk AssetCentre software, nothing must be done within FactoryTalk AssetCentre. To back up the FactoryTalk AssetCentre configuration and data, back up the FactoryTalk AssetCentre database in your SQL server.

For guidelines on how to back up your FactoryTalk AssetCentre database in SQL, see the Knowledgebase Answer ID 59541 Backing up and Restoring FactoryTalk AssetCentre with Microsoft® SQL Server.

SQL Server Data

The FactoryTalk® Alarms and Events History software is configured to log to a SQL database.

These databases include the following:

- For FactoryTalk Alarms and Event database, go to FactoryTalk® Administration Console and expand System>Connections>Databases. Select the database to view the information on the Alarm and Event Historian Database Properties dialog box.
- For FactoryTalk Historian Asset Framework, the SQL Database 'PIFD' contains the Asset Framework data and configuration content.

Backup Verification

We recommend that your system use a dedicated, non-production environment that is capable of accepting and validating backups. You need a strategy for how frequently the backups are validated.

System Restore

We recommend that you consider a strategy for recovering and restoring your PlantPAx system to a known secure state after a disruption or failure.

System recovery and restore to a known secure state means that all system parameters (either default or configurable) are set to secure values. If any security-critical information, such as patches, is installed after the last backup, the information must be reinstalled. For example:

- Security-related configuration settings re-established
- System documentation and operating procedures available
- Application and system software that is reinstalled and configured with secure settings
- Information from the most recent, known secure backup is loaded and the system that is fully tested and functional.

Retention Policy Considerations

There are two ways to retain data: archived records and a detailed backup policy. While archiving provides historical records, backups are typically not useful unless you can access the data for a restore. You must take the time to design a retention policy for the reuse of dated materials.

For example, a backed up .ACD file from the Studio 5000 Logix Designer application could possibly not be saved in the most current version of Studio 5000 environment. Accessing the contents of this .ACD file could be

problematic. But an archived printout of the logic that is stored in PDF format could help restore a system project.

Secure archived data and make sure that you can search for the data if requested. There are numerous reasons to archive data, including, but not limited to, the following:

- Compliance with government regulations
- Retention of production knowledge
- Reduction of backup storage footprint

Consider the following when developing a backup retention policy:

- Location – Backup information is only worthwhile if retrievable for a restore. To mitigate risk, duplicate the backup contents to an off-site location if an 'Act of God' renders the on-site copy unusable.
- Storage – The type of storage medium that is used to backup data can affect how quickly you're able to restore data. Cloud storage provides scalable backup potential and requires the least amount of on-site hardware. But, the cloud requires additional steps if the process facility isn't connected to the enterprise cloud servers. Disk mirroring can provide the fastest time to restore and smaller data loss intervals. This process can cost more than periodic backups to a hard disk drive.
- Security – The confidentiality and importance of backup information must be carefully evaluated. Limit access to the retained backup storage devices and locations to help reduce the risk of threats. Password protection and encryption can improve risk mitigation.
- Cost – The cost of backing up a process system can be justified with one application configuration restore. The time alone to re-engineer a process configuration can justify the cost of physical media and IT infrastructure. Automated backup policies can reduce time and money for IT to complete regular backups.

System Storage Rates

The following tables provide an estimate of storage usage for a PlantPAx system. Evaluate your system size and adjust appropriately according to your corporate policy.

System Operating Assumptions

Description	Small (1)	Medium(2)	Large(3)
Alarms SQL database (alarms/min according to the ISA 18.2 peak alarm rate)	20	50	100
FactoryTalk Historian Event Frames SQL database (event frames per hour)	250	500	1000
FactoryTalk AssetCentre SQL database (commands/min per PlantPAx audit log guidelines)	2	5	10
FactoryTalk Historian points	5000	10,000	20,000

(1) 3000 I/O points and 10 operator workstations
(2) 3000 I/O points and 25 operator workstations
(3) 5000 I/O points and 50 operator workstations

Storage Rates

Description	Small (1)	Medium(2)	Large(3)
Microsoft SQL server	4 GB/month	5 GB/month	9 GB/month
FactoryTalk Historian server	2 GB/month	3 GB/month	6 GB/month

(1) 3000 I/O points and 10 operator workstations
(2) 3000 I/O points and 25 operator workstations
(3) 5000 I/O points and 50 operator workstations

Historical Data

FactoryTalk® Historian SE software captures data for reports to help maximize plant-floor objectives and productivity. The software collects historical points in the system to produce analytical data. Analytical data includes process variables, trends, estimations, and statistical reporting.

For a PlantPAx® system, it's recommended to implement more than one historian server to create a collective of historian servers. A collective provides higher availability with continuous access to data during planned and unplanned outages. Adding redundant node interfaces is also recommended to send time-series data to all servers in the collective.

To streamline the FactoryTalk® Historian SE software configuration, follow this quick start. For experienced users, each step outlines requirements. For more detailed information, follow the referenced links.

Step 1: Configure Servers for a Collective

A collective is a group of historian servers that pool their data resources for high availability.

- You need two or more historian servers for a collective.
- There are requirements for initial configuration, such as the firewall, trusted connections (certificate), and security settings
- Configure PI SDK connections to the historian server on all computers that access historian data.

For more information, see Configure Servers for a Collective.

Step 2: Configure Redundant Node Interfaces

The FactoryTalk® Administration Console contains configuration for server connections and node interfaces.

- A Historian server connection specifies the name of a Historian server or Collective.
- A data collection interface is then created to collect data from an end device.
- A node interface is defined by selecting the type and computer (PASS02A in the example) hosting the interface.

- Create a common folder, on the PASS (PASS01 in the example) with the FactoryTalk® Directory, for synchronization of redundant node interfaces.
- Configure the connection between the Node Interface and the Historian server
- Configure the FactoryTalk® Live Data interfaces between the PASS servers and the Historian servers.

For more information, see Configure Redundant Node Interfaces.

Step 3: Enable Performance Monitor

An interface (PIPerfMon) is available to log system resources for health and performance.

- Create a PIPerfMon system 'user' on the domain controller.
- Configure the PIPerfMon interface after initiating on the FactoryTalk® Directory.
- Create and verify interface health points.
- Enable communication paths.

For more information, see Configure PI Performance Monitor.

Step 4: Configure PI Buffering

PI Buffering helps protect data in the event a client loses connection to the Collective.

- For added security, configure a user account on the domain controller to run the PI Buffer Subsystem service.
- Configure security mappings specifically for the user account.

For more information, see Configure PI Buffering.

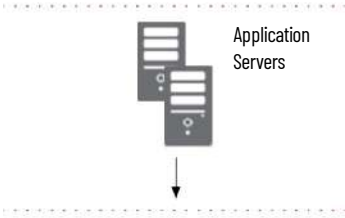
Step 5: Configure Data Collection

FactoryTalk Historian software uses historical points (tags) in the system to produce analytical data for reporting.

- Create or Import Digital States.
- Create Historian Points.
- Define digital historical points.
- Configure Asset Framework.
- Finds system faults.
- Generate reports in PI Builder.
- Configure tags with the PlantPAx® Configuration Tool.

For more information, see Configure Historian Data Collection.

Prerequisites



Following the System Workflow, configure application servers.

A historian application in a PlantPAx system requires:

- Domain controller
- Process Automation System Server (PASS) hosting the FactoryTalk® Directory (PASS01)
- Process Automation System Servers (PASS) for node interfaces (PASS02A, PASS02B)
- Engineering Workstation (EWS)
- Operator Workstation (OWS)
- SQL standard or SQL Express database server
- Asset Framework server

When you deploy a FactoryTalk Historian application in a PlantPAx system:

- Install FactoryTalk Historian servers as a collective.
- Configure a Performance Monitor interface.

The following software must be available:

- FactoryTalk Historian SE Server
- FactoryTalk Historian Asset Framework Server
- FactoryTalk Historian Asset Framework SQL database
- PI Builder Excel® add-in

Your must be familiar with the following utilities:

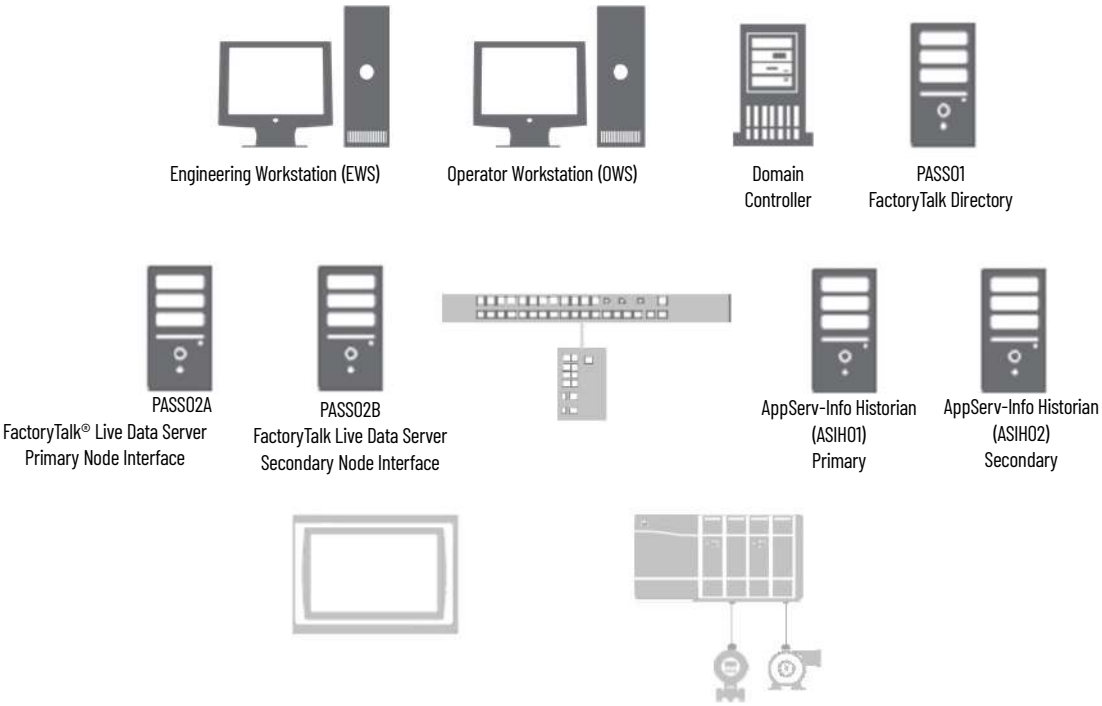
- PI SDK – An object-oriented library that is designed for customizing applications
- Powershell – Command-line shell and scripting language.

For more information, see this additional resource.

Resource	Description
FactoryTalk Historian SE 7.00 Installation and Configuration Guide, publication HSE-IN025	Installation, configuration, and troubleshooting of FactoryTalk Historian Site Edition software.

Required PlantPAx Elements

Configuring historical data collection requires access to the following equipment. All equipment must be physically installed before using this document.



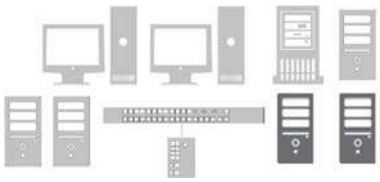
Historical Data

In a PlantPAx system, the FactoryTalk Historian SE software collects, stores, and manages data. The software includes these hardware and software components:

- **Data Sources** - Plant floor devices and instruments that generate data, typically controllers. Other Data Sources can include external databases.
- **Historian SE Interfaces** - The FactoryTalk Historian node interface enables process data to be passed between a FactoryTalk® Live Data Interface (for example, FactoryTalk® Linx) and a FactoryTalk Historian server. Each instance of the interface can provide data to a single FactoryTalk Historian server or collective.
- **Historian SE Server** - Compresses and stores the collected data and acts as a data server for Microsoft® Windows®-based clients applications. It's also possible to use the Historian SE server to interact with data that is stored in external systems.
- **Historian SE Clients** - Microsoft Windows-based applications that are used by plant personnel to visualize the Historian SE data.
- **Historian Asset Framework** - Asset Framework replaces the Historian module database (MDB) with a Microsoft SQL server database for improved scripting and reporting.

Configure Servers for a Collective

A collective is a configuration of multiple servers that act as a logical server in your Historian database to provide high availability (HA), disaster recovery, load distribution, and increased scalability. Each server in a collective is called a member of the collective. When the primary member in a collective becomes unavailable, a secondary collective member continues to collect and provide data access to your Historian clients.



ASIH01
ASIH02

Create Firewall Rule for Historian Servers

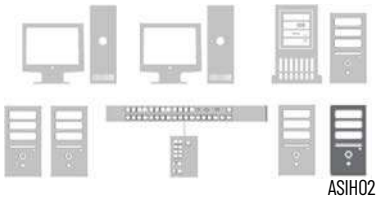
To create a server collective on computers that have the Windows Firewall turned on, you must manually open the TCP 445 port between the two computers. Perform this section on both the primary and secondary Historian servers.

1. Go to Control Panel > Windows Firewall settings on the Historian Server.
2. In the Advanced Settings, select Inbound Rules and create a New Rule.

   For the new rule, specify the following:

On This Page	Configure
Rule Type	Select Port
Protocol and Ports	Configure Specific Local TCP Port as 445
Action	Allow the connection
Profile	Apply the rule to the Domain, Private, and Public
Name	Type a name for this rule (Collective Connection in the example)

Change the Historian Server Identification


ASIH02

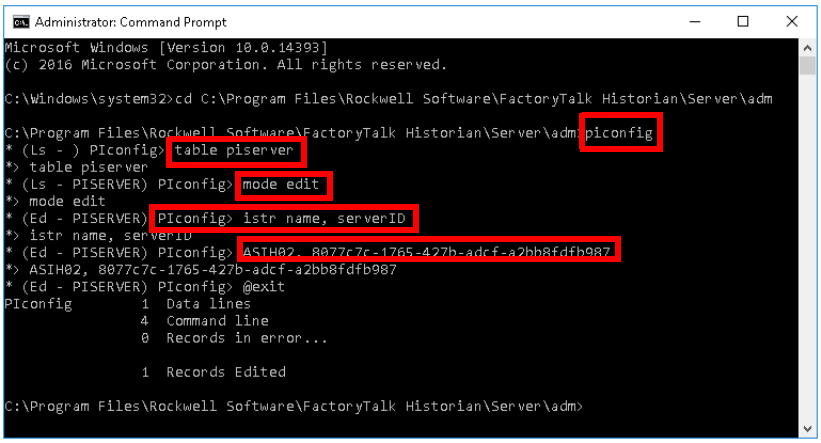
IMPORTANT When planning to use a collection of Historian servers, serverIDs must be unique. You must change the serverID on any additional servers, particularly if the server is cloned or sourced from a virtual template.

To change a server ID, complete these steps.

1. Go to c:\Program Files\Rockwell Software®\FactoryTalk Historian \Server\adm
2. Enter 'cmd' in the address bar to open a command prompt window in this directory.
3. Enter the following commands.

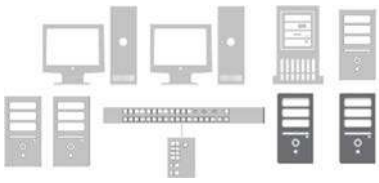
Command	Purpose
`piconfig`	Open the command-line administration tool for the PI Data Archive
`table piserver`	Open the piserver table
`mode edit`	Set the required mode of operation to edit
`istr name, serverID`	Allows you to edit the hostname and serverID
`<hostname>, <new serverID>`	Specify the new server name. <*hostname*> = hostname of the Historian server <*new serverID*> = new server ID
`@exit`	Saves the information and exits the tool

The serverID is a unique identifier (UID), a 32-character string representing each Historian server identification. You can make up your own arbitrary string.



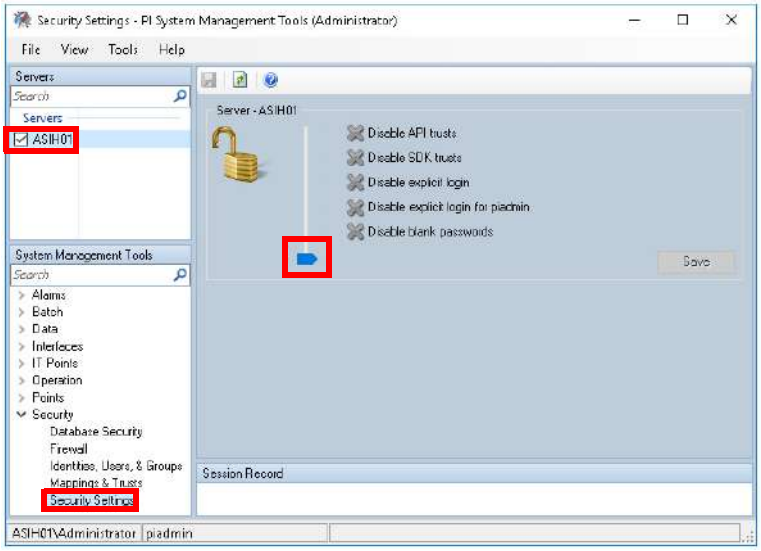
4. The next time you access the secondary Historian server, a Server ID mismatch prompt appears. Select 'Accept the New ID' to continue.

Set Initial Security Settings


ASIH01
ASIH02

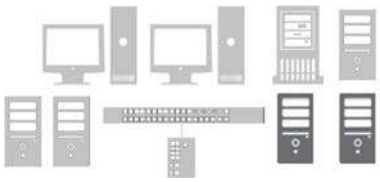
For any Historian server that is going to join a Collective, security settings must be considered for each initial connection. To simplify the connection process, reduce the security levels of both the primary and secondary Historian servers. After the initial connection, the security levels can be modified as needed.

1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools.
2. Select the server in the Collectives and Servers section.
3. In the System Management Tools section, select Security > Security Settings.
4. Set the slider to its lowest point and click Save.



5. Repeat the settings for the secondary server.
6. For the security setting changes to take effect, restart the servers.

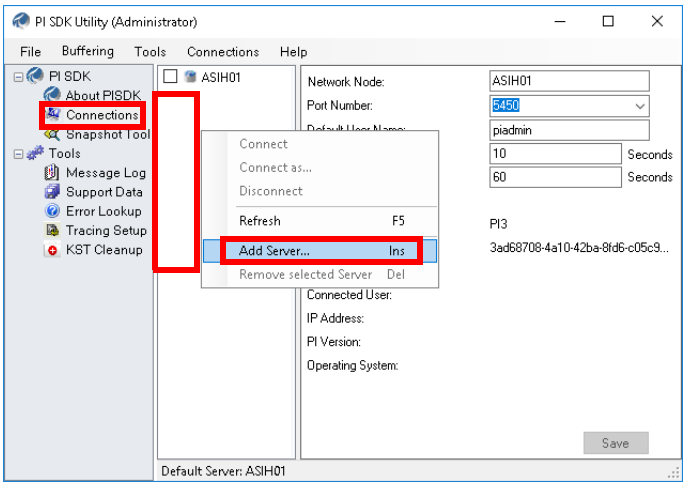
Create Connections Between Historian Servers



ASIH01
ASIH02

The PI SDK Utility is used to create the connection between the Historian servers. This action is required on both servers before creating a collective.

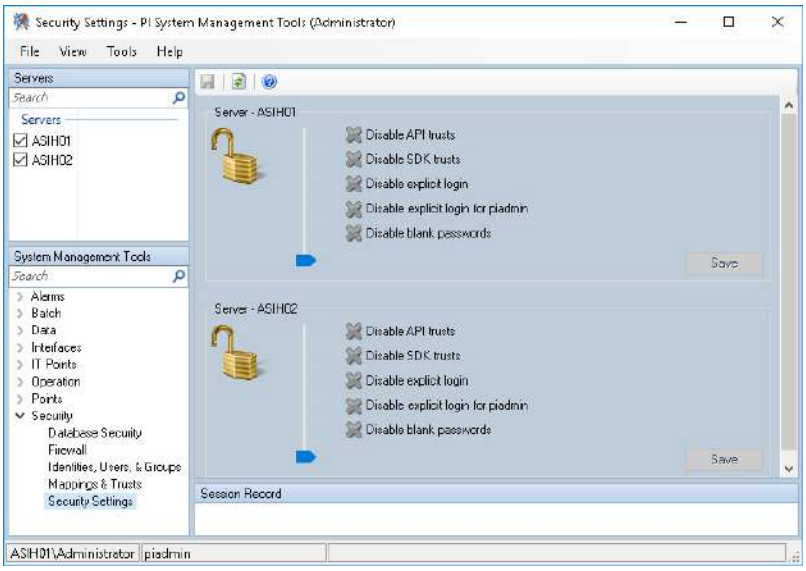
1. Go to Rockwell Software > FactoryTalk Historian SE > FactoryTalk Historian SE System > PISDK Utility.
2. Select Connections and then right-click on the empty area next to the servers.
3. Select Add Server.



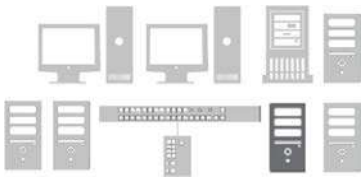
4. Enter the server name in the Network Path dialog box and accept the rest of the default settings.

5. Remove any servers that aren't necessary.
6. To verify the connections, go to Security Settings > PI System Management Tools (Administrator.)

   This example shows servers ASIH01 and ASIH02.



Create the Historian Collective

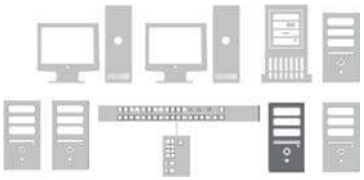


Now that the servers are configured, you can create a Collective by using the PI Collective Manager.

Go to Rockwell Software > FactoryTalk Historian SE> FactoryTalk Historian SE System > PI Collective Manager and complete these steps:

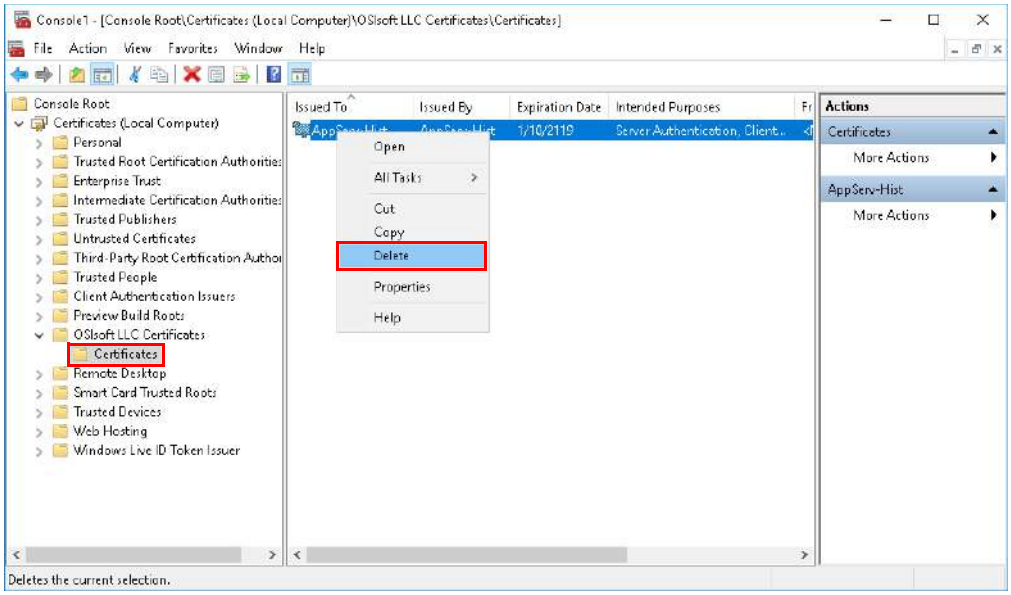
On this Dialog Box	Action
Create New Collective Initial Page	• Select I have verified my backups are valid • Select I have verified my PI interface servers configuration
Create New Collective - Existing or New Primary	Select a newly installed PI server
Create New Collective - Select Primary and Collective name	Select the Collective Primary server and define the properties.
Create New Collective - Select Secondary Servers	Select the Collective Primary server and define the properties.
Create New Collective - Select Archives	• Accept the default number of archives to be copies • Accept the default location for the temporary backup
Create New Collective - Verify Selections	Verify the information
Create New Collective - Conversion Progress	Verify the conversion progress is completed
Server ID Mismatch	Select Accept the new ID
Create New Collective - Finished	Acknowledge the creation of the collective

Delete the Default Security Certificate


ASIH01

Historian Collectives support certificate-based authentication for each server. To verify that the system uses a valid security certificate, start by deleting the default or cloned certificate on the Primary Historian server. This is a required step if the server was cloned or sourced from a virtual template.

1. To access Certificate Manager, click Start and type certlm.msc in the search field.
2. Click Enter.
3. Expand the Certificates folder > OSIsoft LLC Certificates > Certificates.
4. Delete the default certificate.



Generate a New Security Certificate

Code that is provided by OSIsoft generates a new security certificate, that afterwards is to be imported on all other Historian servers in the collective to authenticate.

IMPORTANT Due to the electronic formatting of this user manual, the code may require format corrections if copied from here. Also note the <PlantPAx AppServ-HIST Virtual Template 5.0 VL> virtual template contains properly formatted code on the user desktop.

1. On the Primary Historian server, copy the script as shown and paste into Notepad.

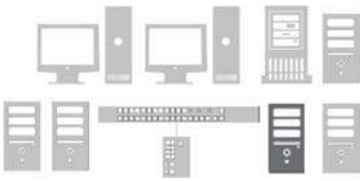
```
$CertStorePathName = "Cert:\LocalMachine\OSIsoft LLC Certificates"

if(!(Test-Path $CertStorePathName))

{
   New-Item -Path $CertStorePathName

}
if( (Get-ChildItem -Path $CertStorePathName | measure).count -eq 0)

{
   $myFQDN=(Get-WmiObject win32_computersystem).DNSHostName+"."+(Get-WmiObject win32_computersystem).Domain

   $DNSName = @($myFQDN)

   #$NewCert = New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -FriendlyName $myFQDN $DNSName -Provider "Microsoft Enhanced RSA and AES
Cryptographic Provider" -HashAlgorithm "SHA256"

   $NewCert = New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName $DNSName -NotAfter $(Get-Date).AddYears(100)

   Move-Item $NewCert.PSPath -Destination $CertStorePathName

}
else

{
   Write-Host("Invalid number of certs detected in OSIsoft LLC certificate store -- please ensure there are no certificates already configured in " + $CertStorePathName)

}
```

2. Use Notepad to remove any new lines, where contiguous code is wrapped.

   You can backspace new lines to rejoin the prior code statements. For example:

3. After the scripting code is realigned, launch an administrative PowerShell window.
4. Copy the script from Notepad and paste into PowerShell.
5. Click Enter to generate a security certificate.

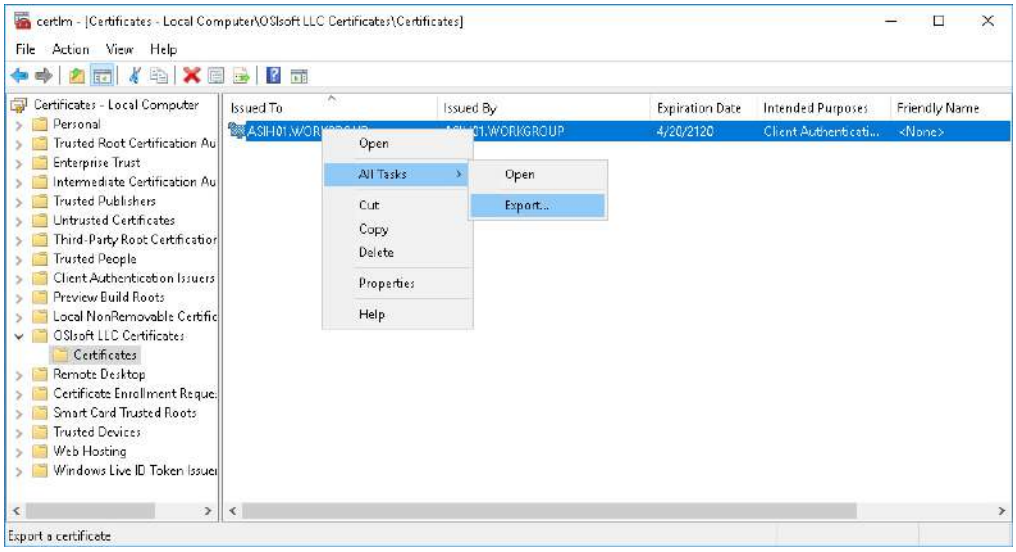
6. Return to the MMC window and refresh the window. To verify that the OSIsoft certificate was recreated. The name should represent the computer name and domain.


ASIH01

Export the Security Certificate

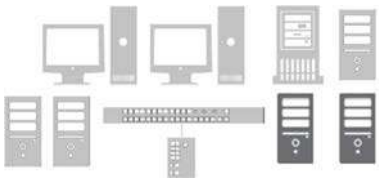
To transfer the new security certificate to all other Historian servers in the Collective, the certificate must be exported as a PFX file.

1. While still on the Primary Historian server, in the MMC window, select the certificate that you've generated and select All Tasks > Export.



2. From the Certificate Export Wizard, complete these steps.

On these Wizard Boxes	Action
Welcome window	• Select Next • Select Yes, export the private key and select Next • Leave defaults, and click Next
Security	• Type a password, confirm, and click Next
File to Export	• Click Browse and type a name for the storage location on your computer • Click Next • Select a file name and click Finish



ASIH01
ASIH02

Import the Security Certificate

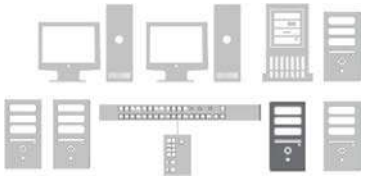
The new security certificate must be imported on all other Historian servers in the Collective before it can synchronize. The import can be done using either the PI Collective Manager software or the Windows Certificate Manager.

For each Historian server, you must copy the new security certificate PFX file first before using one of the following procedures. From the PI Collective Manager:

1. Select the Historian server and select Import Certificate.

2. Browse for your PFX file.
3. Open the certificate and provide the password for this certificate to import the certificate.

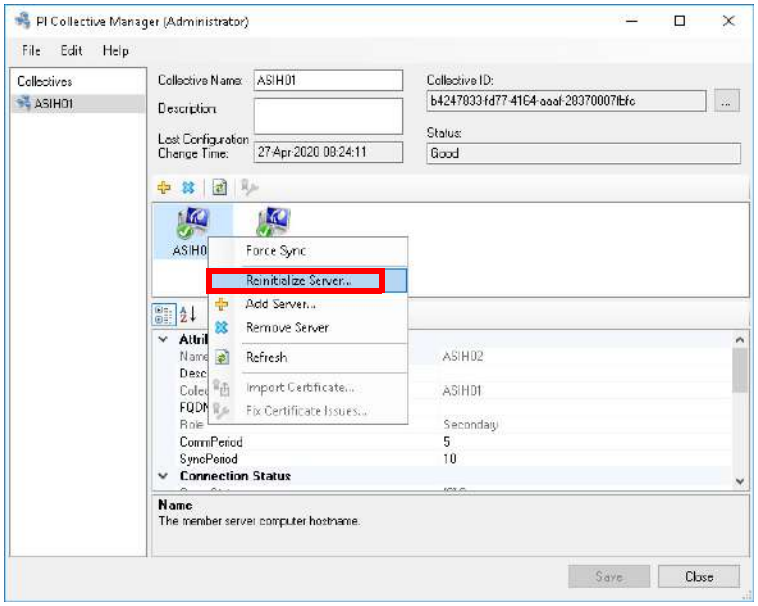
Reinitialize the Secondary Server



ASIH01

Perform this task from the Primary server to synchronize the certificates of any other Historian servers in the collective.

1. From the Collective Manager, select the Secondary server.
2. Select Reinitialize Server.

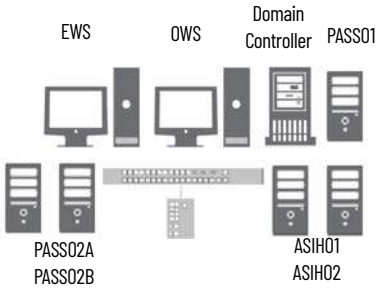


3. From the Archives window, click Next.
4. Verify the backup location and click Next.
5. When the sync process completes, click Finish.
6. If servers show green check boxes, skip step 8, and proceed to Connect another Computer to Historian Server.
7. If the synchronization fails, verify all firewall settings, certificates, and matched server or collective IDs. Then, try again.

   If sync problems remain, contact Technical Support.

Client to Server Connections

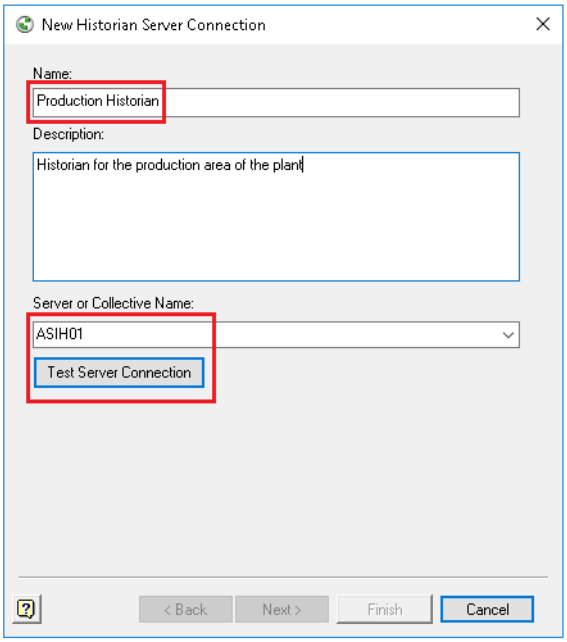
For all servers and workstations that require access to Historian data, use the PI SDK Utility to add a connection to a Historian server or Collective of servers. This includes the PASS servers (PASS01, PASS02A & PASS02B), EWS, and OWS workstations.



Connect another Computer to Historian Server

For each computer that requires a connection to the collective, complete these steps:

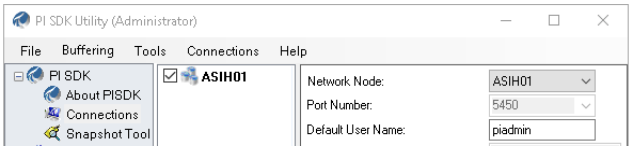
1. Go to Rockwell Software > FactoryTalk Historian SE > FactoryTalk Historian SE System > PISDKUtility.
2. Select Connections and then right-click on the empty area next to the servers to add a new server.
3. Maintain the default connection name of 'Production Historian' for library object reference, then select the Server or Collective Name and click Test Server Connection.



If you're using a collective, enter the primary server.

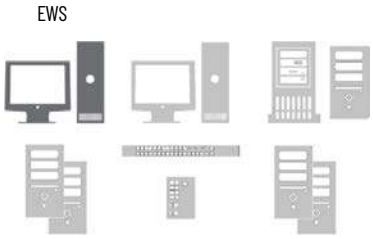
4. Select the box next to the new server.

   The server appears in the middle of the utility for a successful connection.



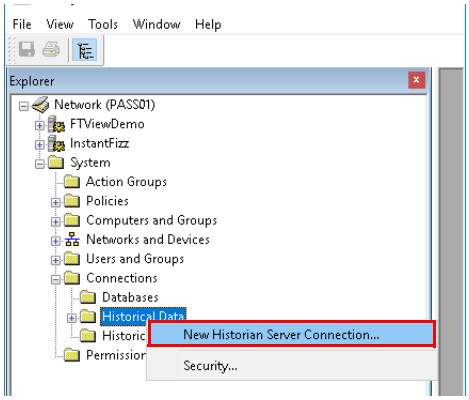
5. Remove any server connections that aren't necessary.

Historian to FactoryTalk Directory Connection



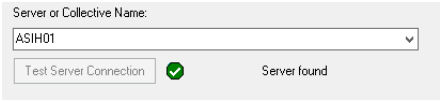
Use the FactoryTalk® Administration Console to add the FactoryTalk Historian server connection to the FactoryTalk Directory.

1. Go to Rockwell Software > FactoryTalk Administration Console and select 'Network' for the directory you want to use.
2. Go to Network > System > Connections > Historical Data and select New Historian Server Connection.



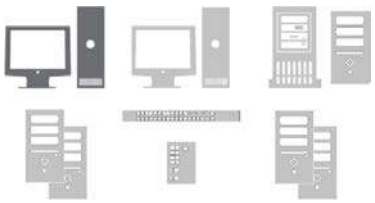
3. Select the Server or Collective Name and click Test Server Connection.

   If the connection is good, a green check mark appears along with the text 'Server Found.'



4. In the FactoryTalk Administration Console, go to Network > System > Connections > Historical Data > Production Historian and choose Properties.
5. Select the Licensing tab and enter how many licenses are stored on the server.
   - If one license is stored locally in each collective server, enter '1' in the Assigned column.
   - If both activation licenses are on the activation server, enter '2' in the Assigned column

EWS



Create a Data Collection Interface

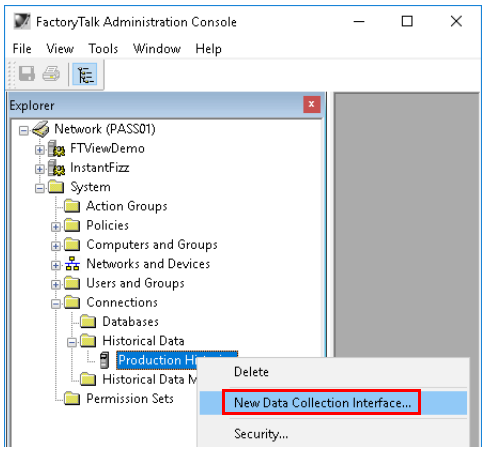
A data collection interface is used to collect data (tags) from data sources, such as Logix 5000™ controllers, and pass it to the FactoryTalk Historian server or collective.

The FactoryTalk Administration Console is used to create and configure the data collection interface.

1. Using an EWS, launch the FactoryTalk Administration Console and expand Historian server connection.

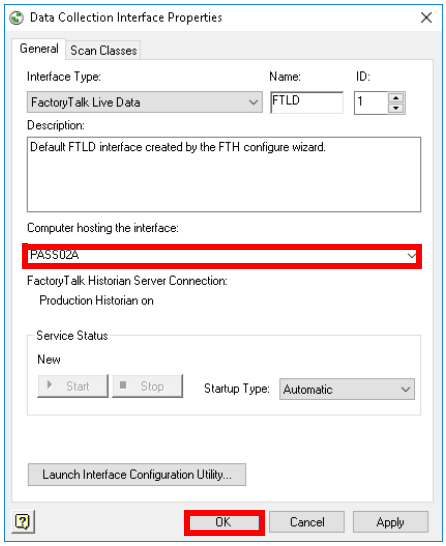
   When a new FactoryTalk Historian server is added, a default node interface is created along with a name FTLD and ID 1 (FTLD1).

2. Delete the default node interface FTLD1.
3. Select the Historian server connection and select New Data Collection Interface.



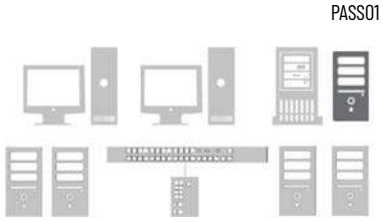
4. Select the Interface Type: (FactoryTalk Live Data), Name: FTLD and ID: 1 and choose the computer hosting the interface.

   For example (PASS02A) where the remote FactoryTalk® Linx data server runs.

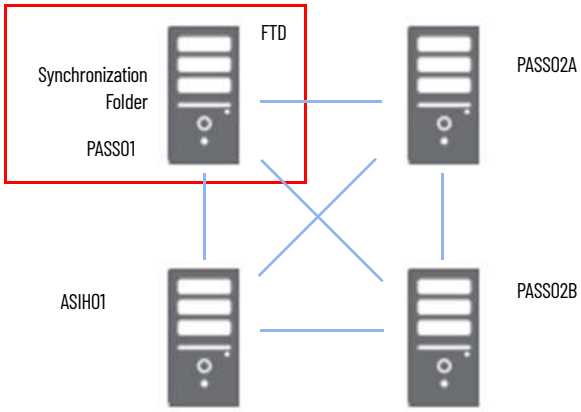


IMPORTANT When redundant node interfaces exist (PASS02A & PASS02B), only one data collection interface is required, and it references the primary (PASS02A) node interface.

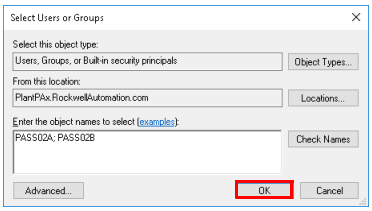
Create a Synchronization Path for Redundant Node Interfaces



A common folder is used for files that are used for handshaking and redundancy. This folder is created on the PASS server that hosts the FactoryTalk Directory.

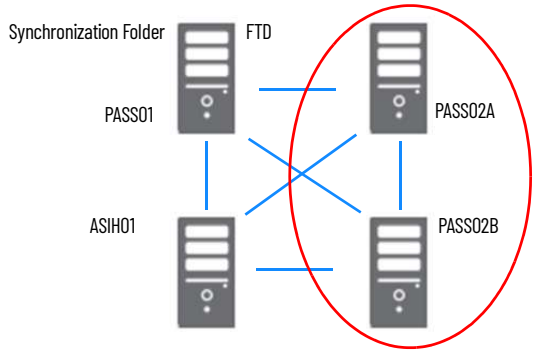


1. On the PASS01, create a folder on Local Disk (C:) named FTHSE_Failover.
2. Specify these properties for the folder.

From this Location	Configure
Sharing Tab	Advanced Sharing
Advanced Sharing	• Select Share this folder • Select Permissions
Permissions for FTHSE_Failover	Add the group Everyone
Select Users, Computers, Service Accounts, or Groups	Select Object Types
Object Types	Select Computers
Select Users, Computers, Service Accounts, or Groups	Enter the PASS servers used as Node Interfaces as the object names to select 
Permissions for FTHSE_Failover	Allow Full Control, Change, and Read permissions for all Node Interface servers

Configure Redundant Node Interfaces

A FactoryTalk Historian node interface enables process data to be passed between a FactoryTalk Live Data server and a FactoryTalk Historian server.



A PlantPAx system with redundant data servers requires configuration of the node interface on the primary and secondary servers (PASS02A and PASS02B).

The PI Configuration Utility (PI ICU) is an application that aids in system management by consolidating the setup and configuration options of each node interface. PI ICU allows you to:

- Configure all interface parameters
- Manage, start and stop interface service
- View and configure interface service dependencies
- Configure and run buffering
- Configures the Universal Interface (UniInt)

UniInt provides generic functions that are 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.

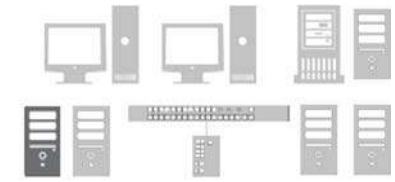
Phase 2 UniInt Failover uses a shared file to synchronize failover operations and provides for hot, warm, or cold failover. The Phase 2 hot failover configuration provides a no data loss solution for a single point of failure similar to Phase 1.

IMPORTANT In this section, only Phase 2 UniInt Failover is addressed.

The UniInt failover scheme requires the data source to 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.



PASS02A

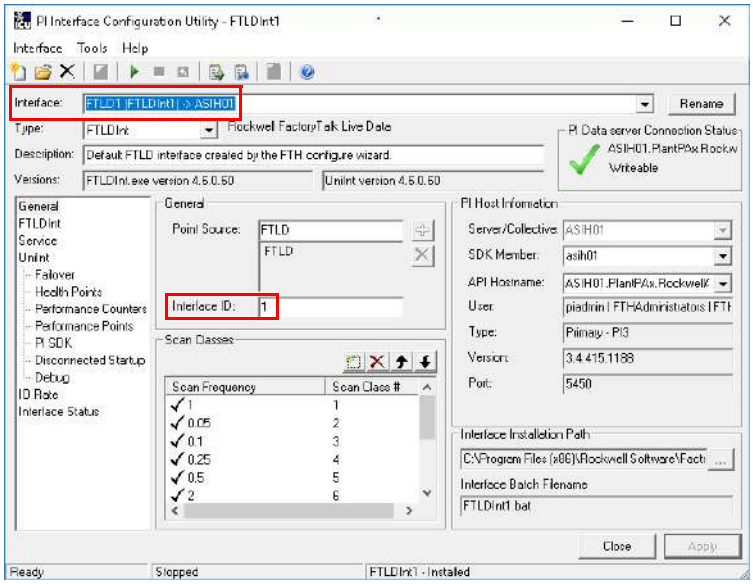
Configure a FactoryTalk Live Data Primary Interface

The primary interface goes on PASS02A and connects data servers to the historian database.

1. Go to Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility and select the interface.

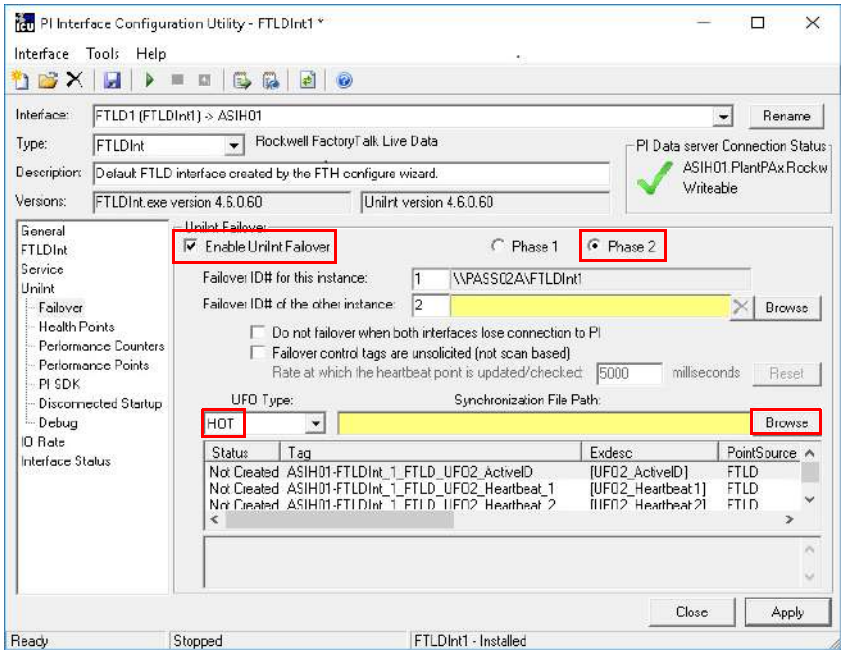
   For example, select 'FTLDint1 (FTLDInt1)->ASIH01.'

2. If the Interface ID isn't already '1', change it to '1'.

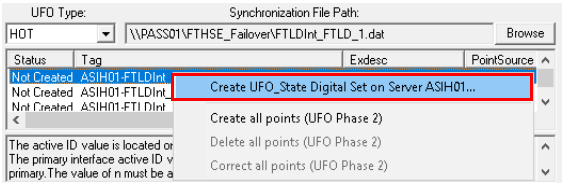


3. Select Service and do one of the following:
   - If prompted, select Yes. The PI ICU sets the PIBufss service to be a dependency of FTLDint1.
   - If you aren't prompted, you must scroll down the Services list and set the PIBufss service to be a dependency of FTLDint1.
4. Go to UniInit > Failover and select the following:

Location	Action
UniInit Failover	Select Enable UniInit Failover and Phase 2
UFO Type	HOT
Synchronization File Path	Path = Network > pass01 > FTHSE_Failover directory (that was created in the previous section)



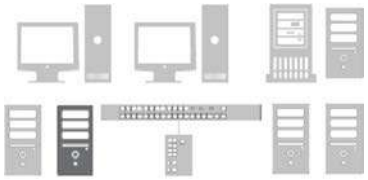
5. Right-click the tag area and select 'Create UFO_State Digital Set on Server ASIH01'.



6. In the tag area, select ‘Create all points (UFO Phase 2')
7. When the status for FTLDInt1_UFO2_ActionID tags changes to 'Created', select Apply.

   The 'UniInt Failover’ configuration isn’t complete until the 'Other' interface is selected' message appears.

Configure a FactoryTalk Live Data Secondary Interface



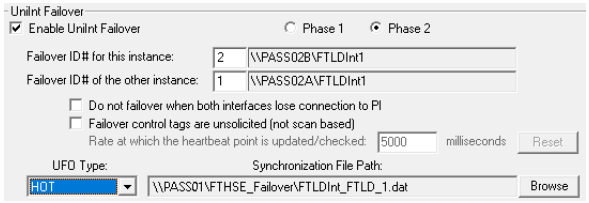
PASS02B

The secondary interface goes on PASS02B and connects data servers to the historian database. The configuration is provided in a .BAT file.

1. Go to Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility.
2. Select the folder symbol to create an interface instance from a .BAT file and enter this information.

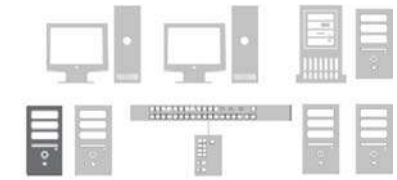
From Location	Action
Open Interface Configuration File Dialog Box	Select the LDInterface folder
Interfaces > LDInterface directory	Select C:\Program Files (x86)\Rockwell Software\FactoryTalk Historian\PIPC\Interfaces\LDInterface\ directory
The Select Host PI Data server/collective dialog box	Select the hose PI Data server/collective and the collective member
Service > Service Configuration >Display name	Enter FTLD1
General > General > Interface ID	Enter 1
UniInit > Failover > UniInit Failover	Select Enable UniInit Failover Select Phase 2
UniInit > Failover > UFO Type	Select HOT
UniInit > Failover > Synchronization File Path	Path = Network > pass01 > FTHSE_Failover
UniInit > Failover > UniInit Failover > Failover ID # for this instance	Enter 2
UniInit > Failover > UniInit Failover > Failover ID # for the other instance	Enter 1 Select the interface file (FTLDInt_FTLD.bat.bak) on the secondary server
Synchronize UFO settings dialog box	Select yes to synchronize the UFO settings

3. The failover and synchronization information appears in the respective fields.



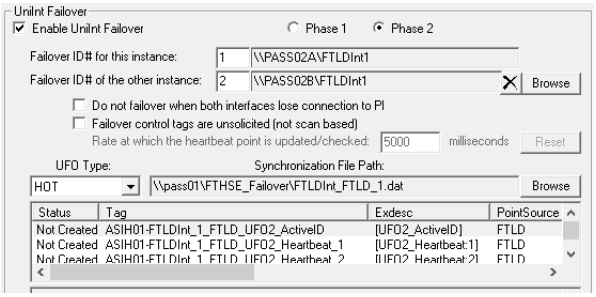
4. In the PI Interface Configuration Utility window, select Apply.

Return to the Primary PASS (PASS02A)

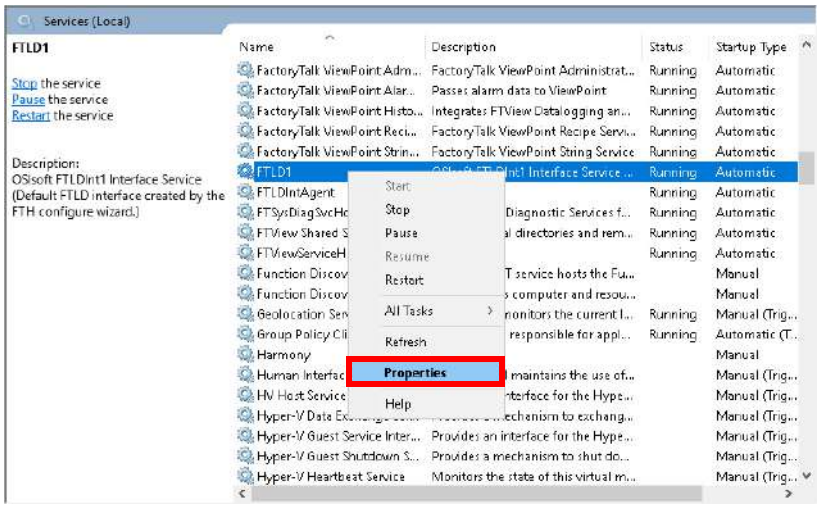


PASS02A

1. Select the interface path for the second interface.



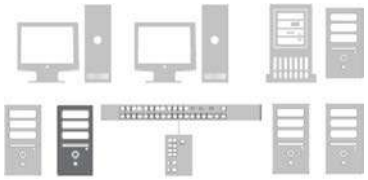
2. Go to Control Panel > Administration Tools > Services and select Properties for FTLD1.



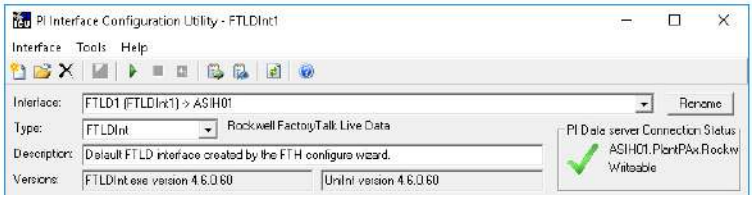
3. From the Log On tab, Select Log on as Local System Account.
4. In the PI Interface Configuration Utility window, select Apply and Play  to start the primary service (if not already running).

5. Select Yes if asked 'Would you like ICU to start this service for you?'

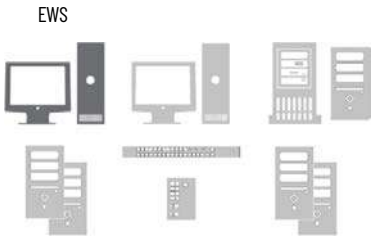
Return to the Secondary PASS (PASS02B).



1. Select the Interface that was created earlier and click Play to start the secondary service.



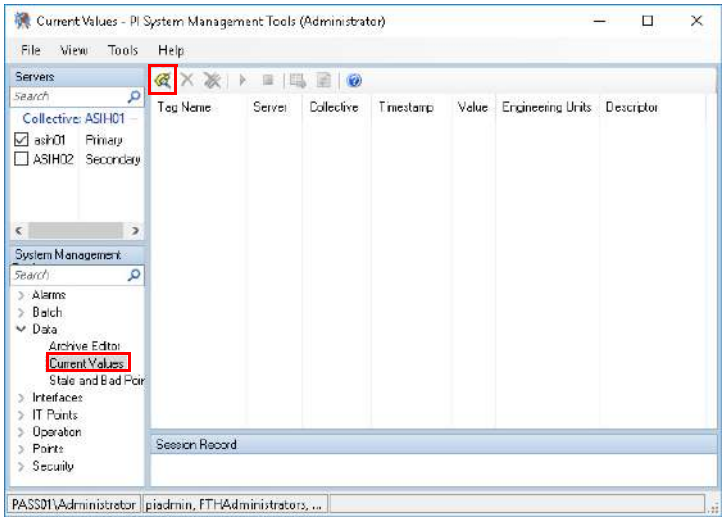
2. Select Yes if asked 'Would you like ICU to start this service for you?'



Confirm Unit Failover Diagnostics

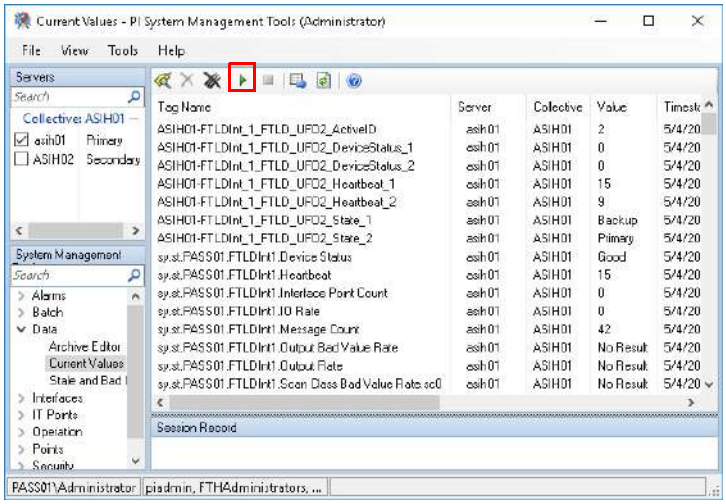
From an EWS, test and confirm the failover diagnostics from the Historian server.

1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools.
2. Select Data > Current Values and select the Tag Search icon.



From Location	Action
Tag Mask field	Enter *FTLD*
Tag Search Dialog Box	Select all tags

3. Select Play to see the online status.



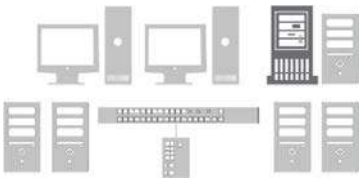
Configure PI Performance Monitor

The Windows Performance Monitor (PerfMon) is a powerful operating system tool to monitor the health of resource usage and processes on a computer.

The PI Interface for Performance Monitor (PIPerfMon) collects performance counter data from Windows performance data providers, local and remote, and sends this data to the Historian server. It's **recommended** to use PIPerfMon in a PlantPAx system.

Create Domain User for PIPerfMon Service

Domain Controller

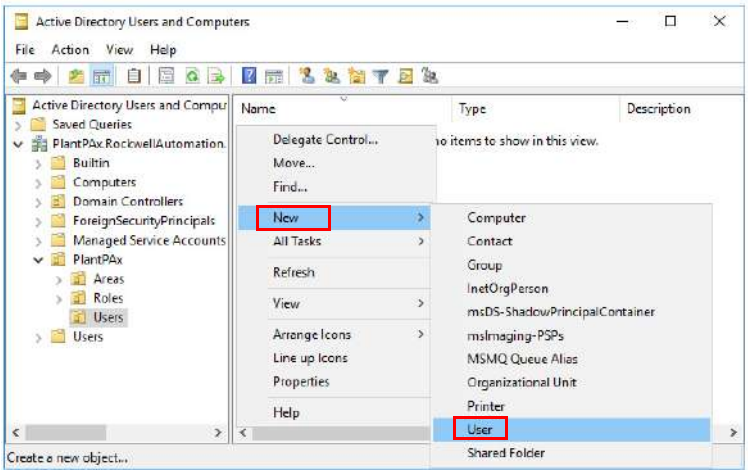


The PIPerfMon service defaults to running in a local account. For PlantPAx systems with a domain, it's recommended running the PIPerfMon service in a domain account. This enhances security and provides access to obtain data for a performance capture among other domain computers.

The domain user account for PIPerfMon service must be created on the domain controller. It's a user account with privileges to run the service on other computers within the domain.

1. From the Server Manager utility on the domain controller, select Tools > Active Directory Users and Computers.

2. Add a new user to the Managed Service Accounts.

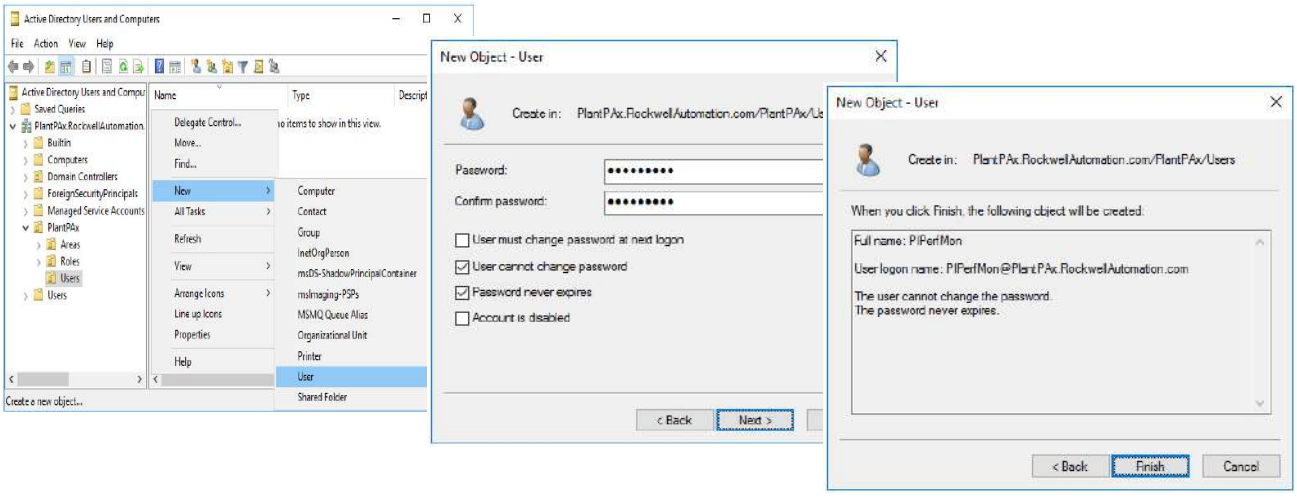


3. Specify these properties for the User.

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
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.

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).

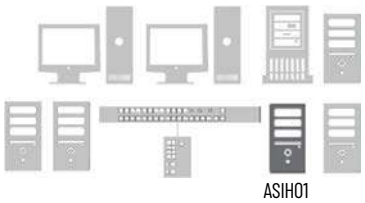
4. Create a password with the following conditions:
   - User cannot change password
   - Password never expires



5. Assign the PIPerfMon profile as a member of Performance Monitor User.

Configure the PIPerfMon Interface

To use PIPerfMon, you must configure an interface name and a points value within the FactoryTalk Directory. The points are the limit that 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.

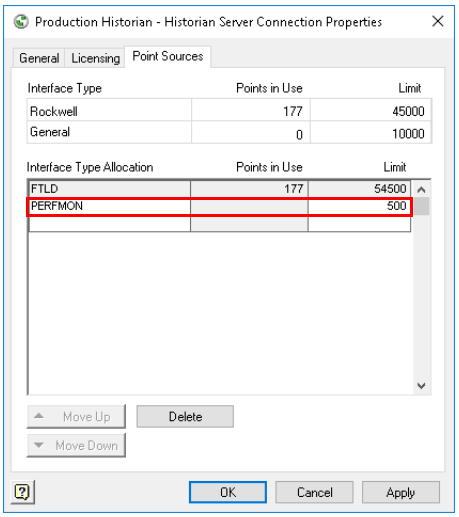


Configure the interface on the primary historian server.

1. Go to Rockwell Software > FactoryTalk Administration Console and select 'Network' for the directory you want to use.
2. Go to System > Connections > Historical Data folders > Production Historian and select properties.

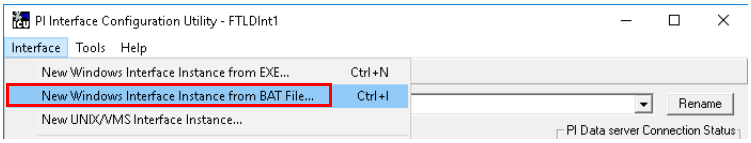
IMPORTANT Be patient because this dialog box could take a few minutes to appear.

3. On the Point Sources tab, type an interface name (such as PerfMon) and a value for the points limit.

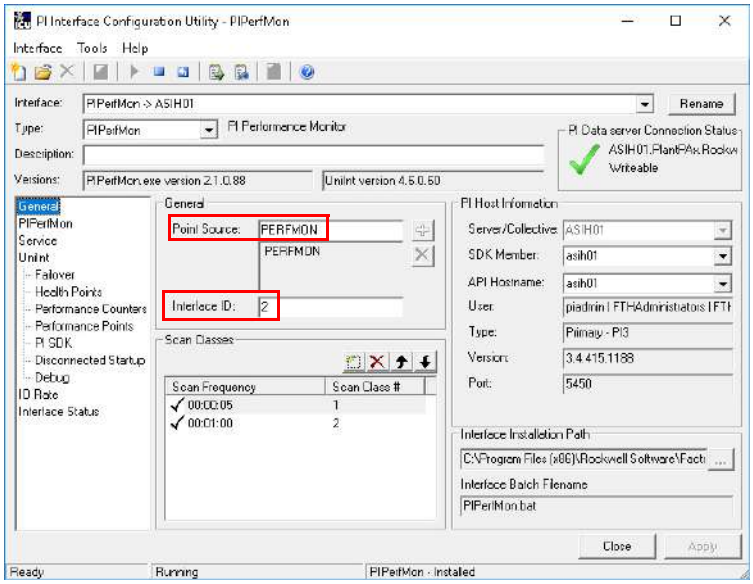


The value is the expected number of performance points in the system.

4. Go to Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility. and select New Windows Interface Instance from BAT file.



5. Select the PiPerMon.bat_new file from C:\Program Files (x86)\Rockwell Software\FactoryTalk Historian\PIPC\Interfaces\PIPerfMon directory.
6. Select the FactoryTalk Historian server as the host PI Data server/ collective.
7. Enter a Point Source name and an Interface ID number.

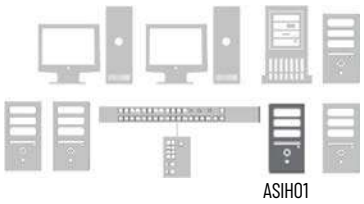


IMPORTANT The Point Source name **must** match the interface name that you typed in the Historian Production dialog box in step 3 on page 221.

The Interface ID number must be unique in the system.

8. Restart the interface service.

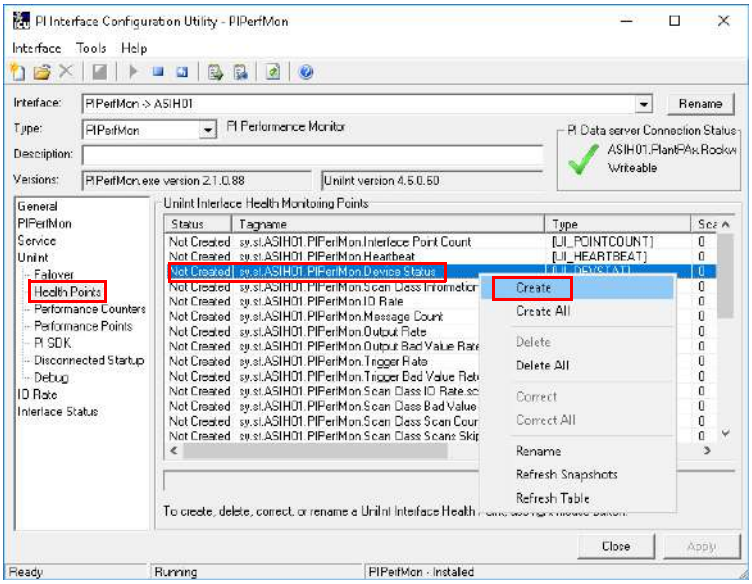
Create PIPerfMon Diagnostic Health Points



For diagnostics, associate the PIPerfMon interface with the health tags that monitor a device heartbeat. The heartbeat count helps to determine if the system is working efficiently. If there's a stoppage, you can analyze what prompted the fault or device error.

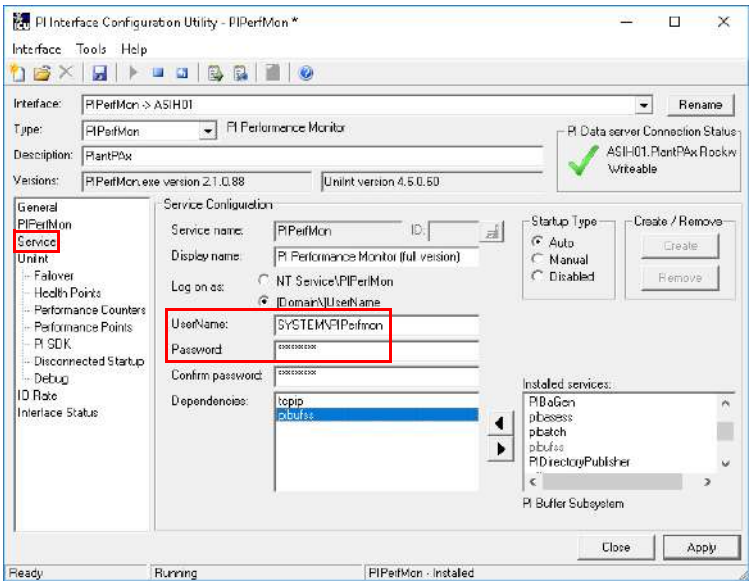
1. Go to Rockwell Software > FactoryTalk Historian SE > Interface Configuration Utility and select the PIPerfMon for the interface.

2. Create the Health Points for PIPerfMon.DeviceStatus.



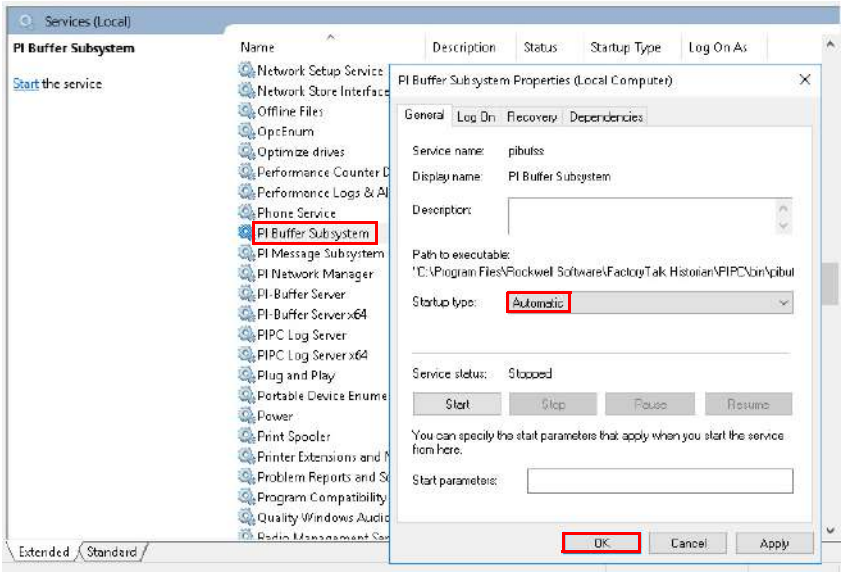
3. Create the Health Points for PIPerfMon.Heartbeat.
4. Go to Service and complete the following information.

From this Section	Action
Installed Services	Move pibufss to Dependencies
Service Configuration	Select Log on as: Domain\Username
UserName	Enter the same user name and password that you initially created for the service. See Create Domain User for PIPerfMon Service on page 219
Password	



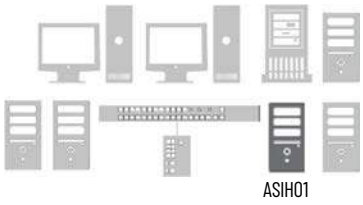
5. Go to Control Panel > Administrative Tools > Services.

6. Select PI Buffer Subsystem, and set the Startup type to Automatic.



7. Restart the interface service from the dialog box.

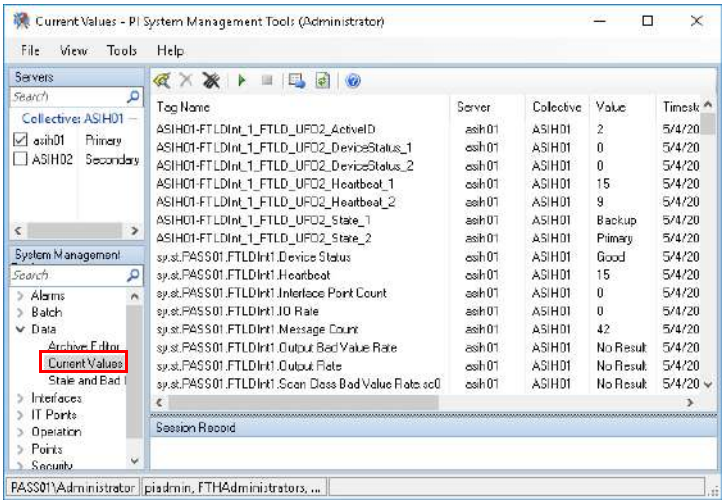
Test the PIPerfMon Interface



From the primary Historian sever, verify that the PIPerfMon interface has a good working status.

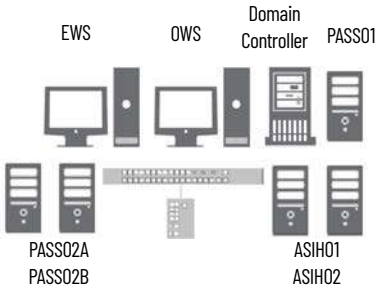
1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools.
2. In the left, top pane, select the appropriate server with the interface.
3. In the lower, left pane, go to Data folder > Current Values.

   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 the PIPerfMon Interface on other Computers

After the PIPerfMon interface is verified to work correctly on the Historian server, you can configure the other servers and workstations that you're collecting data. This requires the domain account to allow PIPerfMon to be added, create a Windows Firewall rule for access and enable the Performance Counter DLL Host service.



1. Go to Control Panel > User Accounts and define this information.

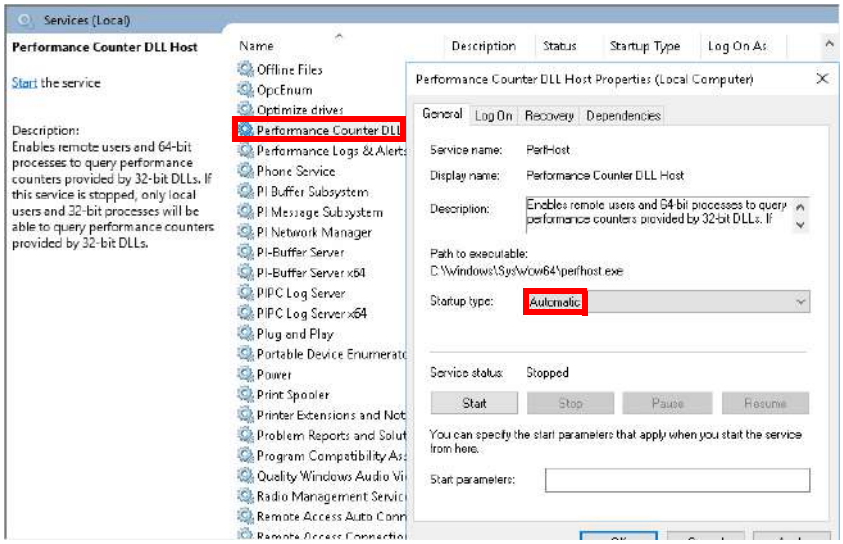
From this Page	Action
Control Panel\User Accounts	Select Manage User Accounts
User Accounts	Select Add
Add a User	Enter the same user name and Domain that you did to grant system access for the PerfMon service. See step 4 on page 223
What level of access do you want to grant this user?	Select Other and choose Performance Monitor Users from the pull-down.

2. Go to the Control Panel > Windows Firewall and define this information.

From this Page	Action
Control Panel\Windows Firewall	Select Advanced settings
Advanced Settings	Create a new inbound rule. 
New Inbound Rule Wizard: File Type	Select Port
New Inbound Rule Wizard: Protocol and Ports	Select TCP and enter the Specific local ports: 135 and 445
New Inbound Rule Wizard: Action	Select Allow the connection
New Inbound Rule Wizard: Profile	The rule applies to Domain, Private, and Public.
New Inbound Rule Wizard: Name	Enter a name for the rule. For example, Perfmon Connection

3. Go to Control Panel > Administrative Tools > Services and find Performance Counter DLL Host.

4. Right-click Performance Counter DLL Host and select Properties.



5. Select Automatic as the Startup type.

Configure PI Buffering

PI Buffering helps to protect local data in the event a client loses connection to the Collective.

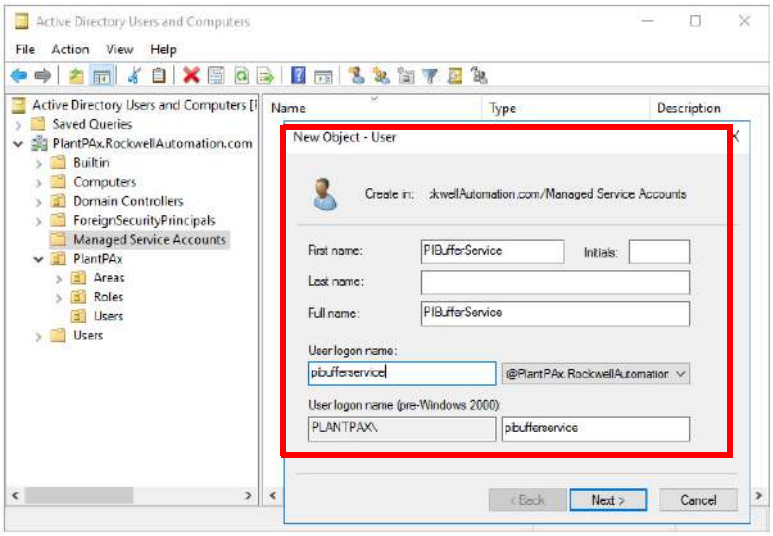
Create Domain User for PI Buffer Service

The PI Buffer service defaults to running in a local account. For PlantPAx systems with a domain, it's **recommended** running the PI Buffer service in a **domain account**. This enhances security and provides access among other domain computers.

The domain user account for PI Buffer service must be created on the domain controller. It's a user account with privileges to run the service on other computers within the domain.

1. From the Server Manager, click Tools and choose Active Directory Users and Computers.
2. Expand your domain folder, right-click Managed Service Accounts and choose New>User.

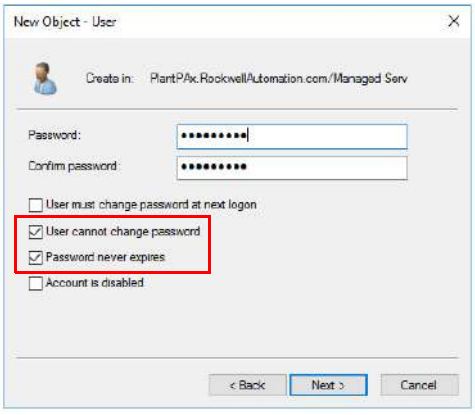
3. Complete the User text boxes.



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 menu to select your domain folder.
User logon name (pre-Windows 2000)	Use the SYSTEM\ default and type the same name for the PI buffering service.

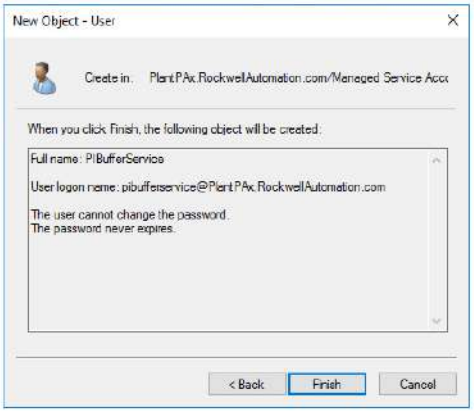
IMPORTANT The logon password creates a service user, not a person. The service user grants access to system computers for placing data into memory (buffer).

4. Type your password twice.



5. Make sure that the following boxes are checked:
   - User cannot change password

- Password never expires (indefinite service for system access)

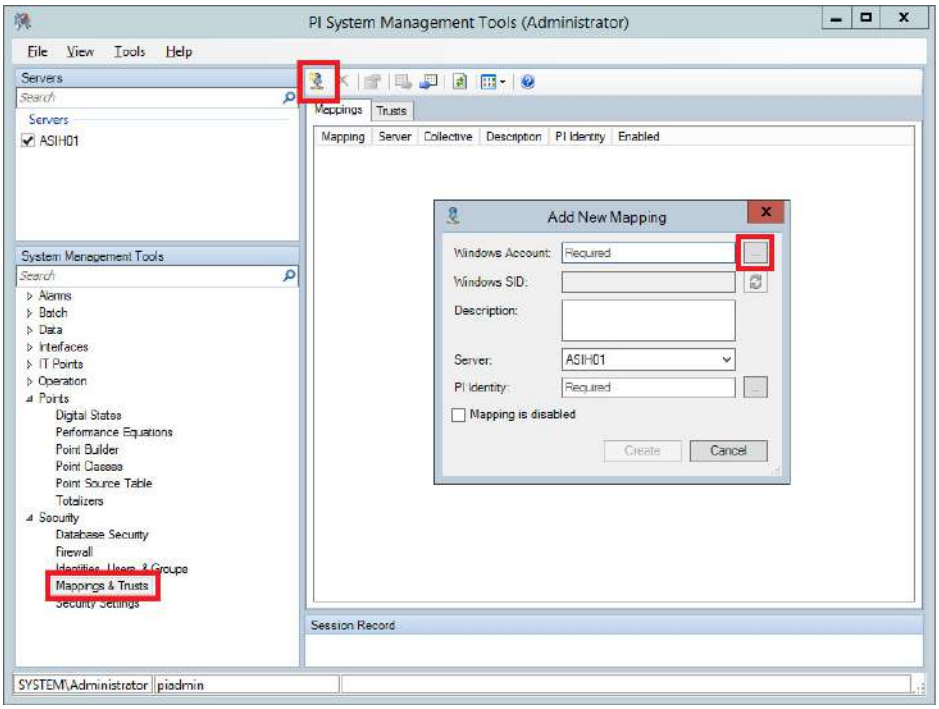


Create Security Mappings

On the Historian server, associate the service user identity with the Historian mapping and trusts.

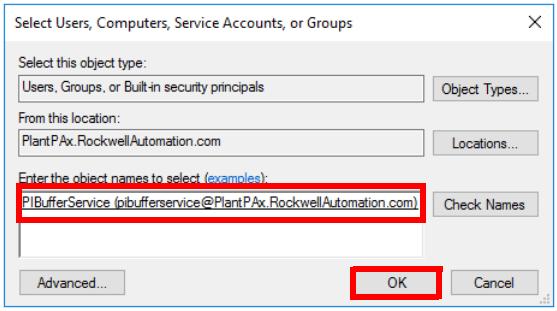
1. Go to Rockwell Software>FactoryTalk Historian SE>System Management Tools.

   The PI System Management Tools window appears.

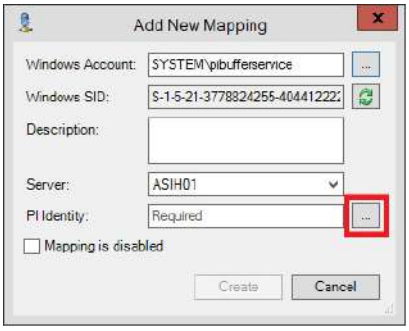


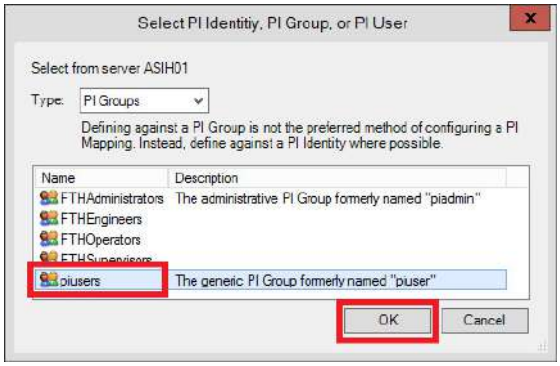
2. Do the following:
   - Under Servers, check the server that you want to set the security settings
   - Under System Management Tools, choose Mappings & Trusts
   - Click Add Mapping icon
   - From the Add New Mapping dialog box (right pane), click Browse (ellipsis '...')

3. Select the PIBufferService user that you created earlier.



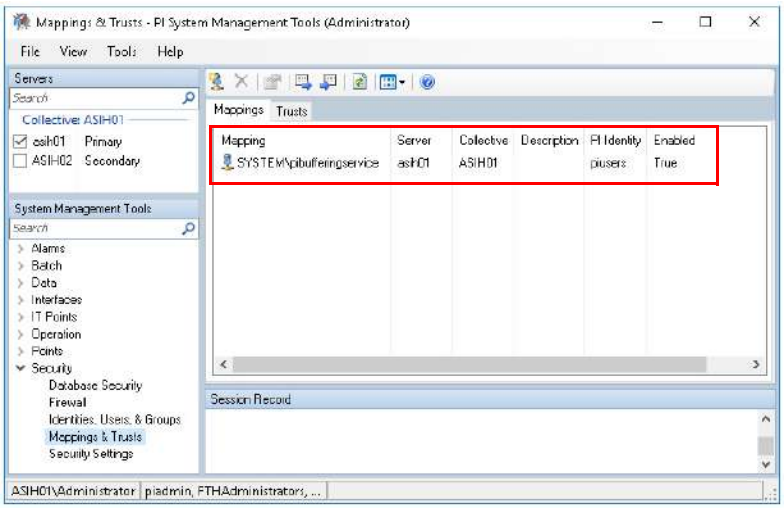
4. On the Add New Mapping dialog box, click Browse and select a group from the Type pull-down menu.
5. Select a desired identity.





6. Click Create.

Your security mapping should look similar to the example.

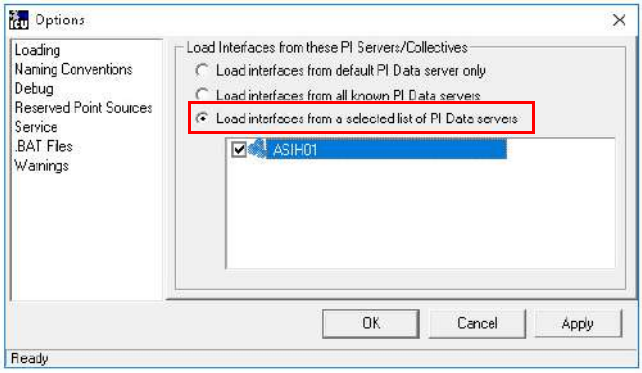


Configure the Buffering Interface

Configure buffering for the server that you're connected, such as PASS02A and PASS02B.

1. Go to Rockwell Software>FactoryTalk Historian SE>Interface Configuration Utility.

   The PI Interface Configuration Utility dialog box appears.
2. From the Tools menu, choose Options.
3. Click 'Load interfaces from a selected list of PI Data servers'.

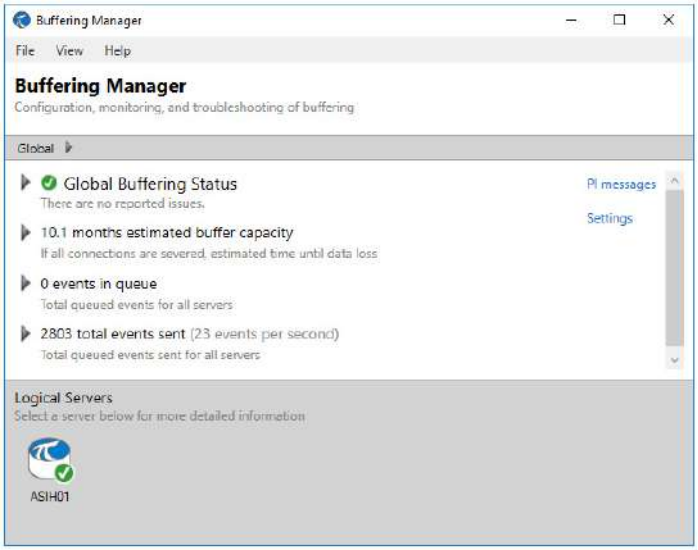


4. Select a server box.
5. From the Tools menu, choose Buffering.
6. Message windows appear.
7. Click Yes, and then 'Continue with configuration' to initiate the Buffering Manager wizard.
8. Complete the Buffering Manager wizard.

Item	Description
Detected PI Interfaces	Select the PI interfaces that you're buffering and click Next.
PI Data Archive security	Click Change, and enter the user name and password that you created earlier. Click Next.
	Click Next twice, and then 'Exit new installation wizard'.
Buffering Manager message windows	Click Yes and OK to confirm PI ICU dependency.

9. From the PI Interface Configuration Utility dialog box, click Tools menu and choose Buffering.

10. Verify that your information matches the dialog box example.



11. Close the Buffering Manager dialog box.
12. From the PI Interface Configuration Utility dialog box, click Tools menu and choose Options.
13. From the Options dialog box, check 'Load interfaces from a selected list of PI servers' and make sure that the server is checked.

Configure the PI Buffer Service Logon

The following procedure applies only if the Change Option wasn't available on the New Install Wizard dialog box.

1. On the PASS server, right-click Start menu and choose Computer Management.
2. Complete the New Install Wizard dialog box.

Item	Description
Local User and Group (left pane)	Open Local Users and Groups, right-click Groups and choose Administrators.
Add name	Click Add and type SYSTEM\pibufferservice.
	Click Check Names, and click OK.
Assign log on service account	From the Start menu, click Programs and choose Administrative Tools>Services.
	Right-click PIBuffer Subsystem and choose Properties.
	On the Log On tab, click Browse.
	Click Locations, choose 'Entire Directory', and click OK.
	Enter SYSTEM\pibufferservice and click Check Names.
	Click OK.

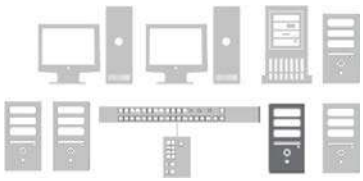
Configure Historian Data Collection

The procedures in this section use the 'System Management Tool' and PI System Explorer within FactoryTalk Historian software. The tool is available for Historian Asset Framework management computers, such as server, node interface, and EWS.

Microsoft® Excel® software is required to enable the bulk editing capability. An additional license is required to use PI Datalink.

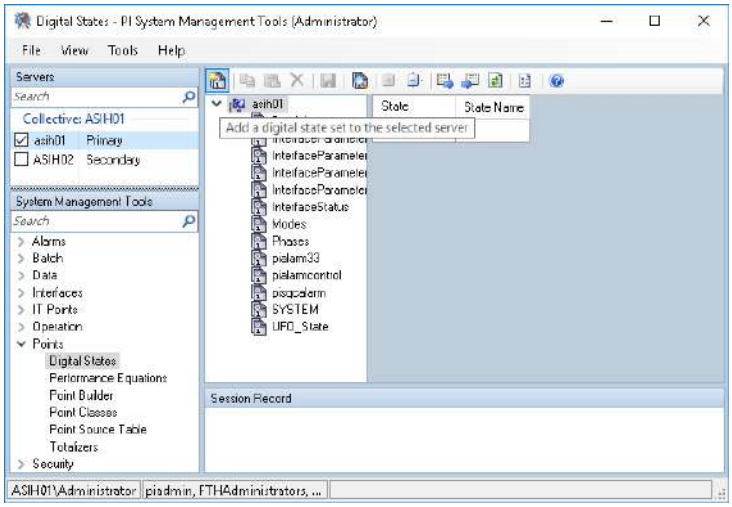
We also document how to manually create Historian tags, digital states, and Asset Framework. We recommend using the section "Configure Asset Framework Databases with the PlantPAx Configuration Tool" on page 248 for creating bulk tags for large process systems.

Create Digital States



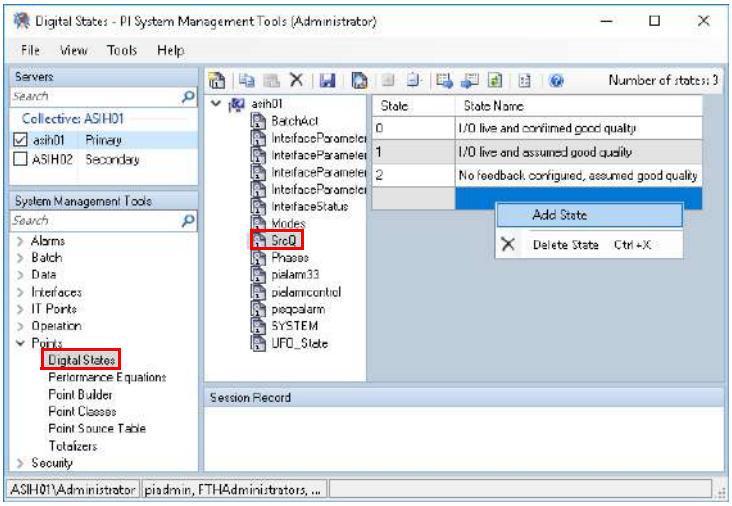
Historian points can be defined as analog or digital. Digital points can be used to enumerate the process states, thus creating a relationship between the value and the text state name. For example: 1 = Good.

1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools and select Points > Digital States
2. Add a Digital State Set to the server.

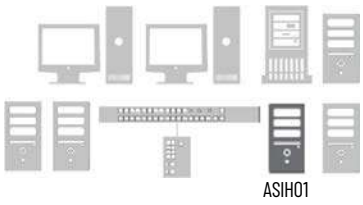


Source Quality Data Examples

Parameter	Data Type	Description
SrcQ	SINT	Final PV source and quality. GOOD 0 = I/O live and confirmed good quality 1 = I/O live and assumed good quality 2 = No feedback configured, assumed good quality TEST 8 = Device simulated 9 = Device loopback simulation 10 = Manually entered value UNCERTAIN 16 = Live input, off-specification 17 = Value substituted at device/bus 18 = Value substituted by maintenance (Has and not Use) 19 = Shed, using last good value 20 = Shed, using replacement value BAD 32 = Signal failure (out-of-range, NaN, invalid combination) 33 = I/O channel fault 34 = I/O module fault 35 = Bad I/O configuration (for example, scaling parameters)



Import Digital Sets and States



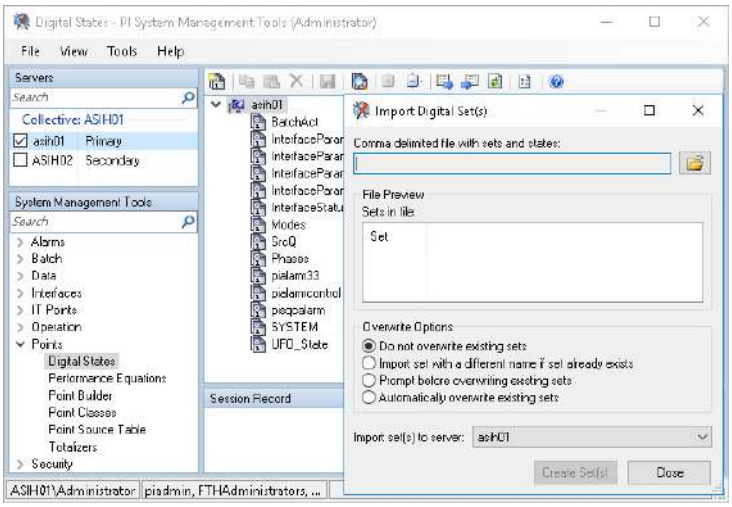
To save time entering common Digital Sets and States, templates are available to import.

A Process Objects Digital Set is available from the PlantPAx Process Library. After downloading the library, the Templates folder contains Historian files.

The PIPermon Digital States are available from a local template in the installation directory.

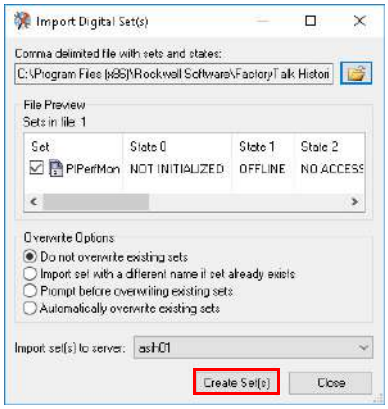
1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools and select Points > Digital States

2. Select Import.

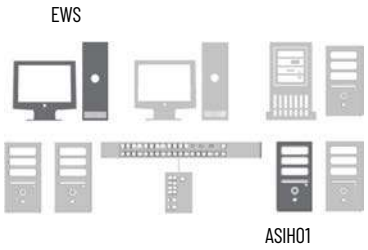


3. Select the PI_PIperfmon_DS.csv file for the Comma delimited file with sets and states. The file is located in C:\Program Files (x86)\Rockwell Software\FactoryTalk Historian\PIPC\Interfaces\PIPerfMon.
4. Select Create the Set(s).

   A minimum number of the recommended Digital Sets is created. This procedure does not create the basic Digital Set file for all Process Objects digital states.

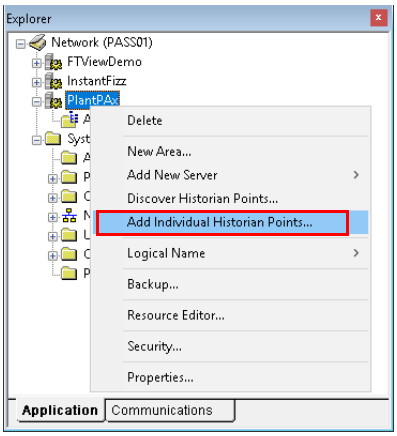


Create Individual Historian Points

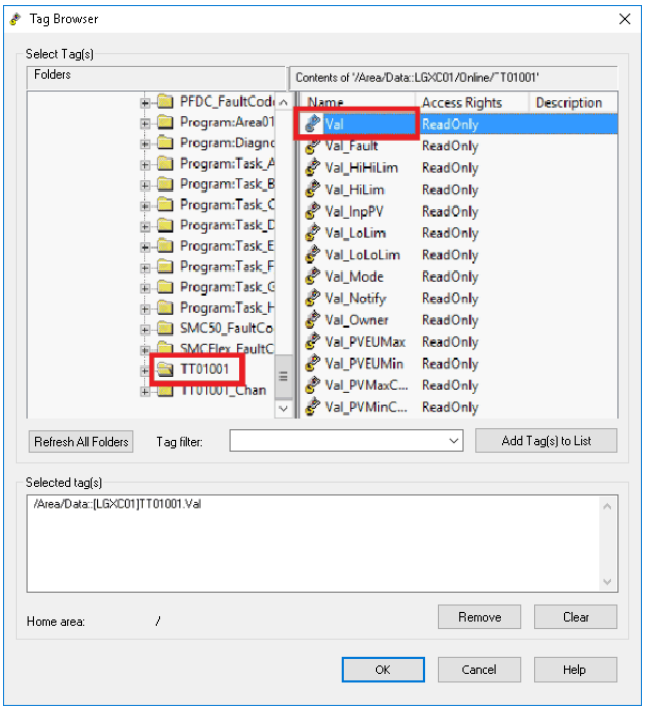


You can create historian points by using the FactoryTalk® Administration Console. Define these points from an engineering workstation or an Historian server. The following is one example.

1. Go to Rockwell Automation Software > FactoryTalk Administration Console and select the network for the type of FactoryTalk directory.
2. In the Explorer pane, select an application (PlantPAx is our example) and choose Add Individual Historian Points.



3. On the Add Historian Points dialog box, select Browse Tags.
4. In the Tag Browser window, select an object tag (TT01001 in the example) in the Folders pane on the left side of the window.

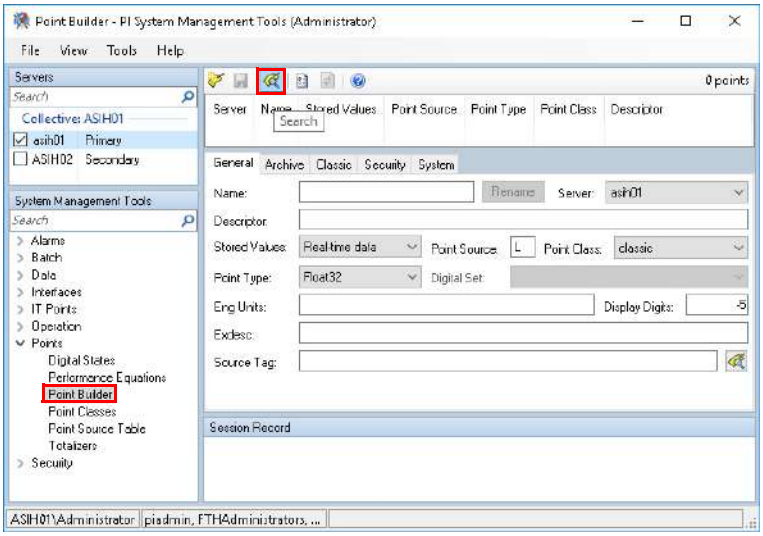


5. In the pane on the right side of the Tag Browser window, double-click the tag to configure as a Historian Point.

   Val (Process Variable Value) is the example.

6. Select Add Tags to List and OK to accept the tags in the list.
7. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools.

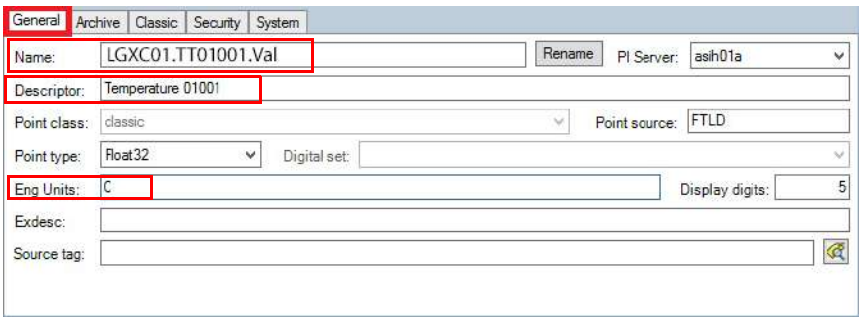
8. In the Servers Pane (or the Servers and Collectives pane if you've a collective), select the historian server.
9. Select Point Builder and search for tags.



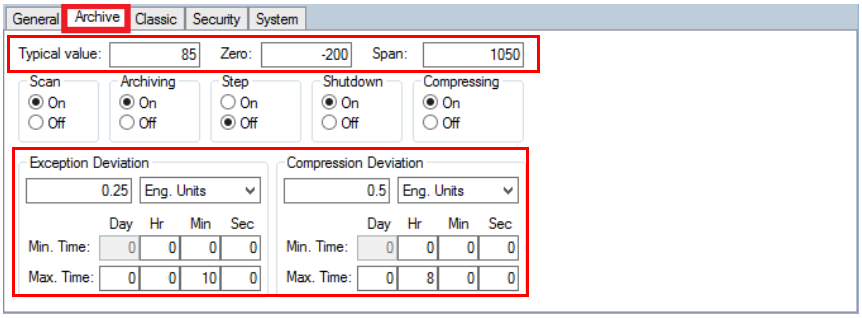
10. In the Tag Search window, type the Tag Mask and select Search.

    You can use an asterisk (*) for a wildcard. The point name and entire path appear on the Point Builder window.

11. Select the tag and select OK.
12. Select the tag and select Rename.
13. Enter a new name in the Rename PI Point dialog box.
    The name must be modified as **OPCTopic.Backingtag.parameter** in order to populate a historical trend in the PlantPAx faceplate. In the following example it isLGXC01.TT01001.Val.
14. In the General tab of the Point Builder dialog box, enter a tag description and engineering units.



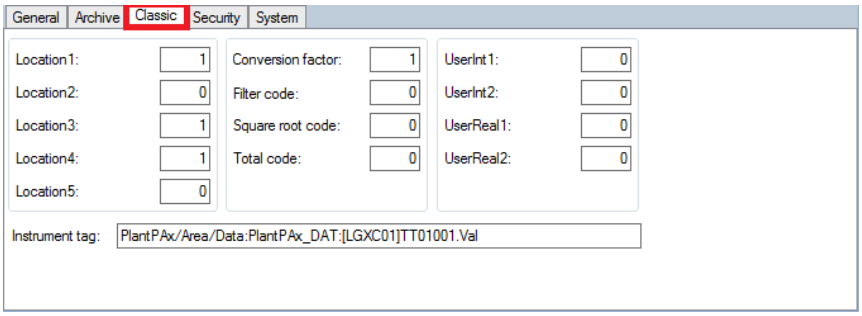
15. In the Archive tab, configure the range (Zero and Span), typical value, and all exception and compression data for the historical point.



IMPORTANT Usually, Minimum Range Value = Zero, Span = Maximum Range Value minus Minimum Range Value. The Typical Value is between the Minimum Range Value and the Maximum Range Value.

16. Select the Classic tab, to view the historical tag path (instrument tag) that includes the Data server name.

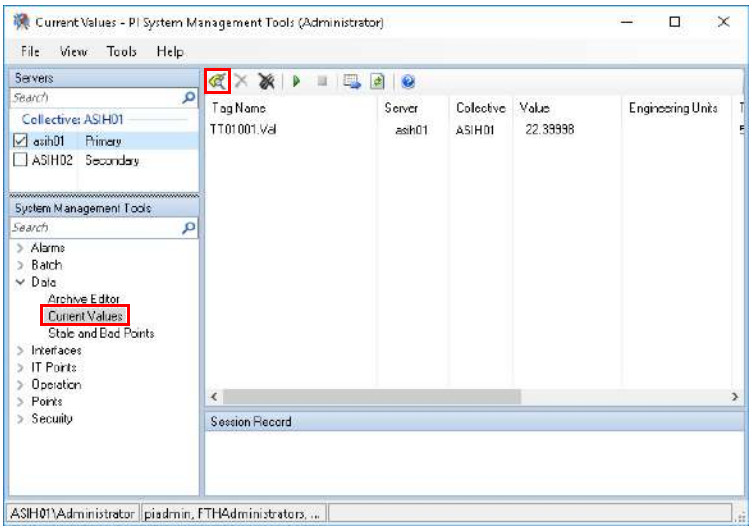
This example shows the FactoryTalk® Linx name, PlantPAx_DAT.
The historical point link is broken if any change is made to the FactoryTalk® Linx application name.



Monitor Historical Data

From the primary Historian server, use the PI System Management Tool to verify Historical data has good values.

1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools and select Current Values and select the search button.

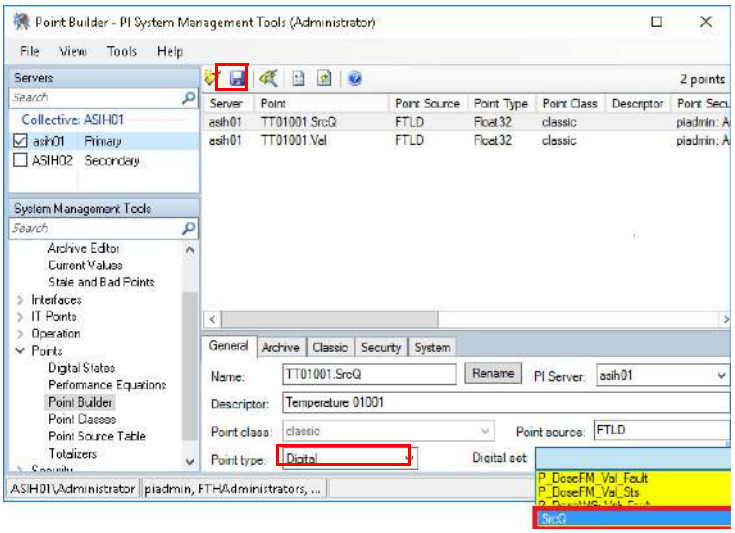


2. Enter a tag mask or an asterisk (*) for all tags.
3. Select any tags that you wish to monitor.
4. To see values change as they periodically refresh, select the Play button.

Define Digital Historical Points

The digital set is available only to a digital points type. The FactoryTalk Administration Console automatically creates a Float32 (Real) point type for each new point.

1. Go to Rockwell Software > FactoryTalk Historian SE > System Management Tools
2. To be able to change the digital set, select Digital for the Point type and then select a Digital Set (SrcQ in the example).



3. Select the Save icon to store the Historian point.

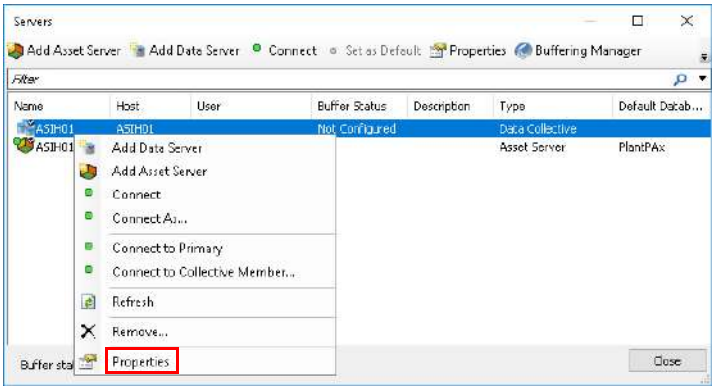
Historian Asset Framework

Use the FactoryTalk Historian Asset Framework to build and deliver model-driven analysis and reporting solutions.

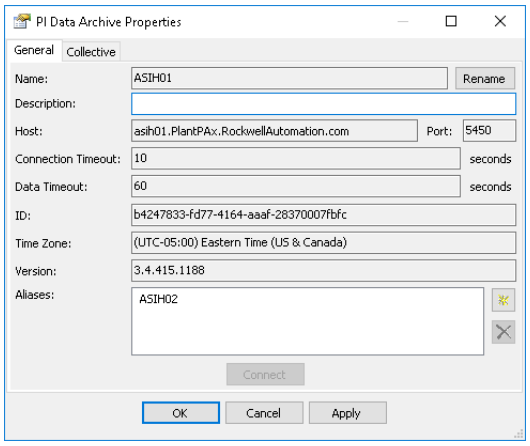
Configure the Connections to the Servers

When a Historian Collective is used, the Asset Framework server and PI Analysis Service must be installed on a separate computer, such as a dedicated SQL server via the AppServ-SQL virtual template.

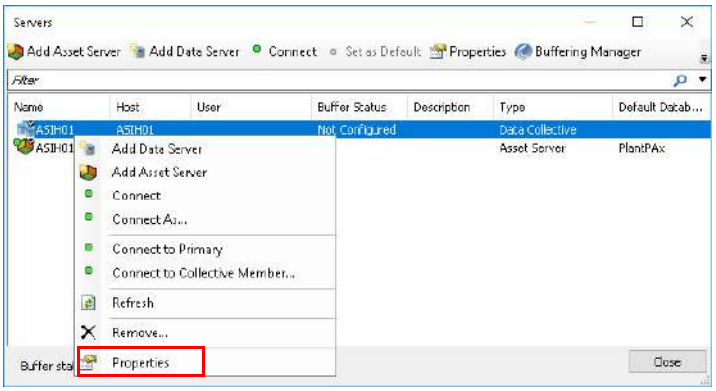
1. Go to Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit) and select File to choose Connections.
2. Select the data collective (ASIH01) and choose Properties.



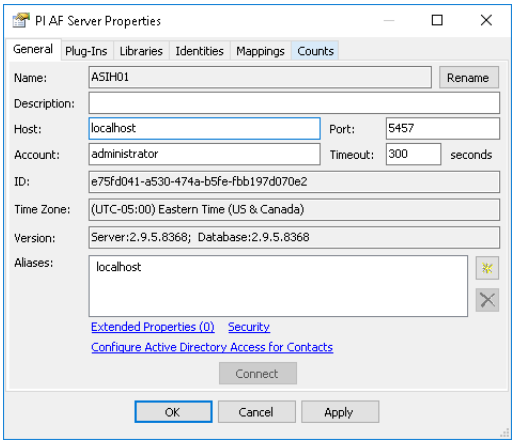
3. Rename or configure this connection as necessary for your system.



4. Select the Asset Server (ASIS01) and choose Properties.



5. Rename or configure this connection as necessary for your system.



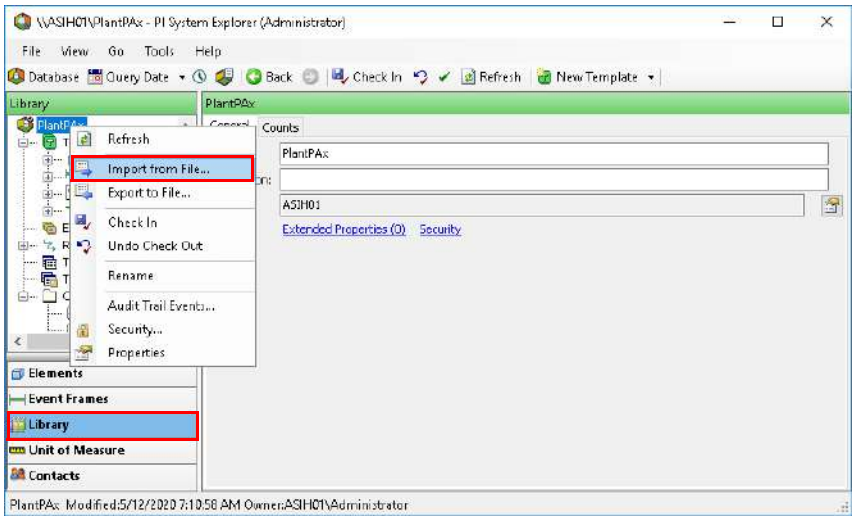
Import Asset Framework Templates

An asset framework provides a means to organize your process equipment assets. Asset Framework Templates are provided in the process library. This download is available online from the Product Comparability and Download Center (PCDC).

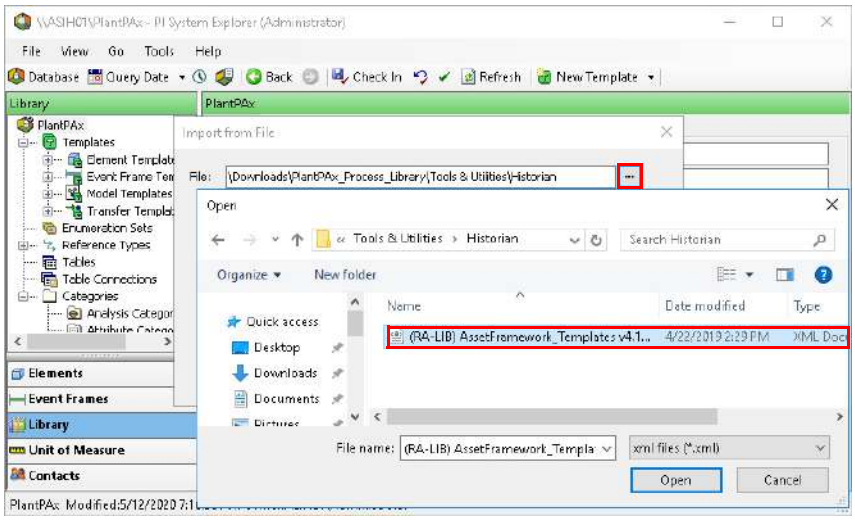
1. Go to Programs > Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit).

IMPORTANT Steps 2 and 3 are only performed the first time that you name the database.

2. Select Yes from the Create Database dialog box to create a user database.
3. Enter the name of the user database.
4. Select Library in the lower, left pane, select the database name and choose Import from File.



5. Browse in your system files to the (RA-LIB) AssetFramework_Templates .xml file and open the file.



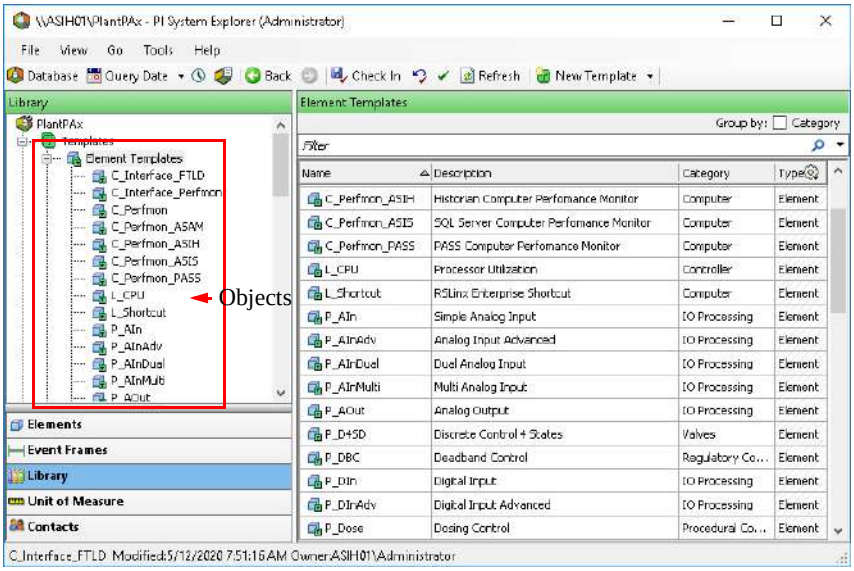
There are these template files:

- Base Asset Framework Template File for standard Asset Framework functionality for the process library, release 4.1 and 5.0.

- Advanced Asset Framework Template File for use with SQL Server Reporting Services reports. These objects use the base template, with additional parameters to enable reporting functionality. For more information, see PlantPAx SQL Process Object and Alarm Reports.

6. Accept the default import options.

   The database now contains the Library object templates.



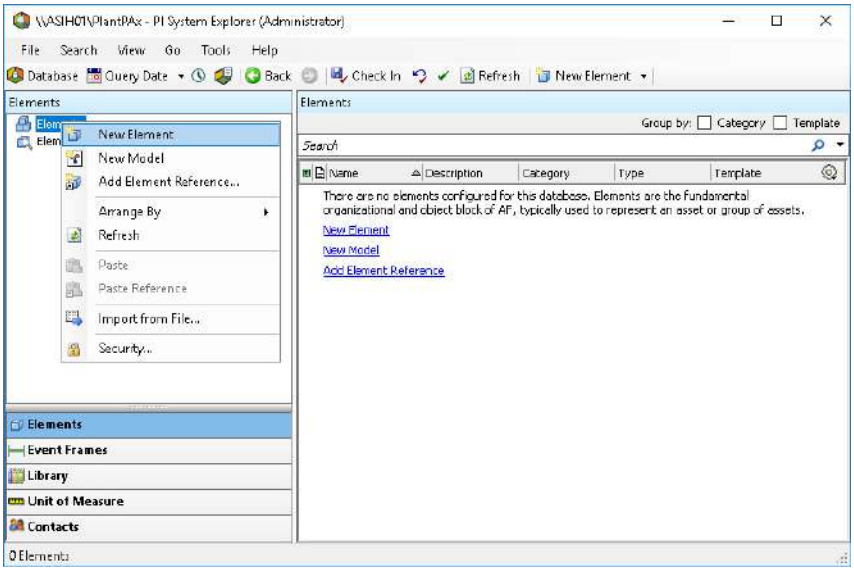
Configure Asset Framework Elements

Associate the tags with historian elements, which are the Process object templates

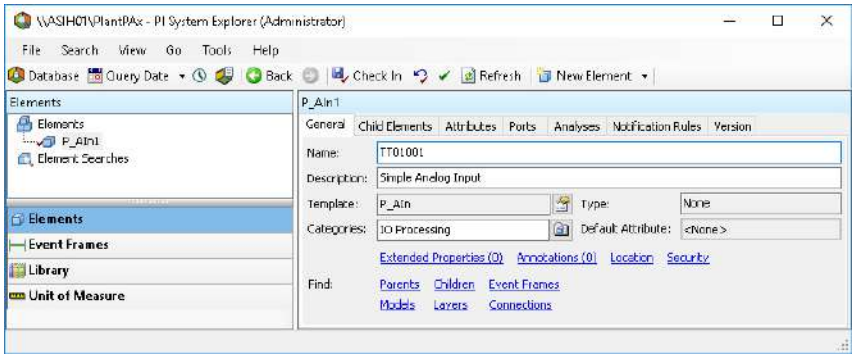
The term ‘element’ is used in the Asset Framework software. For PlantPAx system purposes, ‘element’ can be considered synonymous with ‘objects’ in the process library.

1. Go to Programs > Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit).

2. Select Elements in the lower, left pane, select Element and create a New Element.



3. Select P_AIn in the Choose Element Template dialog box.
4. Type the tag name that is being assigned to the object and check it in.

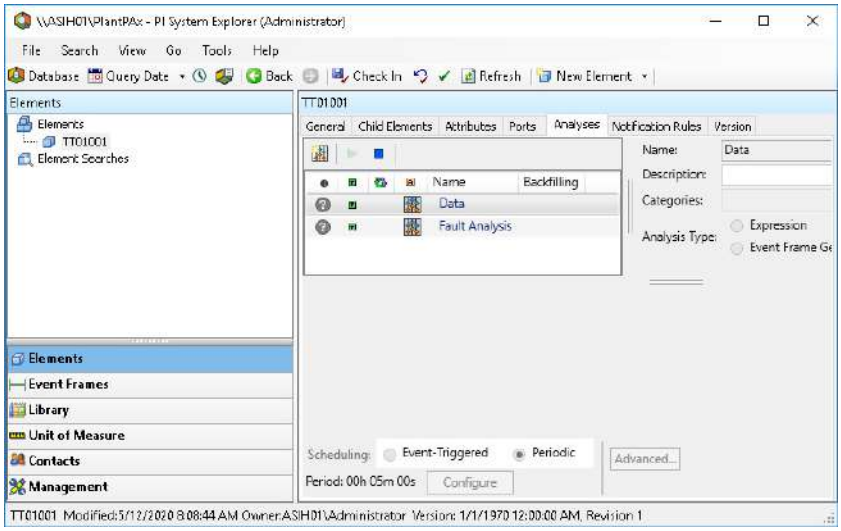


5. Confirm the settings and Check In again to complete the check in process.
6. The current historical value is accessed by selecting the Attributes tab and refreshing.

Search Event Frames

You can search for event frames, for example, if you want to find abnormal conditions that triggered an event.

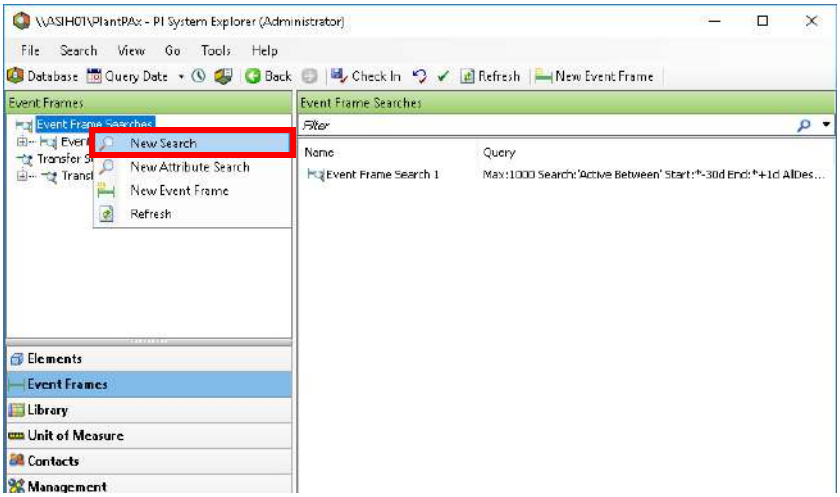
1. Go to Programs > Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit)
2. Select Elements in the lower, left pane of the PI System Explorer dialog box and then select the Analyses tab.



Finding Faults for Analysis

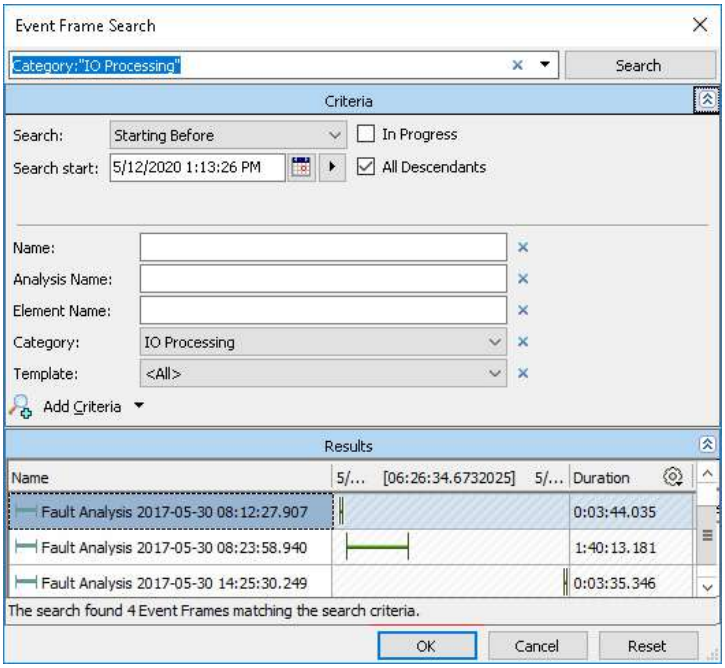
You can also search event frames to assess faults.

1. Go to Programs > Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit)
2. Select Event Frames in the lower, left pane, select Event Frame Searches and choose New Search.



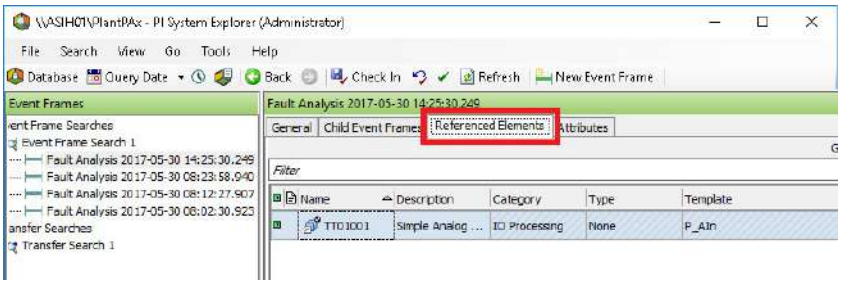
3. Select the desired search criteria and any filters.

The search results for the selected criteria appear at the bottom of the dialog box.



4. To view elements (tags) that are associated with the fault for the selected search criteria, double-click a fault.
5. Select the Referenced Elements tab.

   Each tag (and description) that is assigned to the element appears.



6. To view a description of the abnormal condition, select the Attributes tab.

Tools for Creating Historian Tags

Depending upon how far along you are in your process application build, these can help create tags and other bulk code:

- Application Code Manager software
- PlantPAx Configuration tool
- PI Builder Add-in for Microsoft Excel

Application Code Manager

Application Code Manager (ACM) software supports a historian library to assist with creating historian tags.

Use ACM to create the historian tags when your control strategies in ACM are in the final stages and ready to generate a Logix 5000 Controller .ACD file.

See Chapter 5, Process Applications for specific details on ACM.

After ACM generates historian tags, the .CSV file needs to be copied to the computer that has PI Builder Add-in for Microsoft Excel installed to publish the tags into the historian database.

IMPORTANT If additional control strategies are created using the Logix Designer application, then ACM won't be able to generate the new historian tags. In this scenario, the PlantPAx Configuration Tool may be considered to create the historian tags.

PI Builder Add-in for Microsoft Excel

PI Builder is a Microsoft Excel add-in that lets you use Excel to create, view and modify PI points and Asset Framework objects in your Historian database. With PI Builder you can make bulk tag edits by importing and exporting your spreadsheet.

All functionality of the prior PI Tag Configurator has been replaced with PI Builder, which is included with the PI SMT and PI Data Archive setup kits (as part of the PI AF Client installer).

IMPORTANT Microsoft Excel 32-bit software must be installed for these procedures.

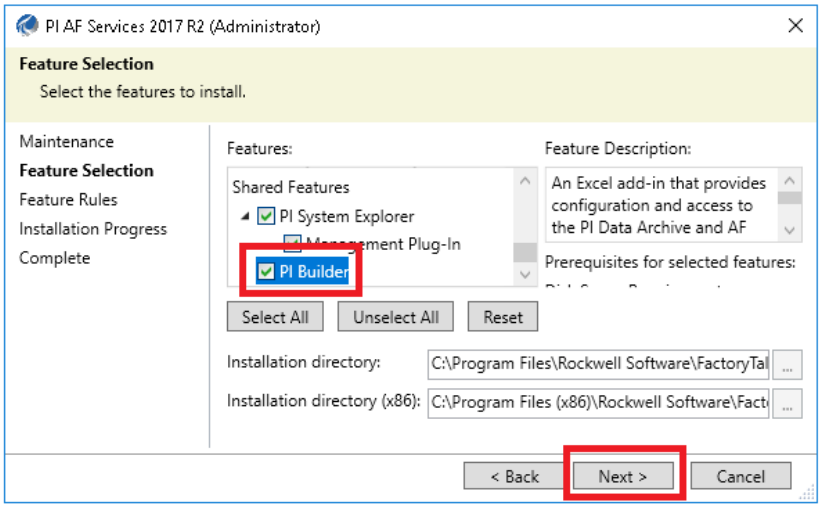
This section uses Microsoft Excel 2013. Your version could be different.

If Microsoft Excel was installed after the Historian software, the PI AF Services will need to be modified to include the PI Builder feature.

1. To start the modification, run file named <PI-AF-Services_2017-R2A_.exe> located in the \Redist\PIAFSetup\ directory of the Historian SE software installation media.

   A maintenance dialog prompts to modify, repair, or uninstall the PI AF Services 2017 R2 installation.
2. Choose to Modify the installation and click Next.

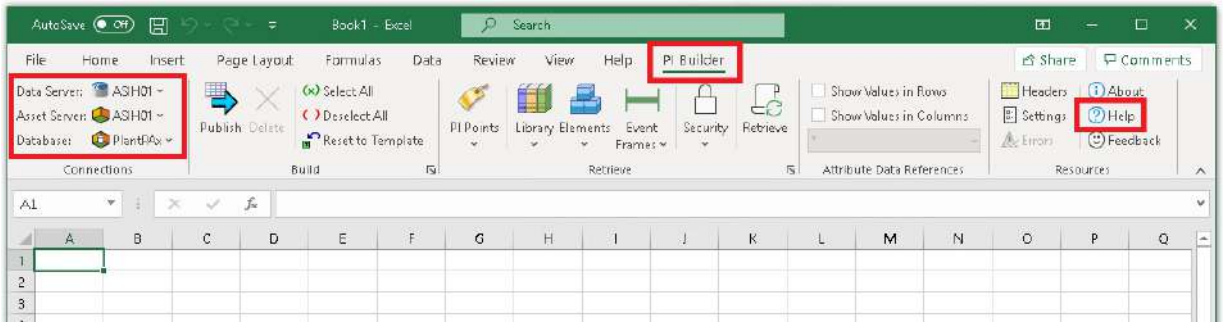
3. Select PI Builder from the list of Features and click Next.



4. Restart the computer after the installation is complete.

To retrieve and publish PI AF objects, PI Builder must connect to a PI AF database and for PI points a PI Data Archiver server.

1. Open your version of Microsoft Excel and click the PI Builder tab.
2. In the Connections group on the upper left corner. Select your Data Server, Asset Server, and Database as available.



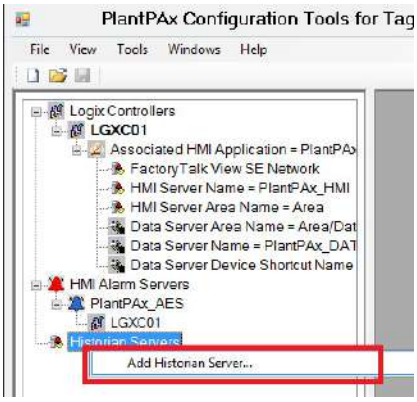
For information on how to publish your historian tags to the historian database, see the PI Builder add-on Help section.

Configure Asset Framework Databases with the PlantPAx Configuration Tool

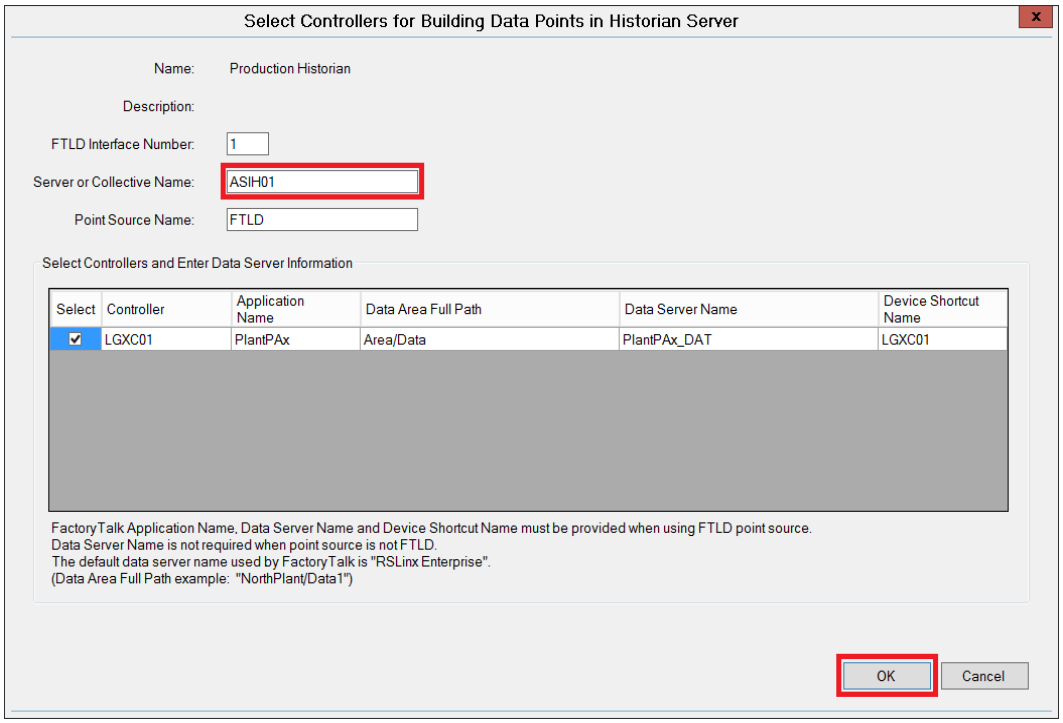
Use the PlantPAx Configuration tool to configure Asset Framework databases with Logix tag elements. This includes the automatic configuration of related PI points in the FactoryTalk Historian data server (PI data server).

This procedure assumes that the controller, HMI server, and the alarm server are configured for using the PlantPAx Configuration Tool.

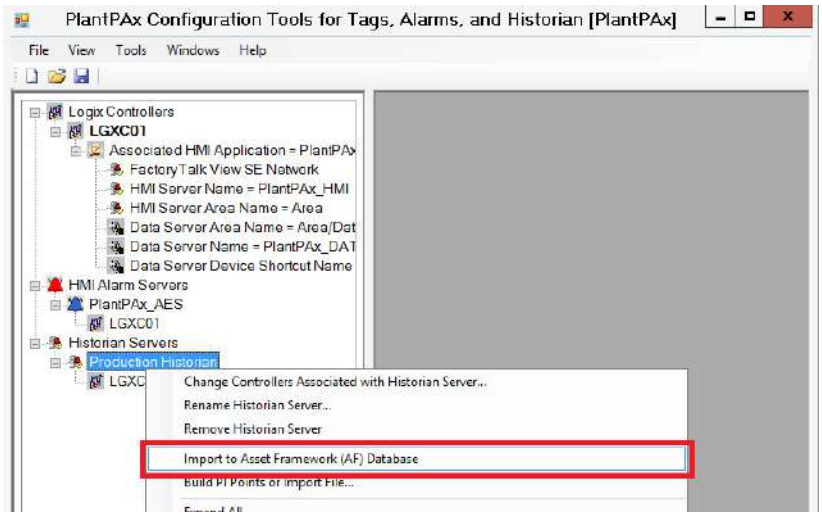
1. Open the PlantPAx Configuration Tool.
2. Add the Historian Server.



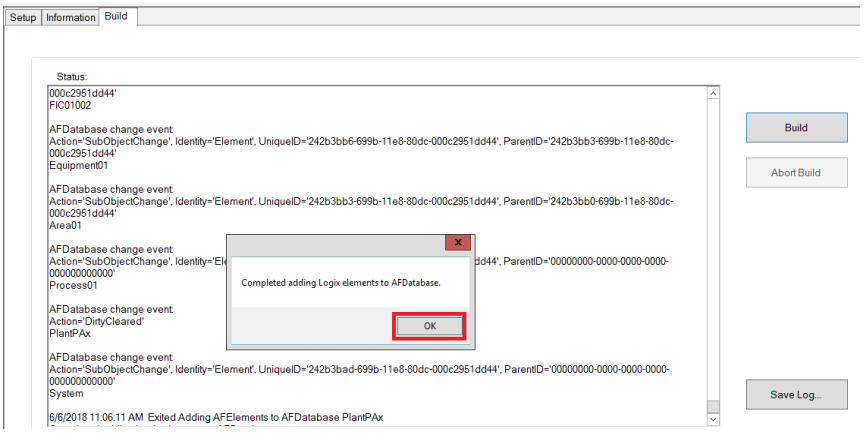
From this Page	Action
Add Historian Server	Type the name of the historian server.
Select Controllers for Building Data Points in Historian Server	Enter the server collective name and select the applicable controllers.



3. Select the Historian server that you just created (Production Historian in our example), and select to Import to Asset Framework (AF) Database



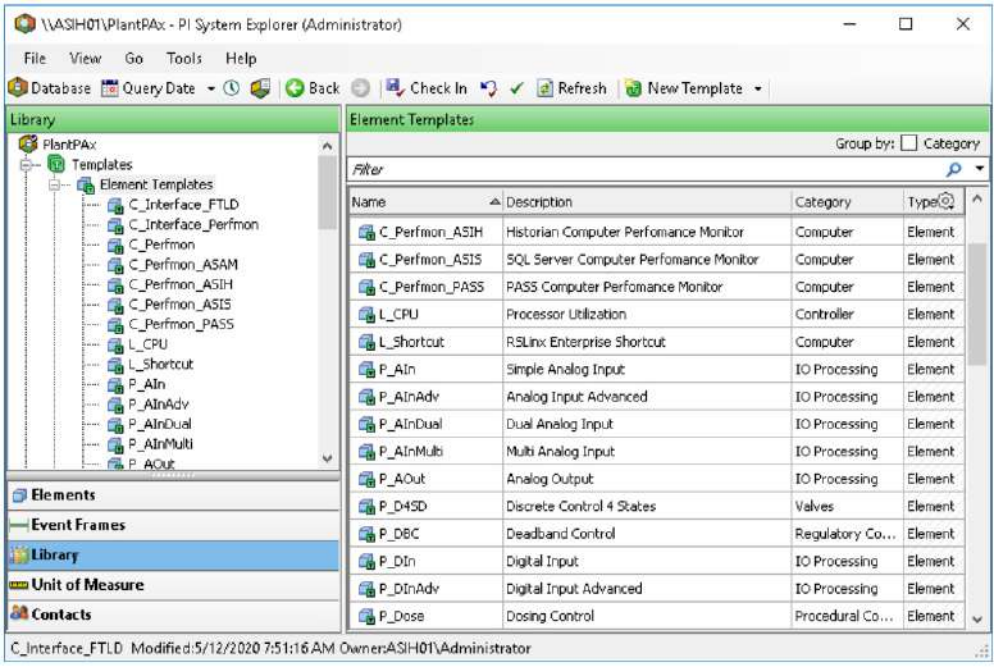
From this Location	Action
Build Tags: Setup Tab	Select Connect
Connect dialog Box	Set the PI Server, AF Server, and AF Database
OK Connected dialog box	Verify that you're connected to the PI Server, AF Server, and AF Database
Build Tags: Setup Tab	Select PI Point Builder Options
FactoryTalk Historian Import File Builder Options dialog box: Naming tab	Use the controller name as a prefix to Historian tags. For example, LGXC01.<*tagname*>
Build Tags: Information Tab	Review and verify the information
Build Tags: Build Tab	Select Build



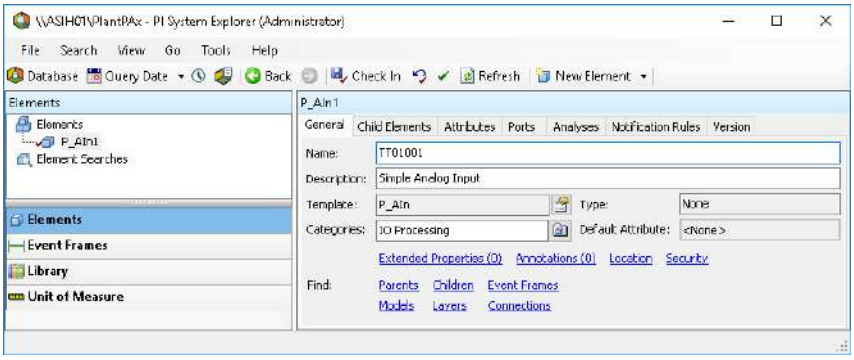
Verify Asset Framework Library and Elements

After using the PlantPAx Configuration Tool, you must verify that the asset framework library and elements are properly imported into the Asset Framework database.

1. Go to Programs > Rockwell Software > FactoryTalk Historian SE > System Explorer (64-bit).
2. Select Library in the bottom left of the system explorer and verify the contents of the library.



3. Select Elements in the bottom left of the system explorer and verify the elements.



Batch Management

PlantPAx® systems support scalable options for batch management that are based on ISA88 standards and can help:

- Automate sequences to reduce time-to-market
- Manage recipes and procedures to focus on yield, throughput, and quality
- Provide models to improve traceability, reporting, and approval controls.

The following options exist for batch management in your PlantPAx system. Controller-based solutions are typically for smaller systems; larger systems require FactoryTalk® Batch applications. The reference links provide more details for each option. Not all controller firmware revisions support all batch solutions.

Step 1: Select the Batch Solution

Scalable offerings and tools range from controller-based to enterprise-wide solutions.

Feature	Logix Batch & Sequence Manager	SequenceManager	FactoryTalk Batch
Deployment	Logix controller code	Firmware-based controller feature	Server-based application
Supported controllers	ControlLogix® 5580 CompactLogix™ 5380 ControlLogix 5570 CompactLogix 5370	ControlLogix 5570 CompactLogix 5370	ControlLogix 5580 CompactLogix 5380 ControlLogix 5570 CompactLogix 5370
Units	Single unit recipes	Single unit recipes	Multiple unit recipes
Phase construction	PhaseManager™ programs	PhaseManager programs	PhaseManager programs
Phase interface	Phase and bit logic	Pull-down menu	Pull-down menu
Max recipes/steps/phases	32	Limited by memory or resources	Limited by memory or resources
Max input/report parameters	4	No max	No max
Parameter expressions	No	Yes	Yes
Parameter data types	BOOL REAL	BOOL INT, INT, DINT REAL	BOOL SINT, INT, DINT REAL
Procedural structure	Sequential Concurrent	Sequential Concurrent Divergent Recurrent	Sequential Concurrent Divergent Recurrent
Recipe design	Tabular HMI configured	SFC like	SFC like
Recipe editing	Runtime via HMI	Import only at runtime	Runtime editing via Recipe Editor
HMI integration	Faceplates	3 Active X	4 Active X API

Feature	Logix Batch & Sequence Manager	SequenceManager	FactoryTalk Batch
Batch reporting	Queue controller services	Event client and archive services	Event client and archive services
FactoryTalk Batch integration	No	Yes	—
Dynamic unit binding	No	No	Yes
Unit arbitration	No	No	Yes

Step 2: Logix Batch and SequenceManager Requirements

The Logix Batch and SequenceManager™ option consists of controller code and visualization elements. You need:

- Logix 5000™ controller
- FactoryTalk® View Studio software
- Logix Batch and Sequence Manager files

For more information, see Logix Batch and Sequence Manager.

Step 3: FactoryTalk Batch Requirements

SequenceManager controls direct PhaseManager programs in this controller-based option. You need:

- Logix 5000 controller
- FactoryTalk® View Studio software
- SequenceManager software

For more information, see SequenceManager Controls.

Step 4: FactoryTalk Batch Requirements

A FactoryTalk Batch application is a server-based option.

AppServ-Batch application server with:

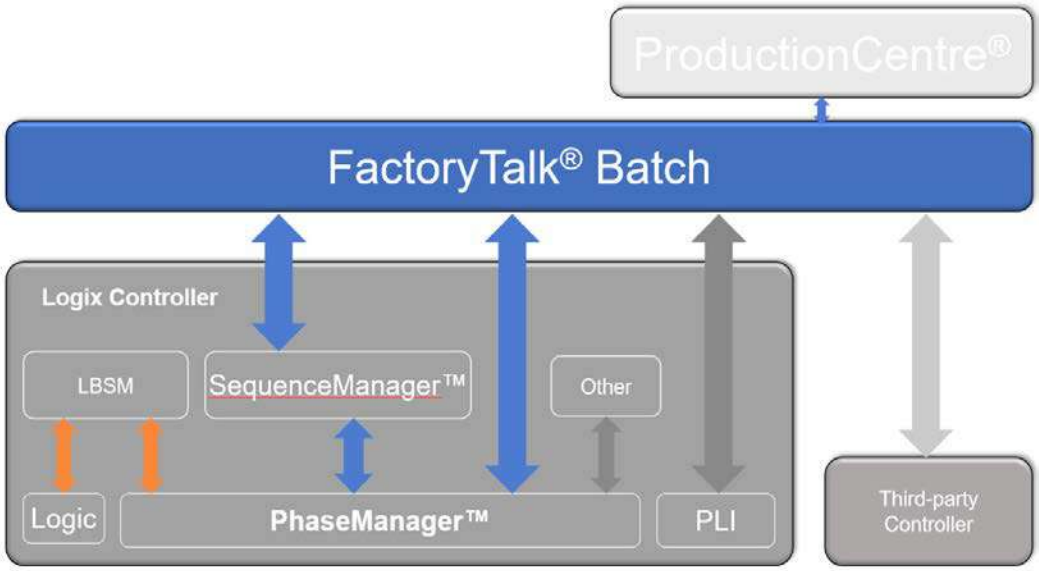
- FactoryTalk Batch server
- FactoryTalk® eProcedure® server
- FactoryTalk® Event Archiver database

AppServ-Info SQL server with:

- SQL server
- FactoryTalk Batch Material server
- Master Recipe storage

For more information, see Factory Talk Batch Application.

The batch solutions work with each other to provide a comprehensive solution.

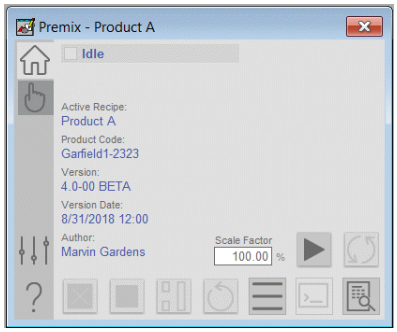


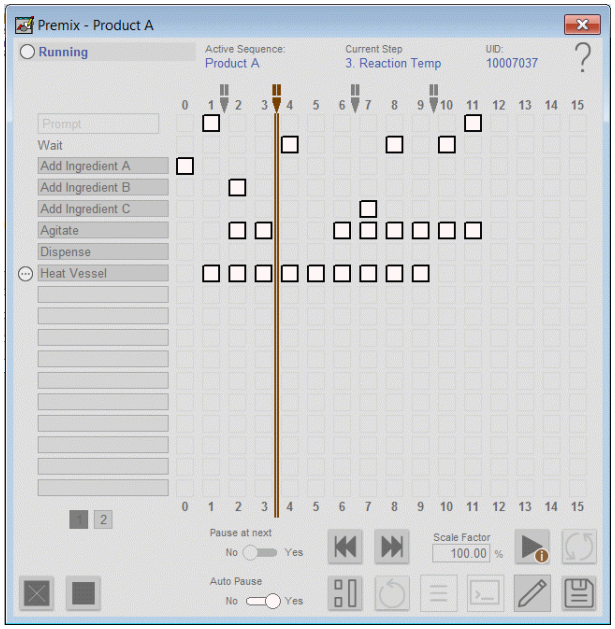
For more information, see these additional resources.

Resource	Description
PlantPAx Logix Batch and Sequence Manager Reference Manual, publication PROCES-RM007	Provides procedures on how to use LBSM to store recipes and sequences equipment and phases to make products.
SequenceManager Controller Reference Manual, publication 1756-RM101	Describes how to install, configure, and run SequenceManager Controls.
FactoryTalk Batch User Manual, publication BATCH-UM011	Contains instructions for configuring security and services, and implementing components, such as the FactoryTalk Batch server, simulator, and performance chart.
PlantPAx Batch Design Considerations Reference Manual, publication PROCES-RM008	Provides guidance on selected batch implementation topics in a PlantPAx system.
Batch Application Toolkit Quick Start, publication IASIMP-QS042	Provides a framework for how to use the tasks to complete the components of the Toolkit.
PhaseManager User Manual, publication LOGIX-UM001	Provides instructions on how to configure and use a Logix 5000 controller with equipment phases.
FactoryTalk Batch PhaseManager User Manual, BATCHX-UM011	Provide instructions on how to use phase logic to integrate FactoryTalk Batch software with a Logix Designer application.

Logix Batch and Sequence Manager

The Logix Batch and Sequence Manager application is controller logic that provides basic batch management for single-unit or multiple-independent unit operations.





An LBSM application is best for:

- Single-unit batch processes, with 5...10 recipes, that can be defined with four real and four Boolean parameters per phase
- Processes that need frequent recipe changes
- Systems where recipe changes must be made through an HMI
- Process skids
- Pilot plants

LBSM Details

The LBSM application provides controller logic and HMI objects.

An LBSM application supports:

- PhaseManager programs and custom sequences
- Maximum of 32 recipes per controller
- Maximum of 32 steps per recipe
- Maximum of 4 real and 4 Boolean Parameters/phase
- Recipe changes are made from the HMI

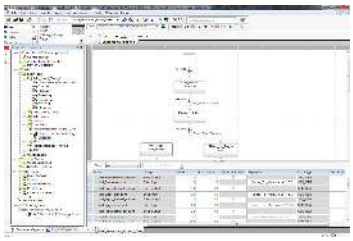
For more information, see PlantPAx Logix Batch and Sequence Manager Reference Manual, publication PROCES-RM007.

SequenceManager Controls

SequenceManager is a firmware-based feature controls direct PhaseManager programs inside a Logix 5000 controller in an ordered sequence.

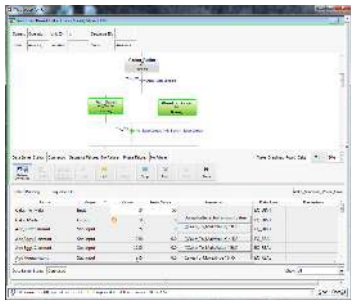
Editor – Logix Designer application

Define a procedural sequence that coordinates the execution of equipment phases



Operator – FTView SE

Monitor and interact with a running procedural sequence in the HMI



Data Collection & Reporting Services

Generate events used to produce batch reports and procedural analysis

A SequenceManager application is best for:

- Small batch systems (single unit)
- Systems with no server connectivity
- Process skids
- Modular systems connected into larger FactoryTalk Batch processes
- Fast processes

SequenceManager Details

The Logix controller must have firmware support to implement a SequenceManager application. Not all controllers support the SequenceManager application.

Use the SequenceManager to model and execute sequential manufacturing processes using the ControlLogix features described in the following tasks:

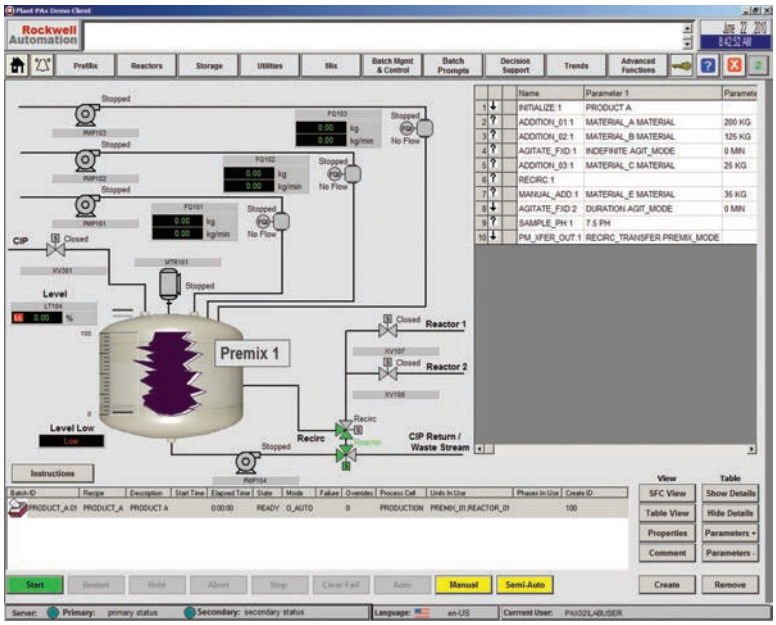
- Configure the coordination of Equipment Phase execution using the Equipment Sequence Editor.
- Execute Equipment Sequence programs using ControlLogix.
- Monitor and manage running Equipment Sequences using the Logix Designer application.
- Enable operators to monitor and manage running Equipment Sequences and Equipment Phases by adding SequenceManager ActiveX controls to FactoryTalk® View SE displays.
- Subscribe and collect generated sequence events using SequenceManager Event Client Service and SequenceManager Event Archiving Service.

For more information, see SequenceManager Quick Start Guide, publication 1756-QS109.

Factory Talk Batch Application

A FactoryTalk Batch application is a server-based, comprehensive approach to batch management.

- Handles complex unit coordination, resource arbitration, and optimization of routes
- Manages recipes including formulations, scaling, secure approvals, and versioning
- Includes integrated visualization and reporting



A FactoryTalk Batch application is best for:

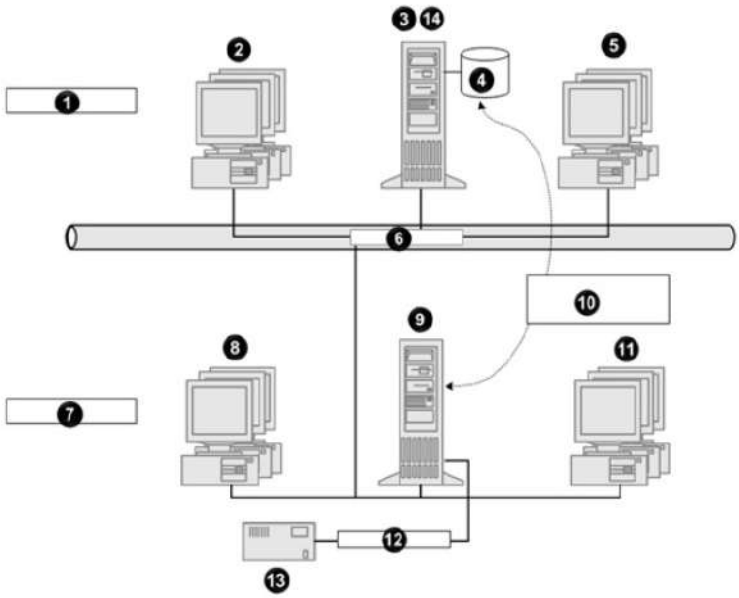
- Multi-unit batch control
- Integration of process skids
- Integration with third-party systems

FactoryTalk Batch Details

A maximum of 10 FactoryTalk Batch servers can exist in a PlantPAx DCS. Follow these guidelines when you install FactoryTalk Batch on the AppServ-Batch server:

- Install the FactoryTalk® eProcedure® server on the same computer as the FactoryTalk Batch server.
- Install the FactoryTalk Batch Material server on a computer with the SQL server. The computer must be different than the computer that hosts the FactoryTalk Batch server.
- Install the FactoryTalk Event Archiver Database and Management Tool on another server from the FactoryTalk Batch server.

Example FactoryTalk Batch Network



No.	Description	No.	Description
1	Site level	8	FactoryTalk eProcedure clients
2	FactoryTalk Batch Material Manager clients	9	FactoryTalk Batch server (1...10) and FactoryTalk eProcedure server
3, 14	FactoryTalk Batch Material server; FactoryTalk Event Archiver database	10	FactoryTalk Batch server connects to SQL server for Master Recipe storage
4	SQL server	11	FactoryTalk Batch clients
5	FactoryTalk Batch clients	12	Proprietary network
6	TCP/IP	13	Process-connected device
7	Plant floor		

For more information, see:

- PlantPAx Batch Design Considerations Reference Manual, publication PROCES-RM008
- FactoryTalk Batch User Guide, publication BATCH-UM011

FactoryTalk Batch Server with Redundant Controllers

Using a FactoryTalk Batch server with redundant controllers requires an understanding of the batch server hold/failure propagation behaviors.

Redundant ControlLogix 5580 controllers do not support ControlNet® communications. This means a FactoryTalk Batch application with active phases isn't a bumpless event when a switchover from primary to secondary controllers occurs.

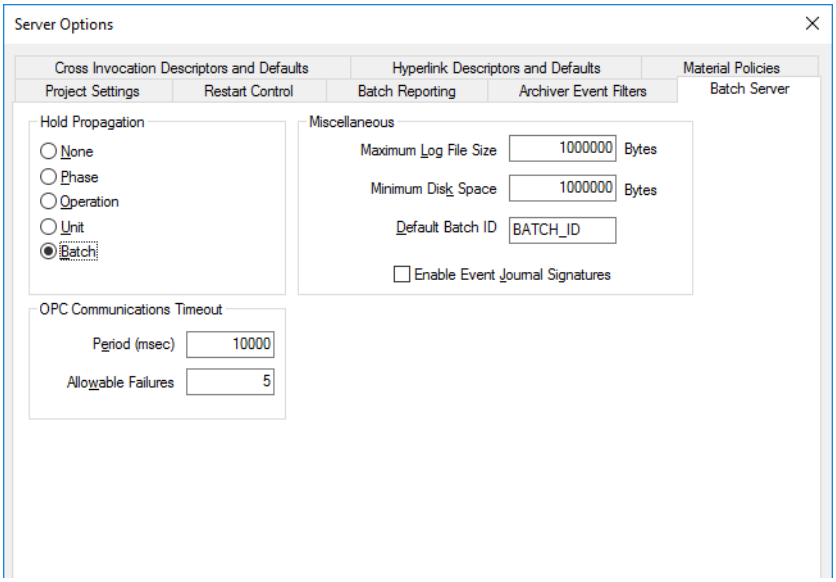
The phases switch over and remain in their respective state and code executes as expected, but the FactoryTalk Batch server observes a brief momentary communication loss over the EtherNet/IP™ network.

This communication loss is enough for the batch server to issue Hold propagation on all recipes with phase actively running in the controller than switched over. In this circumstance, the transitions in the recipe Held while the phases in the controller are still running.

Hold Propagation

The Hold Propagation area lets you indicate the hold propagation type to use when the FactoryTalk Batch server detects a failure that is caused by a watchdog timeout, a handshake timeout, or a phase failure (PHASE_F > 0).

Hold propagation is a configurable selection that defines how the batch server reacts to failures that affect an active control recipe. Configure the selection in the Equipment Editor, which stores the value in the BATCHSVR.INI.



A Hold command that is associated with a failure propagates up through the recipe hierarchy as high as the mode and selected option allows.

Hold Propagation Option	Description
None	The batch server does not issue a Hold command to any level of the running procedure for any phase failure. Therefore, the phase logic is solely responsible for putting a failed phase into Hold.
Phase	The batch server issues a Hold command to only the phase in which the phase failure occurred. This includes only the active step within the operation that experienced the failure, and not the active transition that belongs to the operation. Therefore, only the failed phase is commanded to Hold by the batch server and any other level of the batch remains unaffected such as, any running phase, operation, unit procedure, and the procedure itself
Operation	The batch server issues a Hold command to the running operation in which the phase failure occurred. This includes all active steps and transitions within the operation level of the batch. Therefore, all running phases within this operation, and the active operation transitions are commanded to Hold by the batch server. Any other running operation, unit procedure, and the procedure itself aren't affected by the Hold command; the batch server does not propagate the Hold command to these other levels of the batch.
Unit	The batch server issues a Hold command to the running unit procedure in which the phase failure occurred. All running phases and operations within this unit procedure, and the unit procedure itself, are commanded to Hold by the batch server. This includes all active steps and transitions within these specific levels of the batch operations and the unit procedure. Any other running unit procedure and procedure itself aren't affected by the Hold propagation; the batch server does not propagate the Hold command to these other levels of the batch.
Batch	The batch server issues a Hold command to the entire running procedure in which the phase failure occurred. All running phases, operations, unit procedures, and the procedure itself, are commanded to Hold. This includes all active steps and transitions within all levels of the batch.

The most common event to trigger Hold propagation is an abnormal process condition being continually monitored by the controller.

When an abnormal process event occurs in the system, the controller logic sets phase failure for the appropriate phases actively running in the unit, or units. As a result, the phase failure tags are set with a value greater than zero value by the controller logic. The value corresponds with a known failure condition in the process. The batch server can display the failure to the operators and record the appropriate phase failure event.

State Composite Evaluation

The Hold propagation configuration determines the highest procedure level within the running recipe for which the Hold command from the batch server is issued when a failure is detected.

The state of each batch level (such as procedure, unit procedure, operation) is continually evaluated by the batch server. Each batch level state is based on the composite states of its underlying steps and transitions.

- In the case of an operation, the composite state is based on the state of all active phases and the state of their underlying active phases transitions.
- In the case of the unit procedure, the composite state is based on the state of all active operation steps and the state of their underlying active operation transitions.

- In the case of the procedure, the composite state is based on the state of all active unit procedure steps and the state of their underlying active unit procedure transitions.

Order of Precedence for Batch States

State	Element Type	Priority
RESTARTING	Step‘	12 (highest)
HOLDING	Step	11
ABORTING	Step	
RUNNING	Step	9
ARMING	Transition	9
ARMED	Transition	9
FIRING	Transition	9
STARTING	Step	8
STOPPING	Step	8
HELD	Step	6
HELD	Transition	6
IDLE	Step	5
ABORTED	Transition	4
ABORTED	Transition	4
STOPPED	Step	3
STOPPED	Transition	3
COMPLETE	Step	2
NOTCONNECTED	Step	1
UNKNOWN	Step	0 (lowest)

If the owner of the step (a phase) is EXTERNAL, then the step isn't considered in the calculation.

The determining state for any procedure level (procedure, unit procedure, or operation) is based on the states of the active recipe elements it contains – both, steps and transitions. All these S88 procedure levels are virtual to the PC memory in the batch server, except for SequenceManager operations which reside in the controller, much like most phases.

When a procedure level of a control recipe is connected and commanded by the batch server, the state of each of its procedure levels is derived by a composite state analysis to determine a final state for each procedure level. As the path of recipe execution proceeds through a control recipe, the state of each recipe element object is dynamic, and is continuously updated. The state with the highest priority becomes the state of the procedure level for an operation, unit procedure or procedure.

- In the case of an Operation procedure level, the composite state is based on the state of all active phases e active transitions within the operation.
- In the case of the Unit Procedure level, the composite state is based on the state of all active operation steps and active transitions within the unit procedure.
- In the case of the Procedure level, the composite state is based on the state of all active unit procedure steps and active transitions in the procedure.

Types of Failures

The batch server translates a phase failure value to an enumeration string that presents an actionable string of text to the operators for the type of failure. A phase failure is the most common type of failure. Other types of failures may occur in the batch system such as, a parameter download failure, a report upload failure, a failed phase request, a request timeout, a command timeout, a quality tag status other than good, a watchdog failure, or a communication failure.

In most cases, the batch server reacts to these failures just as it does for the phase failure event with Hold propagation. An exception occurs whenever the batch server experiences a communication failure to a controller, a data server, or a phase.

When communication to the controller or phase is compromised, the Hold propagation only acts on the components of the control recipe that are without risk, or internal to the batch server memory (procedure, unit procedure, operation). In this case, the risk pertains to those components where the phases or SequenceManager operations reside, so Hold propagation isn't executed to the phase level or SequenceManager operations.

If communications are restored quickly so the watchdog in the controller does not time out and place the running phases into a Held state, running phases stay running as if nothing occurred. If communications are restored quickly and the controller phases aren't configured to Hold upon communication loss, then running phases also stay running as if nothing occurred.

This momentary communication blip where phases remain running can cause a dynamic when all other levels (procedure, unit procedure, operation) are sent Hold commands upon failure according to the Hold propagation configuration. As a result, these procedure levels are Held but the composite state of a running phase and Held transition is running state for the operation. This traverses up the control recipe where a running operation step and a Held unit procedure transition evaluates as a running state for the unit procedure, and so on one more level to the procedure. With transitions Held, the recipe can't move transition to other steps, and the recipe could act to an untrained operator as though it's hung, or unresponsive. One solution is to issue a Hold command to the control recipe, then a restart to the control recipe to get all steps and transitions in an active and running state as expected.

In the case of redundant systems with newer ControlLogix firmware revisions that do not use ControlNet communication, the switchover of the controllers where active phases are being run by the FactoryTalk Batch application isn't a bumpless event. The phases switch over and remain in their perspective state and code executes as expected, but the FactoryTalk batch server observes a brief momentary communication loss. This loss is enough for the batch server to issue Hold propagation on all recipes with phase actively running in the controller than switched over. In this circumstance, you can find transitions in the recipe Held while the phases in the controller are still running.

Notes:

Analytics

Analytics is the discovery, interpretation, and communication of meaningful patterns in data. Analytics relies on the application of statistics, computer programming, and operations research to quantify performance.

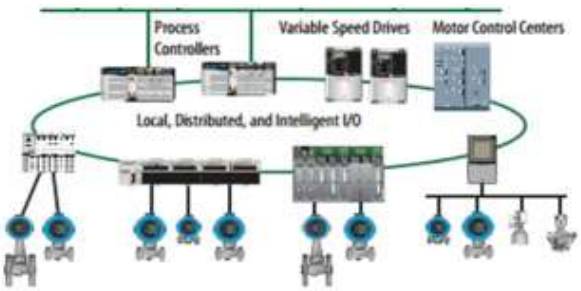
Analytics are the methods that we use to measure our performance and then provide feedback for continuous improvement. Analytics drive business value, regardless of the industry, by helping to:'

- bring a product to market faster
- lower the total cost of ownership because of more effective maintenance
- improve asset utilization by maximizing the throughput
- provide enterprise risk management

The following options exist for analytics applications in your PlantPAx® system. The reference links provide more details for each option.

Step 1: Device Level Options

Allen-Bradley® products have device-level diagnostics that are built in, such as fault and alarm codes for use in fault routines. Other products provide predictive and prescriptive analytics at the device-level of the architecture.



In your overall solution, you can add these additional products to gather device-level analytics:

- FactoryTalk® Analytics™ for Devices
- FactoryTalk® Analytics™ LogixAI®
- PlantPAx® MPC

For more information, see Device Level Analytics

Step 2: System Level Options

FactoryTalk® products that add system-level analytics include:

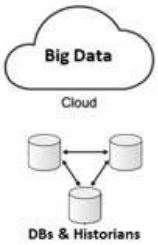
- Pavilion8®
- FactoryTalk® Analytics™ Edge Gateway™
- FactoryTalk® Analytics™ DataView
- FactoryTalk® TeamONE™

For more information, see System Level Analytics

Step 3: Enterprise-Level Options

FactoryTalk products that add enterprise-level analytics include:

- FactoryTalk® Analytics™ Edge ML
- FactoryTalk® Analytics™ DataView

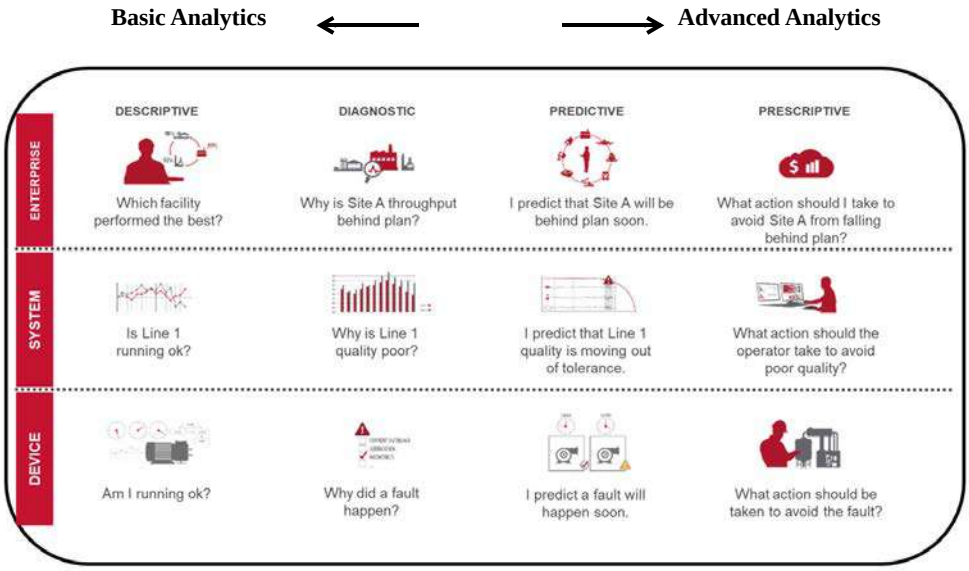


At the Industrial Internet of Things (IIoT) level, you can add:

- Vuforia® Augmented Reality
- ThingWorx® Industrial IoT platform

For more information, see Enterprise-Level Analytics

Information Enables Outcomes



Device Level Analytics

The ControlLogix® and CompactLogix™ process controllers display alarm and troubleshooting details for the embedded process instructions on the property pages for the process instructions.

In your control strategy, you can use:

- Tag-based alarms
- Alarm faceplates
- Automatic device descriptive analysis (firmware revision 33 and greater) to display device fault conditions in applications and client devices that are supported by FactoryTalk® Alarms and Events.

Device-level analytics provide:

- Streaming analysis
- Runtime deployment

- Device data generation

Option	Description	
FactoryTalk Analytics for Devices	Embedded analytics software that lets you implement device level, descriptive, and diagnostics analytics to improve maintenance and engineering reliability. Automated device health diagnostics provides data to an information platform with or without cloud connectivity **PlantPAx specific content:** • Advanced Process Controller action card • E+H device support • Robust HART diagnostic information	**Type:** Descriptive, Diagnostic **Environment:** Appliance on EtherNet/IP™ network Available via the subscription portal **Requirements**: • 6200PC-FTA4DT11M FactoryTalk Analytics for Devices appliance
FactoryTalk Analytics LogixAI	Embedded analytics software that enables controls engineers to apply models to make predictions in ControlLogix applications. Automated modeling capabilities that enable predictive capabilities in the controller.	**Type:** Diagnostic, Predictive **Environment:** ControlLogix chassis Available via the subscription portal **Requirements**: • 1756M-FTALGXAIT11M FactoryTalk Analytics LogixAI appliance
PlantPAx MPC	Model Predictive Control embedded in ControlLogix systems • Multi-variable in and multi-variable out • Predictive control • Reduction in variability	**Type:** Predictive, Prescriptive **Environment:** ControlLogix chassis **Requirements**: • 1756-PPMPC or 9529-PPMPCENM module

System Level Analytics

System-level analytics provide:

- Data management, transformation, and harmonization
- Model training and deployment
- Pattern extractions

Option	Description	
Pavilion8®	Provides closed-loop, prescriptive analytics to continuously maximize process performance in quality, throughput, and efficiency. • Model-based advanced, dynamic control drives stable performance • Integrated MPC, calculation, and soft sensor visualization and performance reporting	**Type:** Predictive, Prescriptive **Environment:** Server based **Requirements**: • Pavilion8 software
FactoryTalk Analytics Edge ML (also applicable at enterprise-level)	A machine learning application that provides expert-driven data analytics within the plant, where low latency is a requirement. • Helps make decisions as close as possible to the data • Reduce loads on controllers by off-loading data preprocessing • Reduces deployment time costs • Out-of-box connectivity reduces design time	**Type:** Predictive **Environment:** Server based Part of the FactoryTalk Analytics; available via the subscription portal **Requirements**: • FactoryTalk Analytics Edge ML base bundle or • FactoryTalk Analytics Platform base bundle
FactoryTalk Analytics DataView (also applicable at enterprise-level)	An analytics visualization tool that lets you access and transform data through storyboards. Gain a business understanding of data to pinpoint opportunities for improvement. • Reduces time to value by reducing the dependence on data architects and data scientists • Enables self-service analytics • Eliminates the need for expensive infrastructure that is associated with traditional warehousing	**Type:** Descriptive, Diagnostic **Environment:** Server based Part of FactoryTalk Analytics; available via the subscription portal **Requirements**: • FactoryTalk Analytics DataView base bundle or • FactoryTalk Analytics Platform base bundle

Enterprise-Level Analytics

Enterprise-level analytics provide:

- Data visualization
- Data mining
- Enterprise resource planning
- Model training
- Model operationalization
- Pattern extraction

Option	Description	
FactoryTalk Analytics Edge ML (also applicable at system-level)	Provides data capture, transformation and analytical capabilities, including predictive machine learning, right on the edge. • Pull structured and unstructured data from multiple sources • Access data in intelligent devices • Preprocess data for analytics • Enable bidirectional, transactional type data • Execute closed-loop, Edge-level machine learning • Develop custom applications and connectors	**Type:** Predictive **Environment:** Server based Part of FactoryTalk Analytics; available via the subscription portal **Requirements**: • FactoryTalk Analytics Edge ML base bundle or • FactoryTalk Analytics Platform base bundle
FactoryTalk Analytics DataView (also applicable at system-level)	An analytics visualization tool that lets you access and transform data through storyboards. Gain a business understanding of data to pinpoint opportunities for improvement. • Reduces time to value by reducing the dependence on data architects and data scientists • Enables self-service analytics • Eliminates the need for expensive infrastructure that is associated with traditional warehousing	**Type:** Descriptive, Diagnostic **Environment:** Server based Part of FactoryTalk Analytics; available via the subscription portal **Requirements**: • FactoryTalk Analytics DataView base bundle or • FactoryTalk Analytics Platform base bundle
Vuforia® Augmented Reality	An industrial augmented reality platform that can improve workforce efficiency and customer satisfaction with real-time, step-by-step work instructions and data. • Work instructions become handsfree and are delivered in real time where assembly or field service take place. • Tribal knowledge of experienced workers is captured and shared with new workers and service technicians. • Remote expertise can be delivered to workers no matter where they are in the world. **PlantPAx specific content:** • Process strategy experience templates provide users with faceplate-like features within an AR experience. The templates enable users to build additional functionality around the PlantPAx information.	**Type:** Descriptive, Diagnostic **Environment:** Cloud-based Part of the FactoryTalk® InnovationSuite Bulletin 95057C; available via the subscription portal **Requirements**: • Vuforia Engine software • Vuforia Studio software • Vuforia Chalk software • Vuforia Expert Capture software
ThingWorx® Industrial IoT platform	An integrated, secure solution to minimize risk, reduce IT burden, and maximize value from the software investment. ThingWorx industrial connectivity provides data access for client applications such as MES and SCADA and IoT and Big Data analytics software. It leverages OPC and IT-centric communication protocols to provide a single source of industrial data. Supported protocols include proprietary protocols (including GE NIO, SuiteLink/FastDDE, and Splunk), IT protocols (including MQTT, REST, ODBC, and SNMP), and flow measurement export to common Oil & Gas industry formats. ThingWorx industrial connectivity provides a single solution to collect, aggregate, and securely access industrial operations data. Connect, manage, monitor, and control diverse automation devices and software applications through one intuitive user interface **PlantPAx specific content:** • Process strategy Thing templates replicate structure and functionality within ThingWorx, which enable users to create an analysis of the objects with Live and Historical Data • ThingWorx mashup templates provide the ability to investigate alarms by area, priority, and other critical alarming criteria. Advanced alarm analysis includes fleeting, chattering, and stale alarm insights. Similar dashboard functionality is also provided for SQL server reporting services.	**Type:** Descriptive, Diagnostic, Predictive, Prescriptive **Environment:** Cloud-based Part of the FactoryTalk Innovation Suite Bulletin 95057C; available via the subscription portal **Requirements**: ThingWorx platform software • Asset Advisor • Operator Advisor • Production Advisor • ControlAdvisor ThingWorx Industrial Connectivity software

PlantPAx SQL Process Object and Alarm Reports

The process library includes standard reports via SQL Server Report Services that support basic and advanced alarm and event reports, along with per process object reporting.

The standard reports use data that is collected via FactoryTalk® AssetCentre, FactoryTalk® Alarms and Events, and FactoryTalk® Historian SE. An SQL Asset Framework processes the data from the system historian and consolidates the data into a central database, based on a reporting schedule.

The PlantPAx reports include:

Category	Reports	
Base	• Analog In (PAI) • Analog Output (PAO) • Deadband Controller (PDBC) • Digital In (PDI)	• Digital Out (PDO) • Totalizer(PDOSE) • Motor (PMTR) • PID Controller (PPID) • Valve (PVLV)
Alarming	Area Based: • Alarm History • Alarm Top • Maintenance (Dashboard) • Chattering • Fleeting • Stale	Object Based: • Alarm Object History
Traceability	• Audit All Data • Audit Sequence of Events • Object Events • System Audit	
System	• Top Logger • Top Logger Detailed • Database Status • Shift Setup	

For more information on how to deploy and utilize the reports, See Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*. Download the PlantPAx SQL Process Object and Alarm Reports file from this public article.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Automatic Diagnostics Compatibility

Automatic diagnostics is a system-level feature in devices that provides device diagnostics to HMIs and other clients, with zero programming. Devices that support automatic diagnostics have the feature enabled by default.

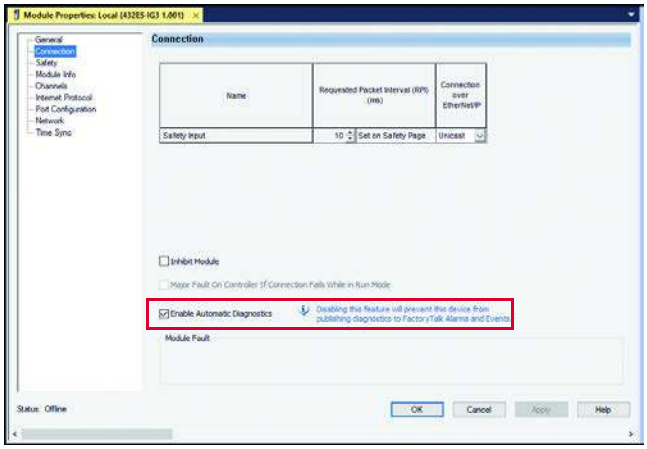
You can deactivate and activate the whole feature while online or offline from the Controller Properties dialog box. You can also deactivate automatic diagnostics for a specific device in the module properties.

Configure Automatic Diagnostics

On the Controller properties Advanced tab, Enable Automatic Diagnostics is a new feature that was added with the process controllers, firmware revision 33. When enabled, it sends analog I/O modules diagnostic information to the Automatic Diagnostics Event Summary object.

If deactivated, you only see Mode changes and loss on communication with controllers in the Automatic Diagnostics Event Summary object.

The automatic diagnostics feature is enabled by default in the Logix Designer application. The deactivation of automatic diagnostics at the device level deactivates all device-driven diagnostics. You still get device faulted/ communication loss diagnostics as the controller drives these diagnostics.



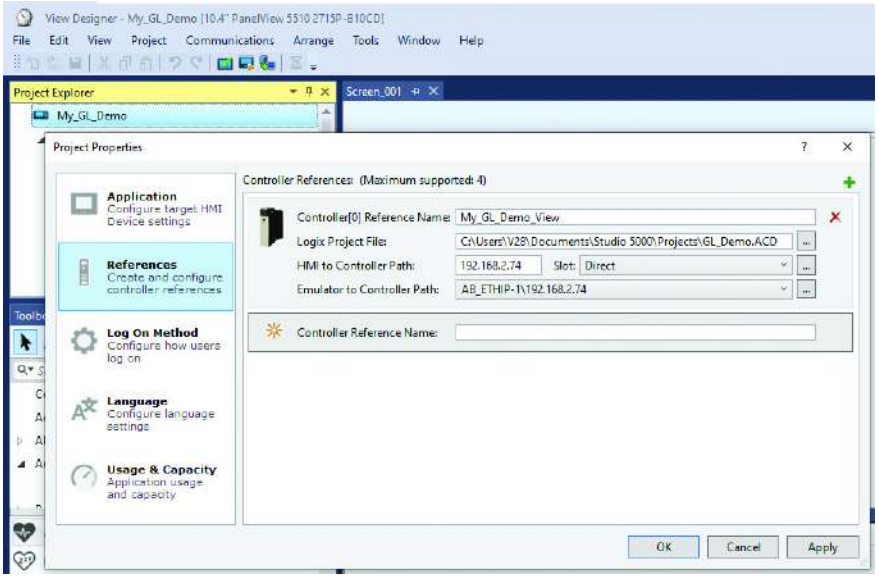
Automatic Diagnostics on PanelView 5000 Display

Automatic diagnostics are enabled by default on all devices. When you use a PanelView 5000 display with firmware revision 8 or later, the automatic diagnostic messages from the device display automatically. For more information, see the Automatic Diagnostics chapter in publication 9324-GR001.

When specific events occur, messages automatically report because the controller links to the PanelView 5000 display. In your View Designer project properties, set the Controller References to the controller of the 432ES network interface module:

- Logix project File
- HMI to controller
- Emulator to controller path

Figure 22 - Bind Controller to PanelView Project



When an event occurs, the diagnostic icon shows the number of active and unsuppressed diagnostic events. Each line entry shows:

- State: Active, inactive, or suppressed
- Event Time: Date and time when the event occurred
- Device Name: Path to the device and the device name
- Message: Preprogrammed message for the diagnostic code
- Diagnostic Code: The diagnostic code that applies to the event

IMPORTANT You can rearrange and configure additional columns. See Studio 5000 View Designer® help for more information.

Figure 23 - Diagnostics Page on PanelView 5510

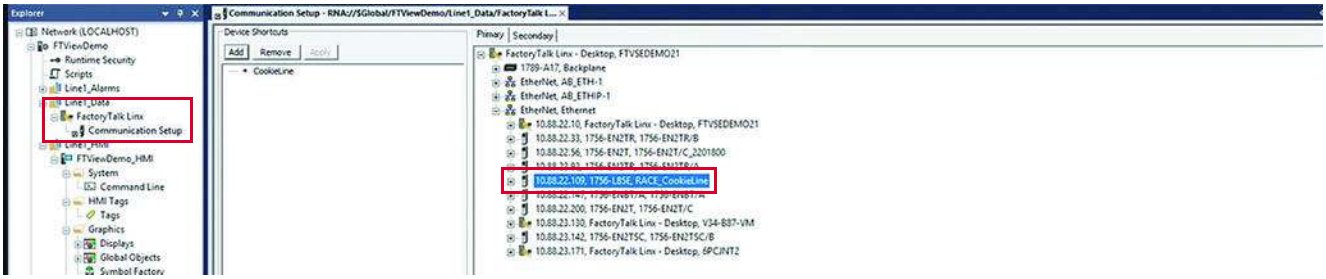
Automatic Diagnostics on FactoryTalk View SE

IMPORTANT Verify that FactoryTalk Alarms and Events is installed and configured before attempting to view automatic diagnostics. For more information, see publication FTAE-RM001.

You can use the Subscribe To setting under FactoryTalk Alarms and Events in FactoryTalk Linx to activate or deactivate diagnostic information that is sent to the Automatic Diagnostics Event Summary object.

Subscribe To

1. To adjust your automatic diagnostics, access the Communication setup and select your device.



2. To receive all notifications from your devices, set the Subscribe To setting to All Alarms & Events Notification Messages.

If the Subscribe To is set to Only Alarms Notification Messages, then the Automatic Diagnostics Event Summary object is blank.

View Automatic Diagnostic Messages

IMPORTANT After Logix version 33 release, any device can participate in automatic diagnostics with an AOP update.

Events are delivered through FactoryTalk® Alarms and Events (FTAE) with FactoryTalk View Site Edition (SE) v12 and greater as a Display Client™.

Figure 24 - FTView SE v12.0 Automatic Diagnostics Example

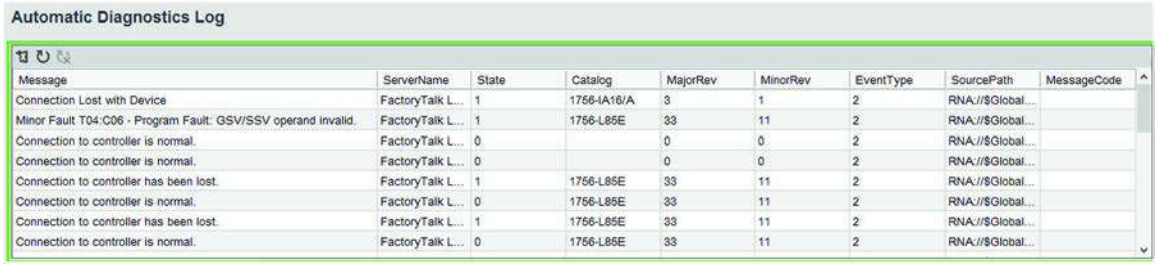
To view these diagnostic messages, you need:

- FactoryTalk Alarms and Events, version 6.20 and greater
- FactoryTalk View SE, version 12 and greater

Automatic diagnostics are enabled by default. Check the configuration of your device to see whether the firmware supports automatic diagnostics.

Automatic Diagnostics History

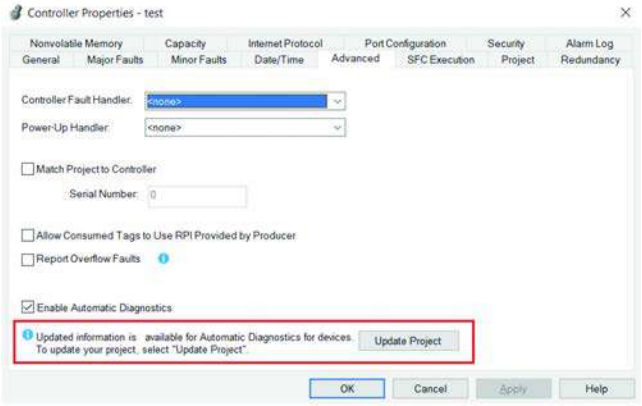
FactoryTalk Alarms and Events (FTAE) keeps a historical log all Automatic Diagnostics activity. The historical log is stored in the same SQL database as the FTAE alarms. FTLinx must be configured to log alarm and event historical information into the SQL database. In the FTView SE application, the historical log is viewed using the data grid control. From the data grid, you can export to CSV.



Online Updates of Device Additional Diagnostics

- Additional device diagnostics are distributed with updated AOPs
- These additional device diagnostics can be added while online to a running controller
- You are notified that updates are available in the following ways:
  - Project verification warning

  - Information message in the controller Properties (Advanced tab)



Additional diagnostics can be downloaded to the controller by pressing the Update Project button.

PlantPAx Security Certification

The PlantPAx® architecture supports IEC-62443-3-3 SL 1 security requirements. To help meet these requirements, reference these publications:

For this information	See
Guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.	System Security Design Guidelines Reference Manual, SECURE-RM001
Network architecture recommendations	Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001
Windows® infrastructure recommendations How to configure and use these Rockwell Automation products: • FactoryTalk® Directory • FactoryTalk® Activation Manager • FactoryTalk® Security • FactoryTalk® AssetCentre	Security Configuration User Manual, publication SECURE-UM001.
How to configure and use CIP Security™ with Rockwell Automation products to improve the security of your industrial automation system	CIP Security™ with Rockwell Automation Products Application Technique, publication SECURE-AT001

PlantPAx Security Architecture

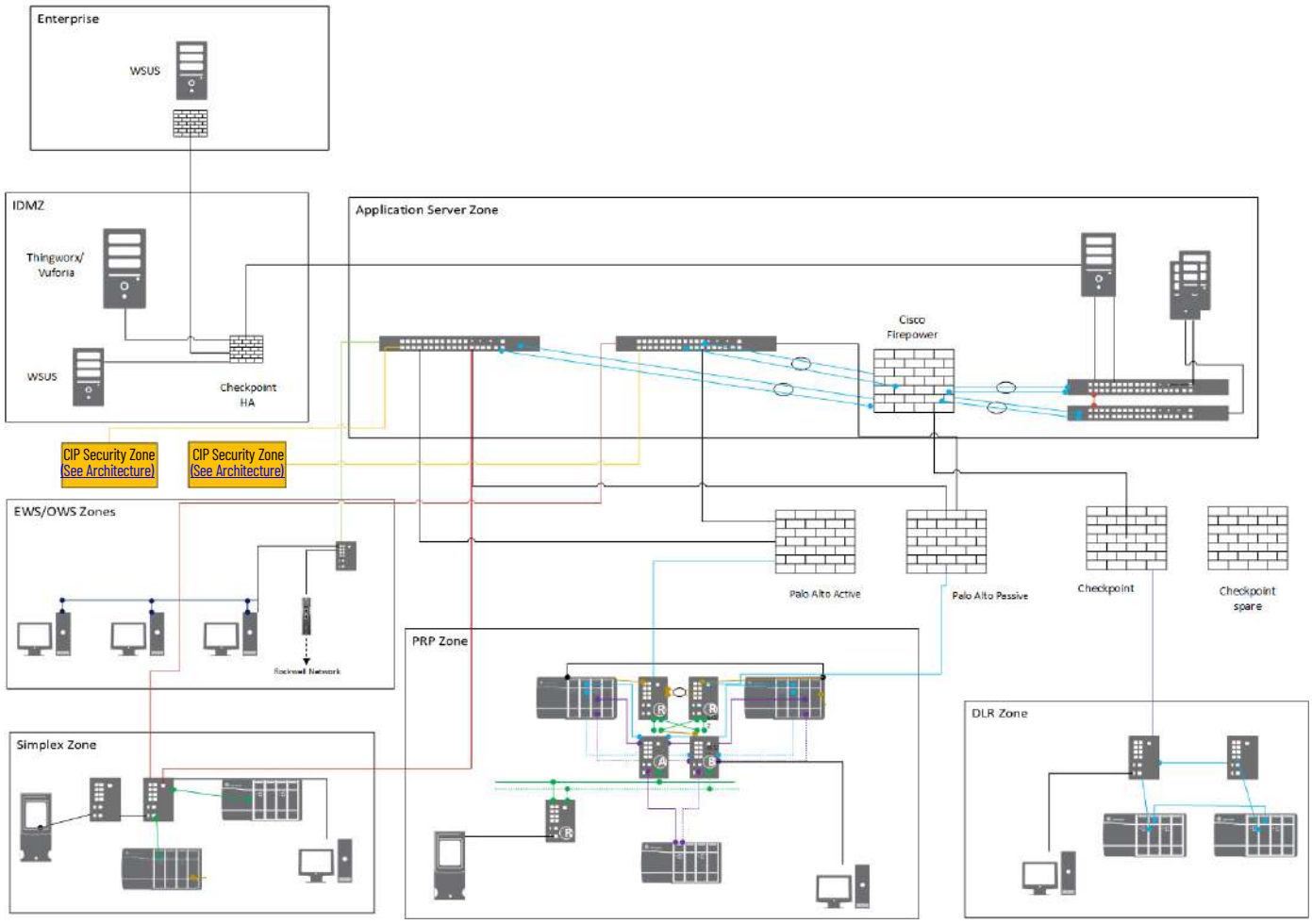
Integrating industrial automation and control systems (IACS) with enterprise-level systems enables better visibility and collaboration, which helps improve efficiency, production, and profitability. But greater connectivity also exposes control systems to additional cybersecurity risks. Availability is the most crucial aspect of a secure IACS. To meet the needs of industrial environments, Rockwell Automation aligns PlantPAx systems that are developed on our technology with the international standard ISA-99/IEC 62443-3-3. This standard is designed specifically for Industrial Automation and Control Systems and defines procedures to implement an electronically secure system.

ISA-99/IEC 62443 is based on seven foundational requirements that cover a defense-in-depth approach that is suited for an IACS. These foundational requirements are:

- FR1: Identification and authentication control (IAC)
- FR2: Use control (UC)
- FR3: System integrity (SI)
- FR4: Data confidentiality (DC)
- FR5: Restricted data flow (RDF)
- FR6: Timely response to events (TRE)
- FR7: Resource availability (RA)

The guidelines and checklists in this appendix present the collective strategy to meet the ISA-99/IEC 62443-3-3 SL1 requirements in conformant PlantPAx systems. The intent of a certified architecture is to demonstrate security competency, as well as to provide a standard, prescriptive reference design.

The certified PlantPAx architecture relies on zones to segment the system.



Zone	Description
IDMZ	An IDMZ is required to connect to the corporate network. This zone contains a firewall stack, a pivot host, SEP Server and WSUS host. Additional hosts can be added, as needed. Configure the IDMZ to separate untrusted (public) zones from the trusted (private) zones. Communication outside of the IDMZ is considered untrusted.
Application Server	The Application Server zone houses all application servers. Each server is deployed on a separate VM. The following mandatory nodes must be deployed: • FactoryTalk Directory server • FactoryTalk® View SE HMI server • FactoryTalk View Data server Other optional servers include: • FactoryTalk® Historian server • FactoryTalk® AssetCentre server • SQL server
EWS/OWS	This zone contains the engineering workstations to provide programmer access and the operator workstations to provide operator access. Each workstation has the necessary software to program or interact with the system. Workstations can be virtualized or they can be ThinManager® clients. Each EWS has: • Studio 5000® environment • FactoryTalk View Enterprise Edition • RSLinx® Classic • FactoryTalk AssetCentre client Additional software includes: • Studio 5000 Application Code Manager, • Microsoft® Office • PuTTY Each OWS has the FactoryTalk View runtime client. Additional software includes: • FactoryTalk Historian client • FactoryTalk AssetCentre client • Microsoft Office
PRP DLR Simplex	The control system is segmented into process areas. Each process area contains the hardware necessary to run and operate that area. The topology of each area can be: • PRP • DLR • Simplex

Trusted Zones

ISA-99/IEC 62443-3-3 SL1 requires the capability to separate trusted and untrusted zones. You can use a standard firewall implementation to separate trusted traffic and untrusted traffic. Standard implementation creates two basic security zones that are known as inside and outside. The inside, or trusted zone, is also referred to as the private zone. The outside, or untrusted zone, is also known as the public zone. The public zone is outside the control of an organization and can be thought of as simply the public Internet.

Rockwell Automation recommends a risk assessment for network security zoning. Your risk assessment and risk posture help determine the trust level of each zone. You can have multiple levels of trust on inside zones with different types of access. For further guidance on risk assessments, see the ISA-99/IEC 62443-3-2 standard.

Certificate Authority

A trusted certificate authority, also known as a commercial certificate authority, is a third-party entity that issues certificates for organizations that request them. They aren't controlled in any way by the person or organization that requests a certificate from them. A trusted CA issues publicly trusted

digital certificates that meet at least the minimum regulatory standards (baseline requirements) that are outlined by the CA/Browser Forum (CA/B Forum).

A private certificate authority, also known as private PKI, is an internal CA that exists within a larger organization (typically an enterprise) that issues its own certificates.

- A private CA functions like its public counterparts, but a private CA's certificates are trusted only by its internal users, clients, and IT systems.
- A private CA issues certificates that restrict access to a select group of users.
- You must configure and host the private CA yourself.

For more information about CAs, see Microsoft Server Certificate Deployment Planning information or the Microsoft documentation for your operating system.

System Security Feature Checklists

Use the following checklists to secure your system.

Identify and authenticate all users.

Requirements for Identification and Authentication Control

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Windows® infrastructure	Yes	Configure and use the following: • Create Active Directory groups and unique users for each zone • Enable 802.1X authentication on all switchports • Implement encryption algorithms for wireless access (such as WPA2 Enterprise, TLS, or IPSEC) • Implement public key infrastructure (PKI) certificates • Authenticate Group membership via a RADIUS server • Enable system notifications • Configure Kerberos • Configure an interactive login policy • Monitor unsuccessful login attempts For more information, see: • Configure System Security Features User Manual, SECURE-UM001 • System Security Design Guidelines Reference Manual, SECURE-RM001 • Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, ENET-TD006 • Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, ENET-TD008 • Site-to-Site VPN to a Converged Plantwide Ethernet Architecture Design and Implementation Guide, ENET-TD012
	Password strength and recommendations	Yes	Follow standard guidelines for password strength and recommendations For more information, see: • NIST Special Publication 800-63B Digital Identity Guidelines • Configure System Security Features User Manual, SECURE-UM001 • System Security Design Guidelines Reference Manual, SECURE-RM001
	Windows domain	Yes	• Configure the PlantPAx domain controller. • Configure all operating system clients as domain members • Enable multi-factor authentication on the domain controller • Create and manage all accounts in the Active Directory • Require administrative credentials to manage account activities For more information, see: • Chapter 2 Domain or Workgroup • System Security Design Guidelines Reference Manual, SECURE-RM001

Requirements for Identification and Authentication Control

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	FactoryTalk Directory software FactoryTalk Security software	Yes	Configure appropriate: • Users, groups, roles • Security policies For more information, see: • Configure System Security Features User Manual, SECURE-UM001. • System Security Design Guidelines Reference Manual, SECURE-RM001
	Wireless access	Optional	Configure and use the following: • Implement encryption algorithms for wireless access (such as WPA2 Enterprise, AES Encryption TLS, or IPSEC) • Obtain access to the IACS from an untrusted network through the IDMZ with multi-factor authentication and certification-base authentication • Use encryption tunnels (such as VPN and IPSEC) between VLANS • Allow remote access only when necessary to authorized users in the Active Directory **Important:** Hardwired connections are always preferred. Never use wireless connections for safety functions. For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001
	FactoryTalk Secure Remote Access	Optional (Required if access via untrusted networks is desired)	Configure appropriate: • Users, groups, roles • Security policies • Logging By default, MFA is enforced for all users Traffic is encrypted For more information, see: • Stratix 4300 Remote Access Routers user manual, 1783-UM014A-EN-P

Define control policies to control the use between users and assets.

Requirements for Use Control

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Windows infrastructure	Yes	Configure and use the following: • Active Directory Groups for each zone • Group membership authentication via RADIUS server • 802.1X authentication on all switchports • Session lock • Remote session termination • Concurrent session control • Interactive login policy • Notifications for unsuccessful login attempts For more information, see: • Configure System Security Features User Manual, SECURE-UM001 • System Security Design Guidelines Reference Manual, SECURE-RM001 • Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, ENET-TD006 • Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, ENET-TD008
	Windows domain	Yes	Configure all operating system clients as domain members For more information, see: • Chapter 2 Domain or Workgroup
	FactoryTalk Directory software FactoryTalk Security software	Yes	Configure appropriate User Groups in each Area to support the segregation of duties and least privilege For more information, see: • Configure System Security Features User Manual, SECURE-UM001.

Requirements for Use Control

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	ThinManager software	Recommended	Manage mobile and portable device access via a ThinManager server and route through the IDMZ. The ThinManager server limits mobile applications to view only. For more information, see" • ThinManager and FactoryTalk View SE Deployment Guide, TM-AT001 • ThinManager User Manual, TM-UM001
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Auditable events • Audit storage capacity • Diagnostics and health log For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001

Protect the integrity of transmitted data. Recognize changes to information during communication.

Requirements for System Integrity

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Windows infrastructure	Yes	Configure and use the Active Directory and domain structure to handle authorization. For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001
	Converged Plantwide Ethernet architecture (CPwE)	Yes	Configure the Industrial Demilitarized Zone (IDMZ) with appropriate firewalls. Use TCP/IP connections between zones. For more information, see: Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, ENET-TD001
	Antivirus software	Yes	Use antivirus and anti-malware software to harden workstations. **Important:** Confirm that antivirus software does not affect control system processing. For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001
	CIP Security™	Recommended	Use FactoryTalk® Policy Manager software (installed on the FactoryTalk Directory Server) to define communication between zones. For more information, see: • CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001 • Deploying CIP Security within a Converged Plantwide Ethernet Architecture, ENET-TD022 • FactoryTalk Policy Manager Getting Results Guide, FTALK-GR001
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Change detection and reporting • Scheduled backups For more information, see: • Configure System Security Features User Manual, SECURE-UM001 • System Security Design Guidelines Reference Manual, SECURE-RM001
	PlantPAx process instructions and object library	Recommended	The process instructions and library objects are designed to work with Rockwell Automation products to provide: • Input validation • Deterministic output • Alarms and error handling For more information, see PROCES-RM200

Protect the confidentiality of communication and data to help prevent unauthorized disclosure.

Requirements for Data Confidentiality

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Converged Plantwide Ethernet architecture (CPwE)	Yes	Segment the network into the required zones and use firewalls. Use conduits to zone-to-zone connections. Use encrypted hard disk drives in computers. If necessary, use cryptographic algorithms according to industry practices. For more information, see: • Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, ENET-TD001 • Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture, ENET-TD002
	CIP Security	Recommended	Use FactoryTalk Policy Manager software (installed on the FactoryTalk Directory Server) to define communication between zones. **Note:** Integrity only does not provide confidentiality. Use CIP Security confidentiality profile if confidentiality is desired. For more information, see: • CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001 • Deploying CIP Security within a Converged Plantwide Ethernet Architecture, ENET-TD022 • FactoryTalk Policy Manager Getting Results Guide, FTALK-GR001
	Wireless access	Recommended	Configure and use the following: • Implement encryption algorithms for wireless access (such as WPA2 Enterprise, AES Encryption TLS, or IPSEC) • Implement the PKI infrastructure to aid device authentication For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001

Segment the network into zones and conduits to manage the flow of data.

Requirements for Restricted Data Flow

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Converged Plantwide Ethernet architecture (CPwE)	Yes	Segment the network into the required zones. • Use a separate VLAN for each zone. • Firewalls provide additional protection For more information, see: • Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, ENET-TD001 • System Security Design Guidelines Reference Manual, SECURE-RM001
	Virtualization	Recommended	PlantPAx uses virtual templates to support partitioning data. For more information, see: • Virtualization on page 280.
	CIP Security	Recommended	Use FactoryTalk Policy Manager software (installed on the FactoryTalk Directory Server) to define conduits. For more information, see: • CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001 • Deploying CIP Security within a Converged Plantwide Ethernet Architecture, ENET-TD022 • FactoryTalk Policy Manager Getting Results Guide, FTALK-GR001
	Network Attached Storage (NAS)	Recommended	Use Network Attached Storage (NAS) in a segmented location to store backups of virtual images, system documentation, and related files where a FactoryTalk AssetCentre application isn't appropriate.

Collect and access security logs.

Requirements for Timely Response to Events

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Audit log accessibility • Continuous monitoring For more information, see: • Configure System Security Features User Manual, SECURE-UM001. • System Security Design Guidelines Reference Manual, SECURE-RM001
	FactoryTalk Secure Remote Access Software	Optional (Required if access via untrusted networks is desired)	For more information, see Remote Access on page 282
	Individual products in the system	Yes	Protect the internally stored audit logs in individual products in the system. Configure the FactoryTalk AssetCentre audit log to collect these individual audit logs. For more information, see the user documentation for the individual products.

Maintain the availability of the system against the denial-of-service events.

Requirements for Resource Availability

✓	Product	Required to Meet IEC-62443-3-3 SL 1	Details
	Windows infrastructure	Yes	Configure the operating system to prioritize control system functionality over antivirus checks and patching. Network redundancy is highly recommended. Configure virtualization software to manage service limitation. Download software patches from trusted sources. For more information, see: • System Security Design Guidelines Reference Manual, SECURE-RM001
	Managed switches	Yes	Configure managed switches for both distribution and access functions. Use QoS and ACLs to configure proper segmentation. For more information, see: • Chapter 4 Network Infrastructure • Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, ENET-TD001
	FactoryTalk AssetCentre software	Yes	Configure and use the following: • Asset inventory • Control system backup • Disaster recovery For more information, see Configure System Security Features User Manual, SECURE-UM001.
	UPS	Yes	Provide your own UPS with separate battery unit and redundant power supplies. Size the UPS so that is correctly supports the system and provides enough power to properly shut down servers and workstations.

Virtualization

The PlantPAx architecture uses virtual templates, VLANS, and zones to support partitioning data, applications, and services. Virtualization is preferred for all server and client operating systems. The VMware platform works with all Rockwell Automation products in the PlantPAx architecture.

The VMware ESXi hypervisor is on each physical server and configured for management by a central vCenter Standard edition server.

In your VMware implementation, make sure:

- If you support remote access, the asset owner can terminate any remote connections.
- The control system continues normal operation during a backup.

- To maintain audit logs of all backup and restore activities.

VLAN Recommendations

Table 9 -

Zone		VLAN	IP Address	Gateway	Subnet Mask
PRP	Management	500	192.168 10.0/26	192.168.10.1	255.255.255 192
	Controller	501	192.168 10.64/26	192.168.10.65	255.255.255 192
	Operator	510	192.168 10.128/26	192.168.10.129	255.255.255 192
	Engineering	511	192.168 10.192/36	192.168.10.193	255.255.255 192
DLR	Management	400	192.168 11.0/26	192.168.11.1	255.255.255 192
	Controller	401	192.168 11.64/26	192.168.11.65	255.255.255 192
	Operator	410	192.168 11.128/26	192.168.11.129	255.255.255 192
	Engineering	411	192.168 11.192/36	192.168.11.193	255.255.255 192
Simplex	Management	300	192.168 12.0/26	192.168.12.1	255.255.255 192
	Controller	301	192.168 12.64/26	192.168.12.65	255.255.255 192
	Operator	310	192.168 12.128/26	192.168.12.129	255.255.255 192
	Engineering	311	192.168 12.192/36	192.168.12.193	255.255.255 192
Server	Management	600	192.168 53.0/24	192.168 53.1	255.255.255 0
	Application	601	192.168 52.0/24	192.168 52.1	255.255.255 0
OWS/EWS	OWS	610	192.168 50.0/24	192.168 50.1	255.255.255 0
	EWS	611	192.168 51.0/24	192.168 51.1	255.255.255 0
IDMZ	Management	700	192.168 105.0/24	192.168 105.1	255.255.255 0
	Wireless	702	192.168 104.0/24	192.168 104.1	255.255.255 0
	IDMZ	703	192.168 100.0/24	192.168 100.1	255.255.255 0
	IDMZ	704	192.168 101.0/24	192.168 101.1	255.255.255 0
	IDMZ	705	192.168 102.0/24	192.168 102.1	255.255.255 0
	IDMZ	706	192.168 103.0/24	192.168 103.1	255.255.255 0
CIP Security Zones	Management	200	192.168.13.0/27	192.168.13.1	255.255.255 224
	Rapid Mix	201	192.168.13.96/27	192.168.13.97	255.255.255 224
	OEM	202	192.168.13.128/27	192.168.13.129	255.255.255 224
	Blend Fill	203	192.168.13.160/27	192.168.13.161	255.255.255 224
	Clean Place	204	192.168.13.192/27	192.168.13.193	255.255.255 224
	Safety	205	192.168.13.224/27	192.168.13.225	255.255.255 224
	Operator	210	192.168.13.32/27	192.168.13.33	255.255.255 224
	Engineering	211	192.168.13.64/27	192.168.13.65	255.255.255 224

- Network Devices first 10 IP addresses start at .2
- Host IP addresses start at .12
- PRP zone devices (10.2...10.11) and hosts (10.12...10.63)

Remote Access

Follow the best practices referred to in Stratix 4300 Remote Access Routers, Publication 1783-um014.

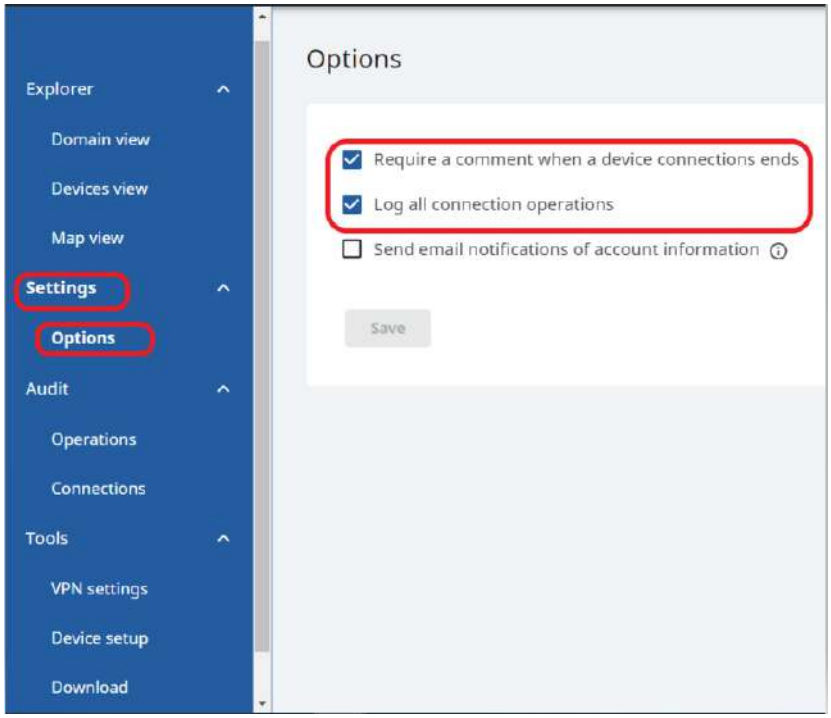
It's required that the following setting be implemented:

- Log all connection operations

It's recommended to require a comment when a device connection ends.

These settings can be enabled by:

1. Log in to the FactoryTalk Remote Access service (via FT Hub)
2. Navigate to Settings > Options >
3. Select the settings and save



CIP Security

CIP Security™ is a standard, open-source communication mechanism that helps to provide a secure data transport across an EtherNet/IP™ network. CIP Security lets CIP™-connected devices authenticate each other before transmitting and receiving data.

CIP Security uses the following security properties to help devices protect themselves from malicious communication:

- Device Identity and Authentication
- Data Integrity and Authentication
- Data Confidentiality

Rockwell Automation uses the following products to implement CIP Security:

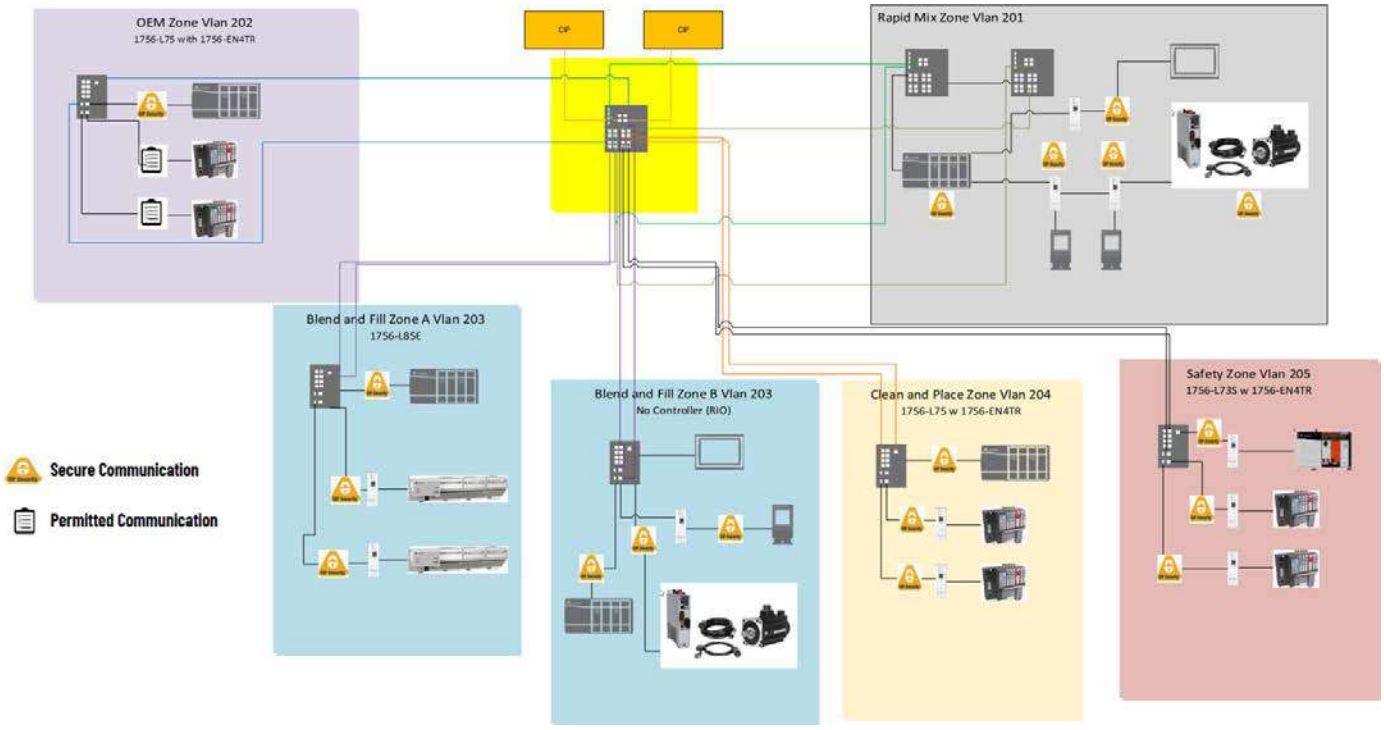
- FactoryTalk® Policy Manager software (includes FactoryTalk System Services, version 6.20 or later)
- FactoryTalk Linx software, version 6.11 or later (lets workstation software communicate securely using CIP Security)
- Studio 5000 Logix Designer® application, version 31.00.00 or later

  This application is required to interface with CIP Security-enabled Logix controllers. The minimum application version varies by controller product family.

For more information on CIP Security, for example, a list of CIP Security-capable products and publications that describe how to use the products, including limitations and considerations, see the following:

- https://www.rockwellautomation.com/en-us/capabilities/industrial-security/security-products/cip-security.html
- CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001

CIP Security Architecture



Notes:

Firewall Configurations

Common Ports

Table 10 shows the most common ports that must be considered during the firewall configuration.

Table 10 - 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 11 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 11 - 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, FactoryTalk® Integrator	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
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, FactoryTalk® View SE, ,FactoryTalk® ViewPoint	FactoryTalk ViewPoint can use any other custom assigned port
123	UDP	NTP	PowerMonitor 3000, AADvance	Network Time Protocol

Table 11 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments
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	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	rnaprpc	FactoryTalk	Object RPC
1331	TCP	rnaserv	FactoryTalk	Service control
1332	TCP	rnaserveping	FactoryTalk	Server health
1433	TCP	N/A	FactoryTalk® AssetCentre (server),	SQL server communication (default port)
1434	UDP	N/A	FactoryTalk AssetCentre (server),	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 isn't 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
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	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

Table 11 - TCP/UDP Port Descriptions

Port	Type	Protocol	Products	Comments
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		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	
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	Four 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	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

Notes:

PlantPAx Deployment Recommendations and Verification Tool

The PlantPAx® verification tool is a Microsoft® Excel® spreadsheet (.xlsx) that helps verify that functionality complies with PlantPAx deployment recommendations.

Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the PlantPAx checklist spreadsheet. Download the spreadsheet from this public article and use the tab that is referenced in each step.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Use the spreadsheet (.xlsx) file as is. There are formulas that correspond to recommended PlantPAx settings. Any edits that you make can affect the validity of the results.

Each section in this appendix contains a checklist that corresponds to a tab in the verification tool. Each item (row) in a checklist corresponds to a row in the verification tool.

Checklist	Description
Design Recommendations Tab	System design considerations and best practices
System Infrastructure Tab	System infrastructure elements that are shared across all servers and workstations
Server or Workstation Tab	Loading and configuration of each individual server and workstation
System Architecture Tab	Design and configuration of your system components
PASS Tab	Design and configuration of the applications that PASS servers host
Controller 5x80 Tab	Application and load on a ControlLogix® 5580 or CompactLogix™ 5380 controller
Controller 5x70 Tab	Application and load on a ControlLogix 5570 or CompactLogix 5370 controller

Design Recommendations Tab

The Design Recommendations tab lists best practices to follow when you design a PlantPAx system.

System ID

Design Recommendation Tab: Overall Considerations

Row	Guidelines	Description
4	PlantPAx Core Software bundle	Catalog number of the PlantPAx Core Software bundle
5	Inventory agent	The System Integrator generated the .raai file via the FactoryTalk® AssetCentre inventory agent The .raai file contains the System ID serial number There could be multiple .raai files, for example, one for each subnet accessible by the FactoryTalk AssetCentre server
6	MyEquipment portal	The System Integrator registered to the system, and provided directions on how to access the MyEquipment portal

The PlantPAx System ID is a unique identifier that helps simplify the management of your application over its lifecycle. The System ID creates a record of the installed hardware and software in the system and provides a dashboard that shows the hardware lifecycle status, notifications of updates and patches, and compatibility information.

The System Integrator uses an Asset Inventory Agent in a FactoryTalk AssetCentre project to generate the System ID and .raai file. The System Integrator registers your System ID with Rockwell Automation and provides you directions on how to access your MyEquipment portal.

Knowledgebase Technote, *PlantPAx System Release 5.10 Configuration and Implementation Tools*, contains the System ID instructions for System Integrators **only** to generate and register a PlantPAx System ID.

You may be asked to log in to your Rockwell Automation web account or create an account if you do not have one. You do not need a support contract to access the article.

Controller Considerations

Design Recommendation Tab: Controller Considerations

Row	Guidelines	Description
7	Controller name	Keep the shortcut, ACD file name, and controller name similar (intuitive). Follow a systematic naming structure to help identify each controller in all system components. Inconsistent naming can create confusion in a production environment.
8	Routine / Tag Names	Follow ISA standards for control strategy and instrument naming schemes. Keep in mind devices that are already labeled in the field and the wire/cable numbers that are in place. Existing names can mean less flexibility for future field device names. ISA tag naming is an industry standard which design firms often follow when developing P&IDs. Link tags in the controller to the P&IDs to help link the process (P&IDs) to the programming within the control system.
9	Controller Organizer	Organize control programs to contain logic based on required execution rates. Organize code in a program within the desired task that aligns with the process area. If code for a given process area must execute at different rates, create multiple programs in different tasks that are related to the same process area. Program names should be the same in the different tasks but with an indication that is embedded within the program name that indicates the task. This helps identify which task the program resides in when the programs are organized in the Logical Organizer.
10	Logical Organizer	In the Logical Organizer, folder names should be the same as the primary graphic display names. The Logical Organizer contains folders which contain the programs for specific process areas. Each folder contains the code that supports the HMI display for a single process area and is aligned with alarm groups. The alarm groups provide navigation to identify which HMI displays contain active alarms. The folders in the Logical Organizer should match the graphical hierarchy (L1, L2 & L3) so that the alarm builder tool creates alarms in the appropriate alarm groups and populates the navigation bars correctly.
11...14	Controller Routines	Have one routine per device to help ensure that online edits only affect that specific device. Name each routine the same as the device name to help identify routines and their devices in the Controller Organizer. Each device (such as motor, valve, PID) should use a standard PlantPAx control strategy that is programmed in function block diagram. Keep supervisory or device control logic external to the device control strategies. This reduces variability among strategies and minimizes the risk of replicating modified control strategies.
15	Controller Programs	Align programs with graphic displays (typically L3 displays) so that the routines in a program have the same primary HMI display. • Alarm annunciation breadcrumbs highlight the associated navigation bar button. • If you add a device to a display, the device is also added to the associated program and alarm group.

Library Considerations

Design Recommendation Tab: Library Considerations

Row	Guidelines	Description
16	Process Library Objects	Do not modify process library Add-On Instructions or graphic objects.

Alarm Considerations

Design Recommendation Tab: Alarm Considerations

Row	Guidelines	Description
17	Standards	Follow ISA 18.2 standards for alarm management
18	ALMA / ALMD Alarm Instructions	Avoid extensive use of ALMA and ALMD instructions. These instructions provide a high-resolution time stamp, but they also use considerable data server bandwidth. Minimize ALMA and ALMD use to only those alarms that require high-resolution time stamps. Instead use tag-based alarms and FactoryTalk® Alarms and Events alarms.

I/O Considerations

Design Recommendation Tab: I/O Considerations

Row	Guidelines	Description
19	RPI	Ideally, the I/O RPI equals half of the task execution time (0.5 * associated task period). The I/O update sampling frequency should be twice the frequency of the logic execution. More frequent sampling over uses I/O communication bandwidth. Less frequent I/O sampling can result in poor control.
20	Consistent I/O Methodology	Select an I/O connection method: I/O mapping, direct I/O connection, aliasing, or program parameters. Choose a method that works best for your installation and consistently apply this method throughout your application.

HMI Considerations

Design Recommendation Tab: HMI Considerations

Row	Guidelines	Description
21	Graphical Framework	Use the Graphic Framework that comes with the process library. This framework helps achieve a consistent delivery of HMI displays.
22	Follow ISA 101 Style Guide	The standards help achieve a consistent delivery of HMI displays. The standards also help draw attention to information that requires attention.
23	Naming Conventions	The naming of graphic displays follows the Logical Organizer hierarchy. This alignment helps locate associated programming for future additions and changes.
24	Design for the Future	Name applications and Areas with future development in mind.

System Infrastructure Tab

The System Infrastructure checklist assumes:

- Your PlantPAx system is operable (for example, the HMI application is running and the latest operating system patches are installed).

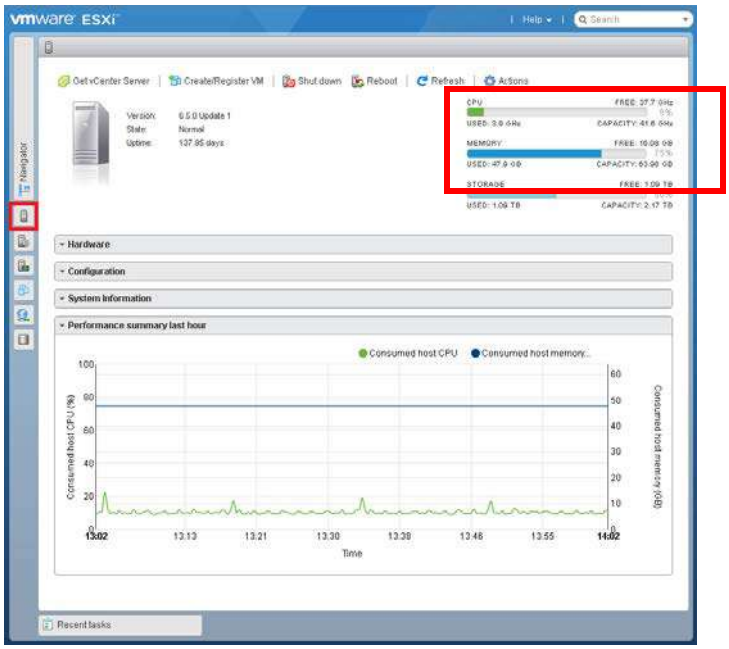
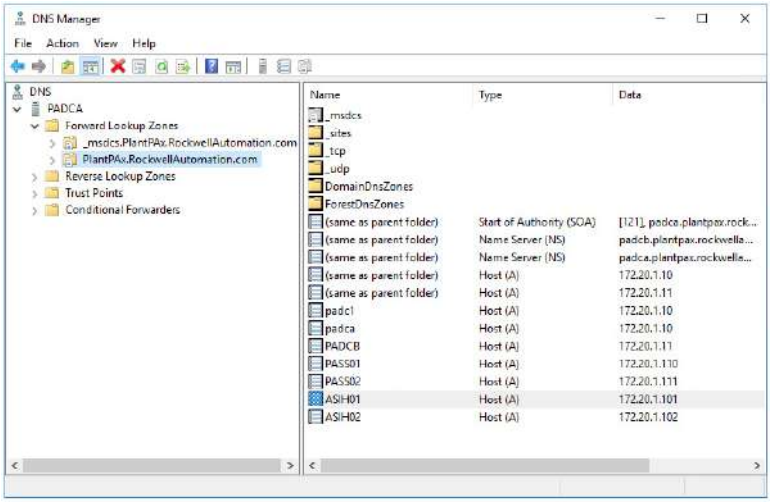
Your system infrastructure has been configured such that:

- You've defined a range of IP addresses for the DHCP server in the domain, if applicable for your system.
- You have created groups and assigned users in the domain controller.
- If you're using virtualization, the VMware vSphere Client software is installed and connected to a vCenter server or ESXi (hypervisor) host.

System Infrastructure Tab

Row	Guidelines	Description
4	Hardware	BIOS Power-Saving Options Disabled? From the computer BIOS, specify whether the BIOS power-saving options are disabled. Power-saving options reduce computer resources for your system elements.
5	Virtualization	Using Virtualization? Specify whether your system uses virtualization. We recommend use of VMware due to the extensive testing and development of PlantPAx virtual templates. VMware also simplifies maintenance, backup, and disaster recovery.

System Infrastructure Tab

Row	Guidelines	Description
6-13	Hypervisors	If you're using virtualization, enter the percentage of CPU use and memory use for each computer. • CPU use recommended to be within 50% of resources • Memory use recommended to be within 50% of resources From the web browser (Firefox recommended), enter the IP address of the vCenter server and log into the web client. If a group of ESXi hosts is available in the selected context, select the host or group of hosts from the Source list to generate an HTML output. Print the output and store with the verification tool. 
14	Domain	All servers and workstations are in the same domain Specify whether all servers and workstations are on a Windows® Domain. On the domain controller, go to Server Manager > Tools > DNS and verify that all servers and workstations are listed in the DNS Manager dialog box.  In the Notes, document any clients that aren't in the domain and why.

Network

To collect the network data, collect the network data manually from the webpages of each switch.

See Chapter 4, Network Infrastructure for details.

System Infrastructure Tab: Network

Row	Guidelines	Description
15	Bandwidth Utilization %	Verify bandwidth < 50%.
16	Packet Error Rate	Verify that there are no packet errors.
17	Temperature OK	Verify that all devices aren't reporting high temperature readings.
18	CPU Utilization %	Verify CPU use ≤ 50%.
19	Memory Utilization %	Verify memory use ≤ 50%.

Servers and Workstations

List the following for each server and workstation in the system (rows 20…93). The Server or Workstation tab is where you record data regarding each server and workstation:

- Computer name
- System role (select from pull-down)

Server or Workstation Tab

The Server or Workstation Name checklist assumes:

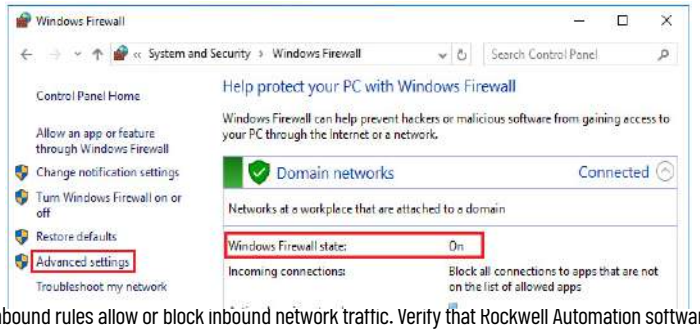
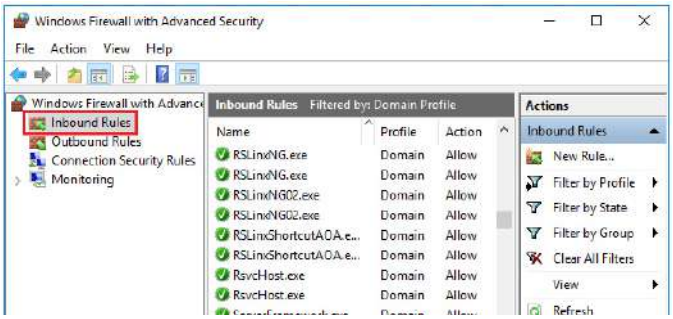
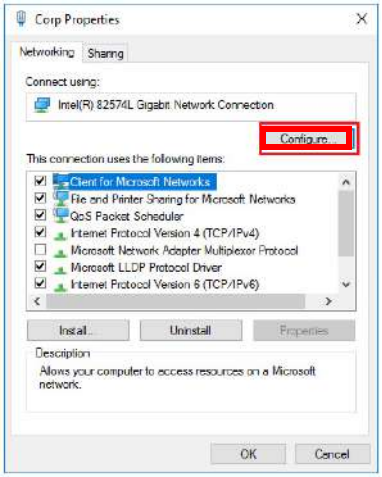
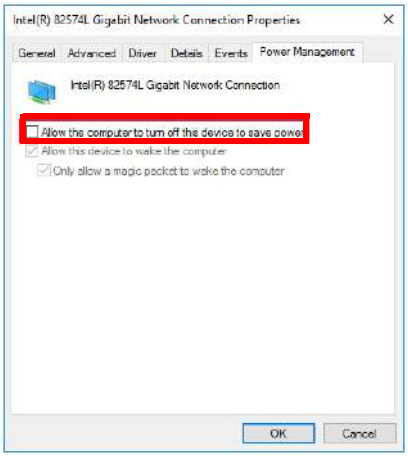
- Your PlantPAx system is operable (for example, the HMI application is running and the latest operating system patches are installed).
- The Performance Monitor (PerfMon) utility is connected to the servers and workstations that are being verified

IMPORTANT Make a copy of this worksheet for each computer (server or workstation) in your system.

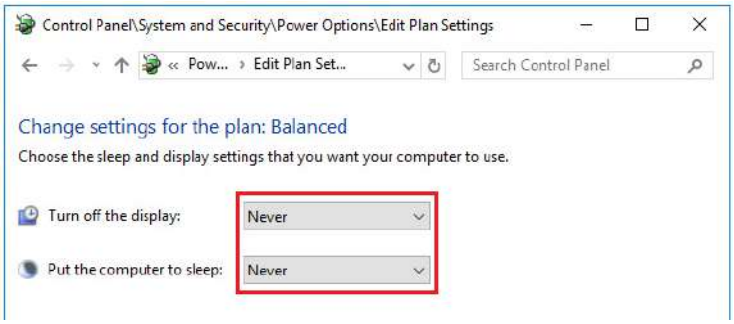
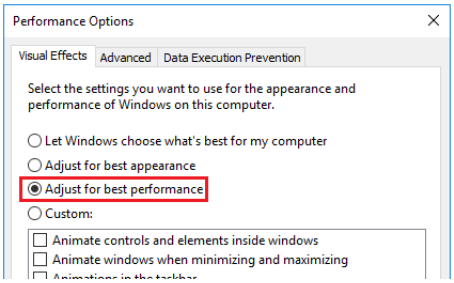
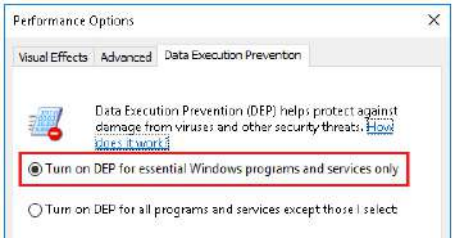
Operating System

Verify these operating system requirements.

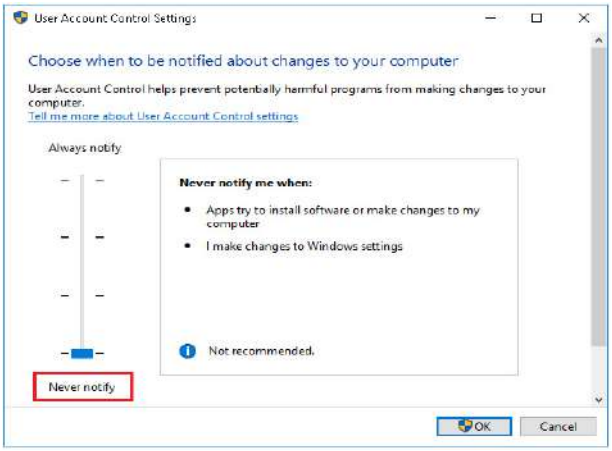
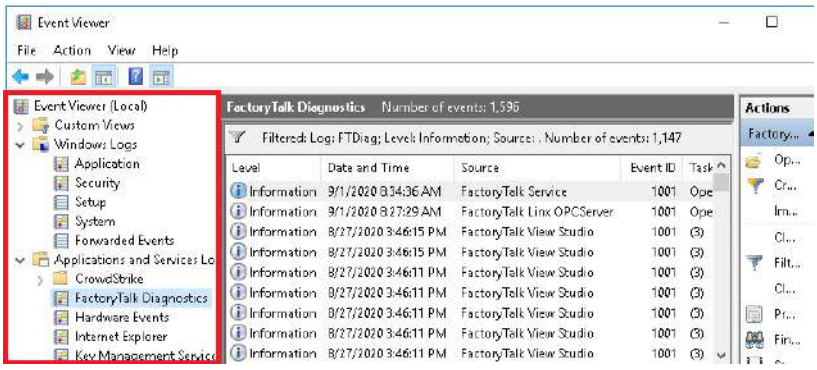
Server or Workstation Tab: Operating System

Row	Guidelines	Description
4	Windows Firewall Being Used	Specify whether the Windows firewall is enabled. For each computer, go to Control Panel > Windows Firewall > Advanced Settings.  Inbound rules allow or block inbound network traffic. Verify that Rockwell Automation software is allowed so that data and information isn't blocked between application servers. 
5	Operating System Valid	Specify whether the server or workstation operating system that you're using matches PlantPAx system recommendations. See the PlantPAx Distributed Control System Selection Guide, PROCES-SG001.
6	Rockwell Software® Patches Applied	Specify whether you installed the latest software patches for the Rockwell Automation software that is in the PlantPAx system. All servers and clients in the system must have the same FactoryTalk® patch updates to avoid unexpected results.
7	NIC Power-Saving Options Disabled	Specify whether you disabled power-saving for the Network Interface Card (NIC).\ For each computer, go to Control Panel > Network and Sharing Center > Properties > Power Management. Make sure the 'Allow the computer to turn off this device to save power' is disabled (no check mark).  

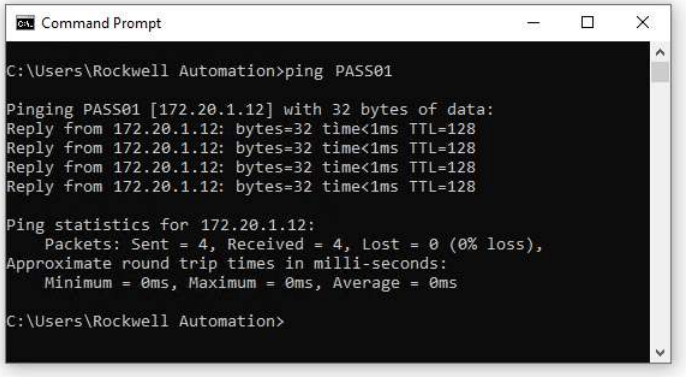
Server or Workstation Tab: Operating System

Row	Guidelines	Description
8	Windows Power-saving Options Disabled	Specify whether you disabled power-saving for the Windows operating system. For each computer, go to Control Panel > Power Options and verify the Change when computer sleeps field is set to Never. 
9	Desktop Experience Enabled in RDS Servers	Windows Server 2016 and newer have Remote Desktop Server (RDS) functionality that is enabled by default. Windows Server 2012 and prior, RDS is disabled by default and you need to enable the functionality. For each computer, go to Server Manager > Local Server and review the Roles and Features listings.
10	Adjust for Best Performance Is Selected	Specify whether Windows settings are enabled for best performance. When Adjust for Best Performance is selected, enhanced features that aren't used are turned off, which yields more memory and performance for the system. For each computer, go to Control Panel >System > Advanced System Settings > Advanced tab > Settings and on the Visual Effects tab, make sure Adjust for best performance is enabled. 
11	Data Execution Prevention Windows Only	Specify whether Data Execution Prevention is enabled for essential Windows programs and services. For each computer, go to Control Panel > System > Advanced System Settings > Advanced tab > Settings and on the Data Execution Prevention tab, make sure 'Turn on DEP ...'is enabled. 

Server or Workstation Tab: Operating System

Row	Guidelines	Description
12	User Account Control Never Notify	Specify whether a user is never notified by the User Account Control. For each computer, open the User Account Control settings and make sure Never Notify is enabled. 
13	Windows Automatic Update Is Disabled	This step is for computers that are not internally managed by a Windows System Update Server (WSUS). Verify that Windows automatic update is disabled. Disabling this functionality helps prevent updates that haven't been qualified by Rockwell Automation from being installed on the workstation or server. For Windows 10, Windows Server 2016, Windows Server 2019 operating systems: 1. Open the Run command (Win + R) and enter: services. msc 2. Select the Windows Update service from the Services list. 3. On the General tab and change the Startup Type to Disabled. 4. Restart the computer. For Windows Server 2012 and prior: 1. For each computer, go to Control Panel > Windows Update and make sure that the update option is disabled. 2. Restart the computer. 
14	Event Viewer Is Not Presenting Errors	Verify that the Event Viewer is not showing errors in the logs. For each computer, go to Administrative Tools > Event Viewer and verify that each log does not contain errors. 

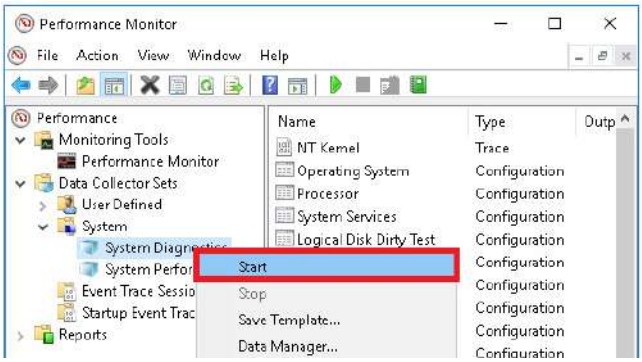
Server or Workstation Tab: Operating System

Row	Guidelines	Description
15	NSLookup Resolved	Verify the mappings of IP addresses to host names 

Performance

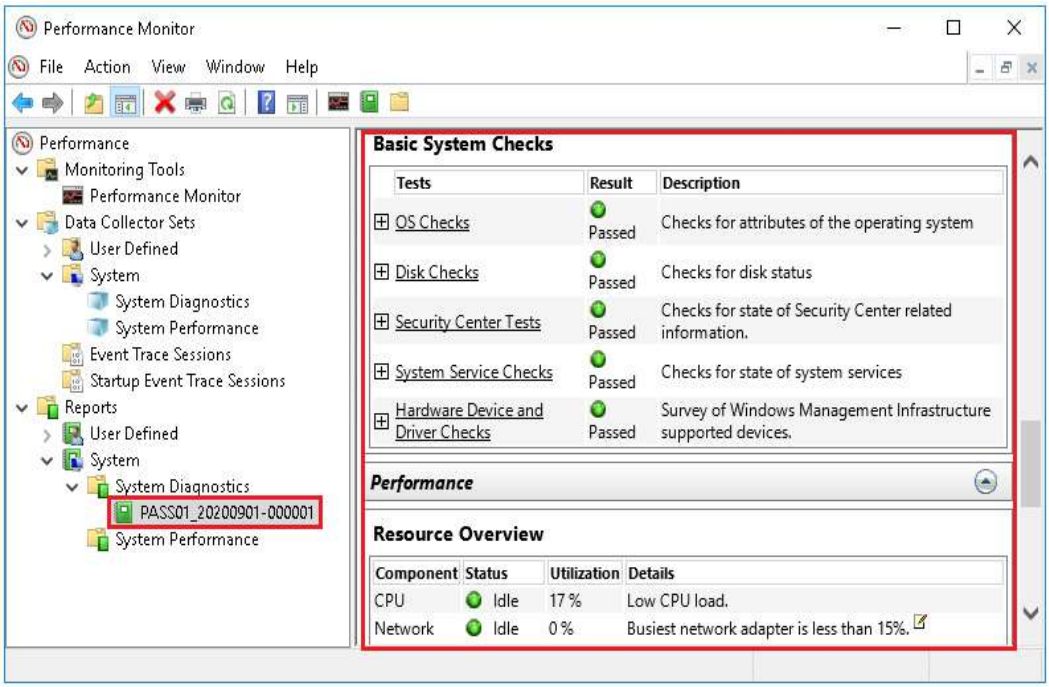
The Windows Performance Monitor (PerfMon) utility provides a snapshot of the current performance of a computer. To generate a performance report, do the following for each server and workstation:

1. From the Performance Monitor utility, go to Data Collector Sets > System > System Diagnostics and select Start.



The system diagnostics procedure takes about 1 minute.

2. To view the report, go to Reports > System > System Diagnostics.



Basic System Checks

Use the performance report from the Performance Monitor utility to verify the basic system checks.

Server or Workstation Tab: Basic System Checks

Row	Guidelines	Description
17	Operating Systems Checks	Verify that the attributes of the operating system conform to PlantPAx system recommendations. Use of not-recommended operating systems can affect system performance.
18	Disk Checks	Verify the status of the disks in the operating system.
19	Security Center Tests	Verify system security-related information.
20	System Service Checks	Verify the state of system services.
21	Hardware Device Driver Checks	Verify the Windows management of supported devices in your PlantPAx system.

Resource Overview

Use the performance report from the Performance Monitor utility to verify the resources.

Server or Workstation Tab: Resource Overview

Row	Guidelines	Description
22	CPU (%)	Verify that the CPU load complies with PlantPAx system recommendations. In a virtual system, the chip set on the host machine (server) can affect CPU capacity.
23	Network (%)	Verify that the busiest network adapter is < 50%.
24	Disk (/sec)	Verify the operations per second performed by the hard disk drive.
25	Memory (%)	Verify the memory capacity of the server or workstation.

System Architecture Tab

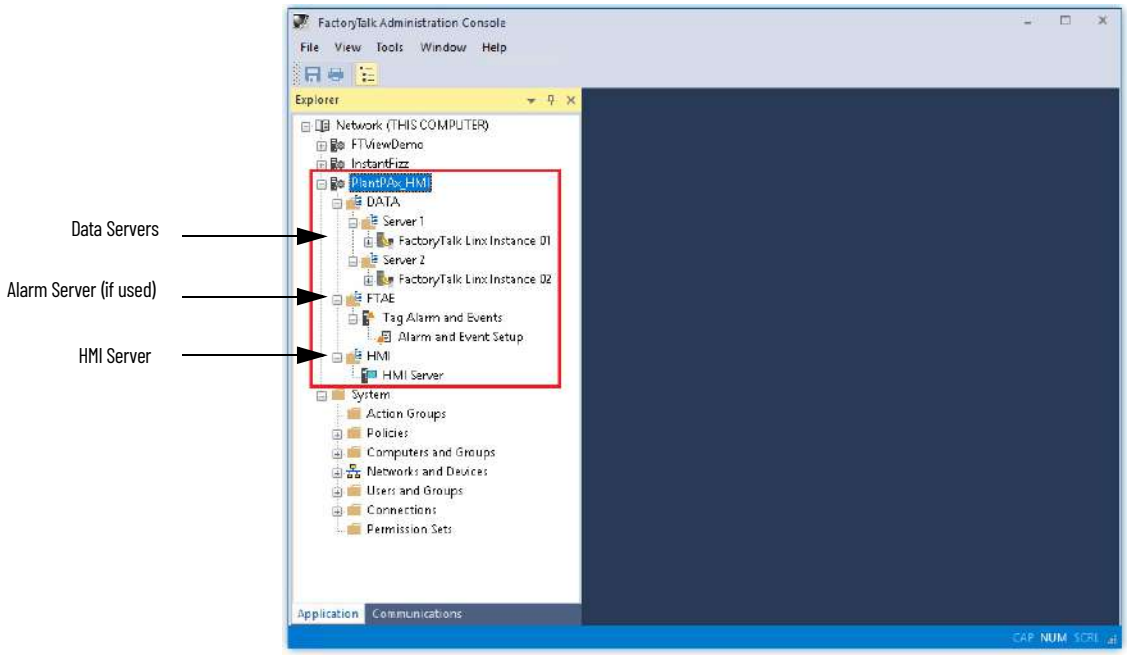
The System Architecture checklist assumes:

- Your PlantPAx system was based on sizing recommendations from a PlantPAx System Estimator project.

  See Chapter 1, System Workflow.
- Your PlantPAx system is operable (for example, the HMI application is running and the latest operating system patches are installed).
- You have configured the following FactoryTalk software that you need for your application servers.

FactoryTalk View Application Design

To verify these attributes, use the FactoryTalk® Administration Console or the FactoryTalk® View Studio software.



Server segregation helps optimize performance. To help prevent unpredictable search results, do **not** insert a server into the application root path.

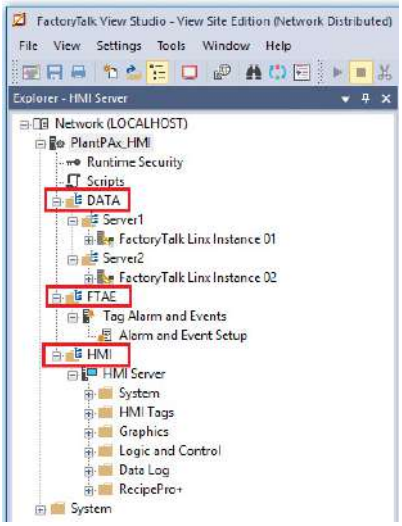
IMPORTANT Each server must be in its own area. This creates a unique path for each server so that clients don't need to examine every server.

Design the system with of future growth in mind. Future growth can affect area names and how you segregate server by controllers within an area.

To improve performance, place:

- Data servers, alarm servers (if used), and Historian interface connectors on the same image
- HMI and other application servers on separate images

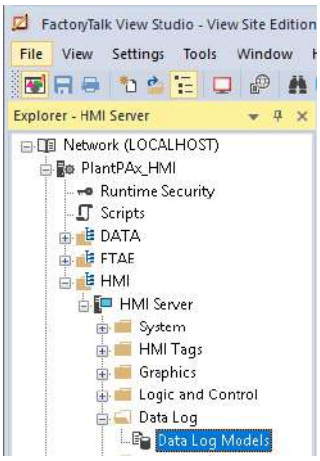
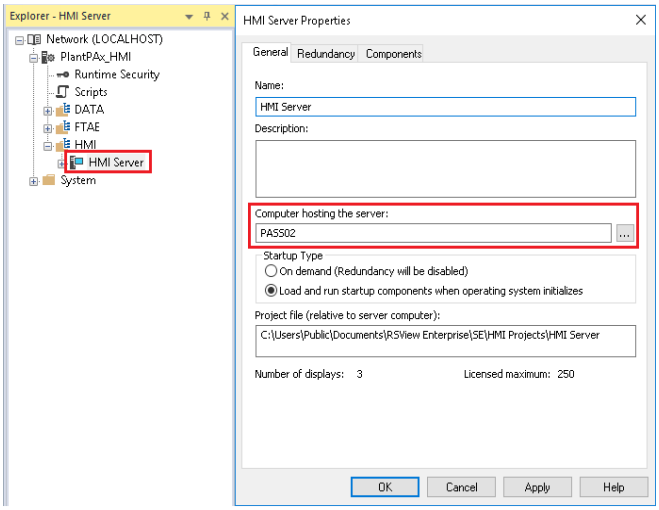
System Architecture Tab: FactoryTalk View Application Design

Row	Guidelines	Description
4	Number of HMI Servers	The system supports 10 HMI servers, whether they're redundant or not (you can have 10 redundant pairs). The number of servers and how they're configured can impact the speed of system communication. Use the application tree in the FactoryTalk Administration Console and select the project to be analyzed. • Reference, identify, and count all HMI servers in your system. • If a server is secondary, do **not** add the secondary HMI server to the count.
5	Number of Alarms Servers	The system supports 10 Tag Alarm and Event servers, whether they're redundant or not (you can have 10 redundant pairs). Use the application tree in the FactoryTalk Administration Console and select the project to be analyzed. • Reference, identify, and count all Tag Alarm and Event servers in your system.
6	Number of Data Servers	The system supports 10 data servers, whether they're redundant or not (you can have 10 redundant pairs). Both FactoryTalk Linx and OPC UA data servers count towards the limit. Use the application tree in the FactoryTalk Administration Console and select the project to be analyzed. • Reference, identify, and count all FactoryTalk Linx and OPC UA data servers in your system.
7	Each Server Is In Its Own Area	Each server must be in its own area. This creates a unique path for each server so that clients don't need to examine every server before they find the data they need. Server segregation helps optimize performance. To help prevent unpredictable search results, do **not** insert a server into the application root path.  For more information see, Knowledgebase Technote *FactoryTalk View SE Area Best Practices*.

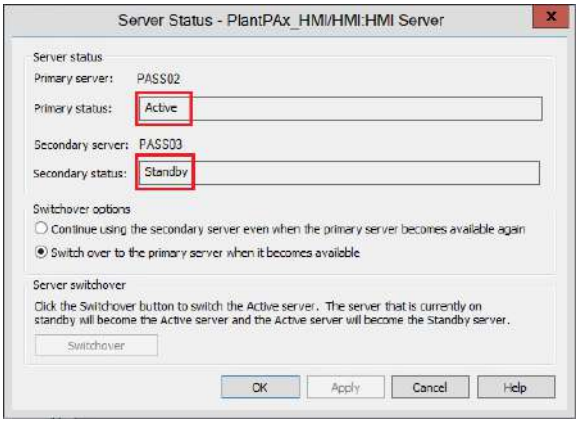
FactoryTalk View HMI Servers

Verify that the HMI servers on the PASS comply with system recommendations.

System Architecture Tab: FactoryTalk View HMI Servers (PASS)

Row	Guidelines	Description
8	Uses Data Logging	We recommend the use of FactoryTalk® Historian software rather than FactoryTalk View SE data logs to collect and analyze system data. To check if data logs are used in a FactoryTalk View SE project, open a Data Log folder in the HMI server. Verify the data log model is empty. 
9	Dedicated Servers	You can have only 1 HMI server per computer. In FactoryTalk® View Studio software, open Properties for each server and confirm the computer host name. 

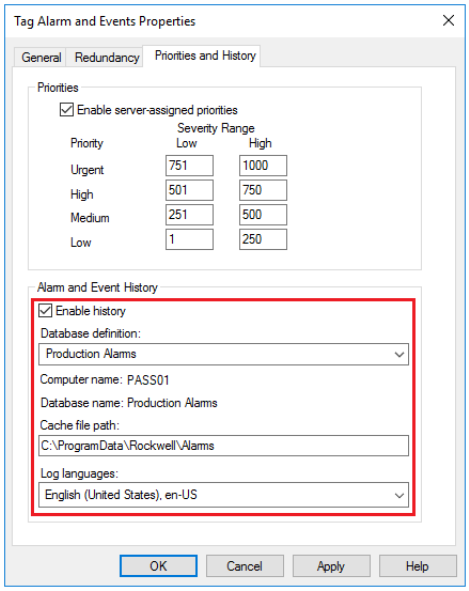
System Architecture Tab: FactoryTalk View HMI Servers (PASS)

Row	Guidelines	Description
10	Redundancy Status	In the FactoryTalk Administration Console, select the HMI server > Server Status.  In the verification tool: • If the status for one server is 'Active' and the other server is 'Standby', record Synched. • If you have different results, choose 'Not Synched' and identify the servers that are 'Not Synched' in the Notes.

FactoryTalk Alarm and Event Servers

Verify that the alarm servers on the PASS comply with system recommendations.

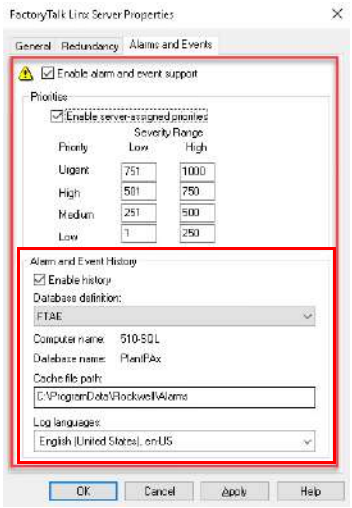
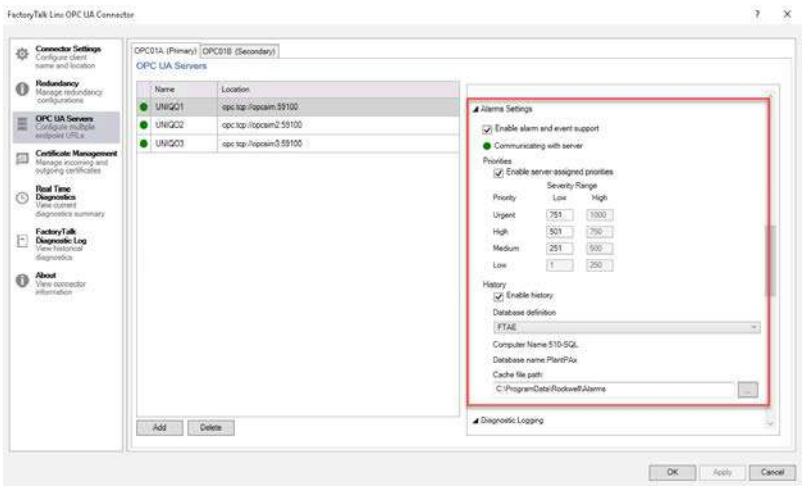
System Architecture Tab: FactoryTalk Alarm and Event Servers (PASS)

Row	Guidelines	Description
11	Dedicated Servers	You can have only 1 alarm server per computer. In FactoryTalk View Studio software, open Properties for each server and confirm the computer host name.
12	Redundancy Status	Use the FactoryTalk Administration Console to select the alarm server > Server Status. In the verification tool: • If the status for one server is 'Active' and the other server is 'Standby', record Synched. • If you have different results, choose 'Not Synched' and identify the servers that are 'Not Synched' in the Notes
13	Alarm & Event History	In the FactoryTalk Administration Console, open the Properties for the alarm server and check Enable History to log alarm history. 

FactoryTalk View Data Servers

Verify that the data servers on the PASS comply with system recommendations.

System Architecture Tab: FactoryTalk View Data Servers

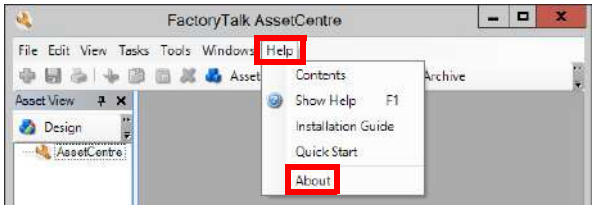
Row	Guidelines	Description
14	Max Number of FTLinx Instances on any PASS	FactoryTalk Linx supports 2 data server instances on one computer. In FactoryTalk View Studio software, open Properties for each server and confirm the computer host name.
15	Dedicated Server for OPC UA	UPC UA data servers should be hosted on a dedicated computer. No additional Data, Alarm or HMI servers should be hosted on the same computer with an OPC UA data server.
16	Redundancy Status	Use the FactoryTalk Administration Console to select the data server > Server Status. For OPC UA, select Properties > Redundancy. In the verification tool: • If the status for one server is 'Active' and the other server is 'Standby', record Synched. • If you have different results, choose 'Not Synched' and identify the servers that are 'Not Synched' in the Notes
17	Alarm & Event History	In the FactoryTalk Administration Console, open the Properties for the data server and check Enable History to log alarm history.  

FactoryTalk AssetCentre Configuration

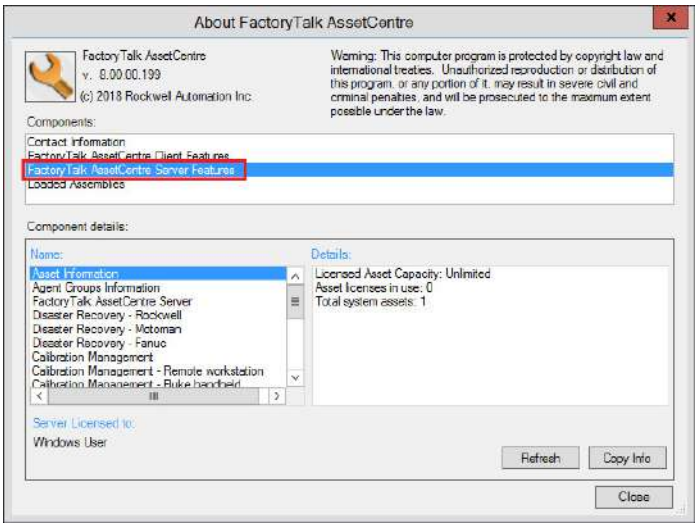
As a rule, do not to exceed 100 assets over a 12-hour period per agent.

To verify the FactoryTalk AssetCentre configuration:

1. On the AssetCentre menu bar, select Help > About.



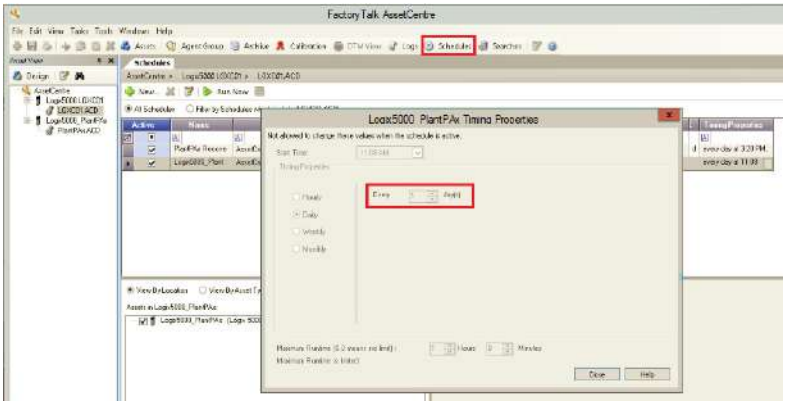
2. In the Components box, select FactoryTalk AssetCentre Server Features.



System Architecture Tab: FactoryTalk AssetCentre (AppServ-Asset Mgmt)

Row	Guidelines	Description
18	Number of Assets	Licensing determines the allowable number of assets. A base license includes 10 assets. From the Details pane of the FactoryTalk AssetCentre dialog box, verify the number of total system assets.
19	Number of Disaster Recovery (DR) Assets	Specify the number of controllers that are configured for Disaster Recovery (requires a Disaster Recovery license). Select Disaster Recovery - Rockwell in the FactoryTalk AssetCentre dialog box.
20	Number of Agents	Agents are programs that communicate with the FactoryTalk AssetCentre server and perform server tasks, such as disaster recovery. By using agents, work is distributed and shared among computers to help spread processing load. View the number of agents in the bottom-right corner of the FactoryTalk AssetCentre dialog box. 

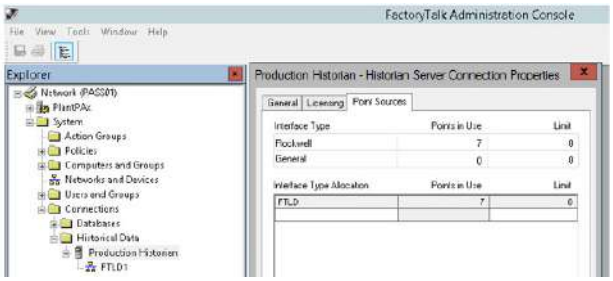
System Architecture Tab: FactoryTalk AssetCentre (AppServ-Asset Mgmt)

Row	Guidelines	Description
21	How Often DR Assets Configured to Upload	Determine the frequency that the assets are scheduled to upload. Enter the number of days between asset uploads from the Schedules > Timing properties dialog box. 

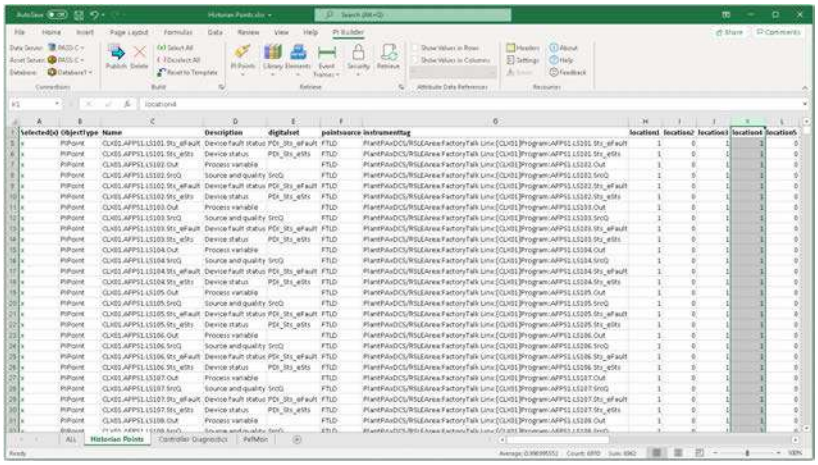
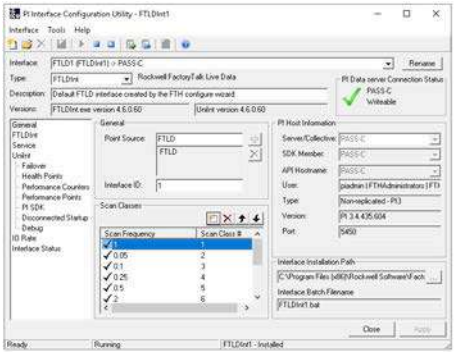
FactoryTalk Historian SE Configuration

Verify that the following FactoryTalk View Historian SE design attributes comply with system recommendations.

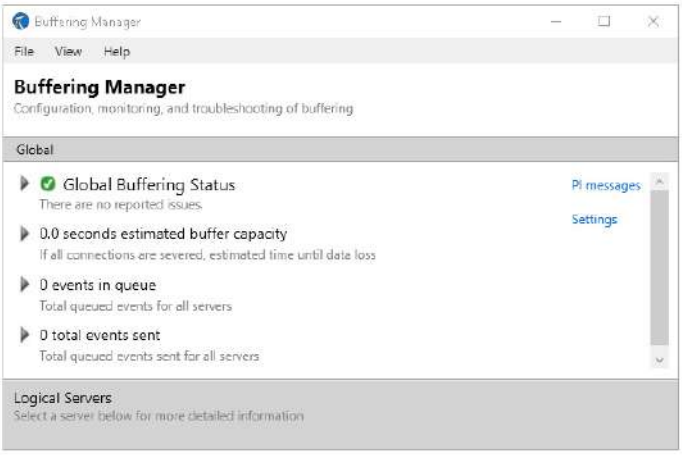
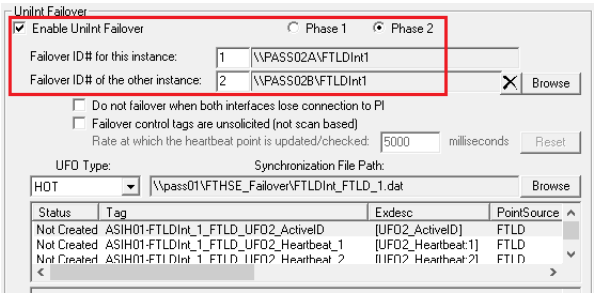
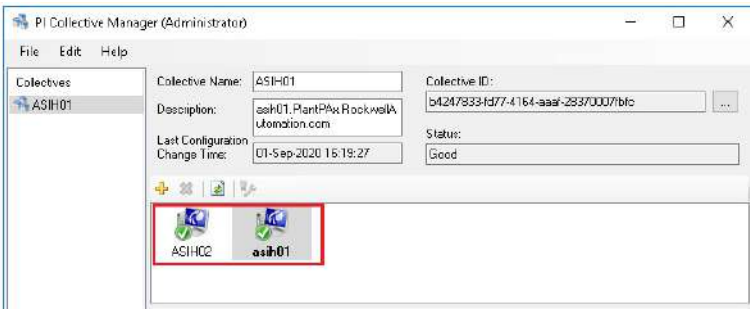
System Architecture Tab: FactoryTalk Historian SE (AppServ-Info)

Row	Guidelines	Description
22	Points In Use	Verify the number of points that are in use. To view the number of points on the FactoryTalk Administration Console dialog box, go to System > Connections > Historical Data and select the Historian SE server. 
23	Points Limit	The limit depends on the points in use and the license limit. This value sets a benchmark that can be compared to future server results. The comparison can identify a potential issue with too many points per license.

System Architecture Tab: FactoryTalk Historian SE (AppServ-Info)

Row	Guidelines	Description
24	Fastest Scan Class	Verify the scan rate that is used in FactoryTalk Live Data to send controller information to the Historian server. This information can be viewed with Point Builder in PI System Management Tools or using the FactoryTalk Historian SE Excel Add-in tool. From Excel, on the PI Builder tab, select PI Points > All Points and select all columns. The column labeled Location 4 is an integer used by many interfaces to specify the scan class of the PI Point.  The PI Interface Configuration Utility defines time period of each class number. For example, the FTLD1 interface contains 10 scan classes in terms of seconds.  Typically, a scan class of 1 second is sufficient. Some tags can require a scan class of 0.5 seconds. Exception reporting and compression reporting for tuning parameters are important for data collection and server loading.
25	Number of Interfaces	Specify the number of FactoryTalk Live Data interfaces in your Historian configuration.

System Architecture Tab: FactoryTalk Historian SE (AppServ-Info)

Row	Guidelines	Description
26	Buffering Enabled and Running	Buffering is recommended to maintain data collection in the event the connection to the server is lost. 
27	Unit Fail Over Enabled and Running	On the Interface Configuration Utility, verify that failover is configured properly. 
28	Collective Enabled and Running	Verify that a collective is properly configured in a redundant Historian systems 

PASS Tab

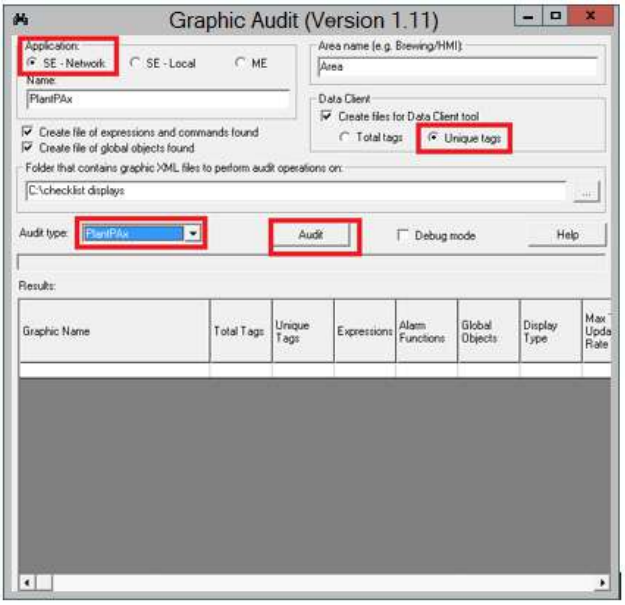
The PASS tab records details about the HMI elements in your application.

IMPORTANT Make a copy of this worksheet for each PASS in your system.

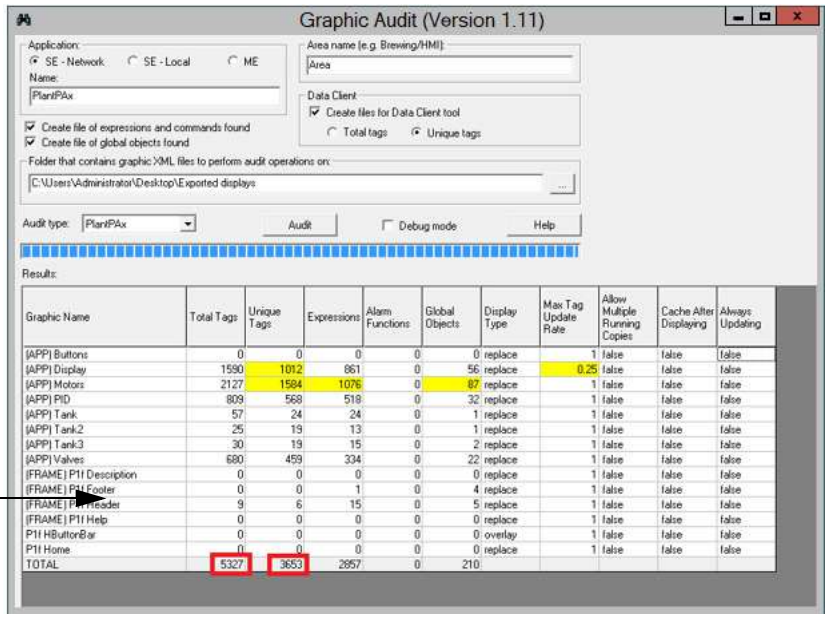
To verify your FactoryTalk® View Site Edition (SE) HMI design elements, use the Rockwell Automation Graphic Audit Tool. The audit tool analyzes exported HMI displays. The Rockwell Automation Graphic Audit Tool can be found in Knowledgebase Technote, PlantPAx System Release 5.20 Configuration and Implementation Tools.

Before you run the audit tool, export the HMI application graphic files to an XML format. Then run the audit tool on the XML file.

Field Description	Application
SE - Network SE - Local ME	Click SE - Network
Name	The Name and Area Name are used only to generate Data Client XML files and are not used in the audit operation. See Graphic Audit Tool Help.rtf file in the zip file for more details.
Area Name (for example, Brewing/HMI)	
Create file of expressions and commands found Create file of global objects found	To create the respective files, check the boxes.
Data Client Create files for Data Client tool Total tags Unique tags	To enable Create files for Data Client, check the box, and then select Unique tags.
Folder that contains graphic XML files to perform audit operations on	Click Browse ('...' ellipsis) to select the directory path where you exported your graphic XML files.
Audit type	Choose PlantPAx from the pull-down menu. This choice uses rules that are specific to the PlantPAx system.



The process displays are listed in the Results pane.



Color-coded cells indicate threshold issues.

These guidelines apply to HMI applications developed via FactoryTalk View SE software. Make sure:

- The FactoryTalk View SE system is correctly installed and configured (software version, operating system, computer requirements) according to the PlantPAx system characterized architecture.
- Design the FactoryTalk View SE system to accommodate future additions.
- Develop your HMI displays according to ISA 101 standards

FactoryTalk View SE System

Verify that the HMI server attributes comply with these recommendations.

PASS Tab: FactoryTalk View SE (HMI)

Row	Guidelines	Description
4	Number of Displays	The total number of displays does not exceed the display license.
5-10	Total Tags on Server Unique Tags Expressions Global Objects	Verify that there are no warnings or errors from the Graphic Audit Tool. Consider simplifying any displays with warnings or errors.
11-15	Display Settings Display Type Display Cache Always Updating Graphic Update Rate	For display settings, specify: • Display Type = Replace • Display Cache = No • Always Updating + not checked Verify that the update rate is within recommendation of 0.5 seconds. Any faster rate has a possible impact on the server and controller.

FactoryTalk Alarms and Events Server

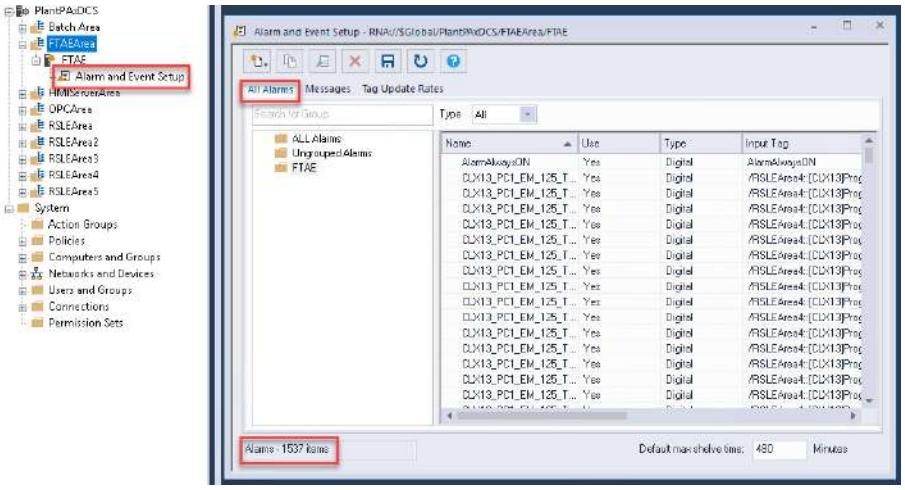
There are two possible types of alarms on the PASS:

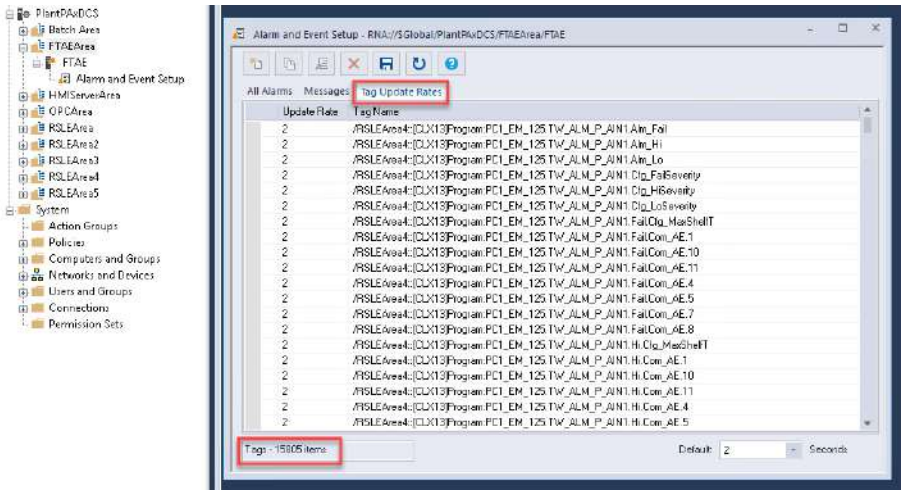
- Server Tag-based alarms
- Logix Tag-based alarms

Server Tag-based Alarms

Server Tag-based alarms that are defined within the FactoryTalk Alarms and Events server (default for 4.6 or earlier PlantPAx system releases that are using the 4.1 or earlier Library of Process objects.)

The FactoryTalk Alarm and Event Setup dialog box provides the data.





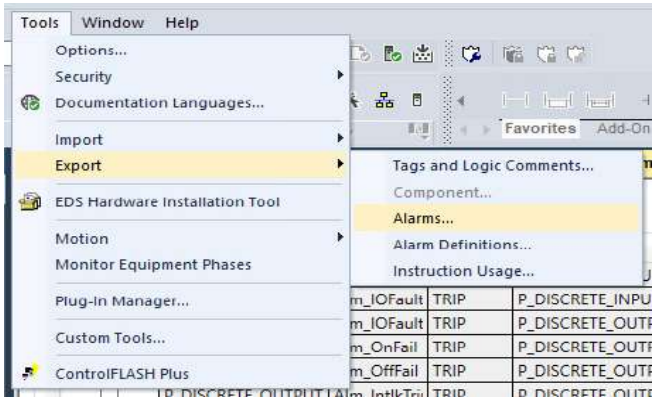
Logix Tag-based Alarms

Logix Tag-based alarms are configured in the Logix Designer software and stored in controller memory. They are processed directly by the FactoryTalk Linx data server and do not require a Tag Alarms and Events server. This alarm type is used by version 5.0 and later of the Process Objects Library.

To determine the number of Logix tag-based alarms:

1. In Logix Designer, export the alarms for each of the controllers with a defined shortcut on the FactoryTalk Linx (Instance 01) data server.

2. Open the export file in Excel and filter on Use = True to total the number of in-use alarms. Record this value in the appropriate row in the Checklist spreadsheet. Repeat these steps for FactoryTalk Linx (Instance 02) if necessary.



3. Verify that the alarm server attributes comply with these recommendations.

PASS Tab: FactoryTalk Alarms and Events

Row	Guidelines	Description
16	Number of Server Tag-based Alarms (FactoryTalk Alarms and Events)	The FactoryTalk Alarms and Events server supports 20,000 Server Tag-based alarms
17	Total Items (Server Tag-based alarms only)	Informational field provides a total number of items on the Tag Update Rates of the FactoryTalk Alarm and Event Setup dialog box
18	Fastest Update Rate (Server Tag-based alarms only)	Update rate recommendation is greater than or equal to 1 second. Default is 2 seconds to help reduce load on the system.
19	All tags associated with Server Tag-based alarms are from a data server that is hosted on the same PASS as the alarm server.	The alarm server references the data server that is hosted on the same computer. Move non-compliant alarms to the appropriate alarm server associated with the data server.
20	Number of Logix Tag-based Alarms (FactoryTalk Linx Instance 1)	FactoryTalk Linx instance 1 supports 15,000 Logix Tag-based alarms
20	Number of Logix Tag-based Alarms (FactoryTalk Linx Instance 2)	FactoryTalk Linx instance 2 supports 15,000 Logix Tag-based alarms
22	Total Alarms (Server Tag-based + Logix Tag-based; sum total of previous 3 rows)	The total number of alarms does not exceed 30,000 per PASS

Generate the FactoryTalk View Report

The FactoryTalk View Report can automatically generate some of the required data for the PASS and Controller worksheets. Use the following steps to configure and generate the report.

IMPORTANT The provided global object, display files, and images in the checklist file must be installed in the HMI before printing the report. The display files include the following:
Images: icon_gray.png, icon_green.png, icon_yellow.png, icon_red.png
Global object: (RA-LIB) Report.ggfx
Displays: (RA-LIB) Report RSLinxE.gfx, (RA-LIB) Report Controller.gfx, (RA-LIB) Report Controller 5x80.gfx
The information can be found in Knowledgebase Technote, PlantPAx System Release 5.20 Configuration and Implementation Tools.

1. For each controller, select the appropriate diagnostic Add-On Instruction. Diagnostic Add-On Instructions are available in the Library of Process Objects. This library can be downloaded from the Product Compatibility and Download Center at rok.auto/pcdc.

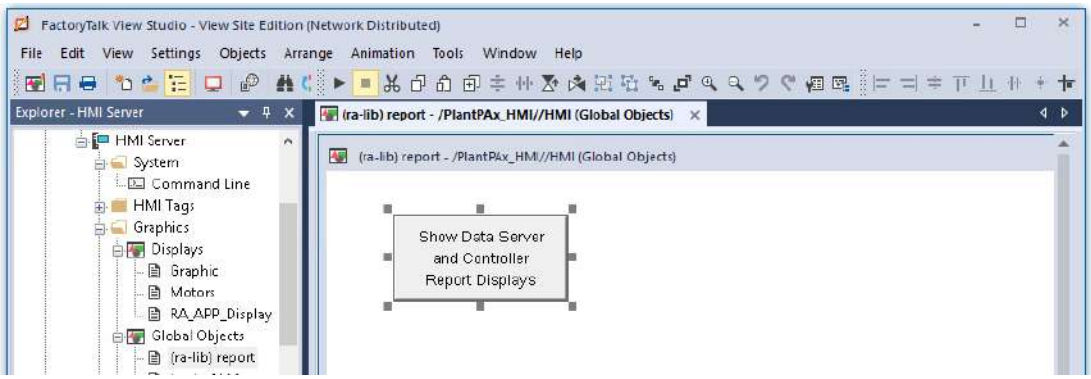
Use the following guidelines to determine which instruction to use.

- If the controller is from the 5x70 family, use the L_CPU instruction.
- If the controller is from the 5x80 family, use either the L_CPU_5X80 instruction (4.1 library and earlier) or the raP_Dvc_LgxCPU_5X80 (5.0 library and later).

2. For each controller, import and configure the appropriate Add-On Instruction. Verify that the instruction's tag is controller-scoped and named “L_CPU” for the L_CPU or L_CPU_5X80. If the raP_Dvc_LgxCPU_5X80 is used the tag name must be “raP_Dvc_LgxCPU”.
3. The instruction must have Data Collection enabled from the maintenance tab on the faceplate.

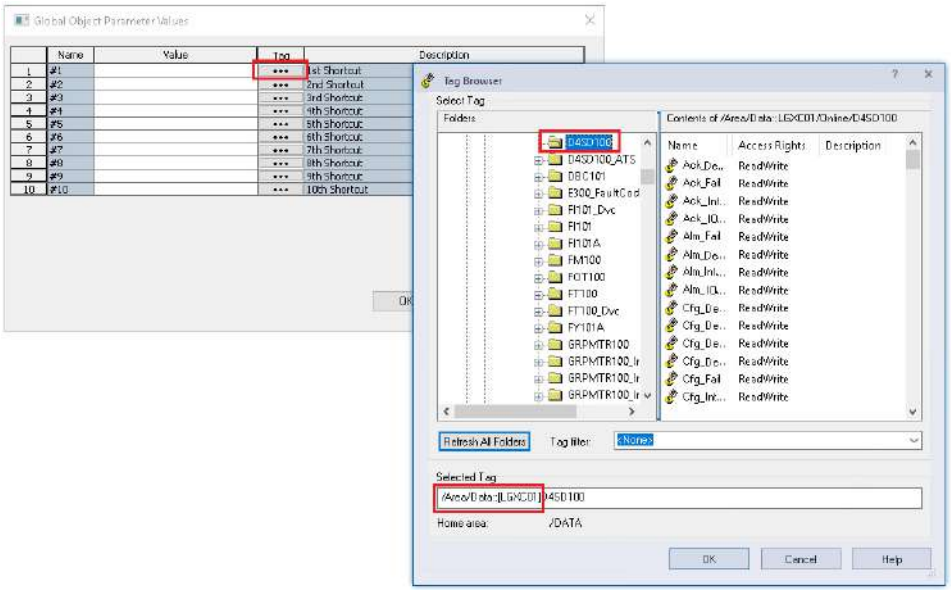
   See Rockwell Automation Library of Logix Diagnostic Objects, publication PROCES-RM003 for more information on the L_CPU and L_CPU_5X80 Add-On Instructions.

   See Rockwell Automation Library of Process Objects, publication PROCES-RM200 for more information on raP_Dvc_LgxCPU_5x80 Add-On Instruction.
4. In FactoryTalk View Studio, go to Global Objects file (RA-LIB) Report and select the Show Data Server and Controller Report Displays button.

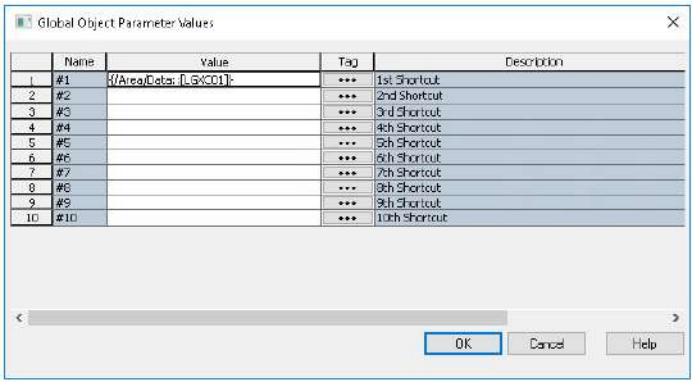


5. Copy the Global Object button and paste on to desired display.
6. Select the button and open the Global Object Parameter Values.

7. Under Tag on the Global Objects Parameter Values dialog box, click Browse (ellipsis '...') browse to select a controller shortcut.



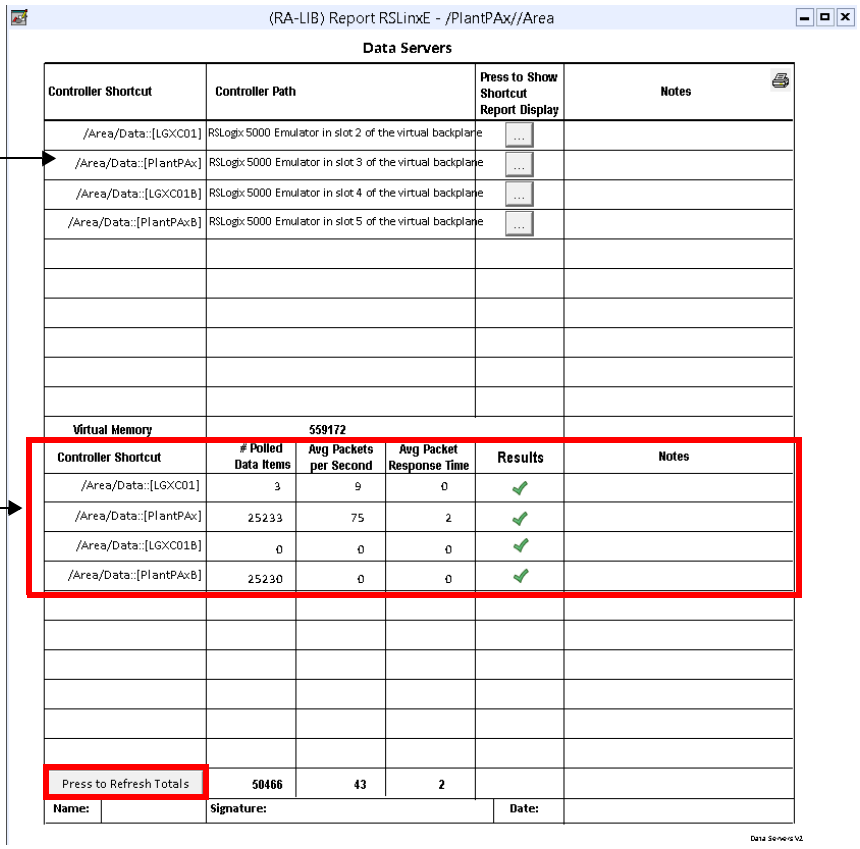
8. Enter a shortcut path. Use the syntax {/Area/Server::[Shortcut]}. Repeat until all shortcuts from FactoryTalk Linx Instance 01 are added. Add a new button and repeat process for FactoryTalk Linx Instance 02 if necessary.



9. Run a FactoryTalk View Client session and click the Show Data Server and Controller Report Displays button to generate a report.

Controller Verification.

Use the information in this section to complete the Checklist.



(RA-LIB) Report RSLinxE - /PlantPAx//Area

Data Servers

Controller Shortcut	Controller Path	Press to Show Shortcut Report Display	Notes
/Area/Data::[LGXC01]	RSLogix 5000 Emulator in slot 2 of the virtual backplane	...	
/Area/Data::[PlantPAx]	RSLogix 5000 Emulator in slot 3 of the virtual backplane	...	
/Area/Data::[LGXC01B]	RSLogix 5000 Emulator in slot 4 of the virtual backplane	...	
/Area/Data::[PlantPAxB]	RSLogix 5000 Emulator in slot 5 of the virtual backplane	...	
Virtual Memory	559172		

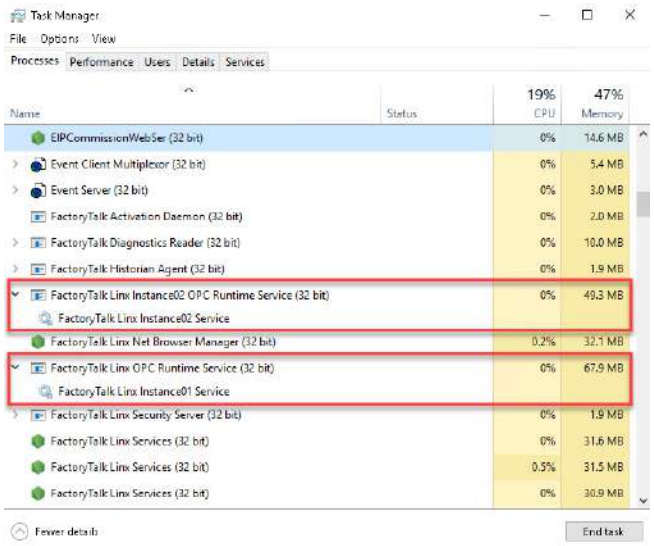
Controller Shortcut	# Polled Data Items	Avg Packets per Second	Avg Packet Response Time	Results	Notes
/Area/Data::[LGXC01]	3	9	0	✓	
/Area/Data::[PlantPAx]	25233	75	2	✓	
/Area/Data::[LGXC01B]	0	0	0	✓	
/Area/Data::[PlantPAxB]	25230	0	0	✓	
Press to Refresh Totals	50466	43	2		
Name:		Signature:		Date:	

Data Servers V2

FactoryTalk Linx Data Server

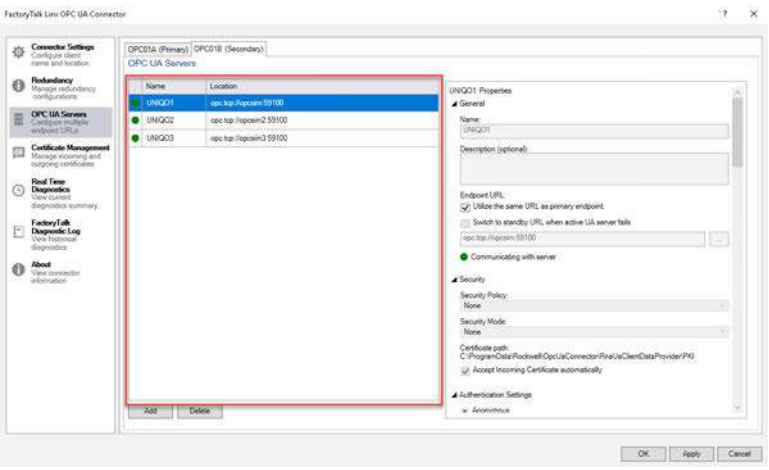
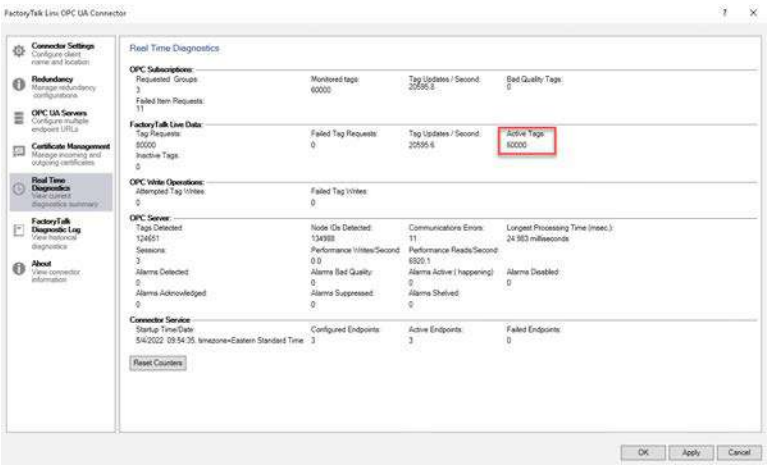
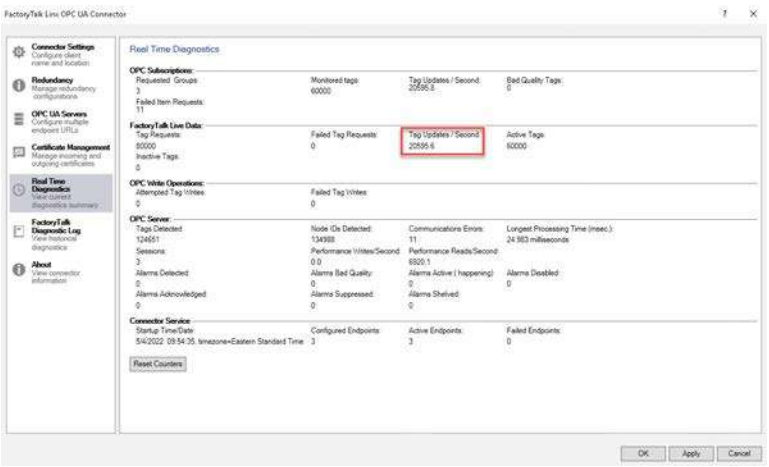
For each shortcut, verify:

PASS Tab: Data Server (FactoryTalk Linx Instance 1 and Instance 2)

Row	Guidelines	Description
23 & 37	Memory Usage	Select Yes or No to indicate if the Data Server is in use. If yes, then record the memory usage (MB) from the computer's task manager. PlantPAx recommends the memory usage of each instance of FactoryTalk Linx not exceed 3,000 MB. 
24-50	Number of Polled Data Items	The number of tags that are polled from the controller.
24-50	Average packets per Second	If your controller consistently exceeds the recommended maximum average packets per second, it's possible your controller is overloaded. Consider reducing the number of HMI data points that are referenced by your HMI displays from that controller. You can also change the display update rate if you're experiencing performance issues.
24-50	Average Packet Response Time	The average packet response time of messages to the controller. If your average packet response time consistently exceeds 200 milliseconds, then it's possible that your communication adapter has a potential bottleneck. Consider the following troubleshooting guidelines if your performance isn't satisfactory: • Examine your network architecture and network hardware. You could be exceeding your switch capacity or capabilities that can cause slow network performance. • You could be using an outdated communication adapter in the path to your controller. Or, you could be exceeding the capabilities of the communication adapter.

FactoryTalk Linx OPC UA Connector

PASS Tab: Data Server (OPC UA Connector)

Row	Guidelines	Description
51	Using OPC UA Connector	The OPC UA connector should be hosted on a dedicated computer with no other servers (HMI, Alarm, or Data) present.
52	Number of OPC UA connections	The OPC UA server shouldn't have more than 20 OPC UA connections. 
53	FactoryTalk Live Data Active Tags	The OPC UA server shouldn't have more than 50,000 active tags. 
54	FactoryTalk Live Data Active Tag Updates/sec	The OPC UA server shouldn't have more than 50,000 tag updates per second. 

PASS Tab: Data Server (OPC UA Connector)

Row	Guidelines	Description
55	Total OPC UA Alarms and Conditions	Determining the number of Alarms and Conditions for each OPC UA server that is configured in the connector. Each connection that is counted in Row 52 must be reviewed individually as specific configurations of OPC UA servers can vary. The sum total of all alarms and conditions across all connected OPC UA servers shouldn't exceed 5000. Consider reducing the number of OPC UA alarms and conditions if there are more than 5000 total across all OPC UA servers.

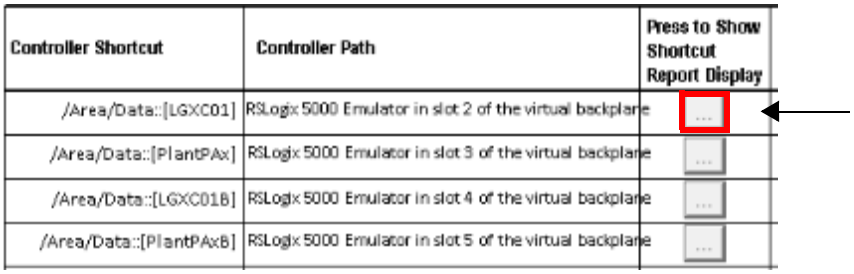
Controller 5x80 Tab

The Controller tab records controller properties.

IMPORTANT Make a copy of this worksheet for each 5x80 controller in your system.

To gather information for the checklist, you can use the FactoryTalk View report, see Generate the FactoryTalk View Report.

Select the button shown in the following display to view the Controller Report Display.



Controller Properties

Verify that the controller properties comply with these recommendations.

Controller 5x80 Tab: Properties

Row	Guidelines	Description
4	Shortcut	Keep the shortcut, ACD file reference, and controller name similar (intuitive).
5	Firmware	Verify the firmware revision.
6	Module	The controller is indicated as available in the PSE. The controllers in the PSE have been characterized for use within a PlantPAx system.
7	Redundancy	Indicate whether you're using a redundant controller (Yes/No).

CPU Use

Verify that the CPU use complies with these recommendations.

Controller 5x80 Tab: CPU Use

Row	Guidelines	Description
8	Logix Engine	At least 25% free for Redundant 5580 controllers. Non-redundant 5x80 controllers can utilize up to 100% of the Logix Engine.
9	Communications Core	At least 40% free.
10	Packet Processing Engine	At least 25% free.

Faults

Verify that the fault handling complies with these recommendations.

Controller 5x80 Tab: Faults

Row	Guidelines	Description
11	Minor Faults Count	Number of minor faults that have occurred within the controller. After clearing the minor faults, monitor for a period of time (at least several controller scans) before reverifying.
12	Task Overlap	Whether a task overlap occurs. A task overlap must be resolved. Use the predefined task model in the process controller or simplify the program. Lengthening the period or raising the relative priority of important tasks disables the predefine task model in a process controller.

Capacity

Verify that the controller capacity complies with these recommendations.

To verify controller capacity, open the controller application file in Logix Designer. Go to Controller Properties > Capacity tab.

Controller 5x80 Tab: Capacity

Row	Guidelines	Description
13 & 14	Program Memory (blocks)	Reserve at least 20%.
15 & 16	Nodes	Reserve at least 20%.

Connections

Verify that the total number of connections is 75% or less of the controller maximum.

Controller 5x80 Tab: Connections

Row	Guidelines	Description
17-25	Total I/O	Total number of connections includes: • I/O • Produced tags • Consumed tags • Messages • Incoming • Unconnected buffers • Message cache

Time Synchronization

Verify that the controller is configured for time synchronization.

Controller 5x80 Tab: Time Synchronization

Row	Guidelines	Description
26	Controller is time synchronized	Denotes if the controller is configured for time synchronization (Yes/No).

Task Structure

Verify the controller program uses only periodic tasks.

Controller 5x80 Tab: Task Structure

Row	Guidelines	Description
27	Only periodic task used	Use only periodic tasks and remove any unused tasks The process controller enforces 4 periodic tasks: Slow, Normal, Fast, and System.

Controller Alarms

Verify the number of controller alarms.

Controller 5x80 Tab: Controller Alarms

Row	Guidelines	Description
28	Total number of Logix Tag-based alarms (both IN-USE and NOT)	The total number of Logix Tag-based alarms (both IN-USE and NOT) stored in a controller shouldn't exceed 10,000. See Logix Tag-based Alarms on page 312 to determine the number of alarms on a controller.
29	Total number of Logix Tag-based alarms (IN-USE only)	The total number of Logix Tag-based alarms (IN-USE only) stored in a controller shouldn't exceed 7,500. See Logix Tag-based Alarms on page 312 to determine the number of alarms on a controller.

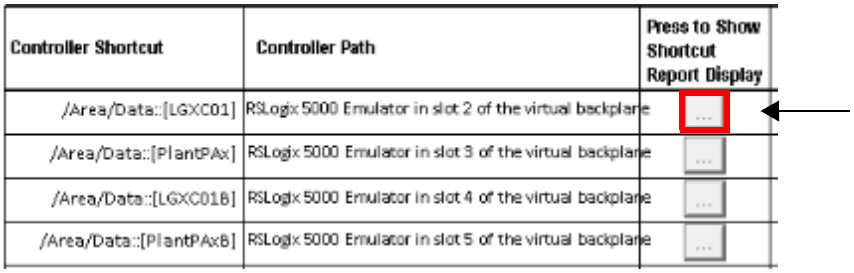
Controller 5x70 Tab

The Controller tab records controller properties.

IMPORTANT Make a copy of this worksheet for each 5x70 controller in your system.

To gather information for the checklist, you can use the FactoryTalk View report, see Generate the FactoryTalk View Report.

Select the button shown in the following display to view the Controller Report Display.



Controller Properties

Verify that the controller properties comply with these recommendations.

Controller 5x70 Tab: Properties

Row	Guidelines	Description
4	Shortcut	Keep the shortcut, ACD file reference, and controller name similar (intuitive).
5	Module	The controller is indicated as available in the PSE. The controllers in the PSE have been characterized for use within a PlantPAx system.
6	Firmware	Verify the firmware revision.
7	Redundancy	Denotes if you're using a redundant controller (Yes/No).

CPU Use

We recommend CPU load in a production environment to be 75% or less. Keep 25% CPU capacity as reserve to handle online edits, data server switchover, and so on.

Verify that the CPU use complies with these recommendations.

Controller 5x70 Tab: CPU Use

Row	Guidelines	Description
8	Free	At least 50% of free for redundant controllers At least 25% for simplex controllers.
9	Total Used	Total CPU utilization
10	Total Used: Periodic Tasks	The percentage of CPU use to run all application code in the controller. Periodic tasks are the only predictable task type on performance and utilization. Keep the number of tasks to 3 or 4 and do not use to organize code into process areas.
11	Total Used: Communication	The percentage of CPU use that is needed to respond to communication requests.
12	Total Used: Motion	The percentage of CPU use that is needed to execute motion.
13	Total Used: Messages	The percentage of CPU use that is needed to process messages.

Controller 5x70 Tab: CPU Use

Row	Guidelines	Description
14	Total Used: Safety	The percentage of CPU use that is needed to execute safety tasks.
15	Total Used: Redundancy	The percentage of CPU use that is needed to process redundancy.
16	Total Used: System	The percentage of system resources

Faults

Verify that the fault handling complies with these recommendations.

Controller 5x70 Tab: Faults

Row	Guidelines	Description
17	Minor Faults Count	Number of minor faults that have occurred within the controller. After clearing the minor faults, monitor for a period of time (at least several controller scans) before reverifying.
18	Task Overlap	Whether a task overlap occurs. A task overlap must be resolved. Make changes such as simplifying programs, lengthening the period, or raising the relative priority of important tasks.

Memory Use

The PlantPAx system requires the free I/O memory to be a minimum of 25% for simplex controllers. We recommend greater than 50% free memory for redundant controllers.

Controller 5x70 Tab: Memory Use

Row	Guidelines	Description
19 & 20	I/O Memory (bytes)	Reserve: • At least 50% for redundant controllers • At least 25% for simplex controllers If the amount exceeds the recommendations, reduce the number of I/O modules that are scanned by this controller, make system changes.
21 & 22	Data and Logic (bytes)	Reserve: • At least 50% for redundant controllers • At least 25% for simplex controllers If the amount exceeds the recommendations, upgrade controller for more memory or make changes to reduce load

Connections

Verify that the total number of connections is 50% or less of the controller maximum.

Controller 5x70 Tab: Connections

Row	Guidelines	Description
23-31	Total I/O	Total number of connections includes: • I/O • Produced tags • Consumed tags • Messages • Incoming • Unconnected buffers • Message cache

Time Synchronization

Verify that the controller is configured for time synchronization.

Controller 5x70 Tab: Time Synchronization

Row	Guidelines	Description
32	Controller is time synchronized	Denotes if the controller is configured for time synchronization (Yes/No).

Task Structure

Verify that the controller program uses only periodic tasks.

Controller 5x70 Tab: Task Structure

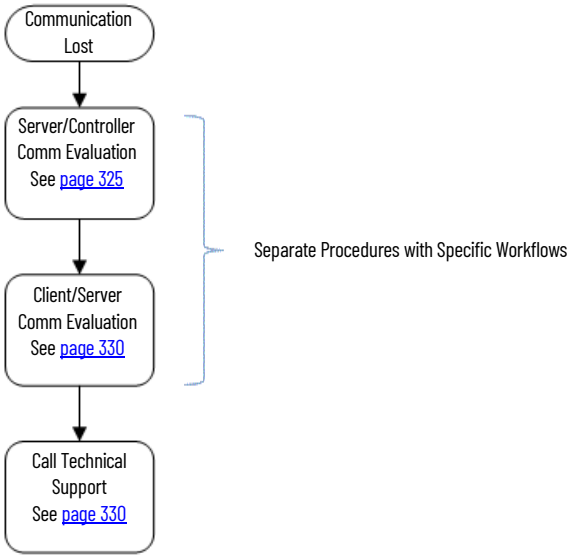
Row	Guidelines	Description
33	Only periodic task used	Use only periodic tasks and remove any unused tasks Use only 2-3 periodic tasks (slow, normal & fast) for logic and remove any unused tasks

PlantPAx Troubleshooting Scenarios

HMI Communication Lost

Figure 25 shows a basic workflow to correct lost communication. To target the root cause, follow this workflow:

Figure 25 - Resolve Lost Communication



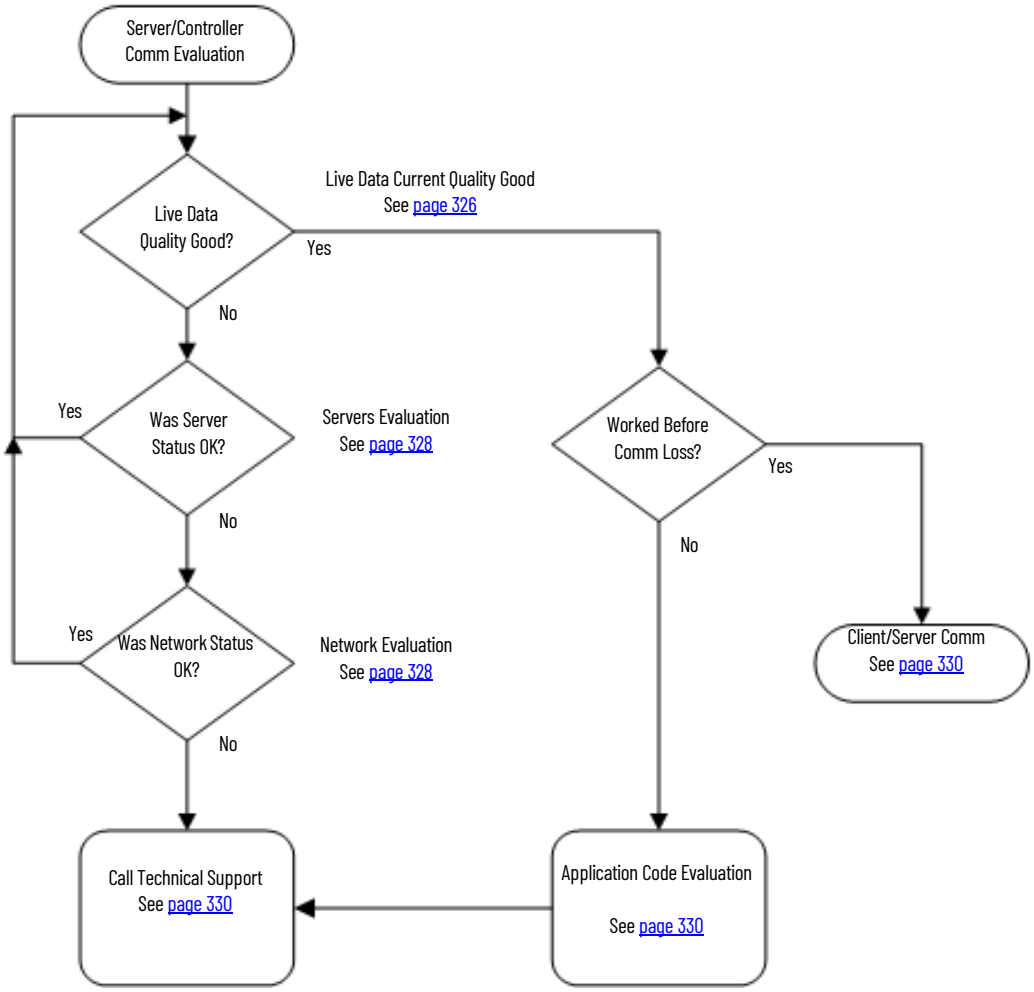
If you can't open a FactoryTalk® View SE client application on your OWS, go directly to the Client/Server Communication Evaluation section on page 330.

Server and Controller Communication Evaluation

Figure 26 shows how to diagnose a loss of communication between the (PASS) server and the controller. Make sure that the server has good quality communication with the controller and follow down the workflow to rule out any network issues.

Click the link or go to the respective page for specific information on each topic. If the server checks out okay, then you have the option to go to the client computer for additional troubleshooting or to call Technical Support.

Figure 26 - Resolve Server to Controller Communication

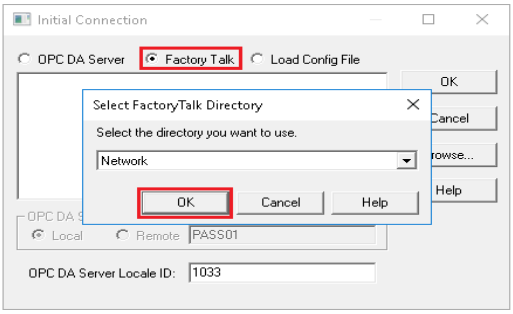


Live Data Current Quality Good

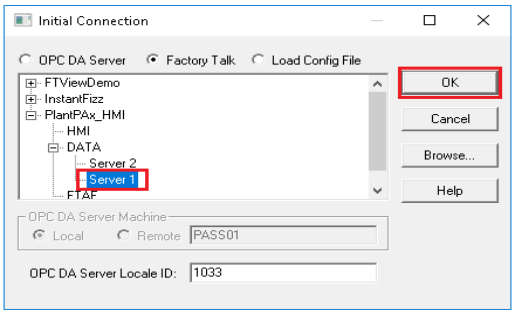
This procedure examines whether the controller communication is available at the server level. If the current quality is 'good', then you can rule out that the server isn't talking to the controller.

1. Go to FactoryTalk Tools > FactoryTalk Live Data Test Client and select FactoryTalk and Network as the Initial Connection.

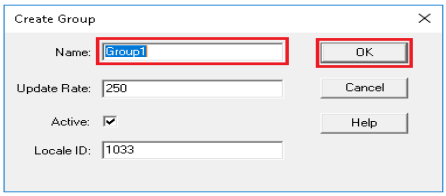
   The Initial Connection dialog box appears.



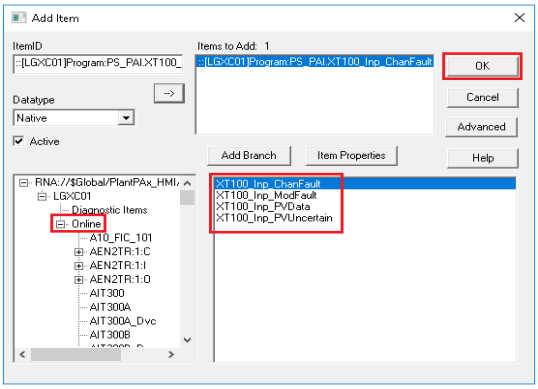
2. Browse to the data server area and click OK.



3. The Create Group dialog box appears.
4. Use the default or type your own group name and click OK.

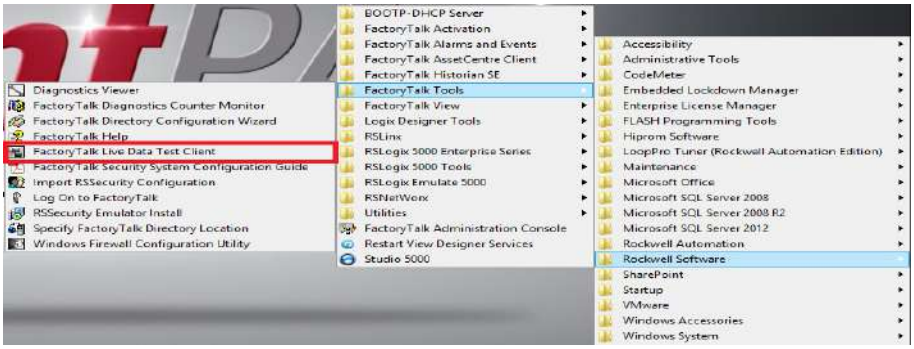


5. In the lower, left pane of the Add Item dialog box, browse to the controller, and select Online.



6. In the right pane, if no tags appear then proceed to Servers Evaluation on page 328. Otherwise, click any tag in the controller and add the item.

   The FactoryTalk® Live Data Test Client dialog box appears.



7. Check that the Current Quality is ‘Good’.

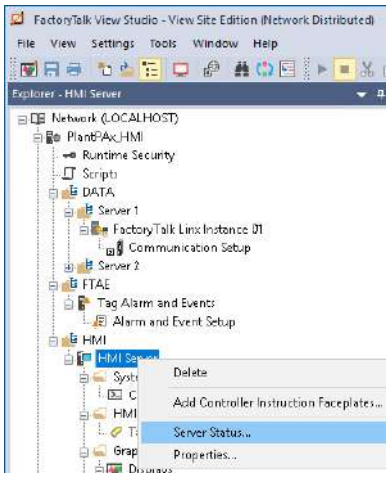
   The ‘Good’ status indicates that you have communication from the server to the controller.

   If the status is ‘Bad’, then proceed to Servers Evaluation.

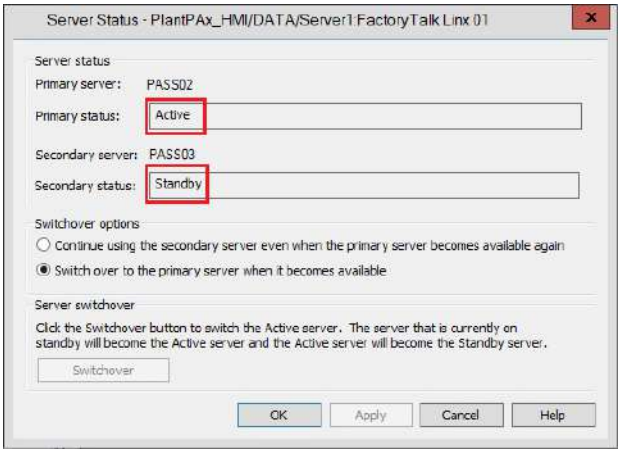
Servers Evaluation

This procedure verifies that at least one server has active status. Complete these steps for the Data server and HMI server.

1. In the FactoryTalk® Administration Console or FactoryTalk View Studio, right-click the Data server and choose Server Status.



The Data server status dialog box appears.



2. Make sure that the status is 'Active' for at least one of the servers.
3. Repeat for the HMI server.

Was Modification Made?

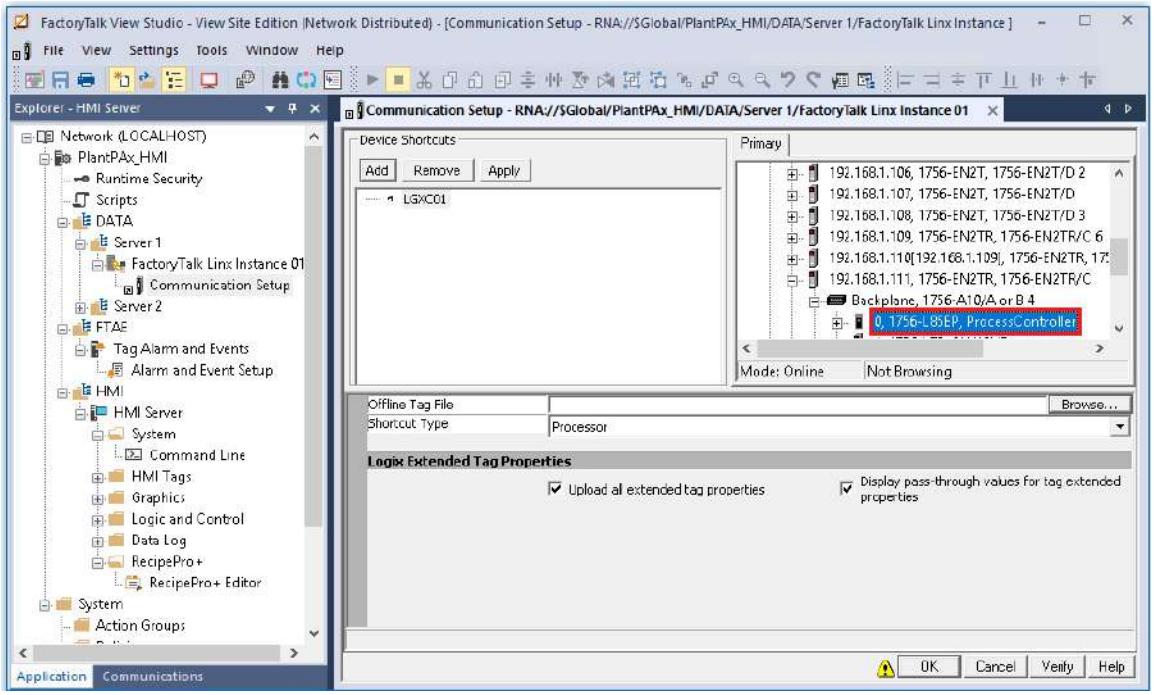
If you found an issue and made a correction, go back and redo the Live Data procedure. Reverify that communication has been established between the server and controller.

Network Evaluation

Now you're analyzing whether the shortcut to the controller is valid. An incorrect path affects the controller communication to the server.

In a redundant system, perform these steps for the Primary and Secondary servers.

1. In the FactoryTalk Administration Console or FactoryTalk View Studio, open the Communications Setup.



2. Select the controller shortcut.

   If the shortcut does not highlight the correct controller, then select the correct controller and save the shortcut.

3. With the correct shortcut selected, expand the backplane.

   If you can browse, then you have communication to the controller. Proceed to Was Modification Made? on page 330.

   If you can't browse, then try to ping the controller from the PASS.

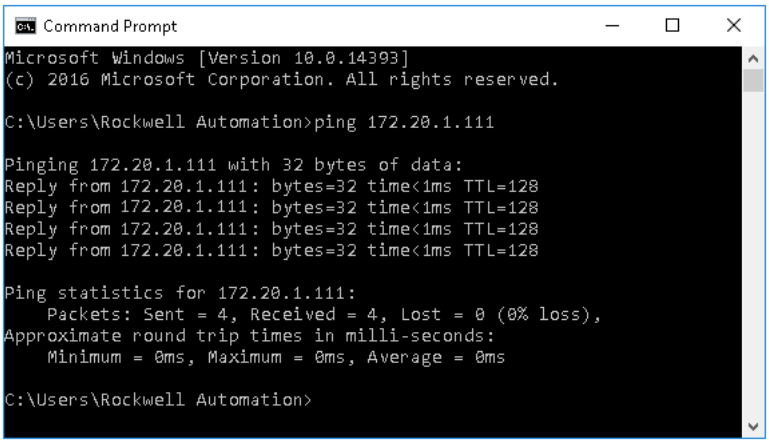
4. To ping the controller, do the following:

   a. Click Start and type CMD into the Search text box.

      A command prompt opens.

   b. Type 'Ping xxx.yyy.zzz.aaa', where the letters represent the IP address of the communication adapter.

5. If the adapter responds, a similar display appears as shown.



6. If your device does not respond, a 'Request Timed Out' message appears.

If the ping is successful, proceed to the next diagnostic action.

7. Repeat steps 2...6 if you're using a redundant Data server.

Was Modification Made?

If you found an issue and made a correction, go back and redo the Live Data procedure. Reverify that communication has been established between the server and controller.

Review Application Code Formatting

If the server and controller are communicating and the problem still exists, we recommend that you check the project application code. Project components could be incorrectly configured.

Verify proper Live Data syntax for the following project elements:

- FactoryTalk View SE or FactoryTalk View ME:
  - Display parameter files
  - Display values, expressions, and animations
  - Global object parameters
  - Command buttons and macros
  - Data logger
  - Event detector
  - Derived tags

Contact Technical Support

Call a Rockwell Automation Technical Support representative if the problem still exists after checking the following:

- Server communication status
- Controller shortcut
- Application code syntax

Email technical support the most recent data that is compiled from the PlantPAx® checklists.

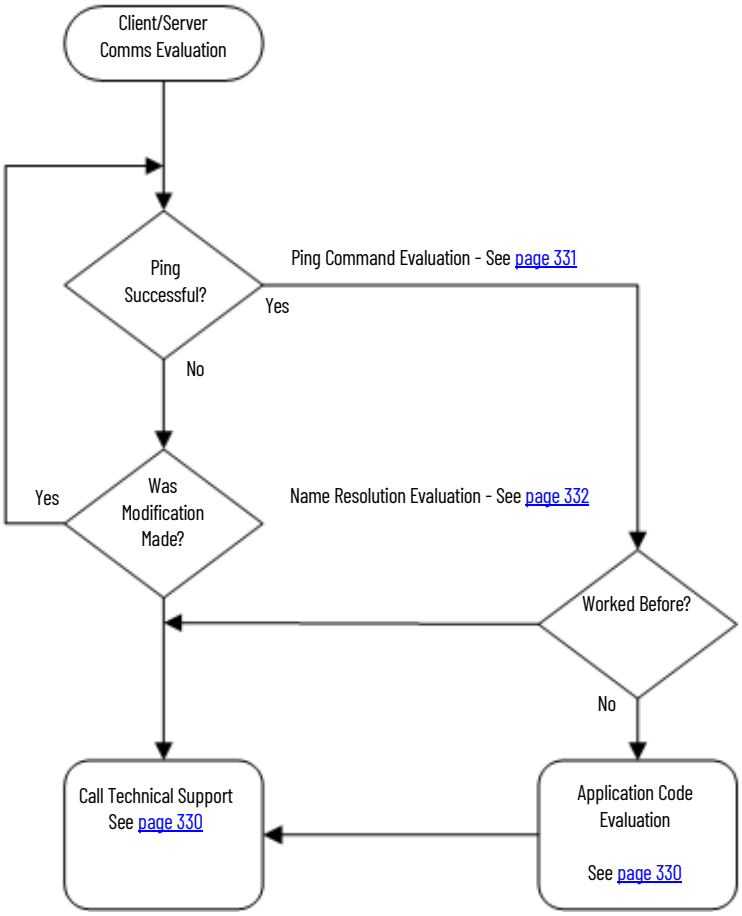
IMPORTANT	If the size of the information packet can't be sent via email, a technical support representative can help you post your information to the Rockwell Automation FTP site.

Client and Server Communication Evaluation

Figure 27 shows a workflow to resolve lost communication between a (PASS) server and a client. Work through the diagnostic activities until you identify an issue.

Click the link or go to the respective page for specific information on each topic. If the issue still exists, contact Technical Support with the details you have compiled to help with a resolution.

Figure 27 - Resolve Server to Client Communication

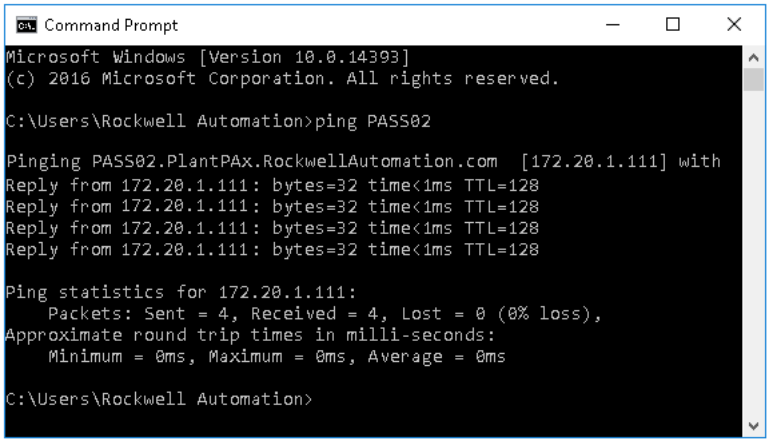


Ping Command Evaluation

To check if the client computer is communicating with the server, start by pinging the computer.

Complete these steps.

1. Click Start and type CMD into the Search text box.
   A command prompt opens.
2. Type 'Ping (and server name)'.
3. If the controller responds, a display appears similar to the following:



4. If your device does not respond, a 'Request Timed Out' message appears.

   If the ping is successful, check your application code for proper syntax. See page 330.

   Also, make sure that the firewall rules are not blocking the communication.

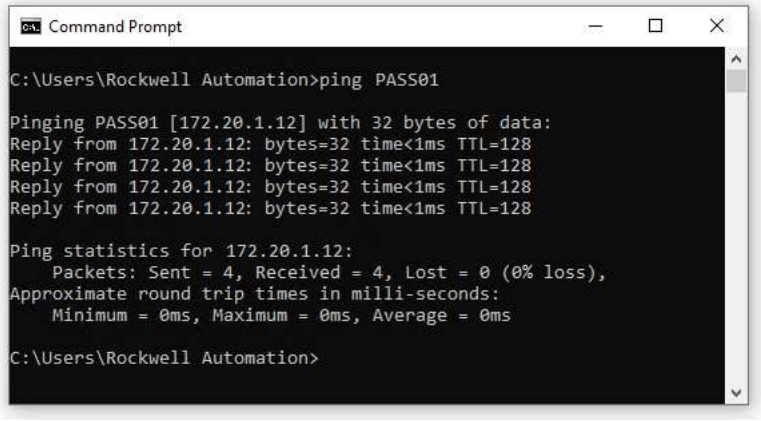
Name Resolution Evaluation

This procedure verifies the mappings of IP addresses to host names. The steps apply if you're using a domain or a work group, with the latter explained last.

1. At the Command Prompt, type the NSLookup and server name and press Enter.
2. Type the name of the server that is being pinged.

   If you receive the message 'DNS Request Timed Out', you typically do not have the Reverse Lookup Zone configured.

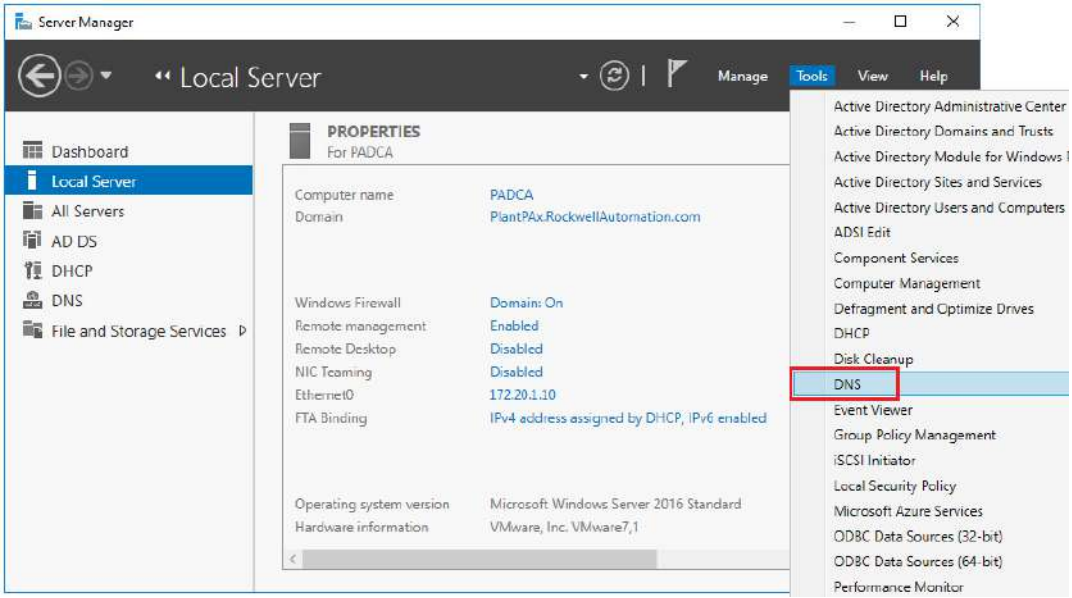
   If the NSLookup ping provides the server name and IP address (as shown in the example), the server communication issue still exists.



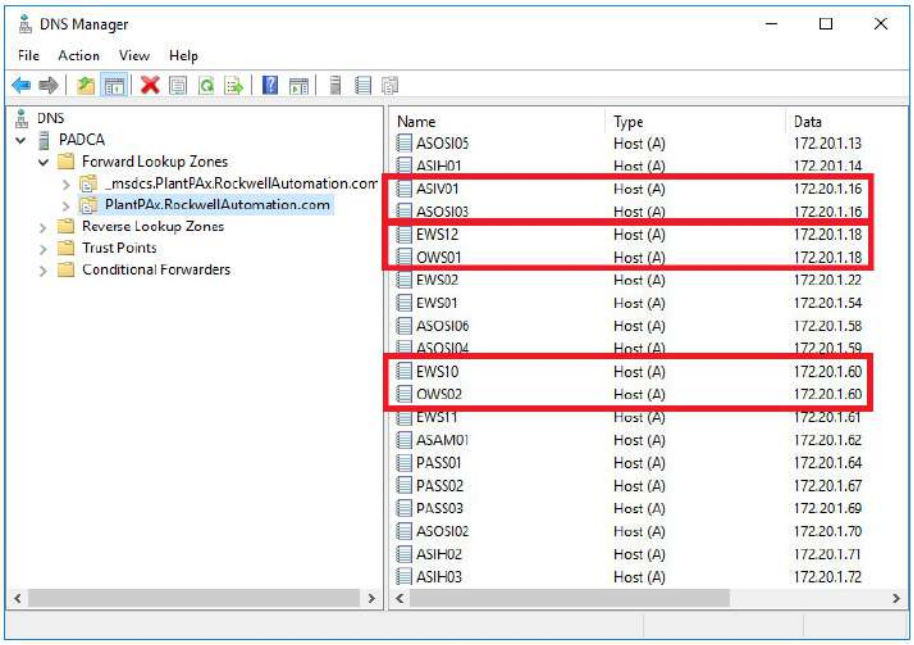
   If the NSLookup ping does not provide a server name and IP address, then proceed with the following instructions on page 332.

To verify that components do not have duplicate IP addresses, complete these steps.

1. From a DNS server, click Tools on the main menu and choose DNS.



The DNS Manager display appears.

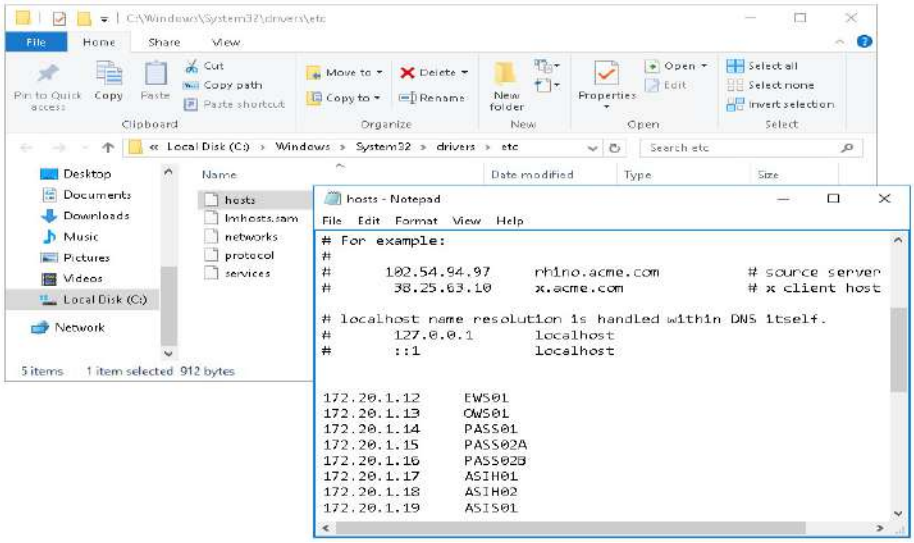


2. Verify that each name has its own IP address to make sure that you're pinging the correct server via the client.

   The example DNS Manager display shows several 'bad' computer names with the same IP address.

3. If you're using a workgroup, open the hosts folder in your Windows local hard disk drive.

4. Using Notepad, open the hosts file.



5. Verify that each name has its own IP address to make sure that you're pinging the correct server via the client.

Was Modification Made?

If you found an issue and made a correction, go back and ping the client computer again.

Review Application Code Formatting

If the server and controller are communicating and the problem still exists, we recommend that you check the project application code. See page 330.

Contact Technical Support

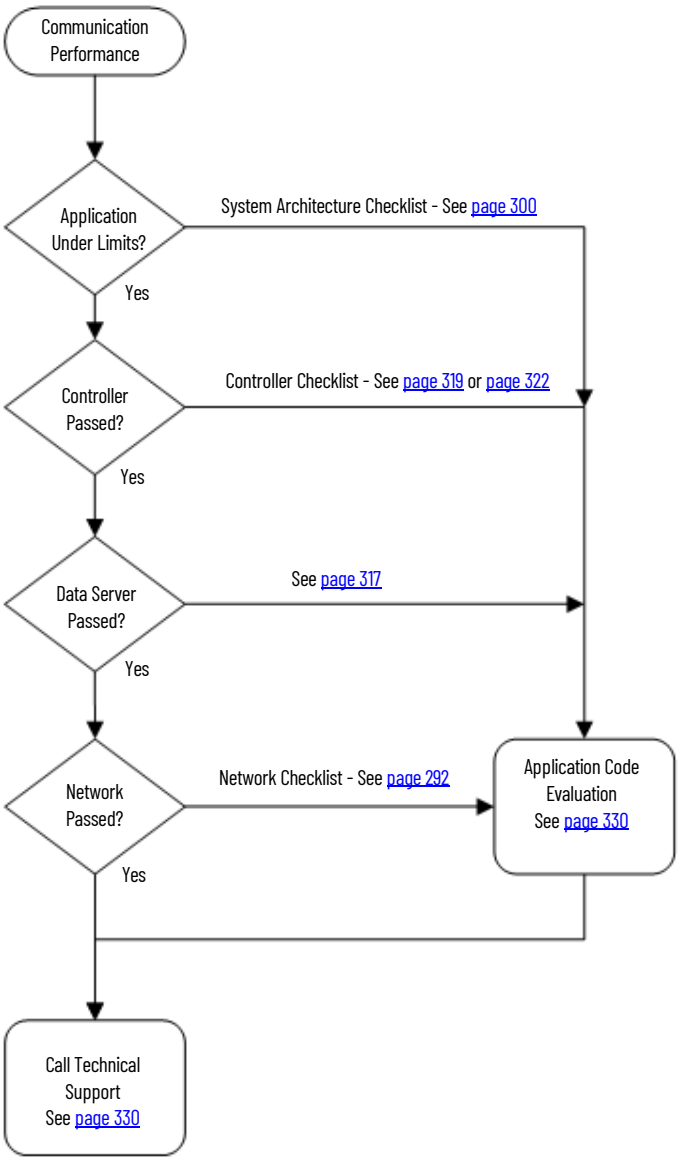
Call a Rockwell Automation technical support representative if the problem still exists. See page 330.

Troubleshooting Scenario: HMI Display Access is Slow

Figure 28 shows a workflow to resolve sluggish HMI displays. To target the root cause, work through the diagnostic activities until you identify an issue.

If the issue still exists, contact Technical Support with the details that you've compiled to help with a resolution.

Figure 28 - Resolve Slow HMI Display Callup



Action	Description
Application Under Limits?	A good starting point is to verify that your system design is within the sizing recommendations for a PlantPAx system. Design attributes include the number of servers, number of assets, and so forth. To verify design attributes, see the System Architecture Tab on page 300.
Controller Passed?	The next step is to check whether your controllers have the CPU and memory usage as prescribed by the PlantPAx guidelines. These percentages vary depending on whether your application uses simplex or redundant controllers. For details, see the Controller 5x80 Tab on page 319 or Controller 5x70 Tab on page 322.
Data Server Passed?	If the application design and controller setup are properly configured, check the Data server. Verify that the server is communicating data from the controllers to the HMI server and operator workstation. For details, see the FactoryTalk Linx worksheet section on page 317.
Network Passed?	The health of the network is critical whether you're using a virtual or traditional operating system. There's a tool for analyzing network infrastructure. For details, see the System Infrastructure Tab on page 292.
Review Application Code Formatting	For details, see page 330.

Notes:

Rockwell Automation Support

Use these resources to access support information.

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

Documentation Feedback

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

Waste Electrical and Electronic Equipment (WEEE)

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

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

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

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication PROCES-UM100D-EN-P - December 2022
Supersedes Publication PROCES-UM100C-EN-P - June 2022