GE

Automation & Controls

Programmable Control Products

PACSystems* Industrial PROFINET Managed Ethernet Switches Secure Deployment Guide (SDG)

GFK-3063

September 2019

For Public Disclosure

Legal Information

Warnings, Cautions, and Notes as Used in this Publication GFL-002

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury, exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Caution

Caution notices are used where equipment might be damaged if care is not taken.

Attention

Indicates a procedure or condition that should be strictly followed.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

GE PROVIDES THE FOLLOWING DOCUMENT AND THE INFORMATION INCLUDED THEREIN AS-IS AND WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED STATUTORY WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

General Contact Information

Online technical support and GlobalCare	www.geautomation.com/support
Additional information	www.geautomation.com
Solution Provider	solutionprovider.ip@ge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this manual, please contact us by telephone or email, or on the web at www.geautomation.com/support

Americas

Phone	1-800-433-2682	
International Americas Direct Dial	1-780-420-2010	(if toll free 800-option is unavailable)
Customer Care Email	digitalsupport@ge.com	
Primary language of support	English	

Europe, the Middle East, and Africa

Phone	+800-1-433-2682	
EMEA Direct Dial	+ 420-296-183-331	(if toll free 800-option is unavailable or if dialing from a mobile telephone)
Customer Care Email	digitalsupport.emea@ge.com	
Primary languages of support	English, French, German, Italian, Spanish	

Asia Pacific

Phone	+86-21-3877-7006 (India, Indonesia, and Pakistan)
	+86-400-820-8208 (rest of Asia)
Customer Care Email	digitalsupport.apac@ge.com
Primary languages of support	Chinese, English

Table of Contents

PACSystems* Industrial Ethernet Switches Secure Deployment Guide (SDG) User Manual GFK-3063 iii

Table of Contents ii

List of Tables .... Error! Bookmark not defined.

Table of Figures v

Chapter 1 About this Guide 6

1.1 Revisions in this Manual 6

1.2 PACSystems Documentation 6

Chapter 2 Introduction 8

2.1 Security 8

2.2 Firewall 8

2.3 Defense in Depth 8

2.4 General Recommendations 9

2.5 Checklist 9

Chapter 3 Communication Requirements 10

3.1 Protocols Supported 10

3.1.1 Ethernet Protocols 10

3.1.2 Serial Protocols 12

3.2 Server 12

3.3 Client 13

3.4 PROFINET 13

3.4.1 Installing an I/O device 13

3.4.2 Network Discovery & Device Identification 14

3.4.3 Using an I/O device 14

3.4.4 Using an IED 15

3.5 Ethernet Firewall Configuration 15

3.5.1 Lower-level Protocols 15

3.5.2 Application Layer Protocols 16

Chapter 4 SecurityCapabilities 17

4.1 Capabilities by Product 17

4.1.1 PACSystems Ethernet Switches 17

4.2 Access Control and Authorization 17

4.2.1 Authorization Framework 17

4.2.2 Specifying Access Rights 18

4.2.3 Summary 19

4.2.4 Plaintext Login 20

4.2.5 Recommendations 20

4.3 Confidentiality and Integrity **22**

4.3.1 Communications Protocols 22

4.3.2 Firmware Signatures 22

4.4 Security Management and Implementation **23**

4.6.1 Privilege Level Configuration 23

4.6.2 Access Management Configuration 24

4.6.3 SSH/TELNET/HTTPS/SNMP Configuration 25

4.5 Limit Control **27**

4. 8 Access Control List (ACL) **28**

4.8.1 Access Control List 28

4.8.2 Ports 29

4.8.3 Rate Limiters 31

4.9 Network Access Server (NAS) **32**

4.10 IP Source Guard **33**

4.10.1 Configuration 33

4.10.2 Static Table 34

4.11 ARP Inspection **35**

4.11.1 ARP Inspection Configuration 35

4.11.2 VLAN Configuration 35

4.11.3 Static Table 36

Chapter 5 Configuration Hardening **37**

5.1 Ethernet Interface **37**

5.1.1 Disabling Ethernet Services 37

Chapter 6 Network Architecture and Secure Deployment 38

6.1 Reference Architecture 38

6.2 Remote Access and Demilitarized Zones (DMZ) 39

6.3 Access to Process Control Networks 39

6.4 Access to PROFINET Networks 39

6.5 Hot Standby CPU Redundancy with PROFINET I/O 40

Chapter 7 Other Considerations 41

7.1 Patch Management 41

7.2 Real-time Communication 41

7.3 GLM Series Compensating Controls 41

7.3.1 Network Bandwidth Limiting 41

7.4 Additional Guidance 41

7.4.1 Protocol-specific Guidance 41

7.4.2 OPC UA Server 42

7.4.3 PROFINET Controller Duplicate IP 42

7.4.4 MRP Ring Ethernet Traffic Storm Prevention 42

7.4.5 Government Agencies and Standards Organizations 42

Table of Figures

Figure 1: PACSystems Deployed in Purdue Model 38

Chapter 1 About this Guide

This document provides information that can be used to help improve the cyber security of systems that include PACSystems products. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring PACSystems products.

Secure deployment information is provided in this manual for the following PACSystems products:

Family	Catalog Number	Description
PACSystems PROFINET/Ethernet Switches	IC086GLM064	10-Port Managed, Gig, 6TX4SFP, PROFINET
	IC086GLM082	10-Port Managed, Gig, 8TX2SFP, PROFINET
	IC086GLM104	14-Port Managed, Gig, 10TX4SFP, PROFINET

1.1 Revisions in this Manual

Rev	Date	Description
	Aug-2019	• Initial release

1.2 PACSystems Documentation

1.2.1 PACSystems Manuals

PACSystems RX7i, RX3i and RSTi-EP CPU Reference Manual	GFK-2222
PACSystems RX7i, RX3i and RSTi-EP CPU Programmer's Reference Manual	GFK-2950
PACSystems RX7i, RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual	GFK-2224
PACSystems TCP/IP Ethernet Communications Station Manager User Manual	GFK-2225
PACSystems Memory Xchange Modules User's Manual	GFK-2300
PACSystems Hot Standby CPU Redundancy User Manual	GFK-2308
Proficy Machine Edition Logic Developer Getting Started	GFK-1918
Proficy Process Systems Getting Started Guide	GFK-2487
PACSystems RXi, RX3i, RX7i and RSTi-EP Controller Secure Deployment Guide	GFK-2830
PACSystems Industrial PROFINET Managed Ethernet Switches Important Product Information (IPI)	GFK-3028
PACSystems Industrial PROFINET Managed Ethernet Switches User's Manual	GFK-3030
PACSystems Industrial PROFINET Managed Ethernet Switches CLI Command Reference Guide	GFK-3061
PACSystems Industrial PROFINET Managed Ethernet Switches Web Configuration Tool Guide	GFK-3062
PACSystems Industrial PROFINET Managed Ethernet Switches MRP Application Guide	GFK-2070
PACSystems Industrial PROFINET Managed Ethernet Switches Installation & Maintenance Requirements	GFK-3098

RX3i Manuals

PACSystems RX3i System Manual	GFK-2314
PACSystems RX3i PROFINET Scanner Manual	GFK-2737
PACSystems RX3i CEP PROFINET Scanner User Manual	GFK-2883
PACSystems RX3i Serial Communications Modules User Manual	GFK-2460
PACSystems RX3i Genius Communications Gateway User Manual	GFK-2892
PACSystems RX3i DNP3 Outstation Module IC695EDS001 User Manual	GFK-2911
PACSystems RX3i IEC 104 Server Module IC695EIS001 User Manual	GFK-2949
PACSystems RX3i Ethernet Network Interface Unit User's Manual	GFK-2439
PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual	GFK-2571

Field Agent Manuals

Field Agents User Guide	GFK-2993
Field Agents Upgrade Guide	GFK-3017
Field Agents Secure Deployment Guide	GFK-3009

Note: A given feature may not be implemented on all PACSystems Ethernet switches (GLM). To determine whether a feature is available on a given model and firmware version, please refer to the *Important Product Information* (IPI) document provided with the product.

In addition to these manuals, datasheets and product update documents describe individual modules and product revisions. The most recent PACSystems documentation is available on the GE Automation & Controls support website www.geautomation.com/support.

Chapter 2 Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 Security

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- **Confidentiality:** Ensure only the people you want to see information can see it.
- **Integrity:** Ensure the data is what it is supposed to be.
- **Availability:** Ensure the system or data is available for use.

GE recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE products

and solutions.

As GE product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in a particular product version as well as the version in which the vulnerability was fixed. GE Product Security Advisories can be found at the following location:

https://digitalsupport.ge.com/communities/en_US/Article/GE-Intelligent-Platforms-Security-Advisories

2.2 Firewall

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

Therefore, GE recommends taking a *Defense in Depth* approach to security.

2.3 Defense in Depth

Defense in Depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent both the firewall and the username/password authentication.

2.4 General Recommendations

The following security practices should be followed when using GE products and solutions.

- The devices covered in this document were not designed for or intended to be connected directly to any wide area network, including but not limited to a corporate network or the Internet at large. Additional routers and firewalls (such as those illustrated in the section, *Reference Architecture*) that have been configured with access rules customized to the site's specific needs must be used to access devices described in this document from outside the local control networks. If a control system requires external connectivity, care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest GE Automation & Controls product security patches, updates, SIMs and other recommendations.
- Use anti-virus software on control products and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control products and keep the whitelist up-to-date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying PACSystems products.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node. (Refer to 3 *Communication* Requirements).
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram. (Refer to Chapter 6, *Network Architecture and Secure Deployment.*)
5. Configure firewalls and other network security devices. (Refer to Section 3.5, *Ethernet Firewall Configuration* and to Chapter 6, *Network Architecture and Secure Deployment*.)
6. Enable and/or configure the appropriate security features on each device. (Refer to Chapter 4, *Security Capabilities*.)
7. On each device, change every supported password to something other than its default value. (Refer to Section **Error! Reference source not found.**, ***Error! Reference source not found.***.)
8. Harden the configuration of each device, disabling unneeded features, protocols and ports. (Refer to Chapter 5, *Configuration Hardening*.)
9. Test/qualify the system.
10. Create an update/maintenance plan

Note: Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance. For more information about security programs in general, refer to Section 7.4, *Additional Guidance*.

Chapter 3 Communication Requirements

Communication between different parts of a control system is, and must be, supported. However, the security of a control system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed, to only what is needed. This can be accomplished by disabling every communication protocol that isn't needed on a particular device (refer to Chapter 5, *Configuration Hardening*), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

GE recommends limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. Successfully doing this requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used with PACSystems Ethernet switches, and indicates the role of each participant in the communication. Lower-level Ethernet protocols are not discussed here, but are instead assumed to be supported when needed by the application protocol. (For example, in order to support SRTP communication between two nodes, the network must also support TCP, IP, and ARP in both directions between the nodes.)

Note: On a PACSystems node such as the RX3i, support for these protocols may be provided by a peripheral module (for example, IC695ETM001, IC695PNC001, or IC695ECM850) or by an interface that is embedded in the CPU/NIU module.

Note: On a PROFINET device, support for these protocols may be provided by a peripheral module (for example, a PROFIBUS or Serial Communications module).

This information is intended to be used to help guide the specification of the network architecture and to help configure firewalls internal to that network, in order to support only the required communications paths for any particular installation.

3.1 Protocols Supported

3.1.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported, and by which Switches. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Supported ETHERNET Protocols

	Protocol	PROFINET Managed Switches		
		IC086GLM064	IC086GLM082	IC086GLM104
Link	ARP	✓	✓	✓
	LLDP	✓	✓	✓
Internet	IPv4	✓	✓	✓
	ICMP	✓	✓	✓

	Protocol	PROFINET Managed Switches		
		IC086GLM064	IC086GLM082	IC086GLM104
Internet	IGMP	✓	✓	✓
Trans	TCP	✓	✓	✓
	UDP	✓	✓	✓
Application Layer	BOOTP Client	✓	✓	✓
	DCE/RPC Client	✓	✓	✓
	DNS Client	N/A	N/A	N/A
	Ethernet Global Data	N/A	N/A	N/A
	FTP Server	N/A	N/A	N/A
	HTTP Server	✓	✓	✓
	HTTPS Server	✓	✓	✓
	Modbus® TCP Master	N/A	N/A	N/A
	Modbus TCP Slave	N/A	N/A	N/A
	OPC UA Server	N/A	N/A	N/A
	PROFINET DCP Client	✓	✓	✓
	PROFINET DCP Server	✓	✓	✓
	PROFINET I/O	✓	✓	✓
	IEC 61850 Client	N/A	N/A	N/A
	DNP3 Outstation	N/A	N/A	N/A
	IEC 60870-5-104 Server	N/A	N/A	N/A
	MRP	✓	✓	✓
	Reliable Datagram Client	N/A	N/A	N/A
	Reliable Datagram Server	N/A	N/A	N/A
	Remote Station Mgr Client	N/A	N/A	N/A
	Remote Station Mgr Server	N/A	N/A	N/A
	Set Temporary IP Server	N/A	N/A	N/A
	SNMP v2c Server	✓	✓	✓
	SNMP v3 Server	✓	✓	✓
	SNTP Client	N/A	N/A	N/A
	SRTP Client	N/A	N/A	N/A
	SRTP Server	N/A	N/A	N/A
	SSH Server	✓	✓	✓
	Telnet Server	✓	✓	✓
	HSB Redundancy	N/A	N/A	N/A

3.1.2 Serial Protocols

In addition to Ethernet, many PACSystems products also support communication over serial ports (RS-232, RS-485, and/or USB). The information provided here should be used to help guide the specification of any external security controls required to restrict remote serial access, as well as the specification of any required physical security.

This section indicates which serial protocols are supported, and by which PROFINET Devices. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Supported Serial Protocols

Protocol	PROFINET Managed Switches		
	IC086GLM064	IC086GLM082	IC086GLM104
Application Specific [1]	N/A	N/A	N/A
ASCII Terminal	✓	✓	✓
Modbus RTU Slave	N/A	N/A	N/A
SNP Slave †	N/A	N/A	N/A

[1] Some switches can be configured so that one or more of their serial ports is controlled by the user application program that is executing on the controller. Such “Application-specific” protocols are outside of the scope of this document and will not be discussed further.

† SNP functionality may be limited. For example, it may only provide Firmware Update Services.

3.2 Server

This section summarizes the available communication-centric functionality, where the communication is initiated by some other device or computer.

Functionality		Required Application Protocols	Example Clients
Ethernet	Service Requests	N/A	N/A
	EGD Consumption	N/A	N/A
	Process EGD Commands	N/A	N/A
	Modbus TCP Slave	N/A	N/A
	Ethernet Station Manager	N/A	N/A
	OPC UA Server	N/A	N/A
	PROFINET Controller command shell	Telnet	telnet.exe on computer
	DNP3 Outstation or Server	N/A	N/A
	IEC 60870-5-104 Server or Slave	N/A	N/A
	Web Server	HTTP	Web browser

Functionality		Required Application Protocols	Example Clients
	Update Web Pages	N/A	N/A
	Network Management	SNMP v2c	SNMP client on computer
	Assign IP before configuring module	Set Temporary IP	Proficy Machine Edition
Serial	Service Requests	N/A	N/A
	Firmware Update	N/A	N/A
	Modbus RTU Slave	N/A	N/A
	Serial Station Manager	N/A	N/A
	Command shell	ASCII Terminal	Terminal emulator on computer
	ECM850 command shell	N/A	N/A

3.3 Client

This section summarizes the available communication-centric functionality, where the communication is initiated by the PACSystems controller. The servers involved in these communications are selected by the user application and/or configuration.

Functionality		Required Application Protocols	Example Servers
Ethernet	SRTP Channels	N/A	N/A
	Modbus TCP Channels	N/A	N/A
	EGD Production	N/A	N/A
	Send EGD Commands	N/A	N/A
	Ethernet Station Manager	N/A	N/A
	Time Synchronization	SNTP	SNTP server
	Assign IP addresses using a centralized database of addresses	BOOTP	BOOTP server
	Lookup IP addresses by Name	N/A	N/A
	IEC 61850 Client	N/A	N/A

3.4 PROFINET

This section describes the communication paths needed to support common operations on a PROFINET network.

3.4.1 Installing an I/O device

Commissioning, adding, or replacing a PROFINET switch requires that the device be assigned a unique name to use on the PROFINET network. Doing this requires supporting the following communication path.

Protocol	Proficy Machine Edition	I/O device
PROFINET DCP	Client	Server

Supporting this path will allow Proficy Machine Edition to directly discover all of the PROFINET devices that are connected to the same subnet as the computer. (Note that this protocol is not routable.) It can then be used to (re-) assign a unique name to the device being installed.

Note: This protocol can also be used to make other modifications to the device, such as assigning a new IP address or resetting it to factory defaults. However, those functions are not generally required when installing a device.

3.4.2 Network Discovery & Device Identification

Proficy Machine Edition can also request information about the devices on a PROFINET network from a PACSystems Controller, and then retrieve additional identification information about each device. This request is sent to the PACSystems Controller using the Service Request protocol (described elsewhere) embedded within the SRTP or SNP protocols. The PACSystems Controller satisfies those requests using the following communication paths.

Protocol	Local I/O controller	Remote I/O controllers and I/O devices
DCE/RPC	Client	Server
PROFINET DCP	Client	Server

No mechanism is provided through this communication path for assigning a name to a new I/O device.

3.4.3 Using an I/O device

Using PROFINET I/O as part of the control application requires that all of the following communication paths be supported throughout the life of the application.

Protocol	I/O controller	I/O devices
DCE/RPC	Client	Server
DCE/RPC	Server	Client
PROFINET DCP	Client	Server
PROFINET I/O	Bi-directional	Bi-directional

In addition, if the PROFINET network is configured to support Media Redundancy (which requires a physical ring topology) then the following application protocol must also be supported.

3.4.4 Using an IED

Using IED's objects as part of the control application requires that all of the following communication paths be supported throughout the life of the application.

Protocol	Local communication module (e.g. ECM850)	IED(s)
IEC 61850	Client	Server

3.5 Ethernet Firewall Configuration

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. This section identifies the EtherTypes and the TCP/UDP ports used by the protocols supported on PACSystems products and PROFINET switches.

Note: Refer to the section Reference Architecture for a diagram showing firewall placement.

This information should be used to help configure network firewalls, in order to support only the required communications paths for any particular installation.

3.5.1 Lower-level Protocols

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application layer are the Transport, Internet, and Link layers.

Information on the supported protocols from these three lower layers is summarized here.

Link Layer Protocols

Protocol	EtherType
ARP	0x0806
LLDP	0x88cc

Internet Layer Protocols

Protocol	EtherType	IP Protocol #
IPv4	0x0800	(n/a)
ICMP	0x0800	1
IGMP	0x0800	2

Transport Layer Protocols

Protocol	EtherType	IP Protocol #
TCP	0x0800	6
UDP	0x0800	17

Each of these lower-level protocols is required by one or more of the Application protocols supported on the PACSystems family of and PROFINET products.

3.5.2 Application Layer Protocols

PROFINET switches are capable of acting as a server, responding to requests sent through any of several different protocols. They are also capable of acting as a client, sending requests to other servers using any of several different protocols. The exact set of protocols that are enabled/used will depend on which modules are installed, how they are configured, and the details of the application program that is running on the CPU.

Protocol	Server TCP Port	Test UDP Port	EtherType (non-IP protocol)
DCE/RPC		34964 on server >1023 on client	
FTP	20, 21		
HTTP	80		
HTTPS	443		
PROFINET DCP			0x8892
PROFINET I/O			0x8892
MRP			0x88e3
SNMP v2c		161 on server >1023 on client	
SNTP		123	
Telnet	23		
Set Temporary IP	1		

Chapter 4 Security Capabilities

This section describes the GE Automation & Controls PROFINET switch capabilities and security features which can be used as part of a defense-in-depth strategy to secure your control system.

4.1 Capabilities by Product

This section provides a summary view of the security capabilities supported on each PROFINET switch.

4.1.1 PACSystems Ethernet Switches

Protocol	PROFINET Managed Switches		
	IC086GLM064	IC086GLM082	IC086GLM104
Predefined set of Subjects & Access Rights	✓	✓	✓
Plaintext Login	✓	✓	✓
Secure Login	✓	✓	✓
Access Control List	✓	✓	✓
Firmware Signatures	✓	✓	✓
Secure Boot	✓	✓	✓

4.2 Access Control and Authorization

The Access Control process can be divided into two phases:

- **Definition** – Specifying the access rights for each subject (referred to as Authorization), and
- **Enforcement** – Approving or rejecting access requests.

This section describes the Access Control capabilities supported by PROFINET switches, which includes its Authorization capabilities.

4.2.1 Authorization Framework

Defining the access rights for each subject implies that the system must have some means to identify each subject. The most familiar way this is achieved is by assigning a unique User ID to each person who will access the system.

GE's Automation & Control PROFINET switches, however, don't provide such a facility – there is no support for creating User IDs. In many cases, a User ID doesn't even have to be specified to authenticate. In such cases, authorization is based on the functionality being used and the password that is provided for authentication. Never-the-less, the authentication features supported on PROFINET switches implicitly define a fixed set of subjects, which are identified here.

The set of implicitly defined subjects will vary depending on the server protocols that are supported, which depends on what modules are installed and how they are configured. Each kind of server has its own set of predefined subjects – there are no subjects that apply across multiple servers (other than *anonymous*). Further, each instance of a server has its own instances of the predefined subjects – access rights for each subject must be separately managed for each instance of a given kind of server.

For example, each PACSystems controller acts as a Service Request server. Therefore, access rights for each PACSystems controller in the system must be independently managed. Similarly, each Ethernet Interface supports the Ethernet Station Manager server. Therefore, access rights for each Ethernet Interface must be individually managed – even when multiple Ethernet Interface modules are located in a single rack, providing service to a single PACSystems controller.

The subjects defined and supported by each server protocol are indicated in the following table.

Functionality		Application Protocol	Subjects Available
Ethernet	Telnet Server	Telnet	Anonymous
	SSH Server	SSH	Anonymous
	Web Server	HTTP	Anonymous
	Web Server Firmware Update	HTTP	Firmware Updater
	Web Server Password Reset	HTTP	Anonymous
	Network Management	SNMP v2c	Anonymous
Serial	Firmware Update	TFTP Client	Anonymous
	Command Shell	ASCII Terminal	Plaintext

4.2.2 Specifying Access Rights

For each subject, PROFINET switches provide predefined access rights. In some cases, those access rights can be partially restricted, while in other cases they either cannot be changed at all, or can only be revoked by disabling the associated server/protocol.

Predefined Access Rights

The Access Rights to data on the PACSystems controller itself, regardless of the protocol being used, are the most complex. The services provided directly by other PROFINET Devices have simple, well-documented access rights and so aren't discussed here further. These specifically include the PROFINET Controller command shell, Ethernet Station Manager, the SNMP server, the Web server, and the FTP server. See the user manuals for each of those services for more details.

PACSystems provides password-based authentication for some, but not all, of its server protocols. PROFINET devices may provide password-based authentication for some, but not all. For each unauthenticated protocol that is enabled, compensating controls may be needed to satisfy the security requirements of a particular installation.

Note: The default configuration for all Server protocols is for no authentication, or for authentication using well-known default values.

4.2.3 Summary

This section summarizes the authentication mechanisms supported by PACSystems for each protocol. It is important to note that some PACSystems controllers only support a subset of the authentication options listed here. Refer to Section 4.1, *Capabilities by Product*, for more details.

Authentication Available on PACSystems Servers

Functionality		Application Protocol	Authentication Options
Ethernet	Telnet Server	Telnet	Anonymous
	SSH Server	SSH	Anonymous
	Web Server	HTTP	None
	Update Web Pages	FTP	Plaintext login
	Web Server Firmware Update	HTTP	None[1]
	Network Management	SNMP v2c	None[2]
Serial	Firmware Update	Tftp Client	None – must be Disabled
	Command Shell	ASCII Terminal	Plaintext login
	ECM850 command shell	ASCII Terminal	Plaintext login

[1] Web Server Firmware Update on the RXi supports a plaintext User ID and password, but they are set to well-known, fixed values.

[2] SNMP v2c supports a plaintext community string. Refer to each PACSystems product manual for details on the community string settings and what SNMP features are accessible by the community string.

Authentication Supported by PACSystems Clients

Functionality		Required Application Protocols	Authentication Supported
Ethernet	SRTP Channels	SRTP	None
	EGD Production	Ethernet Global DataError! Bookmark not defined.	None
	Send EGD Commands	Reliable Datagram Svc	None
	Modbus TCP Channels	Modbus TCP	None
	Ethernet Station Manager	Remote Station Mgr	Plaintext login
	Time Synchronization	SNTP	None
	Assign IP addresses using a centralized database of addresses	BOOTP	None
	Lookup IP addresses by Name	DNS	None

Note: Login is not supported by SRTP Channels, even though passwords may be enabled on the SRTP server. When using SRTP Channels, the SRTP server cannot have password protection enabled for PRIV level 2 if data writes are required.

Authentication Supported by the PROFINET Protocol

The PROFINET I/O specification does not define an authentication mechanism and so none is supported on PACSystems for any PROFINET communications.

4.2.4 Plaintext Login

Authentication for many of the supported protocols involves sending a plaintext password to the PACSystems controller. A plaintext password is sent over the network without any confidentiality protection, such as encryption. The consequence is that any network entity between the two endpoints exchanging authentication information could sniff the network traffic and observe the plaintext password. In some cases, these plaintext passwords cannot be more than seven (7) characters long. When such protocols are required, additional compensating controls may be needed to satisfy the security requirements of a particular installation.

4.2.5 Recommendations

GE strongly recommends that authentication be used for every enabled protocol that supports authentication, that all default passwords be changed, and that access be appropriately restricted to any computer-based file that includes a plaintext password.

When a choice between a plaintext-based login and a Secure Login is available, GE strongly recommends that the Secure Login feature be used since it prevents network entities from sniffing plaintext passwords and increases the password maximum length to 31 characters.

Whenever protocols are used with no authentication mechanism, or when authentication is disabled or relies on sending credentials in plaintext across the network, it is critical to control physical and electronic access to the network to prevent unauthorized messages from being sent and acted upon.

Below are recommended actions to be taken to mitigate the risk of external or internal entities accessing an Industrial Control System (ICS) network and sending unauthorized messages.

Personnel Security Protection

1. All individuals with permission to physically access ICS systems should have background checks and be trained in the proper use and maintenance of ICS systems.

Physical Security Perimeter Protection

1. All ICS hardware should be placed in locked cabinets, with policies and procedures to restrict access to the key.
2. Network equipment such as switches, routers, firewalls, and Ethernet cabling should be physically protected in locked enclosures such as cabinets or closets with policies and procedures to restrict access to these enclosures.
3. Whenever possible, there should be no physical network path from an ICS network to the Internet. It should not be possible for an attacker to reach an ICS network from any Internet-facing computer.
4. Networks should always be physically segmented as suggested in the Reference Network Architecture diagram (**Figure 1**) to avoid exposure to ICS networks.
5. Each ICS system asset should be visibly labeled by a unique identifier, with all expected asset identification

compiled into an access controlled list.

Electronic Security Perimeter Protection

1. All external access to an ICS network should be managed through a Virtual Private
2. Network (VPN) or similar technology leveraging two-factor authentication. Next-Generation Firewalls should be properly configured and deployed at each conduit between physical networks that deny all but the specifically allowed protocol families, source addresses, and destination addresses, and specific application-level commands between the two adjacent networks. For example, a Next-Generation Firewall could prohibit write operations across networks while allowing read operations.
3. If one network node such as a PLC or HMI uses unauthenticated protocols to exchange information or commands with another network node on the same physical network, a Next-Generation Firewall could be deployed between the two network nodes. This Next-Generation Firewall should be configured to explicitly whitelist all expected messages between the two network nodes, and deny all other unexpected messages.
4. To detect and alert for unexpected, unauthenticated messages on a given network, an Intrusion Detection System (IDS) could be configured and deployed. Consider configuring the IDS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
5. To detect and actively prevent unexpected, unauthenticated messages on a given network from reaching a given network node, an Intrusion Prevention System (IPS) could be configured and deployed. Consider configuring the IPS to log all events to a Security Information and Event Management (SIEM) system that aggregates all security information on the ICS network.
6. To limit the impact of the compromise of any single user account, it is recommended to divide *administrators* privileges into several user accounts, each for its own operational function.
7. To limit the impact of the compromise of any single set of credentials (user name, password) for any ICS equipment, it is recommended to never re-use credentials for different tools or purposes.
8. Carefully protect sources of and access to credentials (user names, passwords) for all ICS equipment, including switches, routers, firewalls, IDS, IPS, etc.
9. Enforce a policy of rotating credentials for ICS equipment periodically and after personnel changes. Note that products with no support for enforcement of unique passwords over time should be compensated for with policies and procedures that require a history of unique passwords.

Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

4.3 Confidentiality and Integrity

4.3.1 Communications Protocols

Some communications protocols provide features that help protect data while it is *in flight*– actively moving through a network. The most common of these features include:

- **Encryption** – Protects the confidentiality of the data being transmitted.
- **Message Authentication Codes** – Ensures message authenticity and integrity by cryptographically detecting message tampering or forgery. This ensures the data originated from the expected source and was not altered since it was transmitted, regardless of whether it was malicious or not.

Currently, none of the communications protocols supported by PACSystems provide either of these features, as detailed in the following table. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Protocol-provided Security Capabilities

Transport Medium	Protocol	Data Encryption	Message Authentication Codes
Ethernet	BOOTP	N	N
	DCE/RPC	N	N
	Ethernet Global Data	N	N
	FTP Client	N	N
	HTTP	N	N
	HTTPS	Y	N
	PROFINET DCP	N	N
	PROFINET I/O	N	N
	MRP	N	N
	~~RDS~~	~~N~~	~~N~~
	SNMP v2c	N	N
	SNMP v3	Y	Y
	SNTP	N	N
	SSH	Y	Y
	Telnet	N	N
Serial	ASCII Terminal	N	N

4.3.2 Firmware Signatures

Some PACSystems controllers have digitally signed firmware images to provide cryptographic assurance of the firmware's integrity. For controllers that support this feature, a digital signature is used to verify that any firmware being loaded onto the controller was supplied by the General Electric Company, and has not been modified. If the digital signature validation fails, the new firmware will not be installed onto the device.

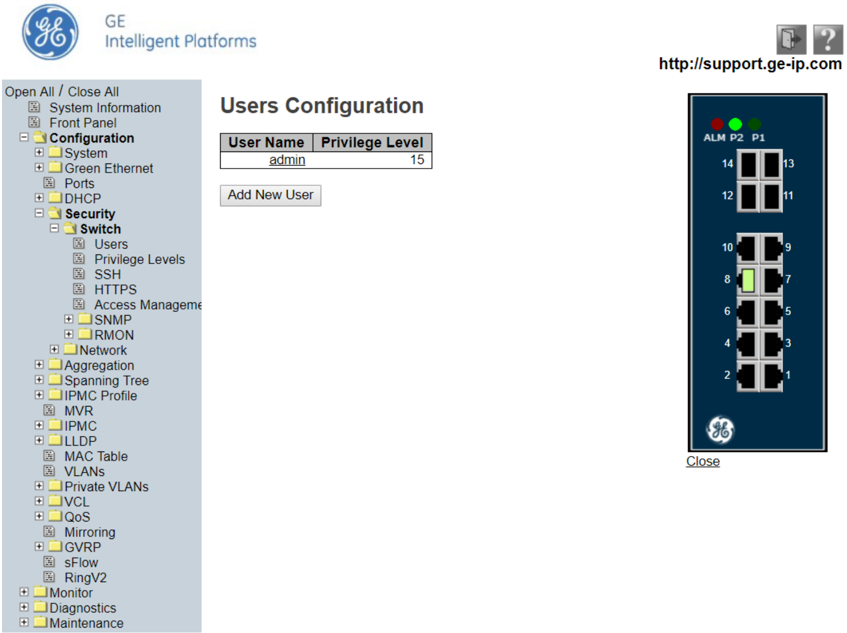
4.4 Security Management and Implementation

4.6.1 Privilege Level Configuration

It provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

If User's Privilege Level is equal to or higher than Group's Privilege Level, it permit User to work in this Group with Read-only or Read/write mode.

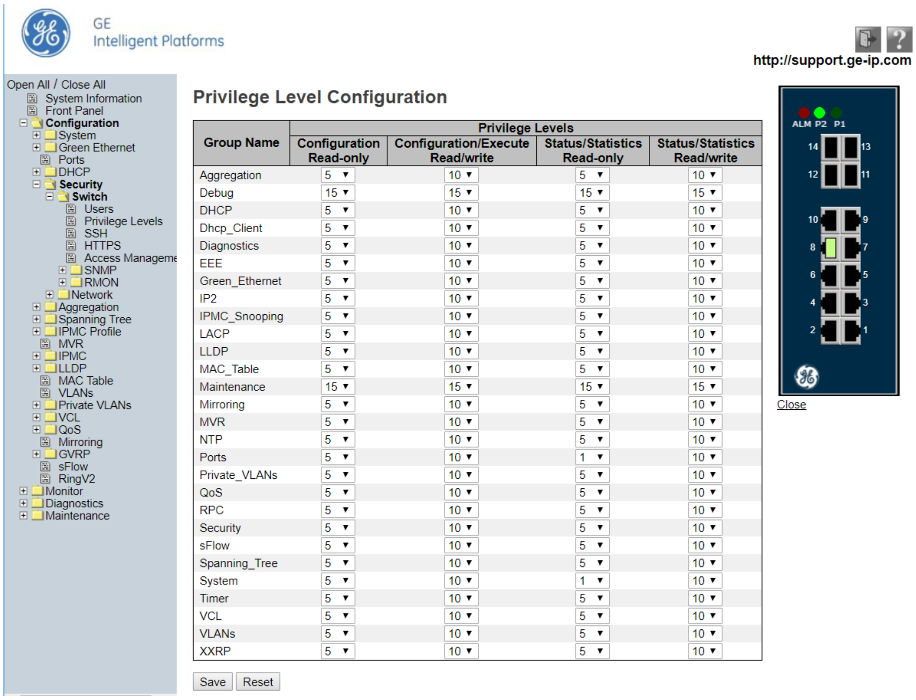
1. The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.



Users Configuration

User Name	Privilege Level
admin	15

2. Every group has an authorization Privilege level for the following subgroups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.



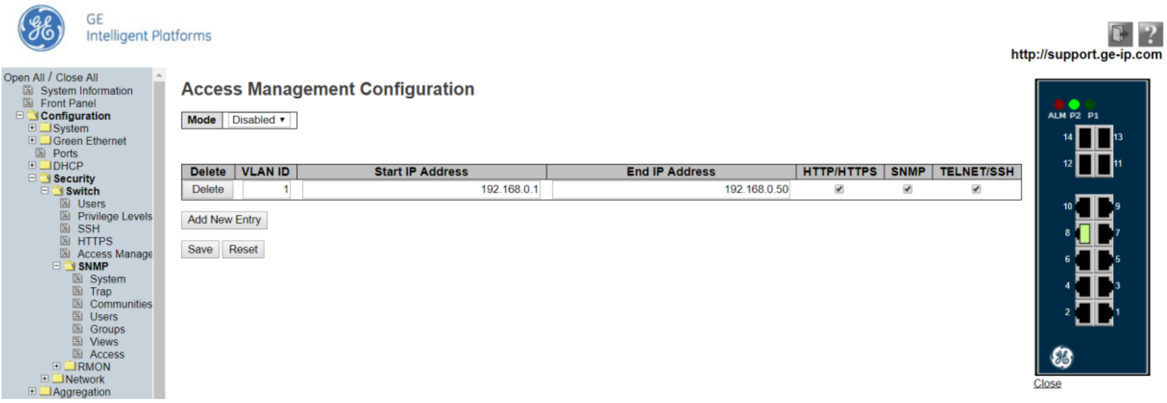
Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
Green_Ethernet	5	10	5	10
IP2	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RPC	5	10	5	10
Security	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
XXRP	5	10	5	10

4.6.2 Access Management Configuration

Configure access management table. Access Management indicates that the host can access the switch from indicated protocol interface if the host IP address matches the IP address range provided in the entry. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Protocol	Access Management
VLAN	Indicates the VLAN ID for the access management entry.
IP	Indicates the IP address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.



Access Management Configuration

Mode	Disabled ▾

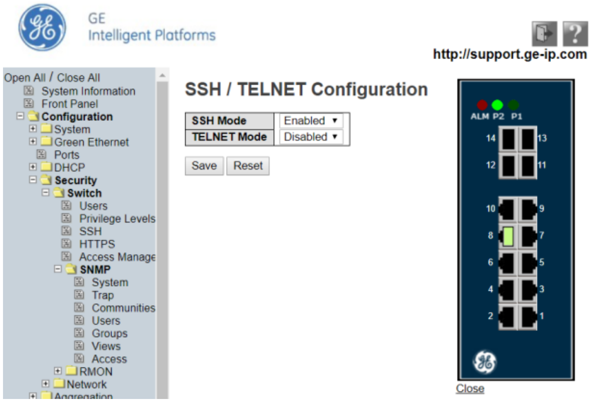
Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	192.168.0.1	192.168.0.50	☑	☑	☑

Add New Entry

Save Reset

4.6.3 SSH/TELNET/HTTPS/SNMP Configuration

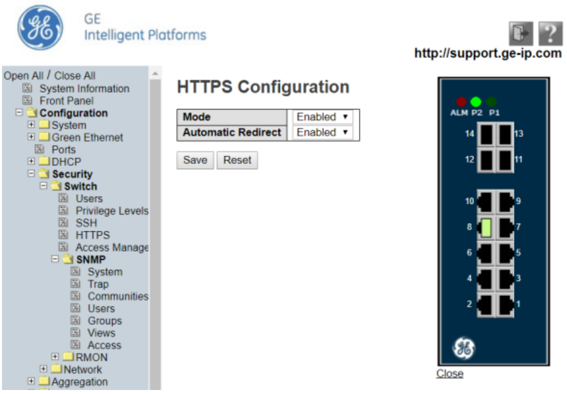
Protocol	Mode
SSH	Indicates the SSH mode operation. Possible modes are: Enabled/Disabled
TELNET	Indicates the TELNET mode operation. Possible modes are: Enabled/Disabled
HTTPS	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled/Disabled
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.



SSH / TELNET Configuration

SSH Mode	Enabled ▾
TELNET Mode	Disabled ▾

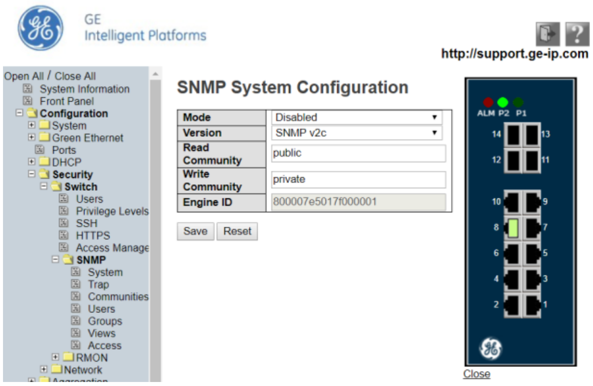
Save Reset



HTTPS Configuration

Mode	Enabled ▾
Automatic Redirect	Enabled ▾

Save Reset



SNMP System Configuration

Mode	Disabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

SNMP System Configuration:

1. Version : Indicates the SNMP supported version. Possible versions are
   SNMP v1: Set SNMP supported version 1.
   SNMP v2c: Set SNMP supported version 2c.
   SNMP v3: Set SNMP supported version 3.

2. Read Community:
   Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
   The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

3. Write Community :
   Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
   The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

4. Engine ID :
   Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

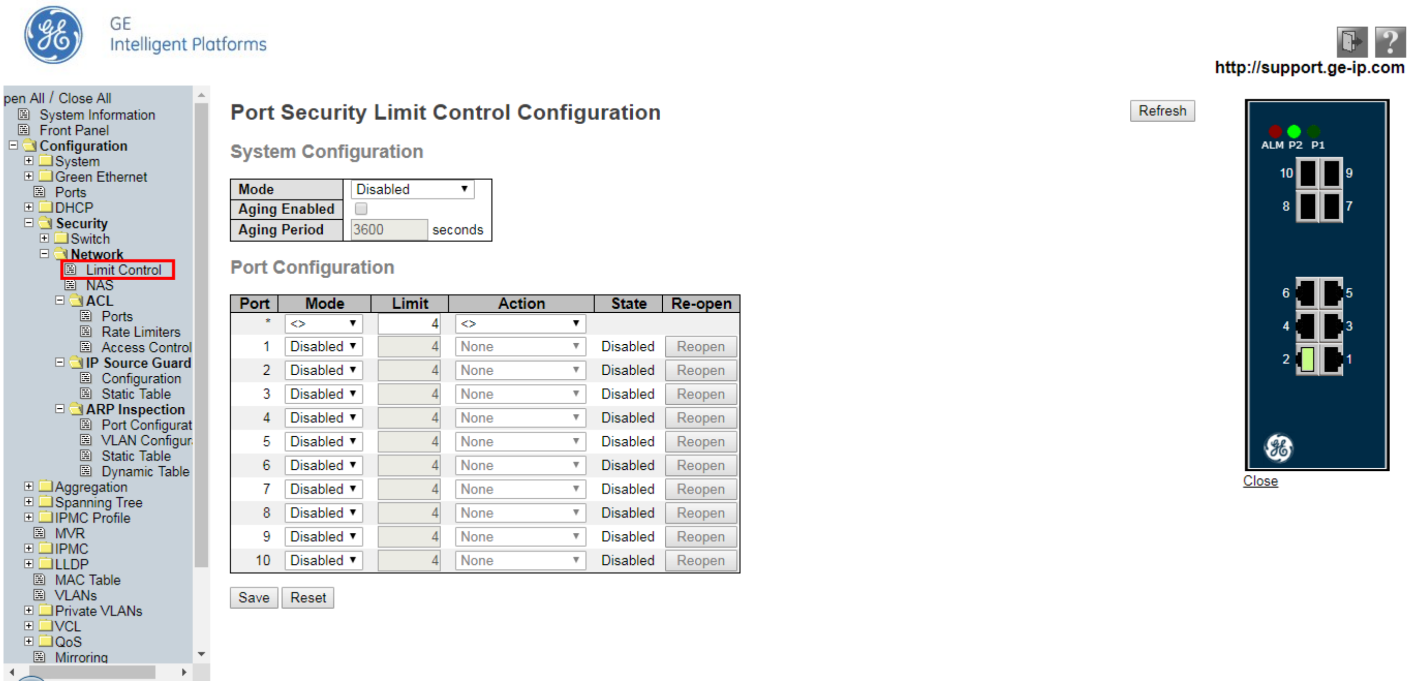
4.5 Limit Control

Limit Control allows for limiting the number of users on a given port. The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learn on the port.

If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

Four actions description

Action	Description
None	Do not allow more than Limit MAC addresses on the port, but take no further action.
Trap	If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
shutdown	If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button.
Trap & Shutdown	If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.



Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	□
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen

Save Reset

Port Security Limit Control Configuration – configure the Port Security Limit Control system and port settings

4. 8 Access Control List (ACL)

ACL is the list table of ACEs (Access Control Entry), containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

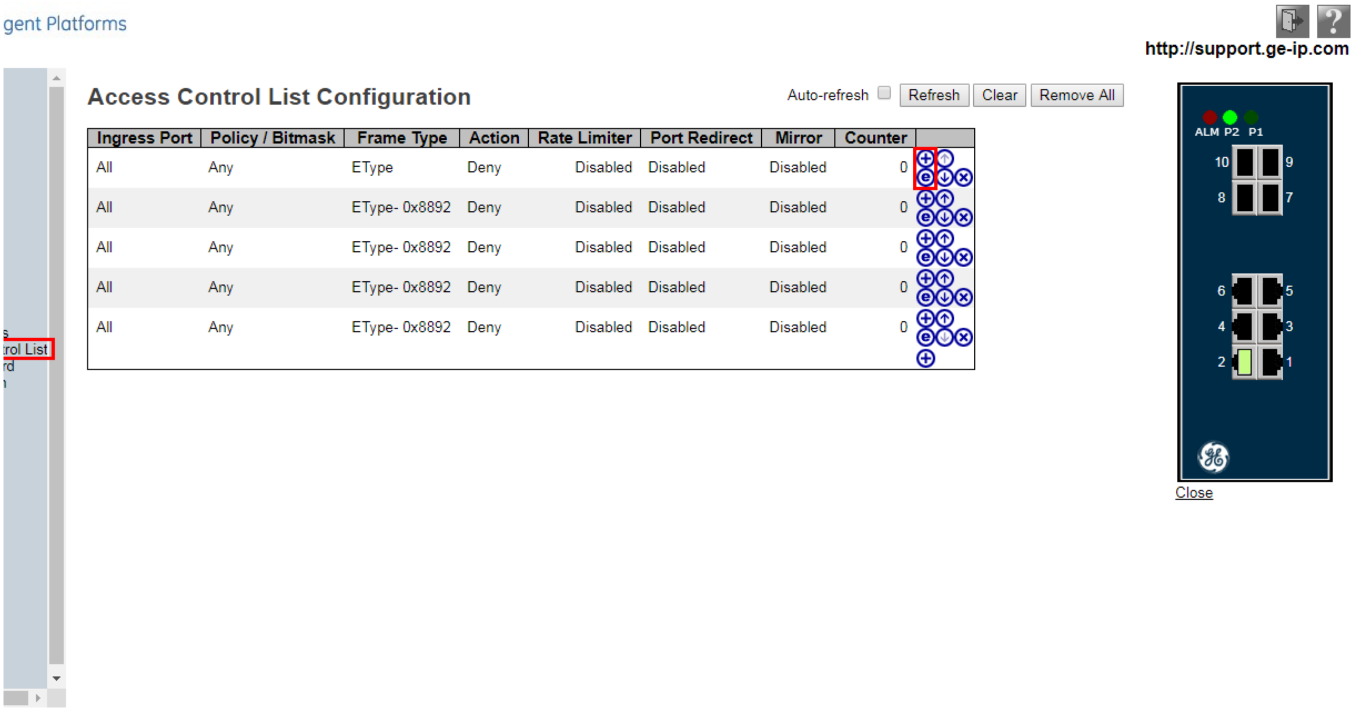
There are three associated with the manual ACL configuration:

- **Access Control List**
- **Ports**
- **Rate Limiters**

4.8.1 Access Control List

There are number of parameters that can be configured with an ACE. For example, if frame matching the ACE that you configure (like frame type, policy filter) then will do action (permit / deny / filter) and also can logging or shutdown the port.

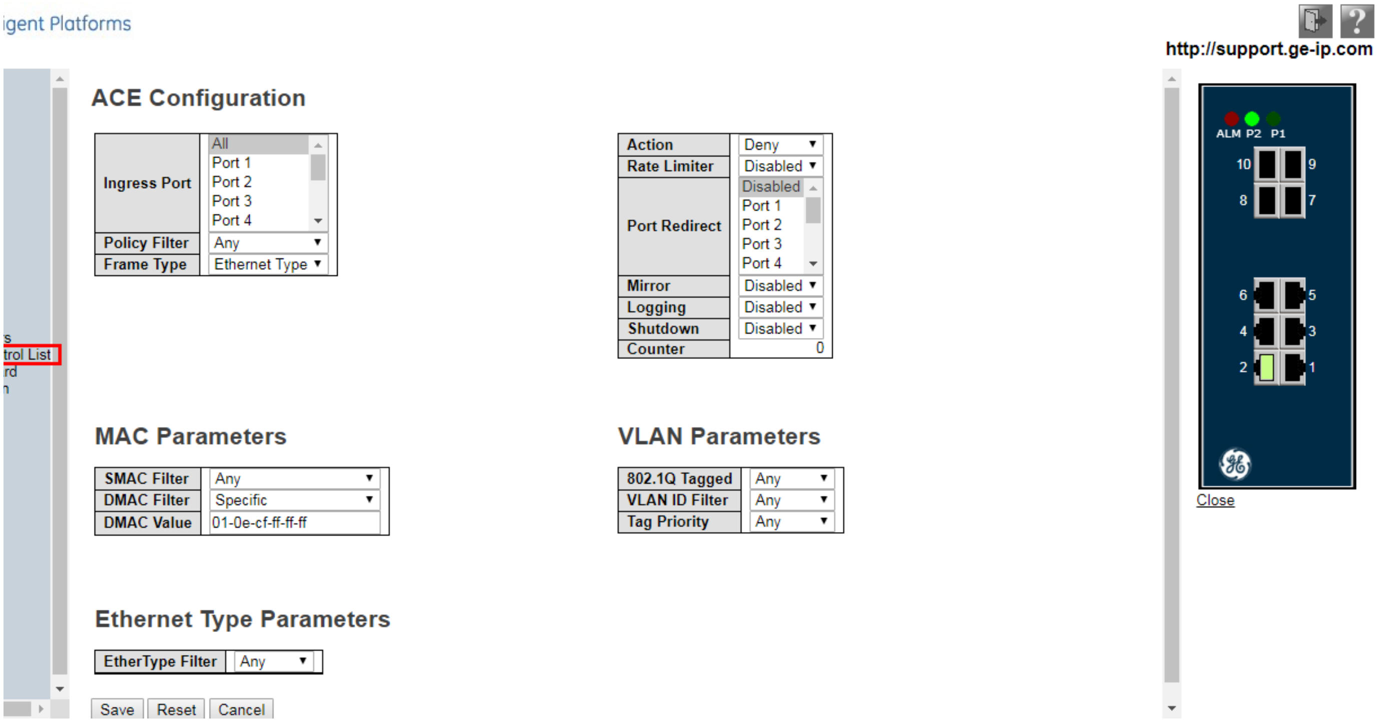
An ACE can be associated with a Policy, one ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" configuration.



Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter
All	Any	EType	Deny	Disabled	Disabled	Disabled	0
All	Any	EType- 0x8892	Deny	Disabled	Disabled	Disabled	0
All	Any	EType- 0x8892	Deny	Disabled	Disabled	Disabled	0
All	Any	EType- 0x8892	Deny	Disabled	Disabled	Disabled	0
All	Any	EType- 0x8892	Deny	Disabled	Disabled	Disabled	0

Access Control List Configuration – shows the ACEs in a prioritized way, highest (top) to lowest (bottom)



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Any
DMAC Filter	Specific
DMAC Value	01-0e-cf-ff-ff-ff

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

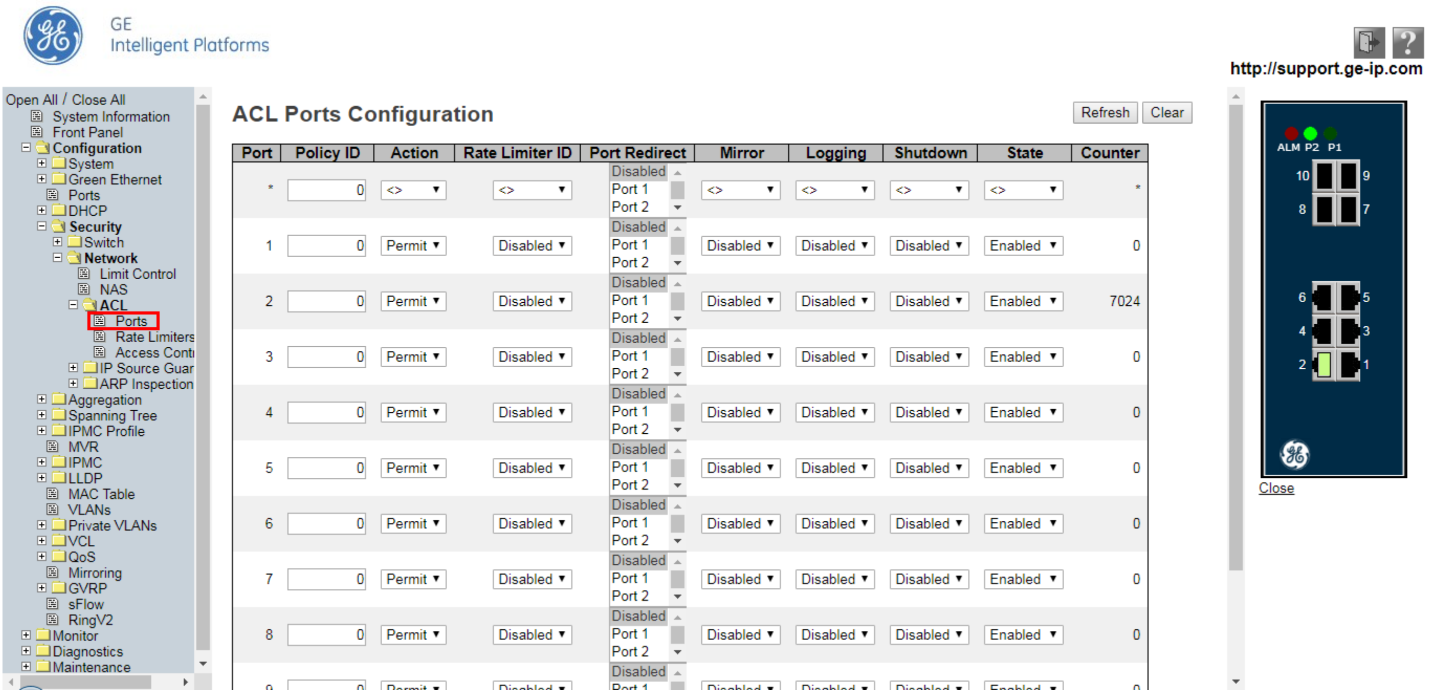
EtherType Filter	Any

Save Reset Cancel

ACE Configuration – An ACE consists of several parameters

4.8.2 Ports

1. The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" configuration. Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. ACL Ports configuration can also use to shutdown the nonuse port.

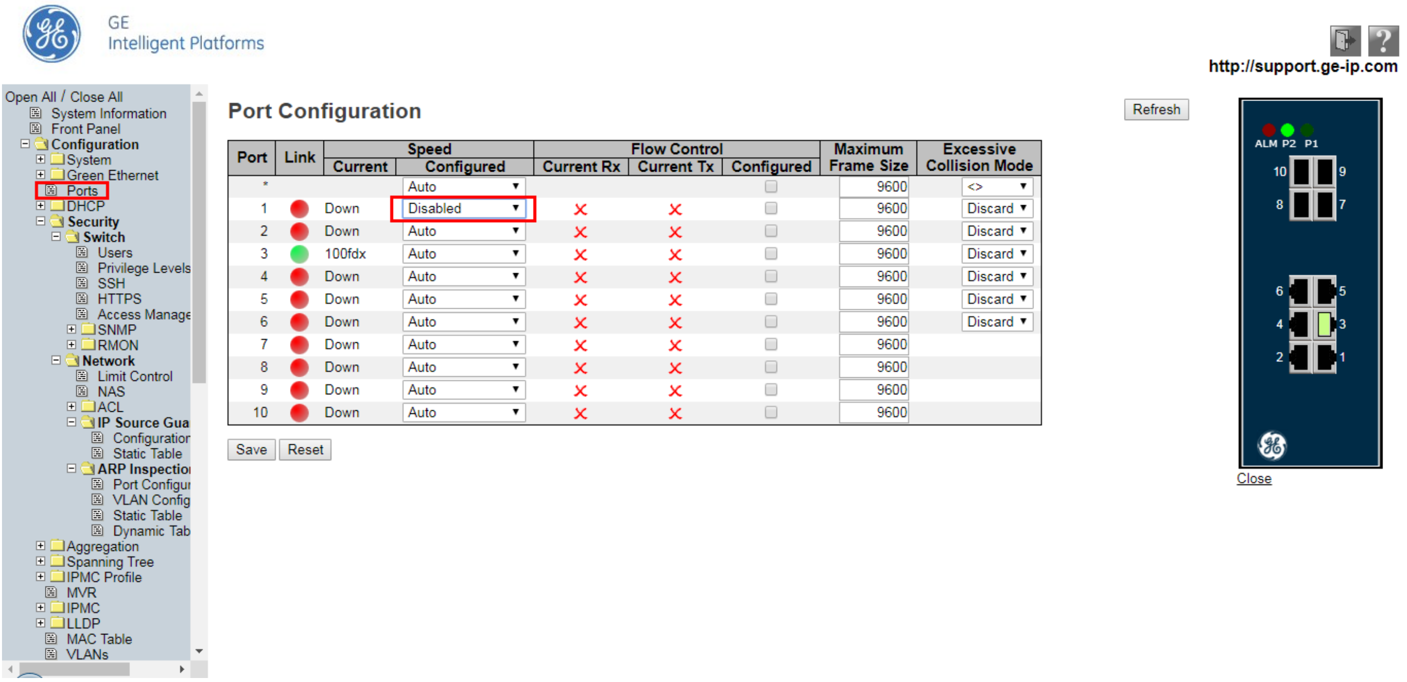


ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	7024
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1	Disabled	Disabled	Disabled	Enabled	0

ACL Ports Configuration – Configure the ACL parameters of each switch port

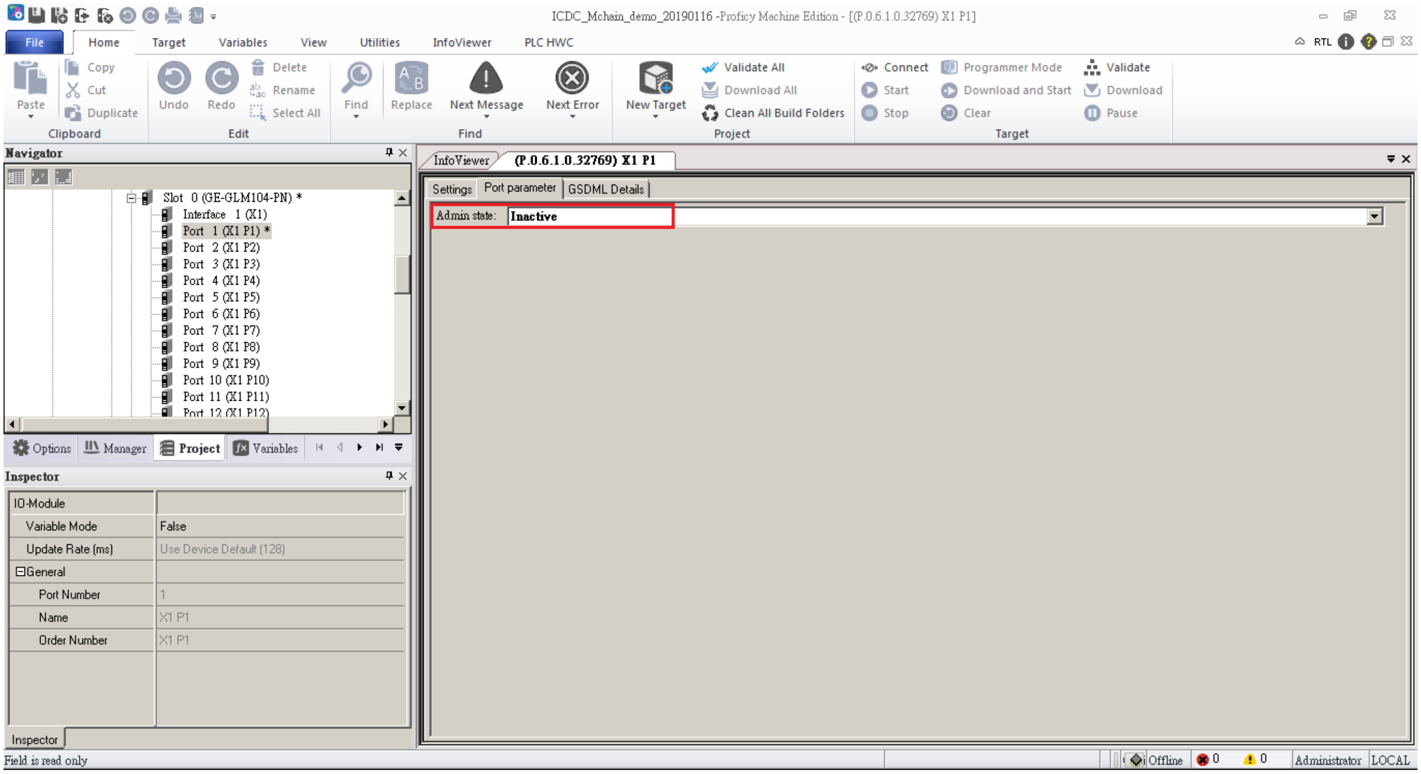
2. There are another method to denied to specific traffic objects, use port configuration or Proficy Machine Edition (PME) to shutdown the nonuse port :



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			Auto			□	9600	<>
1	🔴	Down	Disabled	✗	✗	□	9600	Discard
2	🔴	Down	Auto	✗	✗	□	9600	Discard
3	🟢	100fdx	Auto	✗	✗	□	9600	Discard
4	🔴	Down	Auto	✗	✗	□	9600	Discard
5	🔴	Down	Auto	✗	✗	□	9600	Discard
6	🔴	Down	Auto	✗	✗	□	9600	Discard
7	🔴	Down	Auto	✗	✗	□	9600	
8	🔴	Down	Auto	✗	✗	□	9600	
9	🔴	Down	Auto	✗	✗	□	9600	
10	🔴	Down	Auto	✗	✗	□	9600	

Port Configuration – Speed configured set “disabled” to shutdown nonuse port



Admin state: Inactive

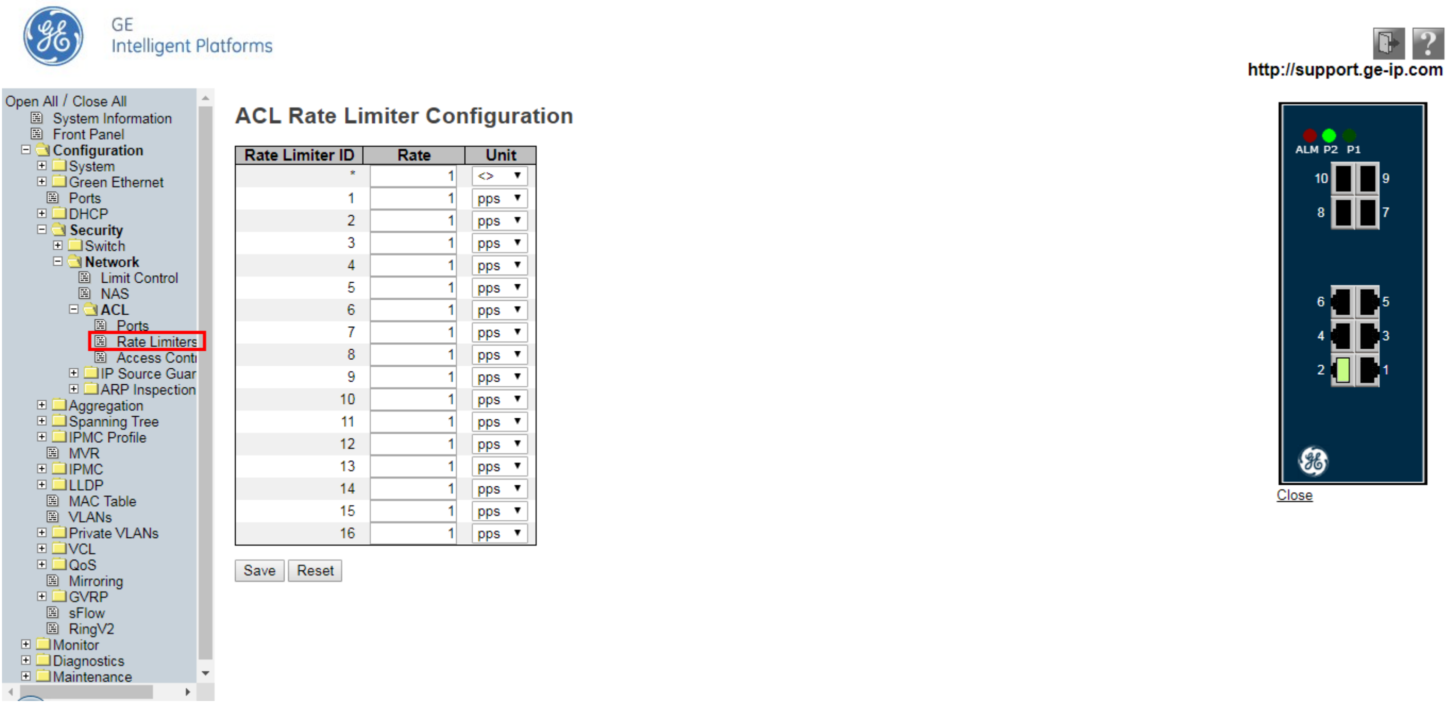
IO-Module	
Variable Mode	False
Update Rate (ms)	Use Device Default (128)
⊟General	
Port Number	1
Name	X1 P1
Order Number	X1 P1

Proficy Machine Edition (PME) – Admin state set "Inactive" to shutdown nonuse port

4.8.3 Rate Limiters

Configure the rate limiter for the ACL of the switch.

There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" configuration can assign a Rate Limiter ID to the ACE(s) or ingress port(s).



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

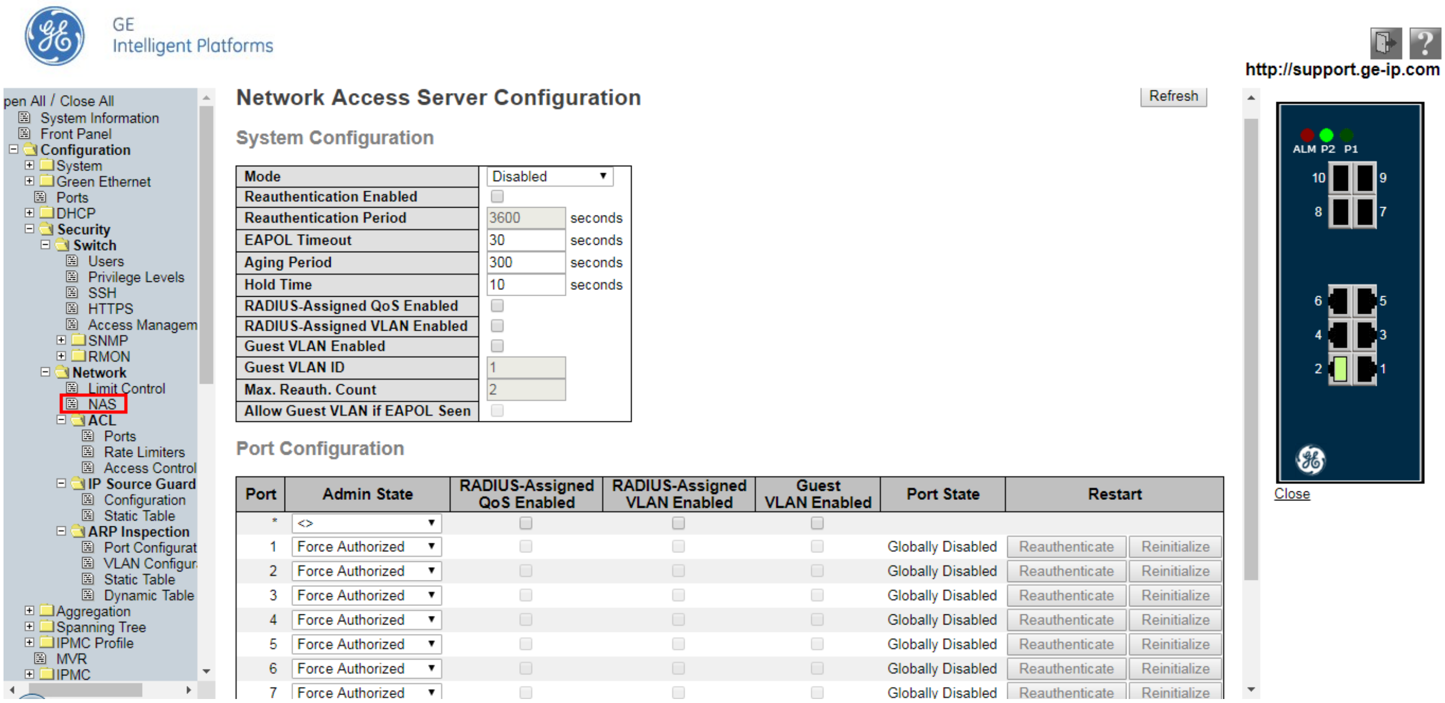
ACL Rate Limiter Configuration – configure the rate limiters

4.9 Network Access Server (NAS)

The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource.

NAS allows to configure the IEEE 802.1X and MAC-based authentication system and port settings.

- **IEEE 802.1X** – defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.
- **MAC-based authentication** – allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Network Access Server Configuration – configuration consists of two sections, a system- and a port-wide

4.10 IP Source Guard

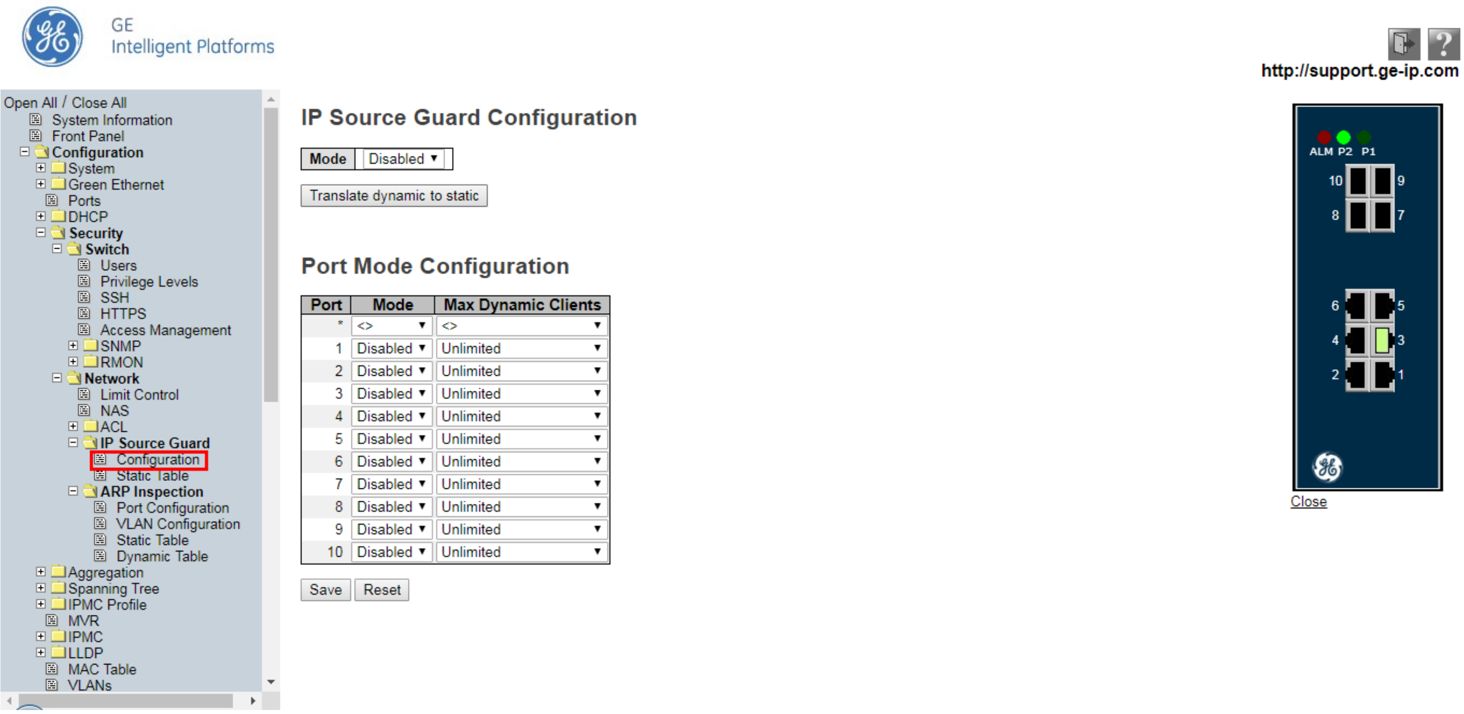
IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings.

It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

4.10.1 Configuration

The IP Source Guard configuration consists of two sections, a system- and a port-wide:

- **Mode of IP Source Guard Configuration** – Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled
- **Port Mode Configuration** – Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.



IP Source Guard Configuration

Mode	Disabled

Translate dynamic to static

Port Mode Configuration

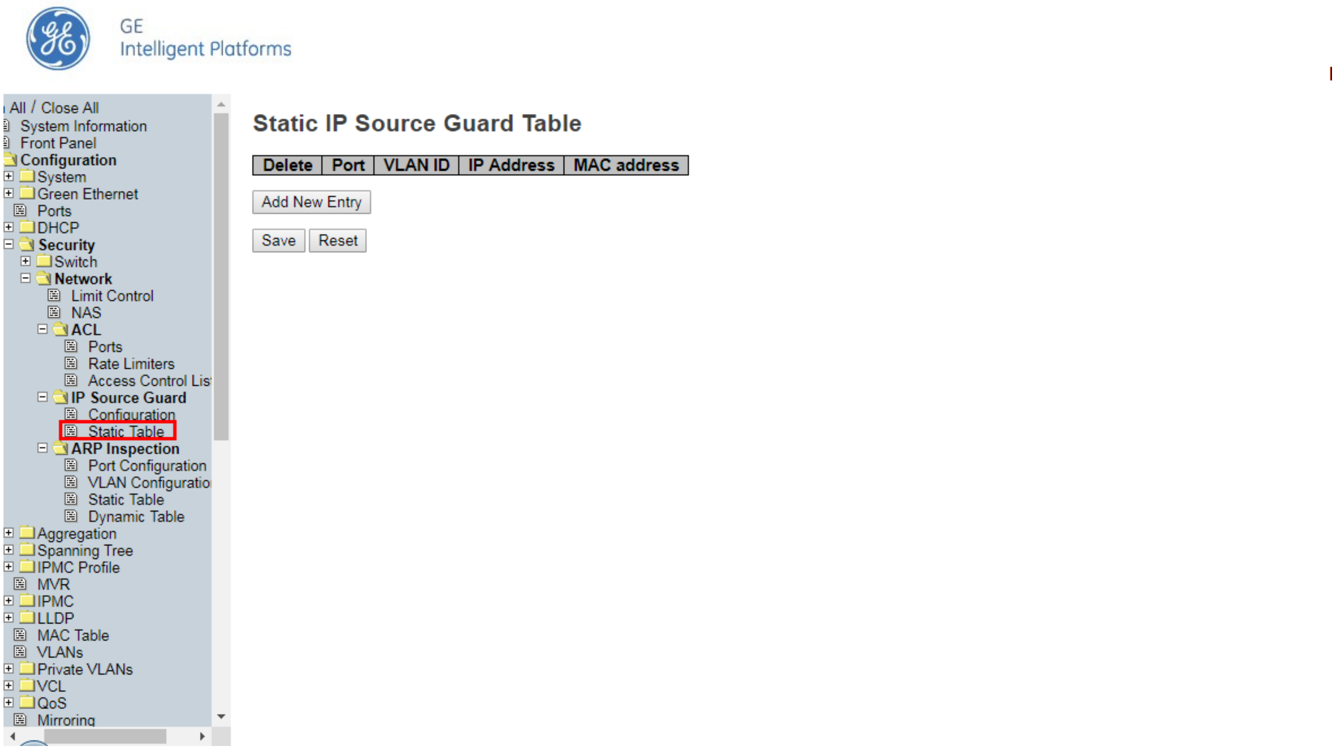
Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited

Save Reset

IP Source Guard Configuration – configuration consists of two sections, a system- and a port-wide

4.10.2 Static Table

Creates a static IP source entry for the current interface.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address

Add New Entry

Save Reset

Static IP Source Guard Table – Creates a static IP source entry for the current interface.

4.11 ARP Inspection

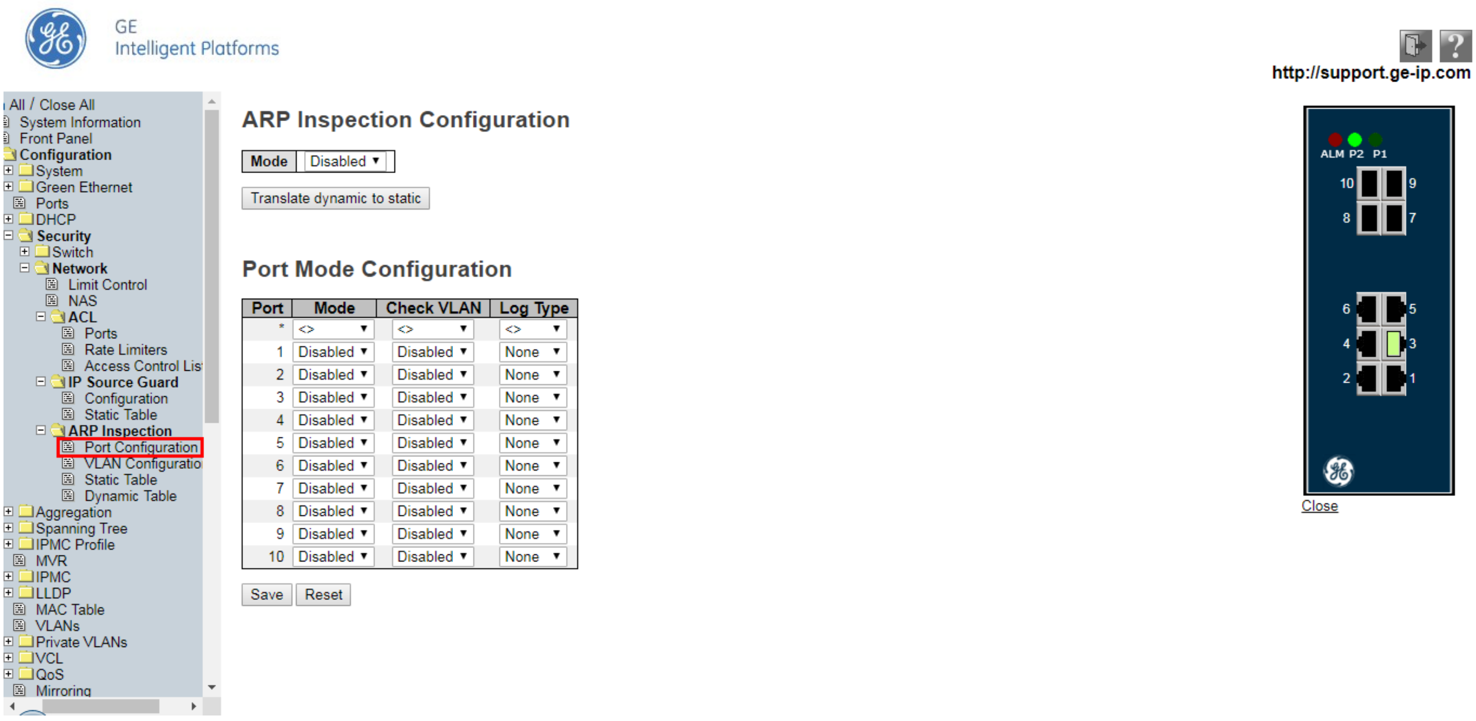
ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches.

This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

4.11.1 ARP Inspection Configuration

The ARP inspection configuration consists of two sections, a system- and a port-wide:

- **Mode of ARP Inspection Configuration** – Enable the Global ARP Inspection or disable the Global ARP Inspection
- **Port Mode Configuration** – Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port



ARP Inspection Configuration

Mode	Disabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<> ▾	<> ▾	<> ▾
1	Disabled ▾	Disabled ▾	None ▾
2	Disabled ▾	Disabled ▾	None ▾
3	Disabled ▾	Disabled ▾	None ▾
4	Disabled ▾	Disabled ▾	None ▾
5	Disabled ▾	Disabled ▾	None ▾
6	Disabled ▾	Disabled ▾	None ▾
7	Disabled ▾	Disabled ▾	None ▾
8	Disabled ▾	Disabled ▾	None ▾
9	Disabled ▾	Disabled ▾	None ▾
10	Disabled ▾	Disabled ▾	None ▾

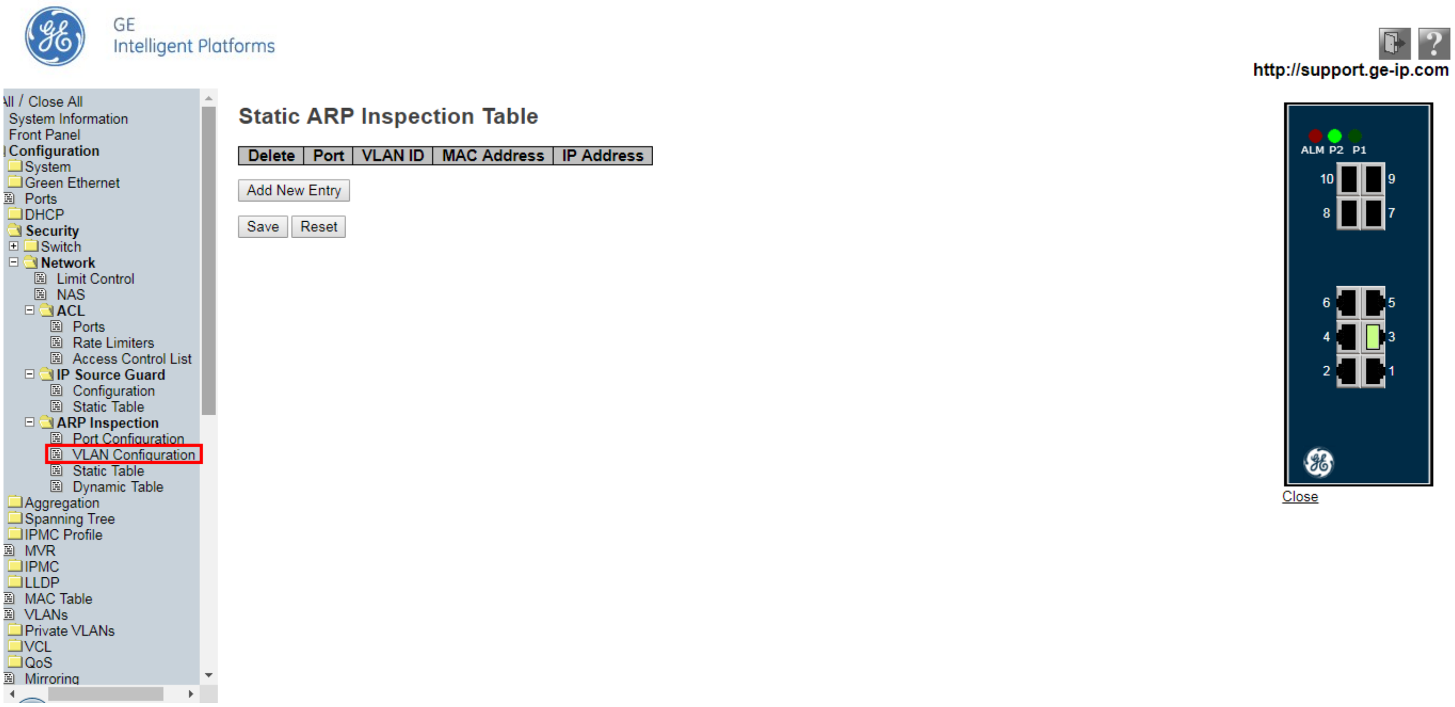
Save Reset

ARP Inspection Configuration – configuration consists of two sections, a system- and a port-wide

4.11.2 VLAN Configuration

Specify ARP Inspection is enabled on which VLANs.

1. You have to enable the port setting on Port mode configuration. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.
2. You can specify which VLAN will be inspected on VLAN mode configuration. The log type also can be configured on per VLAN setting.



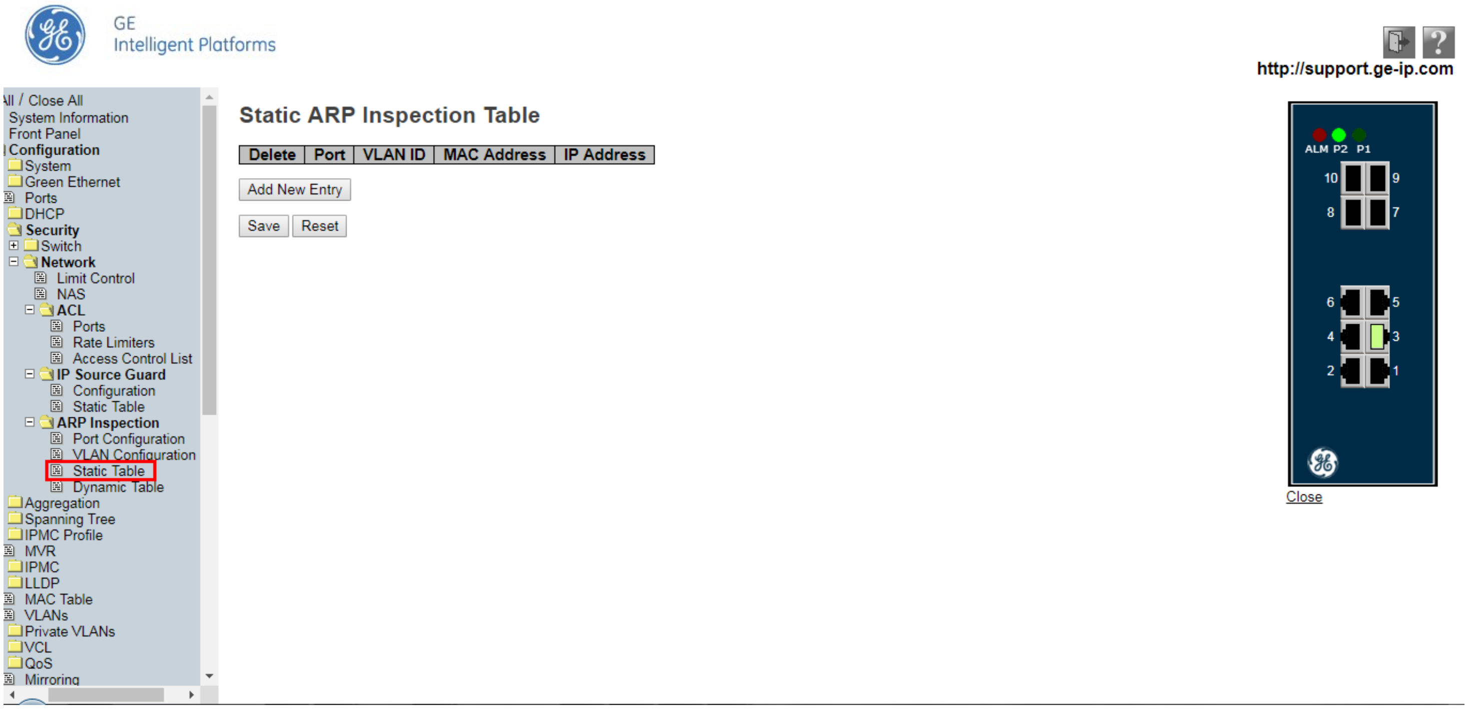
Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address

VLAN Mode Configuration – Specify ARP Inspection is enabled on which VLANs

4.11.3 Static Table

Creates a static ARP entry.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address

Static ARP Inspection Table – Creates a static ARP entry.

Chapter 5 Configuration Hardening

This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of the PACSystems and PROFINET products that are present in a particular installation. Configuration Hardening should be considered in addition to enabling and using security features such as Authentication, Access Control and Authorization.

GE recommends disabling, on each PACSystems and PROFINET product, all ports, services and protocols that aren't required for the intended application.

5.1 Ethernet Interface

This section provides information to use when hardening the configuration of a GLM Switch Ethernet Interface. These settings should be considered when configuring any GLM Switch Ethernet Interface.

The Ethernet Interface can be configured to disable a number of services. The table below lists those services and indicates the configuration value that will disable each. Note that some of these settings will not entirely close the TCP/UDP port, but they will still reduce the attack surface.

5.1.1 Disabling Ethernet Services

Service	Parameter name	Value
Telnet	Telnet terminal service	Disabled
SSH	Secure Shell	Disabled
IP Routing	Gateway IP Address	0.0.0.0
SNMP	Simple Network Management Protocol	Disabled
SNTP Client	Network Time Sync	None
Web Server	WEB Service	HTTPs is Enabled HTTP is Disabled

These settings are default factory configuration in GLM Switches. Please don't enable it. For more information on these parameters, refer to the *GLM Switches User Manual,* GFK-3030.

Chapter 6 Network Architecture and Secure Deployment

This section provides security recommendations for deploying PACSystems PROFINET Managed Ethernet Switches and PROFINET devices in the context of a larger network.

6.1 Reference Architecture

The following figure shows a reference deployment of GE's Automation & Control components using the logical segmentation of the Purdue Enterprise Reference Architecture, otherwise known as the Purdue Model.

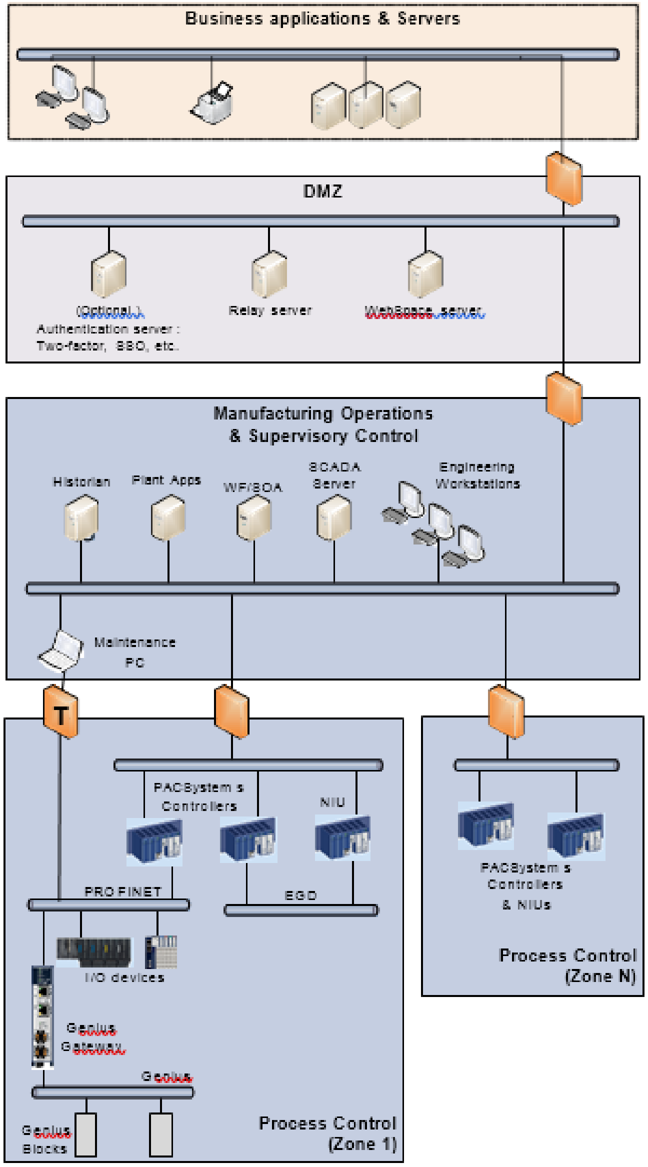


Figure 1: PACSystems Deployed in Purdue Model

The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet using a Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks.

6.2 Remote Access and Demilitarized Zones (DMZ)

A DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

If direct communication to a control network is required from the business network or from the internet, carefully control, limit and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN) and even then, restrict the allowed protocols/ports to just the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

6.3 Access to Process Control Networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. For example, since Proficy Machine Edition uses SRTP to download the application to the PACSystems controllers and NIUs, then SRTP traffic must be allowed through the firewall. However, if a particular protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. If, in addition to that, a controller has no other need for that protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol itself.

Note: Network Address Translation (NAT) firewalls typically do not expose all of the devices on the trusted side of the firewall to devices on the untrusted side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the trusted side of the firewall to a different IP address/port on the untrusted side of the firewall. Since communication to PACSystems controllers will typically be initiated from a computer on the untrusted side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

6.4 Access to PROFINET Networks

Commissioning and maintaining the devices on the PROFINET network requires the ability to communicate from a computer to the devices on that network. For example, if a PROFINET device fails and needs to be replaced, the replacement device will need to be assigned a name. As described in Section 0,

Functionality		Required Application Protocols	Example Servers
Ethernet	SRTP Channels	N/A	N/A
	Modbus TCP Channels	N/A	N/A
	EGD Production	N/A	N/A
	Send EGD Commands	N/A	N/A

	Ethernet Station Manager	N/A	N/A
	Time Synchronization	SNTP	SNTP server
	Assign IP addresses using a centralized database of addresses	BOOTP	BOOTP server
	Lookup IP addresses by Name	N/A	N/A
	IEC 61850 Client	N/A	N/A

PROFINET, this is done using the PROFINET DCP protocol. However, to help ensure that the Maintenance computer cannot be used to launch attacks on the devices using other protocols, the firewall it connects through should block all protocols that are not needed for performing the maintenance functions.

Note: Since the PROFINET DCP protocol is not routable, the firewall used will most likely need to be configured so it operates in *Transparent* mode (This is noted by the use of a “T” on the firewall in the Reference Architecture diagram.). This will allow the Maintenance computer to be part of the same subnet as the PROFINET devices, as required by the PROFINET DCP protocol.

6.5 Hot Standby CPU Redundancy with PROFINET I/O

Hot Standby CPU Redundancy allows a critical application or process to continue operating if a failure occurs in any single component. A Hot Standby system employs two CPUs:

- an Active unit that is actively controlling the process at a given moment, and
- a Backup unit that is synchronized with the Active unit and can take over the process in a bumpless fashion, should that become necessary.

The two units are synchronized when both are in Run Mode, the Backup unit has received the latest status and synchronization information from the Active unit via a redundancy link, and both are running their logic solutions in parallel.

Chapter 7 Other Considerations

7.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected PACSystems product be temporarily taken out of service.

If temporarily taking a controller out of service in order to apply security fixes is expected to cause an unacceptable disruption to the system's availability, then consider designing the control system to use redundancy. PACSystems supports Hot-Standby CPU Redundancy which will allow many, if not all, security fixes to be applied to the redundant controllers while continuing to control the process.

Finally, some installations require extensive qualification be performed before changes are deployed to the production environment. While this requirement is independent of security, ensuring the ability to promptly apply security fixes while minimizing downtime may drive the need for additional infrastructure to help with this qualification.

7.2 Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the PROFINET I/O, Ethernet Global Data, and Reliable Datagram Service protocols are generally expected to operate with small, known, worst-case bounds on their communications latency and jitter. As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

7.3 GLM Series Compensating Controls

7.3.1 Network Bandwidth Limiting

The RX7i Ethernet interfaces (i.e. the IC698ETM001 module and RX7i CPU Ethernet daughterboards) are not capable of sustaining Ethernet communications above a speed of 10 Mbps, or 10% of each 100 Mbps connection. Above this threshold, ARP, IMCP, UDP, and TCP services may become unavailable. Care must be taken to design and implement the network to prevent excessive traffic to RX7i Ethernet interfaces.

In order to reduce the likelihood of intentional or accidental network flooding that could cause a loss of availability in RX7i Ethernet interfaces, GE strongly encourages following the relevant recommendations in Section 4.2.5. To further mitigate the loss of availability for a particularly critical asset, a switch or firewall configured for ingress and egress rate-limiting can be placed directly between the RX7i module and the rest of the network. In the event of a network storm, the switch or firewall will selectively drop traffic to limit the rate of traffic that reaches a given RX7i module.

7.4 Additional Guidance

7.4.1 Protocol-specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document. This includes, but is not limited to the following document:

- PROFINET Security Guideline (TC3-04-0004a) by PROFIBUS INTERNATIONAL

7.4.2 OPC UA Server

When running an OPC UA Server with a *Limited Communications Window*, the server can process enough requests to use the entire window, which will add that time to your PLC Logic sweep. For example, a 100 ms *Limited Backplane Communications Window* could add the full 100 ms to your PLC Logic Sweep. Caution should be taken to ensure the Communication Window is configured within the tolerances of the system.

7.4.3 PROFINET Controller Duplicate IP

The duplicate IP address handling for the RX3i PROFINET Controller (IC695PNC001 firmware revision 2.26 and above) and the Embedded PROFINET Controller on the RX3i CPE330, CPE400 and RSTi-EP CPE100 behaves as follows:

In each case, the system has an active PROFINET network with a PROFINET Controller connected to at least one PROFINET Device.

1. If a second PROFINET Controller with an identical IP address to the active PROFINET Controller is added to the network, the second Controller will not enter the network and will log a fault to indicate *Duplicate IP Detected*. The first Controller will maintain all device connections.
2. If a device with an identical IP address to an active PROFINET Controller is added to the network, the Controller will log a *Duplicate IP Detected* fault and maintain all device connections.
3. If a device with an identical IP address to an active PROFINET Device is added to the network, the Controller will log a *Duplicate IP Detected* fault and maintain all device connections.

7.4.4 MRP Ring Ethernet Traffic Storm Prevention

The RX3i CPE330, CPE400 and RSTi-EP CPE100 LAN 2 and the RX3i PNC001 can all be configured as an MRP Ring Manager (MRM). However, none of these defaults to be an MRM.

To prevent an Ethernet Traffic Storm, the physical ring must not be completely connected until the MRM configuration is stored to an Ethernet node on the ring. Failure to have an active MRM configured in an Ethernet ring configuration will result in an Ethernet Traffic Storm caused by the ring's network loop topology. An Ethernet Traffic Storm will prevent communication to all Ethernet nodes connected to the ring until the ring is physically broken or an MRM is configured.

Before clearing and power cycling the configuration of a CPE330 that is configured as an MRM in a ring topology, it is recommended that either (a) the ring be broken by physically disconnecting an Ethernet port on any network node in the ring, or (b) some other network node in the ring be configured as a MRM.

In order to prevent storms in a ring where a PROFINET Controller is configured as an MRM, the controller will maintain that functionality even after a clear and power cycle, and will continue to do so until a different configuration is stored to that controller, providing the new configuration prevents the controller from operating as an MRM. It is still recommended that the ring be broken by physically disconnecting an Ethernet port on any network node in the ring until a single MRM is configured for the ring.

7.4.5 Government Agencies and Standards Organizations

Government agencies and international standards organizations may provide guidance on creating and maintaining a robust security program, including how to securely deploy and use Industrial Control Systems. For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and on

Recommended Practices for cybersecurity with Industrial Control Systems. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing & operating a cyber-security program, including recommended technologies for industrial automation and control systems. Such documentation, when appropriate, should be considered in addition to this document.

GE Automation and Controls
Information Centers

Headquarters:
1-800-433-2682 or 1-434-978-5100
Global regional phone numbers
are available on our web site
www.geautomation.com

Additional Resources

For more information, please visit our web site:

www.geautomation.com