

IEF-G9010 Series User Manual

Version 1.2, February 2022

www.moxa.com/product

MOXA®

© 2022 Moxa Inc. All rights reserved.

IEF-G9010 Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2022 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About the IEF-G9010 Series	6
Introduction	6
Main Functions	7
2. Getting Started	8
Getting Started Task List	8
Opening the Management Console	9
Changing the Administrator's Password	10
3. The System Screens.....	11
Device Information	11
Secured Service Status.....	11
System Resources	12
WAN Interface Summary	12
LAN Interface Summary	12
Throughput/Connection	12
4. The Visibility Screens.....	13
Enabling Active Query	13
Viewing Asset Information	14
Viewing Real-time Network Application Traffic	15
5. The Network Screens.....	16
Port Settings	16
Configuring Port Settings.....	16
Port Mapping.....	17
Network Interface.....	17
Configuring the LAN Network Interface	18
Configuring the DMZ Network Interface.....	19
Configuring the WAN Network Interface	21
Device Operation Modes	23
Selecting the Operation Mode	24
6. The NAT Screens.....	27
NAT Rules.....	27
Configuring 1-to-1 NAT Rules.....	27
Configuring Multi 1-to-1 NAT Rules.....	28
Configuring Port Forwarding	29
Application-layer Gateways (ALG).....	30
Configuring ALG Settings.....	31
7. The Routing Screens.....	32
Static Routes.....	32
Configuring Static Routes	32
8. The Object Profiles Screens	34
Configuring IP Object Profiles	34
Configuring Service Object Profiles.....	35
Configuring Protocol Filter Profiles.....	36
Enabling the Drop Malformed Option for an ICS Protocol	39
Advanced Settings for the Modbus Protocol.....	39
Advanced Settings for the CIP Protocol	42
Advanced Settings for S7Comm	45
Advanced Settings for S7Comm Plus.....	49
Advanced Settings for SLMP	52
Advanced Settings for MELSOFT.....	55
Advanced Settings for TOYOPUC	58
Configuring IPS Profiles.....	61
9. The Security Screens	64
Cybersecurity.....	64
Configuring Cybersecurity – Denial of Service Prevention	64
Policy Enforcement	65
Configuring Policy Enforcement	65
Adding Policy Enforcement Rules (For Gateway Mode Only)	65
Adding Policy Enforcement Rules (For Bridge Mode Only)	67

Managing Policy Enforcement Rules	70
10. The Pattern Screens	71
Viewing Device Pattern Information	71
Manually Updating the Pattern.....	71
11. The Log Screens	72
Viewing Cybersecurity Logs.....	72
Viewing Policy Enforcement Logs	73
Viewing Protocol Filter Logs.....	74
Viewing Asset Detection Logs	74
Viewing System Logs	75
12. The Administration Screens	76
Account Management	76
Built-in User Accounts.....	77
Adding a User Account	77
Changing Your Account Password	77
Configuring Password Policy Settings.....	79
System Management.....	80
Configuring the Device Name and Device Location Information	80
Configuring the Management Client Access Control List.....	80
Configuring Management Protocols and Ports.....	81
The Sync Setting Screen.....	81
Enabling SDC Management.....	81
The Syslog Screen	82
Configuring Syslog Settings	82
Syslog Severity Levels	83
Syslog Severity Level Mapping Table.....	83
The System Time Screen	84
Configuring System Time	84
The Back Up/Restore Screen	85
Backing Up a Configuration.....	85
Restoring a Configuration	85
The Firmware Management Screen	86
Viewing Device Firmware Information	86
Updating the Firmware.....	86
Rebooting and Applying Firmware	87
The Reboot System Screen	87
Rebooting the System.....	87
13. Supported USB Devices.....	88
Loading Pattern Files.....	88

Terms and Acronyms

The following table lists the terms and acronyms used in this document.

Term/Acronym	Definition
ALG	Application Layer Gateway
CEF	Comment Event Format
CIDR	Classless Inter-Domain Routing
DPI	Deep Packet Inspection
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Information Technology
NAT	Network Address Translation
SDC	Security Dashboard Console
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition

1. About the IEF-G9010 Series

Introduction

The IEF-G9010 Series next generation firewalls are a highly integrated industrial multiport firewall with NAT and IPS functions. They are designed for Ethernet-based security applications in factory networks and provide an electronic security perimeter to protect critical cyber assets such as pump-and-treat systems in water stations, DCS systems in oil and gas applications, and PLC/SCADA systems in factory automation. The firewall's web-based console provides an intuitive graphical user interface for device configuration and security policy settings. The IEF-G9010 Series protects your individual assets with OT visibility, cybersecurity, and OT protocol whitelisting.

Traditionally, IT and OT operate on separate networks, each with their own transportation team, goals, and needs. In addition, industrial environments are equipped with tools and devices that are traditionally unable to interface with a corporate network, thus making provisioning security updates or patches in a timely manner difficult. Therefore, the demand for security products that provide comprehensive asset protection and visibility are on the rise.

Moxa's Industrial Network Defense Solutions provide a wide range of security products that cover both the IT and OT layers. These easy-to-build solutions provide active and immediate protection to the Industrial Control System (ICS) environments with the following features:

- Certified industrial-grade hardware that complies with the size, power consumption, and durability requirements for OT environments and can tolerate a wide range of temperature variations
- Threat detection and interception against the spread of worms
- Intrusion Prevention System and Denial-of-Service (DoS) protection against attacks that target vulnerable legacy devices
- Virtual patch protection against OT device exploits

Main Functions

The IEF-G9010 Series is a transparent network security device. Below are the main functions of the product:

Extensive Support for Industrial Protocols

The IEF-G9010 Series supports the identification of a wide range of industrial control protocols, including Modbus and other protocols used by industry leaders such as Siemens, Mitsubishi, Schneider Electric, ABB, Rockwell, Omron, and Emerson. In addition to allowing OT and IT security system administrators to work together, this feature also enables the flexibility to deploy defense measures in appropriate network segments and seamlessly connects them to existing factory networks.

Policy Enforcement for Mission-critical Machines

The IEF-G9010 Series' core technology allows administrators to maintain a policy enforcement database. By analyzing Layer 3 to Layer 7 network traffic between mission-critical production machines, policy enforcement filters control commands of specific protocols and blocks traffic that is not defined in the policy rules. This feature can help prevent unexpected operations, block unknown network attacks, and block other traffic that matches the policy for sending data to these mission-critical machines.

Improve Shadow OT Visibility by Integrating IT and OT Networks

The IEF-G9010 Series integrates and coordinates your IT and OT networks with each other and grants visibility of your shadow OT environment.

Intrusion Prevention and Intrusion Detection

IPS/IDS provides a powerful, up-to-date, first line of defense against known threats. Vulnerability filtering rules provide effective protection against all potential exploits at the network level. Manufacturing personnel manage patching and updating, providing pre-emptive protection against critical production failures, and additional protection for old or terminated software.

Switch Between Two Flexible Modes, 'Monitor' & 'Prevention'

The IEF-G9010 Series can easily switch between the 'Monitor' and 'Prevention' modes. The 'Monitor' mode will log traffic without interfering, while 'Prevention' mode will filter traffic based on policies you create. These modes work together to preserve your productivity while maximizing security.

Top Threat Intelligence and Analytics

The IEF-G9010 Series provides advanced protection against unknown threats with its up-to-date threat information.

Centralized Management

Security Dashboard Console (SDC) provides a graphical user interface for policy management in compliance with a manufacturing SOP. It centrally monitors operational information, edits network protection policies, and sets patterns for attack behaviors.

The following protections are deployed throughout the entire information technology (IT) and operational technology (OT) infrastructure. These include:

- A centralized policy deployment and reporting system
- Full visibility into assets, operations, and security threats
- IPS and policy enforcement configurations can be assigned per device group, allowing all devices in the same device group to share the same policy configuration
- Management permissions for device groups can be assigned per user account

Flexible Segmentation and Isolation

The IEF-G9010 Series is the ideal solution to segment a network into easily manageable security zones. The firewall can isolate connectivity between the different facilities and production zones to increase security against outside attacks and to create highly secure isolated network zones that can contain threats if they occur.

2. Getting Started

This chapter describes the IEF-G9010 Series and how to get started with configuring the initial settings.

Getting Started Task List

This task list provides a high-level overview of all procedures required to get the IEF-G9010-2MGSFP Series up and running as quickly as possible. Each step links to more detailed instructions later in the document.

Steps Overview:

1. Open the management console.
For more information, see [Opening the Management Console..](#)
2. Change the administrator password.
For more information, see [Changing the Administrator's Password.](#)
3. Configure the link speed of the Ethernet ports to suit the network environment.
For more information, see [Configuring Port Settings.](#)
4. Change the default web interface IP address.
The default IP address is **192.168.127.254** and is bound to the **LAN1** port.
For more information, see [Configuring the LAN Network Interface.](#)
5. Configure the network interface.
For more information, see [The Network Screens.](#)
6. Configure the system time.
For more information, see [Configuring System Time.](#)
7. (Optional) Configure the Syslog settings.
For more information, see [Configuring Syslog Settings.](#)
8. Configure Object Profiles.
For more information, see [The Object Profiles Screens.](#)
9. Configure security policies.
For more information, see [The Security Screens.](#)
10. Configure the device name and device location information.
For more information, see [Configuring the Device Name and Device Location Information.](#)
11. (Optional) Configure access control list from management clients.
For more information, see [Configuring the Management Client Access Control List.](#)
12. (Optional) Configure management protocols and ports.
For more information, see [Configuring Management Protocols and Ports.](#)
13. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device.
For more information, see [Manually Updating the Pattern.](#)
14. (Optional) Enable the device to be managed through SDC.
For more information, see [Enabling SDC Management.](#)
15. (Optional) Configure the password policy.
For more information, see [Configuring Password Policy Settings.](#)

Opening the Management Console

The IEF-G9010 Series provides a built-in management web console that you can use to configure and manage the product. The management console can be accessed through any supported any web browser.

The management console supports Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; or Edge version 15 or later.

Steps:

1. In a web browser, type the address of the IEF-G9010 Series in the following format:
https://192.168.127.254
The login screen appears.



NOTE

The default IP address of the IEF-G9010 Series is 192.168.127.254 with subnet 255.255.255.0. Before connecting a PC/Laptop to the IEF-G9010 Series, the PC's IP address should be set to an IP address that is able to access the default IP address. After that, connect the PC and the IEF-G9010 Series using an Ethernet cable.



NOTE

The IEF-G9010 Series uses an automatically generated self-signed SSL certificate to encrypt communications to and from the client accessing the device. Given that the certificate is self-signed, most browsers will not trust the certificate and will give a warning that the certificate being used is not signed by a known authority.



NOTE

For security reasons, the web management console can only be accessed through port 1.

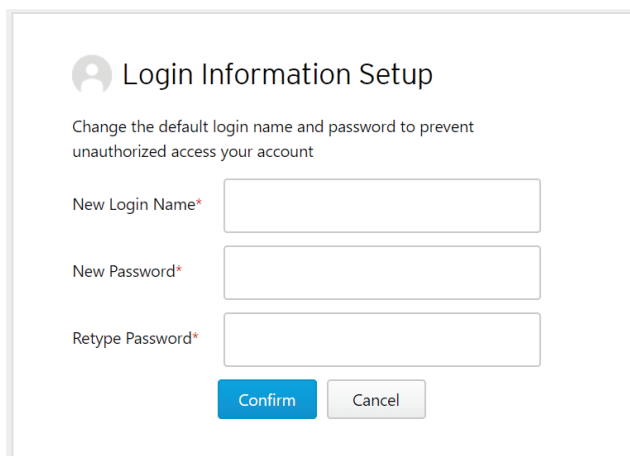
2. Enter your login credentials (user ID and password). Use the default administrator login credentials when logging in for the first time:
 - User ID: admin
 - Password: moxa

The screenshot shows a login interface with the following elements:

- A header with a person icon and the text "Log On".
- A text input field containing the user ID "admin".
- A password input field with masked characters "....".
- A teal "Log On" button.

3. Click **Log On**.

- When you log in for the first time, the IEF-G9010 Series will request you to create a new admin account and change the default password for security reasons. Enter the new username and password and click **Confirm**.



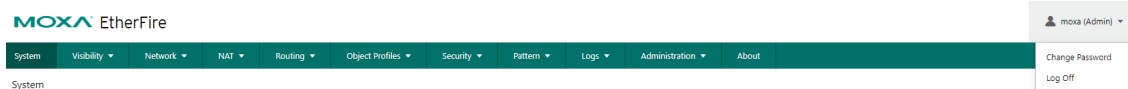
- The system will return to the login screen. Use the new admin account and password to log in.

Changing the Administrator's Password

To change the password of the IEF-G9010 Series, you have to log in to the web console with the admin credentials.

Steps:

- In a web browser, type the address of the IEF-G9010 Series in the following format:
https://192.168.127.254
The login screen appears.
- Log in as the administrator.
- Click the admin account icon at the top-right corner and select **Change Password**.
- Proceed to change the password.

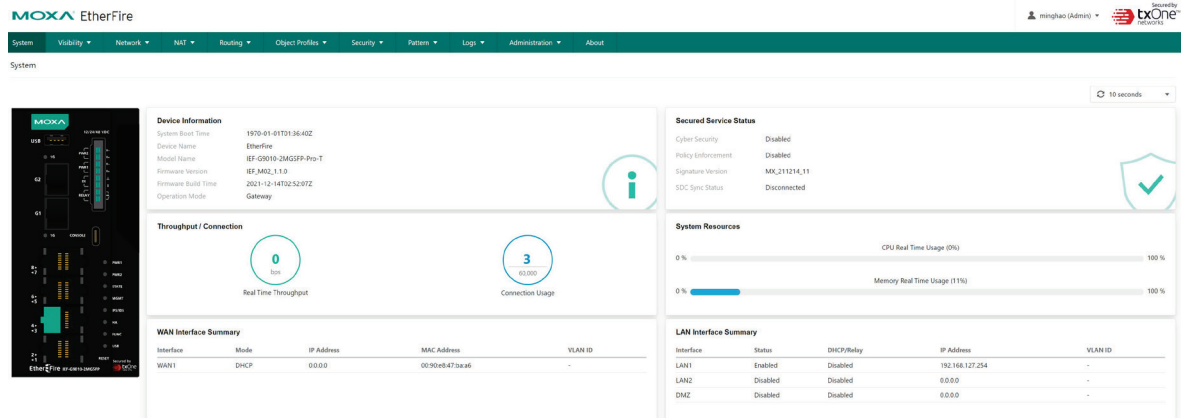


NOTE

If you forgot the administrator account and password, the only way to retrieve your administration access is to reset the IEF-G9010 Series device to factory default settings by pressing and holding the reset button for more than 10 seconds. The MANAGED LED will begin to blink every half-second, which means the system is resetting itself to factory defaults. DO NOT power off the device while it is loading the default settings.

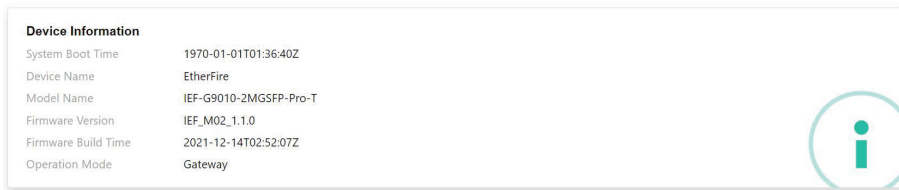
3. The System Screens

Monitor your system information, system status, and system resource usage on the system screen.



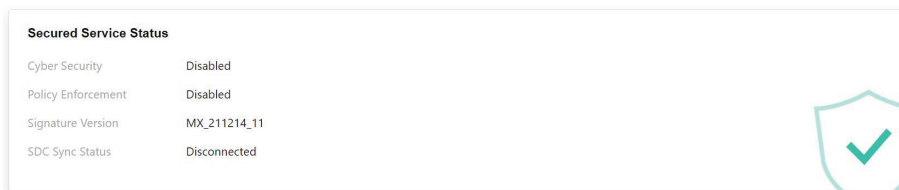
Device Information

This widget shows the system boot time, device name, model, firmware version, and firmware build date and time.



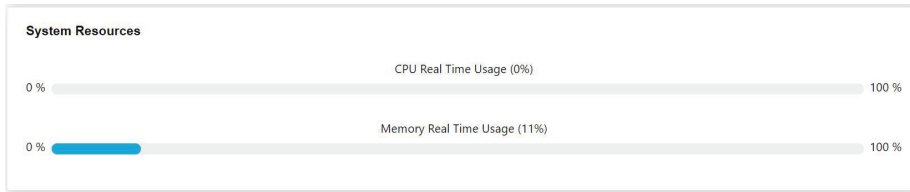
Secured Service Status

This widget shows the status of the device's security services, the current pattern version, and the sync status with SDC.



System Resources

This widget shows the resource usage of the device.



Item	Description
CPU Utilization	Real-time CPU utilization % (Based on the refresh time settings)
Memory Utilization	Real-time memory utilization % (Based on the refresh time settings)

WAN Interface Summary

This widget shows summary information for the WAN interface.

WAN Interface Summary				
Interface	Mode	IP Address	MAC Address	VLAN ID
WAN1	DHCP	0.0.0.0	00:90:e8:47:ba:a6	-

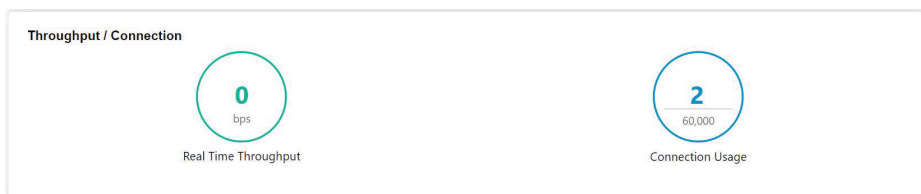
LAN Interface Summary

This widget shows summary information for the LAN1, LAN2, and DMZ interfaces.

LAN Interface Summary				
Interface	Status	DHCP/Relay	IP Address	VLAN ID
LAN1	Enabled	Disabled	192.168.127.254	-
LAN2	Disabled	Disabled	0.0.0.0	-
DMZ	Disabled	Disabled	0.0.0.0	-

Throughput/Connection

This widget shows the real-time throughput and connection usage of the device.



4. The Visibility Screens

The Visibility screen gives you an overview of your managed assets. The screens provide you with timely and accurate information on the assets that are managed by the IEF-G9010 Series.

Visibility > Assets View

Active Query in Inline Mode 10 Sec

Assets Information

Host Name	PLC Sample	IP Address	192.168.1.10
Model Name	LOGIX5561	MAC Address	00:1d:9c:11:22:33
Vendor Name	Rockwell	Interface	Port1
Assets Type	PLC	First Seen	2019-11-22T07:51:49+08:00
Serial Number	SN 123 456-7890	Last Seen	2020-07-28T07:51:49+08:00
OS	Windows 2000		

Real Time Network Application Traffic 10 Sec

No	Application Name	TX	RX
1	Modbus	964.94 GB	655.53 GB
2	SLMP	673.36 GB	766.10 GB
3	-	541.82 GB	482.64 GB
4	-	640.75 GB	432.98 GB
5	-	513.75 GB	530.23 GB

Number of active assets: 5 / 50 Real time network application traffic: 8 / Device

The assets, listed on the screen, are automatically detected by IEF-G9010 Series devices.



NOTE

The term **asset** in this chapter refers to the devices or hosts that are protected by the IEF-G9010 Series.

Enabling Active Query

Active Query can detect inactive or dormant assets or passive assets on the network. Active Query is only available in Inline Mode. In Offline Mode, the Active Query toggle will be inactive.



NOTE

In firmware v1.1, Active Query supports 4 protocols (Modbus, CIP, OMRON FINS, and SMB).

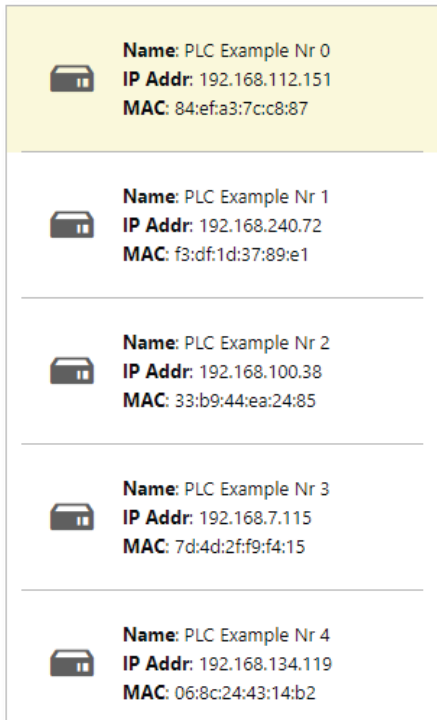
Steps:

1. Go to [Visibility] > [Assets View].
2. Click the **Active Query in Inline Mode** toggle in the top-left.

Viewing Asset Information

Steps:

1. Go to [Visibility] > [Assets View].
2. Click an asset icon to view more detailed information.



3. The [Assets Information] pane shows the following information for the asset:

Field	Description
Vendor Name	The vendor name of the asset.
Model Name	The model name of the asset.
Asset Type	The asset type of the asset.
Host Name	The name of the asset.
Serial Number	The serial number of the asset.
OS	The operating system of the asset.
MAC Address	The MAC address of the asset.
IP Address	The IP address of the asset.
First Seen	The date and time the asset was first seen.
Last Seen	The date and time the asset was last seen.

Viewing Real-time Network Application Traffic

Steps:

1. Go to [Visibility] > [Assets View].
2. Click an asset icon to view more detailed information.
3. The [Real Time Network Application Traffic] pane shows a list of network traffic statics of the asset.

Field	Description
No.	Ordinal number of the application traffic.
Application Name	The application type of the traffic.
TX	The amount of traffic transmitted by this application.
RX	The amount of traffic received by this application.



NOTE

Click **Manual Asset Info Refresh** to refresh the displayed information.



NOTE

You can specify the refresh time from the [Refresh Time] drop-down menu.

5. The Network Screens

This chapter describes how to configure the physical ports and network interfaces of the IEF-G9010 Series.

Port Settings

The [Port Settings] tab allows you to enable or disable the ports and configure the port link speed.



NOTE

The term **Port** in the document refers to physical ports to which network cables are connected.

Configuring Port Settings

Steps:

1. Go to [Network] > [Port Settings].

Network > Port Settings

Port Name	Enable Status	Link Speed Setting	Link Status	Description
PORT1	Enabled	Auto Negotiation	--	--
PORT2	Enabled	Auto Negotiation	--	--
PORT3	Enabled	Auto Negotiation	--	--
PORT4	Enabled	Auto Negotiation	--	--
PORT5	Enabled	Auto Negotiation	--	--
PORT6	Enabled	Auto Negotiation	1 Gbps Full Duplex	--
PORT7	Enabled	Auto Negotiation	--	--
PORT8	Enabled	Auto Negotiation	--	--
G1	Enabled	Auto Negotiation	--	--
G2	Enabled	Auto Negotiation	--	--

2. Click on a port in the [Port Name] column to configure the port.
3. Use the toggle to enable or disable the port.
4. (Optional) Enter a description for the port.
5. Select the port speed and negotiation method from the [Link Speed] drop-down menu.
6. Click **Ok**.

Port Configuration

Enable Port:

Port Name: PORT6

Description:

Link Speed: Auto Negotiation

Ok Cancel



NOTE

The panel image on the page shows a graphical representation of the ports on the device that are connected.



NOTE

Click the [Manual Port Info Refresh] button in the top-right to refresh the displayed information manually.

Port Mapping

Use the [Port Mapping] tab to view the port and interface mapping.

Steps:

Go to [Network] > [Port Mapping].

The Port Mapping tab will appear. This tab shows the mapping between the physical ports and the WAN and LAN interfaces.

	PORT1	PORT2	PORT3	PORT4	PORT5	PORT6	PORT7	PORT8	G1	G2
Network Interface										
WAN1 (Specify one interface only)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LAN1	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
LAN2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DMZ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Network Interface

Use the [Network Interface] tab to configure the following settings:

- The settings of the device's network interfaces
- DHCP settings on the LAN interface
- The WAN connection type



NOTE

The term **Network Interface** or **Interface** in this document refers to the logical interface that maps to one or more physical ports.



NOTE

The default web management console IP address is **198.168.127.254** and is bound to the LAN1 network interface.

Configuring the LAN Network Interface

Steps:

1. Go to [Network] > [Network Interface].

The Network Interface tab will appear.

Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	DHCP Client	0.0.0.0	0.0.0.0	-	-
LAN1	On	DHCP Service Disabled	192.168.127.254	255.255.255.0	-	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click on **LAN1** or **LAN2** in the [Interface] column to configure the port.

The Edit Network Interface window will appear.

Edit Network Interface

Network Interface

Enable Network

Network Interface Name LAN1

Description

Network Settings

IP Address* 192.168.127.254

Subnet Mask* 255.255.255.0

Enable VLAN ID

VLAN ID* 0

DHCP Service

DHCP Service Disabled

Ok Cancel

3. Use the toggle to enable or disable the interface.
4. (Optional) Enter a descriptive name for the interface.
5. In the [Network Settings] section, configure the following settings:
 - a. **IP Address:** Enter a valid IP address.
 - b. **Subnet Mask:** Enter the subnet mask.
 - c. (Optional) **Enable VLAN ID:** Use the toggle to enable or disable VLAN ID tagging.
 - d. (Optional) **VLAN ID:** If VLAN ID is enabled, specify a VLAN ID.

6. In the [DHCP Service] section, choose the DHCP Service mode:
 - a. **Disabled:** Disable DHCP services on the interface.
 - b. **DHCP Server:** Enable DHCP services on the interface. Configure the following additional settings:

DHCP Service

DHCP Service	<input type="text" value="DHCP Server"/>
Start IP Address*	<input type="text" value="192.168.127.1"/>
End IP Address*	<input type="text" value="192.168.127.100"/>
Gateway Address*	<input type="text" value="192.168.127.254"/>
Lease Time*	<input type="text" value="86400"/> ⓘ
DNS Server 1	<input type="text" value="8.8.8.8"/>
DNS Server 2	<input type="text" value="8.8.8.9"/>

- i. **Start IP Address:** Enter the starting IP address of the DHCP address pool.
 - ii. **End IP Address:** Enter the ending IP address of the DHCP address pool.
 - iii. **Gateway Address:** Enter the gateway IP address that will be assigned to DHCP clients.
 - iv. **Lease Time:** Specify the time (in seconds) that a client device can use the assigned IP address provided by the DHCP server.
 - v. (Optional) **DNS Server 1,2:** Enter the primary and secondary DNS server that will be assigned to DHCP clients.
- c. **DHCP Relay:** Configure the interface to act as a relay to a remote DHCP server. Configure the following additional settings:

DHCP Service

DHCP Service	<input type="text" value="DHCP Relay"/>
Interface	<input type="text" value="WAN1"/>
Relay Server Address*	<input type="text" value="192.168.50.1"/>

- i. **Relay Server Address:** Enter the IP address of the remote DHCP server.

7. Click **Ok**.

Configuring the DMZ Network Interface

Steps

1. Go to [Network] > [Network Interface].
The Network Interface tab will appear.

Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	DHCP Client	0.0.0.0	0.0.0.0	-	-
LAN1	On	DHCP Service Disabled	192.168.127.254	255.255.255.0	-	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click on **DMZ** in the [Interface] column to configure the port.
The Edit Network Interface window will appear.

Edit Network Interface

Status

Network Interface Name DMZ

Description ⓘ

Network Settings

IP Address*

Subnet Mask*

VLAN ID ⓘ

DHCP Service

DHCP Service

Start IP Address*

End IP Address*

Gateway Address*


Lease Time* ⓘ

DNS Server 1

DNS Server 2

3. Use the toggle to enable or disable the interface.
4. (Optional) Enter a descriptive name for the interface.
5. In the [Network Settings] section, configure the following settings for the interface:
 - a. **IP Address:** Enter a valid IP address.
 - b. **Subnet Mask:** Enter the subnet mask.
 - c. (Optional) **VLAN ID:** If VLAN ID is enabled, specify a VLAN ID.

6. In the [DHCP] section, choose the DHCP service type
 - a. **Disabled:** No DHCP service will be provided on this interface.
 - b. **DHCP Server:** This interface will provide DHCP service to the devices that connect to the interface. Configure the following additional settings:

DHCP Service	<input type="text" value="DHCP Server"/>
Start IP Address*	<input type="text" value="192.168.254.1"/>
End IP Address*	<input type="text" value="192.168.254.100"/>
Gateway Address*	<input type="text" value="192.168.254.254"/>
Lease Time*	<input type="text" value="86400"/> 
DNS Server 1	<input type="text" value="8.8.8.8"/>
DNS Server 2	<input type="text" value="8.8.8.9"/>

- i. **Start IP Address:** Enter the starting IP address of the DHCP address pool.
 - ii. **End IP Address:** Enter the ending IP address of the DHCP address pool.
 - iii. **Gateway Address:** Enter the gateway IP address that will be assigned to DHCP clients.
 - iv. **Lease Time:** Specify the time (in seconds) that a client device can use the assigned IP address provided by the DHCP server.
 - v. (Optional) **DNS Server 1,2:** Enter the primary and secondary DNS server that will be assigned to DHCP clients.
- c. **DHCP Relay:** This interface will relay the traffic from the clients to a relayed server for DHCP service. Configure the following additional settings:

DHCP Service	<input type="text" value="DHCP Relay"/>
Interface	<input type="text" value="WAN1"/>
Relay Server Address*	<input type="text" value="192.168.50.1"/>

- i. **Relay Server Address:** Enter the IP address of the remote DHCP server.

Configuring the WAN Network Interface

Steps:

1. Go to [Network] > [Network Interface].
The Network Interface tab will appear.

Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	DHCP Client	0.0.0.0	0.0.0.0	-	-
LAN1	On	DHCP Service Disabled	192.168.127.254	255.255.255.0	-	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click on **WAN1** in the [Interface] column to configure the port.
The Edit Network Interface window will appear.

3. Use the toggle to enable or disable the interface.
4. (Optional) Enter a descriptive name for the interface.
5. In the [Network Settings] section, choose a Connection Type:
 - a. **Static IP:** Configure a static IP address for this interface. Configure the following additional settings:

- i. **IP Address:** Enter a valid IP address.
- ii. **Subnet Mask:** Enter the subnet mask.
- iii. **Gateway Address:** Enter the gateway IP address.
- iv. (Optional) **DNS Server 1,2:** Enter the primary and secondary DNS server.
- v. (Optional) **Enable VLAN ID:** Use the toggle to enable or disable VLAN ID tagging.
- vi. (Optional) **VLAN ID:** If VLAN ID is enabled, specify a VLAN ID.

- b. **DHCP Client:** Configure the interface as a DHCP client that will receive its IP address information from a DHCP server. Configure the following additional settings:

Network Settings

Connection Type: DHCP Client

Get IP Address Automatically:

Enable VLAN ID:

VLAN ID*: 0

- i. (Optional) **Enable VLAN ID:** Use the toggle to enable or disable VLAN ID tagging.
 - ii. (Optional) **VLAN ID:** If VLAN ID is enabled, specify a VLAN ID.
6. Click **Ok**.

Device Operation Modes

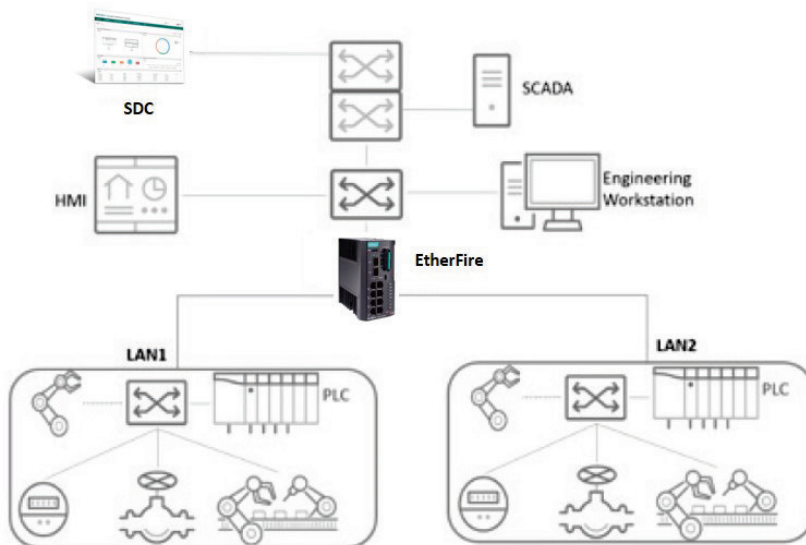
The IEF-G9010 Series can function in one of two operation modes:

- **Gateway Mode**
- **Bridge Mode**

Refer to the following sections for more information.

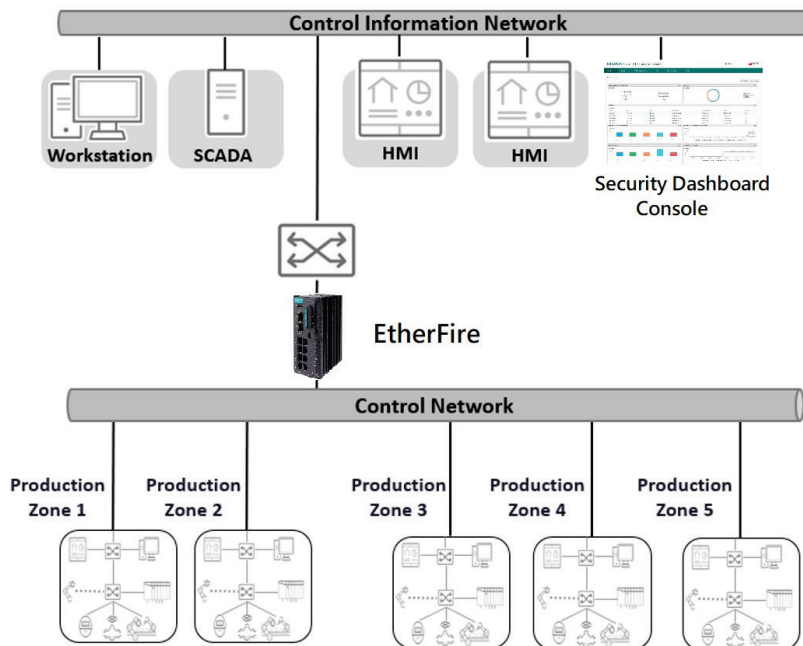
Gateway Mode

When in Gateway Mode, the IEF-G9010 Series acts as a gateway with NAT functionality connecting multiple different network segments while actively analyzing, filtering, and taking actions on all traffic that passes through it.



Bridge Mode

When in Bridge Mode, the IEF-G9010 Series sits in the direct communication path between the source and the destination, actively analyzing, filtering, and taking actions on all traffic that passes through it.



Selecting the Operation Mode

The Operation Mode screen can be accessed by going to [Network] > [Operation Mode].

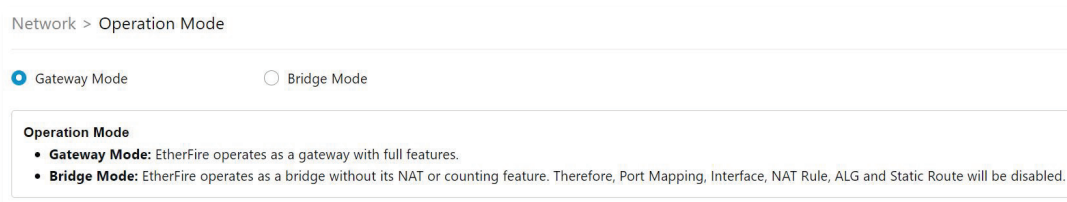
From the [Operation Mode] screen you can configure or view the following:

- The current operation mode of the device
- The network settings for Bridge Mode (When the device is in Gateway Mode)
 - IP Address
 - Subnet Mask
 - Gateway Address
 - DNS
 - VLAN ID
 - STP (Spanning Tree Protocol)
- The LAN1 network settings for Gateway Mode (When the device is in Bridge Mode, view-only)
 - IP Address
 - Subnet Mask
- The LAN1 DHCP service settings for Gateway Mode (When the device is in Bridge Mode, view-only)
 - DHCP Service
 - Start IP Address
 - End IP Address
 - Gateway Address
 - Lease Time

Switching to Bridge Mode

Steps:

1. Go to [Network] > [Operation Mode].
The [Operation Mode] tab will appear.



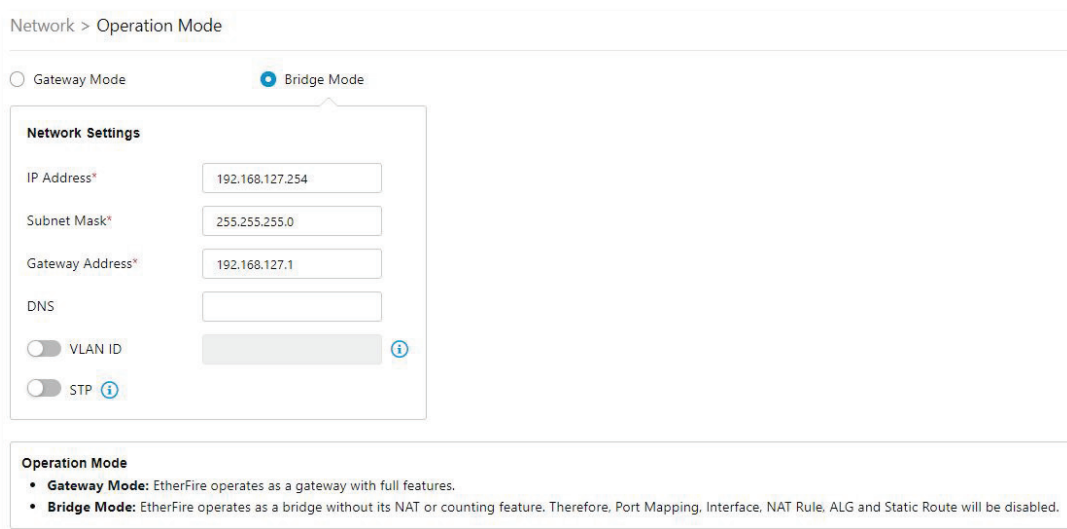
Network > Operation Mode

Gateway Mode Bridge Mode

Operation Mode

- **Gateway Mode:** EtherFire operates as a gateway with full features.
- **Bridge Mode:** EtherFire operates as a bridge without its NAT or counting feature. Therefore, Port Mapping, Interface, NAT Rule, ALG and Static Route will be disabled.

2. Click the [Bridge Mode] radio button.
The [Network Settings] section for Bridge Mode will appear.



Network > Operation Mode

Gateway Mode Bridge Mode

Network Settings

IP Address* 192.168.127.254

Subnet Mask* 255.255.255.0

Gateway Address* 192.168.127.1

DNS

VLAN ID

STP

Operation Mode

- **Gateway Mode:** EtherFire operates as a gateway with full features.
- **Bridge Mode:** EtherFire operates as a bridge without its NAT or counting feature. Therefore, Port Mapping, Interface, NAT Rule, ALG and Static Route will be disabled.

3. In the [Network Settings] section, configure the following network settings:
 - a. **IP Address:** Enter a valid IP address.
 - b. **Subnet Mask:** Enter the subnet mask.
 - c. **Gateway Address:** Enter the gateway address.
 - d. (Optional) **DNS:** Enter a DNS address.
 - e. (Optional) **VLAN ID:** Use the toggle to enable or disable VLAN ID. If enabled, enter the VLAN ID.
 - f. (Optional) **STP:** Use the toggle to enable or disable STP (Spanning Tree Protocol).
4. When finished, click **Save**.



NOTE

When switching from Gateway to Bridge Mode, the Port Mapping, Network Interface, NAT Rules, ALG, and Static Route functions will be unavailable and cannot be configured.



NOTE

Policy enforcement rule configurations are not compatible between Gateway and Bridge Mode. Therefore, policy enforcement rules must be reconfigured after switching operation modes.

Switching to Gateway Mode

1. Go to [Network] > [Operation Mode].
The [Operation Mode] tab will appear.

Network > Operation Mode

Gateway Mode Bridge Mode

Network Settings

IP Address*

Subnet Mask*

Gateway Address*

DNS

VLAN ID

STP

Operation Mode

- **Gateway Mode:** EtherFire operates as a gateway with full features.
- **Bridge Mode:** EtherFire operates as a bridge without its NAT or counting feature. Therefore, Port Mapping, Interface, NAT Rule, ALG and Static Route will be disabled.

2. Click the [Gateway Mode] radio button.

Network > Operation Mode

Gateway Mode Bridge Mode

Operation Mode

- **Gateway Mode:** EtherFire operates as a gateway with full features.
- **Bridge Mode:** EtherFire operates as a bridge without its NAT or counting feature. Therefore, Port Mapping, Interface, NAT Rule, ALG and Static Route will be disabled.

3. When finished, click **Save**.



NOTE

In Bridge Mode, the LAN1 network settings and LAN1 DHCP Service for Gateway Mode are view-only.



NOTE

Policy enforcement rule configurations are not compatible between Gateway and Bridge Mode. Therefore, policy enforcement rules must be reconfigured after switching operation modes.

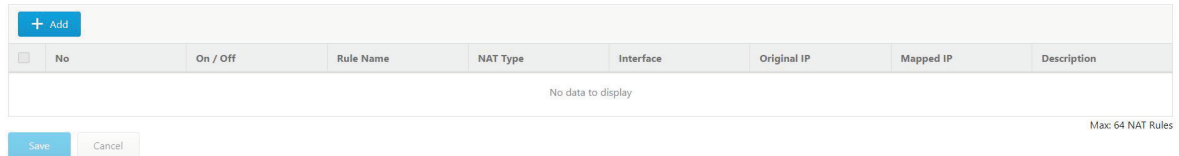
6. The NAT Screens

This chapter describes how to configure Network Address Translation (NAT) rules and how to enable or disable application-layer gateways (ALG).

NAT Rules

Use the [NAT] tab to configure the following settings:

- 1-to-1: The simplest form of NAT for point-to-point translation of IP addresses.
- Multi 1-to-1: This form of NAT allows you to map multiple public destination IP addresses of incoming traffic to multiple private IP addresses within the local network and vice versa. These rules can also allow you to map a source IP address from your local network to outgoing traffic.
- Port forwarding address translation for incoming traffic on the WAN interface.



The following table describes the basic tasks you can perform from the [NAT Rule] tab.

Task	Description
Add a NAT rule	Click Add to create a new NAT rule.
Edit a NAT rule	Click on the name of an existing NAT rule to edit it.
Delete a NAT rule	Select one or more NAT rules and click Delete .
Copy a NAT rule	Select one or more NAT rules and click Copy .

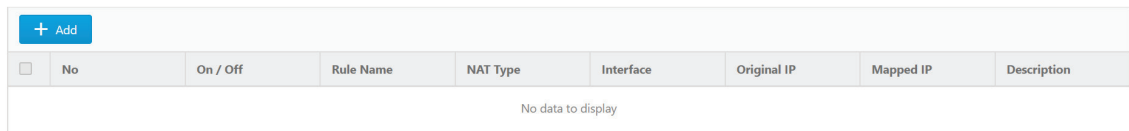
Configuring 1-to-1 NAT Rules

1-to-1 NAT rules allow you to map a destination IP address for incoming traffic to an IP address within the local network and vice versa. That is, these rules can also allow you to map a source IP address from your local network to outgoing traffic.

Steps:

1. Go to [NAT] > [NAT Rule].

The NAT Rule tab will appear.



2. Do one of the following:
 - a. Click **Add** to create a new rule.
 - b. Click on the name of an existing NAT rule to edit it.

3. Configure the following settings:

- a. **Enable NAT Rule:** Use the toggle to enable or disable the NAT rule.
 - b. **NAT Type:** Select **1 to 1 NAT** from the drop-down list.
 - c. **Rule Name:** Enter a name for the rule.
 - d. (Optional) **Description:** Enter a description for the rule.
 - e. **Incoming Interface:** Select the interface that will process incoming traffic for this rule from the drop-down list.
 - f. **Original IP:** Enter the destination IP to be translated. When the device receives packets on the specified [Incoming Interface], if the destination IP of the packet matches the [Original IP], it will be changed to the [Mapped IP].
 - g. **Mapped IP:** Enter the IP address the [Original IP] will be mapped to. This is usually a private IP address within your local network.
 - h. (Optional) **Enable NAT Loopback:** Use the toggle to enable or disable NAT loopback.
4. Click **Ok** to close the Create Rule window.
 5. On the Rules overview page, click **Save** to save your settings.

Configuring Multi 1-to-1 NAT Rules

Multi 1-to-1 NAT rules allow you to map multiple public destination IP addresses of incoming traffic to multiple private IP addresses within the local network and vice versa. That is, these rules can also allow you to map a source IP address from your local network to outgoing traffic.

The following table shows an example:

Original Destination IP	Mapped Destination IP
172.1.1.5	192.168.100.5
172.1.1.20	192.168.100.20
172.1.1.50	192.168.100.50
172.1.1.69	192.168.100.69

Steps:

1. Go to [NAT] > [NAT Rule].

The NAT Rule tab will appear.

2. Do one of the following:
 - a. Click **Add** to create a new rule.
 - b. Click on the name of an existing NAT rule to edit it.
3. Configure the following settings:

- a. **Enable NAT Rule:** Use the toggle to enable or disable the NAT rule.
 - b. **NAT Type:** Select **Multi 1 to 1 NAT** from the drop-down list.
 - c. **Rule Name:** Enter a name for the rule.
 - d. (Optional) **Description:** Enter a description for the rule.
 - e. **Incoming Interface:** Select the interface that will process incoming traffic for this rule from the drop-down list.
 - f. **Original IP:** Enter the destination IP addresses to be translated using CIDR (Classless Inter-domain Routing) format, for example 172.1.1.0/24. When the device receives packets on the specified [Incoming Interface], if the destination IP of the packet matches the [Original IP], it will be changed to the [Mapped IP]. These IP addresses are usually assigned by the ISP (Internet Service Provider).
 - g. **Mapped IP:** Enter the IP addresses the [Original IP] will be mapped to using the CIDR (Classless Inter-domain Routing) format, for example 192.168.100.0/24. This is usually a private IP address within your local network.
 - h. (Optional) **Enable NAT Loopback:** Use the toggle to enable or disable NAT loopback.
4. Click **Ok** to close the Create Rule window.
 5. On the Rules overview page, click **Save** to save your settings.

Configuring Port Forwarding

Port forwarding rules allow you to map a host IP address to forward incoming traffic to another IP address within the local network.

Steps:

1. Go to [NAT] > [NAT Rule].
The NAT Rule tab will appear.

+ Add									
<input type="checkbox"/>	No	On / Off	Rule Name	NAT Type	Interface	Original IP	Mapped IP	Description	
No data to display									

2. Do one of the following:
 - a. Click **Add** to create a new rule.
 - b. Click on the name of an existing NAT rule to edit it.

3. Configure the following settings:

- a. **Enable NAT Rule:** Use the toggle to enable or disable the NAT rule.
 - b. **NAT Type:** Select **Port Forward** from the drop-down list.
 - c. **Rule Name:** Enter a name for the rule.
 - d. (Optional) **Description:** Enter a description for the rule.
 - e. **Incoming Interface:** Select the interface that will process incoming traffic for this rule from the drop-down list.
 - f. **Protocol:** Select the protocol that will be processed by the rule.
 - g. **Original IP:** Enter the port range to be translated. When the device receives packets on the specified [Incoming Interface], if the destination IP of the packet matches the [Original IP], it will be changed to the [Mapped IP] IP address and port range.
 - h. **Mapped IP:** Enter the IP address and port range the [Original IP] will be mapped to. This is usually a private IP address within your local network.
 - i. (Optional) **Enable NAT Loopback:** Use the toggle to enable or disable NAT loopback.
4. Click **Ok** to close the Create Rule window.
 5. On the Rules overview page, click **Save** to save your settings.

Application-layer Gateways (ALG)

An application-layer gateway (ALG) allows client applications with server applications through server ports that are opened to client applications. These ports are usually dynamically assigned in the application protocol. An ALG understands application protocols, recognizes application-specific commands, and helps open device ports to enable communications. Without an ALG, client applications like FTP would be unable to transfer files when the FTP client is located within a NAT network.

Use the [ALG Settings] tab to configure the following settings:

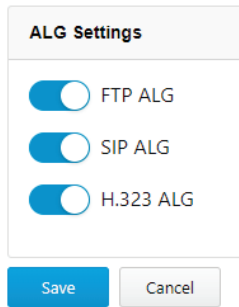
- Enable or disable the FTP, SIP, and H.323 ALG

Configuring ALG Settings

Steps:

1. Go to [NAT] > [ALG].

The ALG Settings tab will appear.



The screenshot shows a configuration window titled "ALG Settings". Inside the window, there are three toggle switches, each with a blue indicator that it is turned on. The switches are labeled "FTP ALG", "SIP ALG", and "H.323 ALG". Below the switches, there are two buttons: a blue "Save" button and a grey "Cancel" button.

2. Use the toggles to enable or disable the FTP, SIP, and H.323 ALG.
3. Click **Save**.

7. The Routing Screens

This chapter describes how to configure and view static routes on the device.

Static Routes

Static routes are generally used when no appropriate dynamic route is available, or when you want traffic to follow a specific route as opposed to following the dynamic route that is automatically learned and generated by the device.

Use the [Static Route] tab to view a list of all configured static routes on the device and to create new or edit existing static routes.

Routing > Static Route

No.	On / Off	Rule Name	Destination Address	Gateway / Interface	Metric	Description
No data to display						

The following table describes the basic tasks you can perform from the [Static Route] tab.

Task	Description
Add a static route	Click Add to create a new static route.
Edit a static route	Click on the name of an existing static route to edit it.
Delete a static route	Select one or more static routes and click Delete .
Copy a static route	Select one or more static routes and click Copy .

Configuring Static Routes

Steps:

1. Go to [Routing] > [Static Route].

The Static Route tab will appear.

Routing > Static Route

No.	On / Off	Rule Name	Destination Address	Gateway / Interface	Metric	Description
No data to display						

2. Do one of the following:
 - a. Click **Add** to create a new static route.
 - b. Click on the name of an existing static route to edit it.
3. Configure the following settings:

- a. **Enable Static Route:** Use the toggle to enable or disable the route.
 - b. **Rule Name:** Enter a name for the route.
 - c. (Optional) **Description:** Enter a description for the route.
 - d. **Destination Address:** Enter the route's destination address.
 - e. **Subnet Mask:** Enter the subnet mask. If the destination is a single IP address, the subnet should be set to 255.255.255.255. If the destination is a subnet, enter the subnet mask to match the destination IP range, for example 255.255.255.0.
 - f. Configure the Next Hop Type.
 - i. **Gateway IP Address:** If the next hop is a gateway, enter the gateway's IP. The gateway must be in the same network as the forwarding interface.
 - ii. **Network Interface:** If the next hop is an interface on the device, select the interface from the drop-down menu.
 - g. **Metric:** Enter a metric for the route. This determines which static route to use based on the specified metric. A lower number represents a higher priority.
4. Click **Ok**.
 5. On the Routes overview page, click **Save** to save your settings.

8. The Object Profiles Screens

Object profiles simplify policy management by storing configurations that can be used by the IEF-G9010 Series.

You can configure the following types of object profiles for this device:

- **IP Object Profile:** Contains the IP addresses that you can apply to a policy rule.
- **Service Object Profile:** Contains the service definitions that you can apply to a policy rule. TCP port range, UDP port range, ICMP, and custom protocol number are defined here.
- **Protocol Filter Profile:** Contains more sophisticated and advanced protocol settings that you can apply to a policy rule. Details of ICS (Industrial Control System) protocols are defined here.
- **IPS Profile:** Contains the settings of IPS (Intrusion Prevention System) pattern rules that you can apply to a policy rule.

The following table describes the tasks you can perform when you view a list of the profiles:

Task	Description
Add a profile	Click Add to create a new profile.
Edit a profile	Click on the name of an existing profile to edit it.
Delete a profile	Select one or more profiles and click Delete .
Copy a profile	Select a profile and click Copy .

Configuring IP Object Profiles

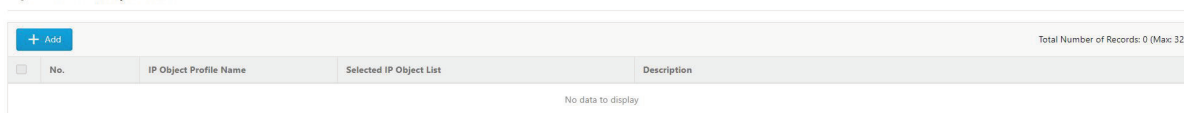
You can configure the IP address in an IP object profile, which can be used by other policy rules. The types of IP address you can assign are:

- Single IP address
- IP ranges
- IP subnets

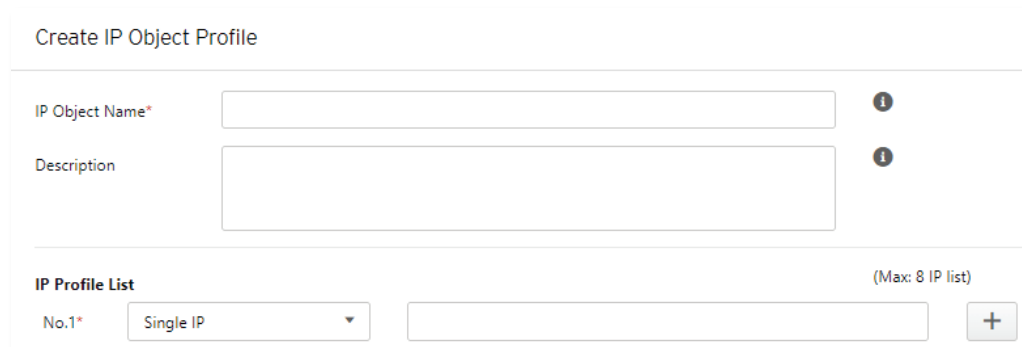
Steps:


1. Go to [Object Profile] > [IP Object Profile].

Object Profiles > IP Object Profile



2. Do one of the following:
 - a. Click **Add** to create a new profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:



- a. **IP Object Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
 - c. **No:x:** In the [IP Profile List] section, specify an IP address, an IP range, or an IP subnet.
Click the  button to add another entry. You can add up to 8 entries.
4. Click **OK**.

Configuring Service Object Profiles

In a service object profile, you can define the following:

- TCP protocol port range
- UDP protocol port range
- ICMP protocol type and code
- Custom protocol with a specified protocol number



NOTE

The term **protocol number** refers to the protocol number defined in the internet protocol suite.

Steps:

1. Go to [Object Profile] > [Service Object Profile].

Object Profiles > Service Object Profile

+ Add				Total Number of Records: 0 (Max: 32)
No.	Service Object Name	Service Object Information	Description	
No data to display				

2. Do one of the following:
 - a. Click **Add** to create a new profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:


Create Service Object Profile

Service Object Name* ⓘ

Description ⓘ

Service Object List (Max: 8 service list)

No.1*	<input type="text" value="TCP"/>	Protocol Number	<input type="text" value="6"/>	Service Port	<input type="text" value="0"/>	~	<input type="text" value="0"/>	<input type="button" value="+"/>
-------	----------------------------------	-----------------	--------------------------------	--------------	--------------------------------	---	--------------------------------	----------------------------------

- a. **Service Object Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
 - c. **No:x:** In the [Service Object List] section, specify the protocol type and port range (TCP, UDP), type and code (ICMP), or protocol number (Custom).
Click the  button to add another entry. You can add up to 8 entries.
4. Click **OK**.

Configuring Protocol Filter Profiles

A protocol filter profile contains more sophisticated and advanced protocol settings that you can apply to a policy rule.

The following can be configured in a protocol filter profile:

- Details of ICS protocols, including:
 - Modbus
 - CIP
 - S7COMM
 - S7COMM_PLUS
 - PROFINET
 - SLMP
 - FINS
 - MELSOFT
 - SECS/GEM
 - TOYOPUC
 - IEC61850-MMS
- General protocols, including:
 - HTTP
 - FTP
 - SMB
 - RDP
 - MQTT

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

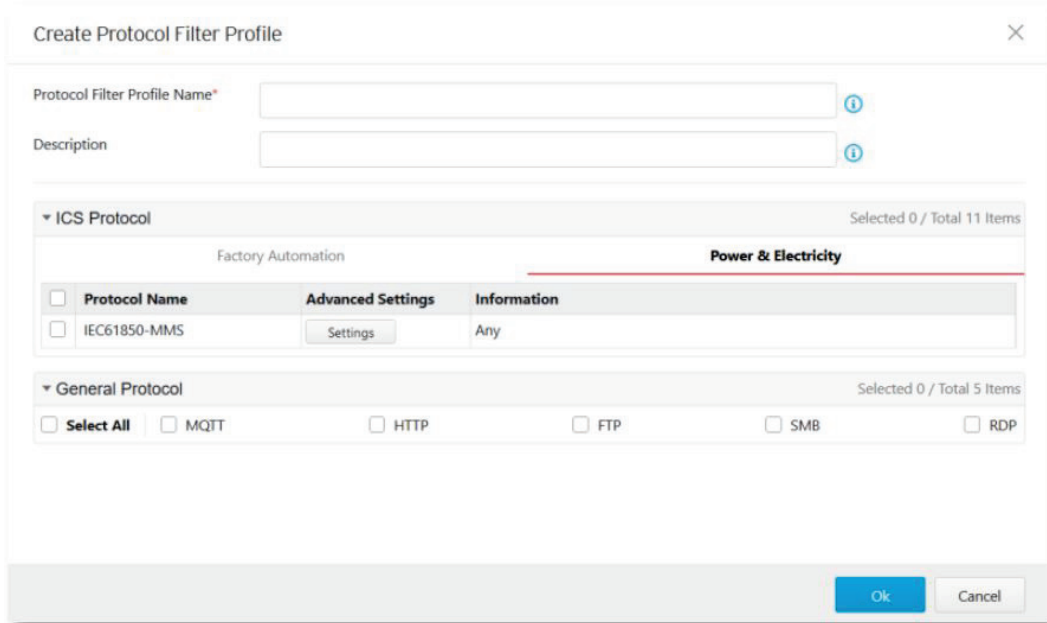
Factory Automation Power & Electricity

<input type="checkbox"/> Protocol Name	Advanced Settings	Information	Drop Malformed ⓘ
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

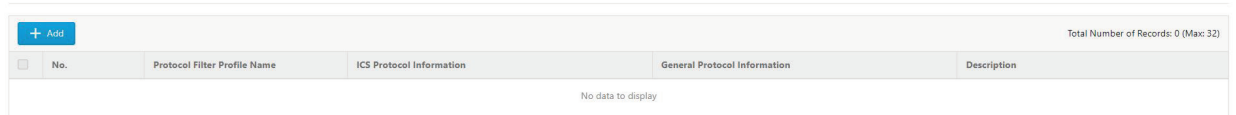
Ok Cancel



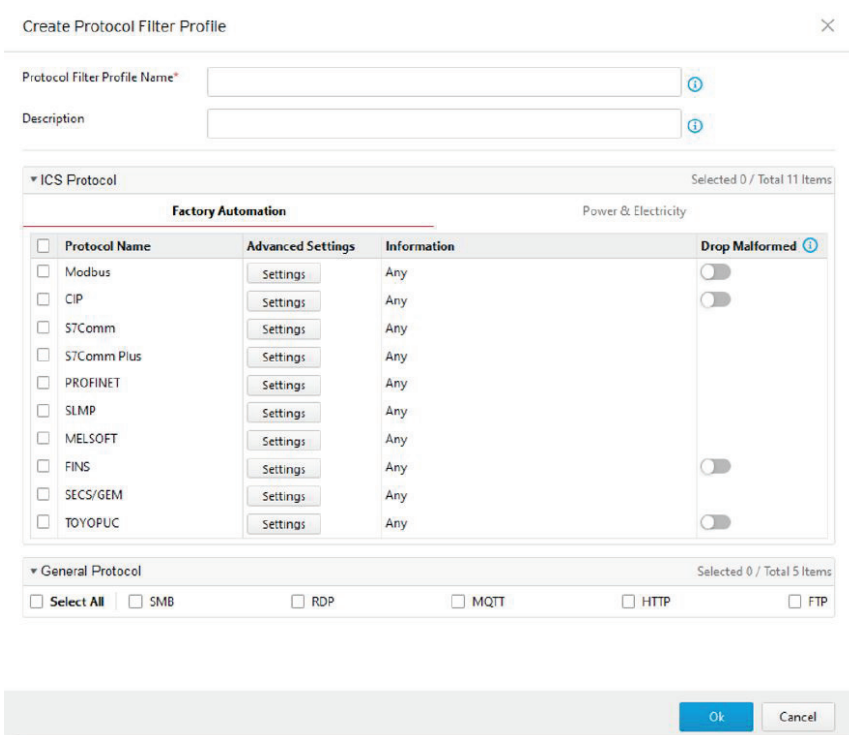
Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].

Object Profiles > Protocol Filter Profile

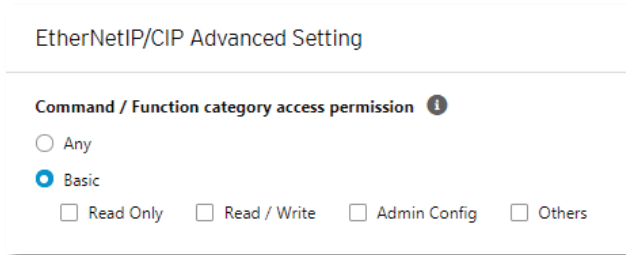


2. Click **Add** to add a protocol filter profile. The [Create Protocol Filter Profile] screen will appear.
3. Configure the following settings:



- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] section, select the protocols you want to include in the protocol filter profile.

- a. Click [Settings] next to a protocol, and select one of the following:



EtherNetIP/CIP Advanced Setting

Command / Function category access permission ⓘ

Any

Basic

Read Only Read / Write Admin Config Others

- i. **Any:** Specify all available commands or function access in this protocol.
- ii. **Basic:** Select multiple commands from the following:
- Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
- b. (Optional) Configure advanced protocol settings. Refer to the following sections:
- i. [Advanced Settings for the Modbus Protocol](#)
 - ii. [Advanced Settings for the CIP Protocol](#)
 - iii. [Advanced Settings for S7Comm](#)
 - iv. [Advanced Settings for S7Comm Plus](#)
 - v. [Advanced Settings for SLMP](#)
 - vi. [Advanced Settings for MELSOFT](#)
 - vii. [Advanced Settings for TOYOPUC](#)
5. Enable the Drop Malformed function. Refer to [Enabling the Drop Malformed Option for an ICS Protocol](#).
6. In the [General Protocol] section, select the protocol(s) you want to include in the protocol filter profile.
7. Click **OK**.

Enabling the Drop Malformed Option for an ICS Protocol

When configuring an ICS protocol, you can enable the [Drop Malformed] function for specific protocols from the protocol profile.

If the [Drop Malformed] option is enabled, the IEF-G9010 will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, the IEF-G9010 will drop the packets of that ICS protocol.



NOTE

In firmware 1.1, 4 protocols support the Drop Malformed option: Modbus, CIP, OMRON FINS and TOYOPUC.

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

Advanced Settings for the Modbus Protocol

The device features more detailed configurations for the Modbus ICS protocol. Through the [Advanced Settings] pane, you can further specify the code/function, unit ID, and address/addresses range against which the function will operate.

Modbus Advanced Setting
✕

Command / Function category access permission ⓘ

Any
 Basic
 Read Only Read / Write Admin Config Others

Professional Setting

Function list: 0x01: Read Coils ▼

Function Code: 0x01 ⓘ

Unit ID: 0 ⓘ

Address: Any ▼ ⓘ

Max: 8 function code list

	No	Function Code	Function Code List	Unit ID	Address
<input type="checkbox"/>					

No data to display

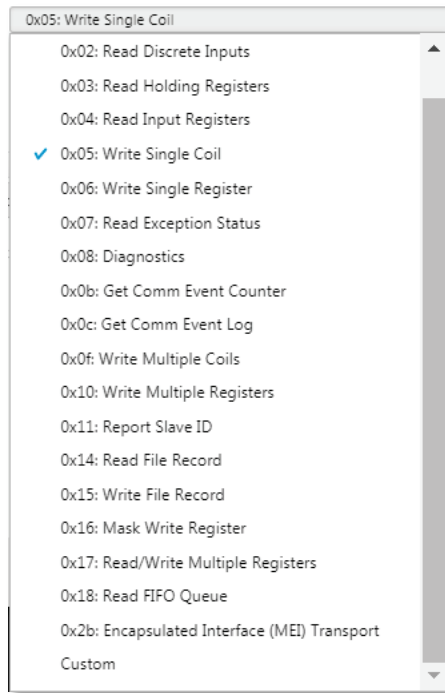
Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> STComm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> STComm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] section, select the protocols you want to include in the protocol filter profile.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol
 - ii. **Basic:** Select multiple commands from the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

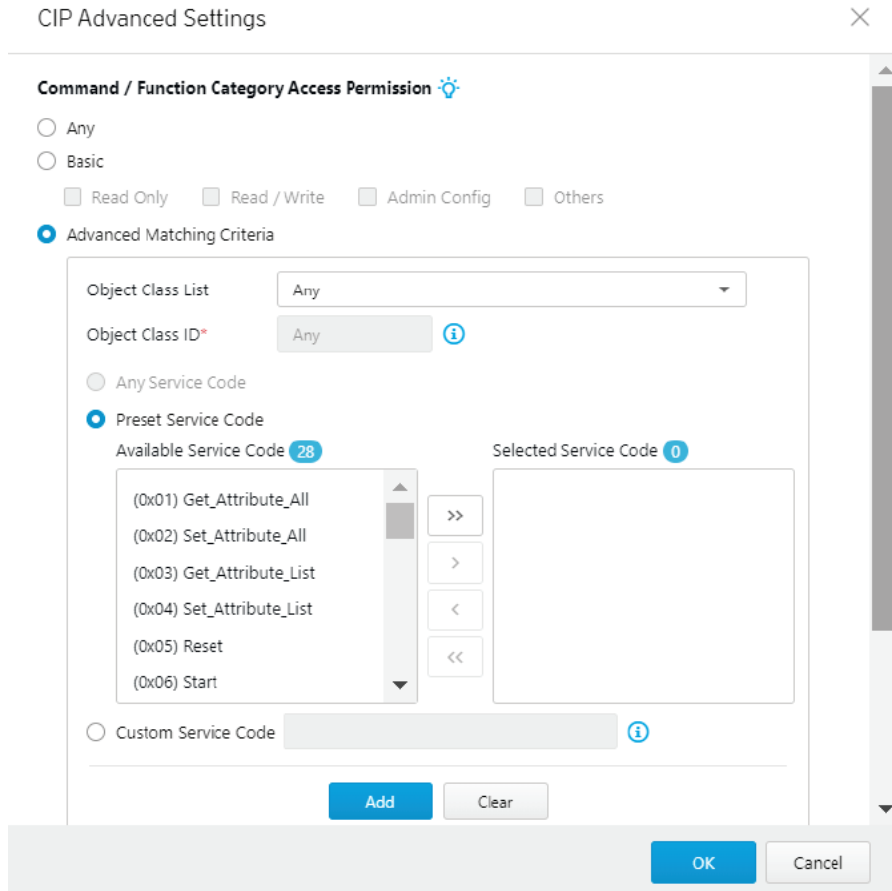
- b. Select the [Modbus] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [Modbus] and select [Advanced Matching Criteria].
 - ii. From the [Function List] drop-down menu, select a function for this protocol.



- iii. If you want to specify a function code by yourself, select [Custom] and enter a function code in the [Function Code] field.
 - iv. Enter a unit ID in the [Unit ID] field.
 - v. Enter the address or address range against which the function will operate.
 - vi. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - vii. Click **OK**.
5. In the [General Protocol] section, select the protocol(s) you want to include in the protocol filter profile.
 6. Click **OK**.

Advanced Settings for the CIP Protocol

The device features more detailed configurations for the CIP ICS protocol. Through the [Advanced Settings] pane, you can further specify the Object Class ID and Service Code against which the function will operate.



Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

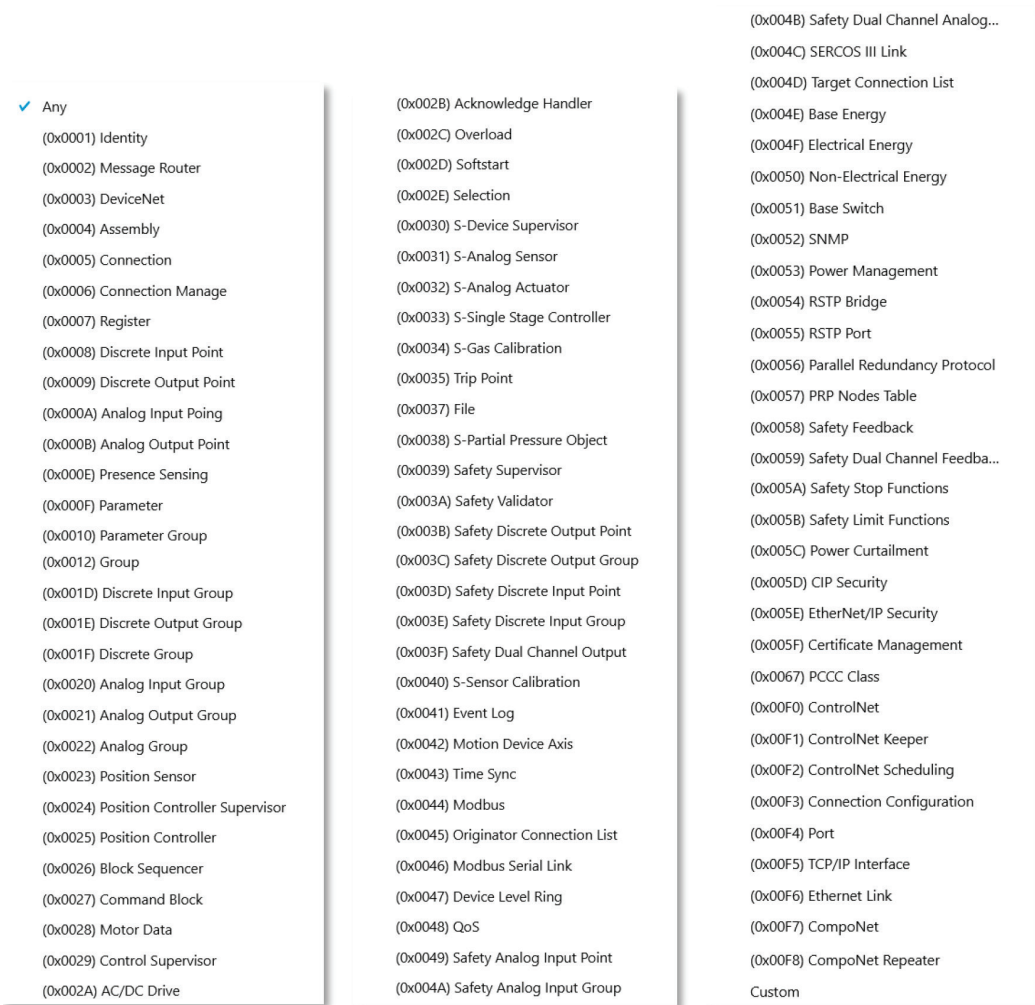
▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

Ok Cancel

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
 - ii. **Basic:** Multiple selections of the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- b. Select the [CIP] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [CIP] and select [Advanced Matching Criteria].
 - ii. From the [Object Class List] drop-down menu, select a function for this protocol.

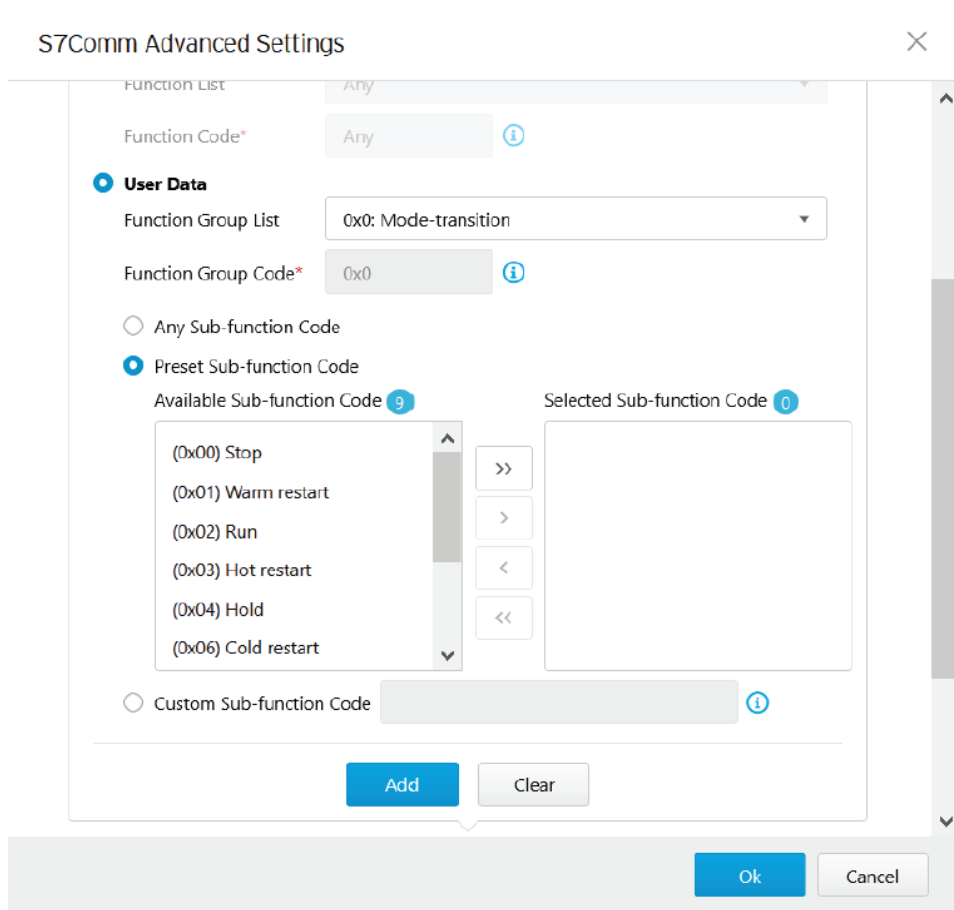


- iii. If you want all service codes within the specified function to be applied, select [Any Service Code].
 - iv. If you want to specify one or more function codes, move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.
 - v. If you want to specify a custom service code, select [Custom Service Code] and enter a service code in the [Custom Service Code] field.
 - vi. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - vii. Click **OK**.
5. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
 6. Click **OK**.

Advanced Settings for S7Comm

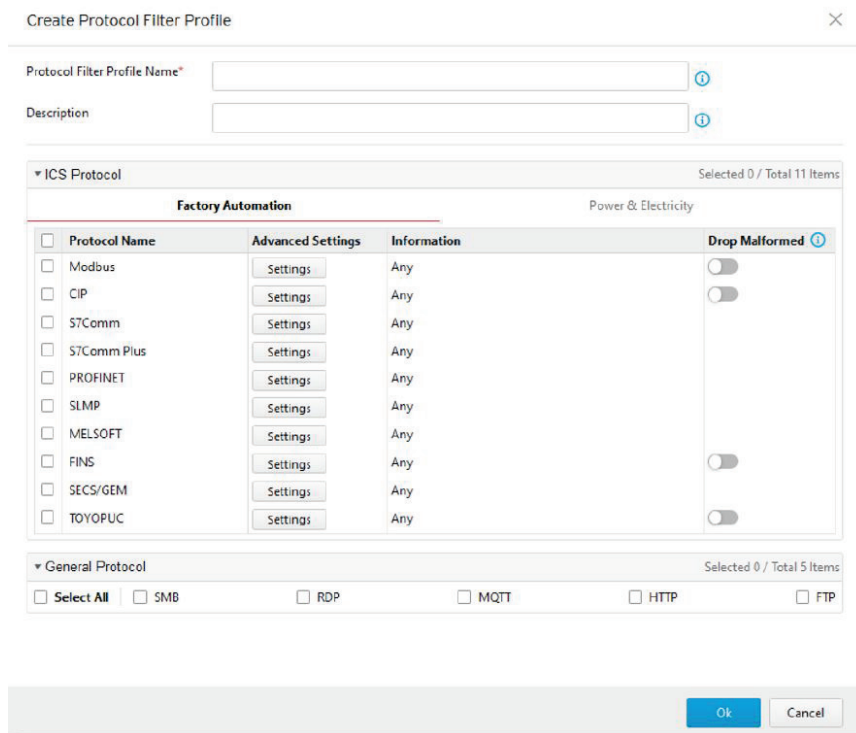
The device features more detailed configurations for the S7Comm ICS protocol. Through the [Advanced Settings] pane, you can further specify the function code, function group code, and sub-function code against which the function will operate.

The screenshot shows the 'S7Comm Advanced Settings' dialog box. It has a title bar with a close button (X) and a scroll bar on the right. The main content is under the 'Advanced Matching Criteria' section, which is selected with a radio button. There are three main sections: 'Job', 'User Data', and 'Sub-function Code'. The 'Job' section has a 'Function List' dropdown set to 'Any' and a 'Function Code*' text box set to 'Any' with an information icon. The 'User Data' section has a 'Function Group List' dropdown set to 'Any' and a 'Function Group Code*' text box set to 'Any' with an information icon. The 'Sub-function Code' section has three radio buttons: 'Any Sub-function Code' (selected), 'Preset Sub-function Code', and 'Custom Sub-function Code'. Below these are two large empty boxes: 'Available Sub-function Code' and 'Selected Sub-function Code', both with a '0' in a blue circle. Between these boxes are four buttons: '>>', '>', '<', and '<<'. At the bottom right, there are 'Ok' and 'Cancel' buttons.



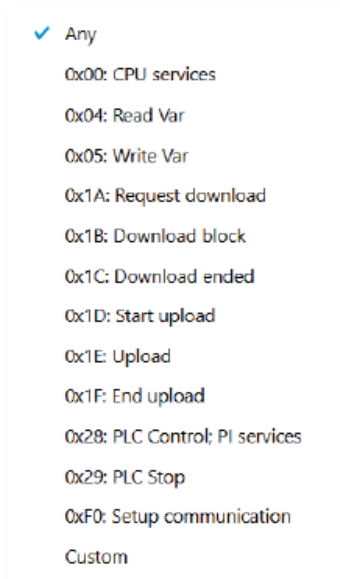
Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
2. Configure the following settings:

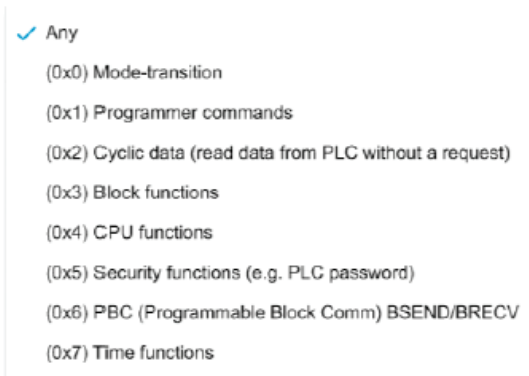


- a. **Protocol Filter Profile Name:** Enter a name for the profile.
- b. (Optional) **Description:** Enter a description for the profile.
3. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
 - ii. **Basic:** Multiple selections of the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. Select the [S7Comm] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [S7Comm] and select [Advanced Matching Criteria].

- ii. If you want to specify a function from the Job category, select the [Job] category and select a function from the [Function List] drop-down menu.



- iii. If you want to specify a function group from Userdata category, select the [Userdata] category and select a function from the [Function Group Code] drop-down menu.



- iv. If you want all sub-function codes within the specified function group code to be applied, select [Any Sub-function Code].
 - v. If you want to specify one or more sub-function codes, select [Preset Sub-function Code] and move the sub-function code(s) from the [Available Sub-function Code] to the [Selected Sub-function Code] field.
 - vi. If you want to specify a custom sub-function, select [Custom Sub-function Code] and enter a sub-function code in the [Custom Sub-function Code] field.
 - vii. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - viii. Click **OK**.
4. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
5. Click **OK**.

Advanced Settings for S7Comm Plus

The device features more detailed configurations for the S7Comm Plus ICS protocol. Through the [Advanced Settings] pane, you can further specify the function code against which the function will operate.

S7Comm Plus Advanced Settings ✕

Command / Function Category Access Permission ⓘ

Any

Basic

Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Function Code list: (0x04B1) Error

Function Code*: 0x04B1 ⓘ

Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No	Function
No data to display		

Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

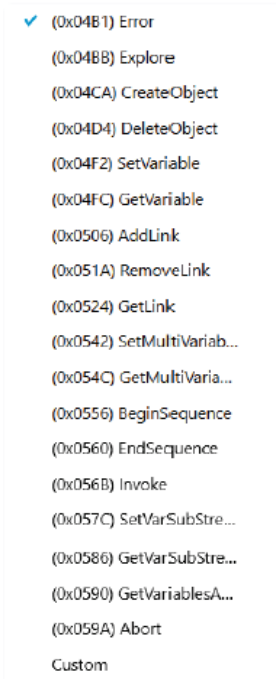
▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

Ok Cancel

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile
4. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
Basic: Multiple selections of the following:
Read Only: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
Read/Write: Read and write commands sent from HMI/EWS/SCADA to PLC.
Admin Config: Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
Others: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- b. Select the [S7Comm Plus] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [S7Comm Plus] and select [Advanced Matching Criteria].
 - ii. From the [Function List] drop-down menu, select a function for this protocol.



- iii. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - iv. Click **OK**.
5. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
6. Click **OK**.

Advanced Settings for SLMP

The device features more detailed configurations for the SLMP ICS protocol. Through the [Advanced Settings] pane, you can further specify the command code against which the function will operate.

SLMP Advanced Settings ✕

Command / Function Category Access Permission ⓘ

Any

Basic

Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Command Code list: (0x0101) Read Type Name ▾

Command Code*: 0x0101 ⓘ

Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No	Command
No data to display		

Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

Ok Cancel

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
 - ii. **Basic:** Select multiple commands from the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- b. Select the [S7Comm Plus] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [SLMP] and select [Advanced Matching Criteria].
 - ii. From the [Command Code List] drop-down menu, select a function for this protocol.



- iii. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - iv. Click **OK**.
5. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
6. Click **OK**.

Advanced Settings for MELSOFT

The device features more detailed configurations for the MELSOFT ICS protocol. Through the [Advanced Settings] pane, you can further specify the command code against which the function will operate.

MELSOFT Advanced Settings

Command / Function Category Access Permission ⓘ

Any

Basic

Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Command Code list: (0x0101) Read CPU Model Name ▼

Command Code*: 0x0101 ⓘ

Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No	Command
No data to display		

Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

Factory Automation Power & Electricity

<input type="checkbox"/> Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

Ok Cancel

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
 - ii. **Basic:** Select multiple commands from the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- b. Select the [MELSOFT] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [MELSOFT] and select [Advanced Matching Criteria].
 - ii. From the [Command Code List] drop-down menu, select a function for this protocol.



- iii. Click **Add**. Repeat the above steps to add more protocol definition entries.
 - iv. Click **OK**.
5. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
6. Click **OK**.

Advanced Settings for TOYOPUC

The device features more detailed configurations for the TOYOPUC ICS protocol. Through the [Advanced Settings] pane, you can further specify the command code, preset sub-command code, and custom sub-command code against which the function will operate.

TOYOPUC Advanced Settings

Command / Function Category Access Permission ⓘ

Any

Basic Setting

Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Command Code List: (0x32) Function Call

Command Code: 0x32 ⓘ

Preset Sub-cmd Code

Available Sub-cmd Code 14

- (0x0000) Reset
- (0x0001) Scan Resumption
- (0x0002) Scan Stop, Stop Break
- (0x0003) Pseudo-Scan Stop, Break
- (0x0011) Reading CPU Status
- (0x0021) Reading Execution Priority Steady State

Selected Sub-cmd Code 0

Custom Sub-cmd Code ⓘ

Add Clear

Total Number of Records: 0 (Max: 32)

No	Command	Sub-cmd
----	---------	---------

OK Cancel

Steps:

1. Go to [Object Profile] > [Protocol Filter Profile].
2. Do one of the following:
 - a. Click **Add** to add a protocol filter profile.
 - b. Click on the name of an existing profile to edit it.
3. Configure the following settings:

Create Protocol Filter Profile

Protocol Filter Profile Name*

Description

▼ ICS Protocol Selected 0 / Total 11 Items

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7Comm Plus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

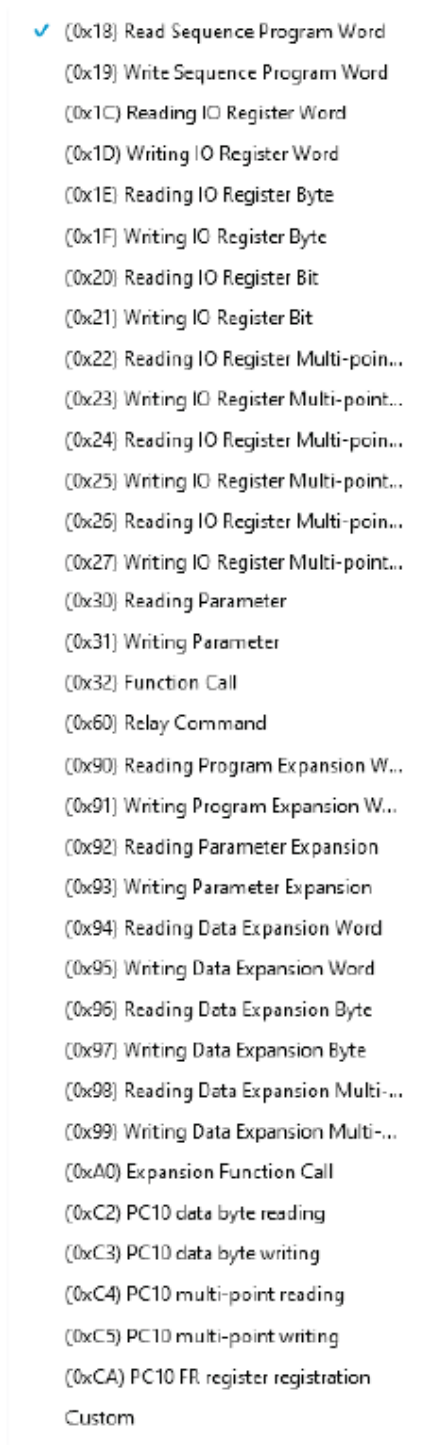
▼ General Protocol Selected 0 / Total 5 Items

Select All SMB RDP MQTT HTTP FTP

Ok Cancel

- a. **Protocol Filter Profile Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - i. **Any:** Specify all available commands or function access in this protocol.
 - ii. **Basic:** Select multiple commands from the following:
 - Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read/Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands from EWS to PLC.
 - Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- b. Select the [TOYOPUC] protocol to configure advanced settings for this protocol:
 - i. Click [Settings] besides [TOYOPUC] and select [Advanced Matching Criteria].
 - ii. From the [Command Code List] drop-down menu, select a function for this protocol.



- iii. If you want to specify one or more sub-command codes, select [Preset Sub-cmd Code] and move the Command code(s) from the [Available Sub-cmd Code] field to the [Selected Sub-cmd Code] field.
- iv. If you want to specify a custom sub-command code, select [Custom Sub-cmd Code] and input a service code in the [Custom Sub-cmd Code] field.
- v. Click **Add**. Repeat the above steps to add more protocol definition entries.
- vi. Click **OK**.



NOTE

The [Preset Sub-cmd code] and [Custom Sub-cmd] functions do not support all command codes. Only the "(0x32) Function Call" and "(0xA0) Expansion Function Call" command codes are supported.

5. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
6. Click **OK**.

Configuring IPS Profiles

An IPS profile contains more sophisticated pattern rules for more granular control and can be applied to policy rules. The following can items be configured in an IPS profile:

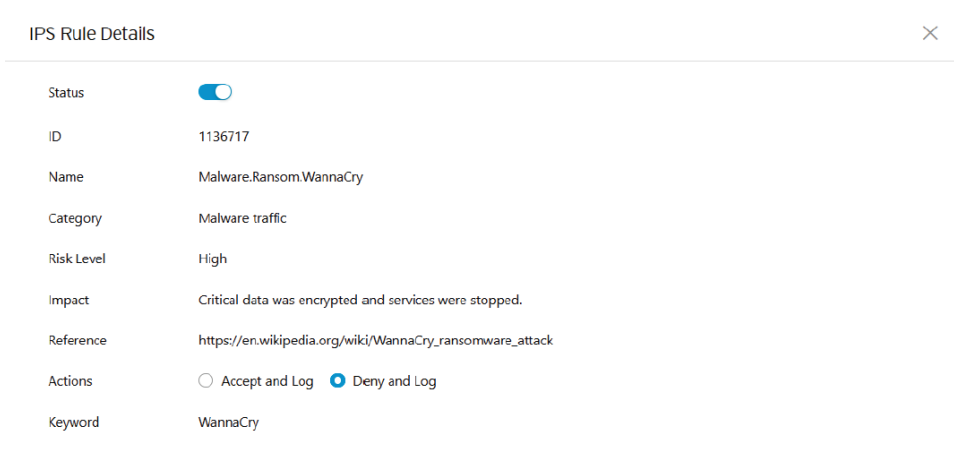
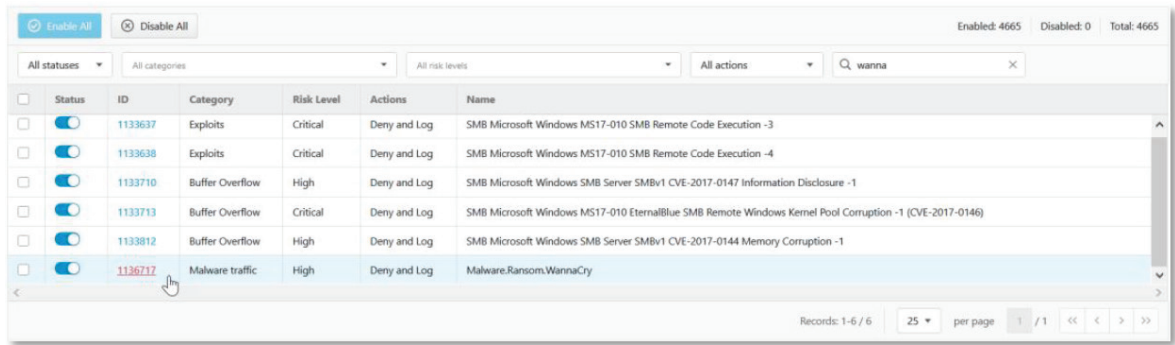
- The IPS protocol category details:
 - File Vulnerabilities
 - Buffer Overflow
 - Exploits
 - Malware Traffic
 - Reconnaissance
 - Web Threats
 - ICS Threats
 - Others
- The IPS protocol risk level:
 - Information
 - Medium
 - High
 - Critical
- The default action for IPS patterns:
 - All Actions
 - Accept and Log
 - Deny and Log

Object Profiles > IPS Profile

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	IPS_Rule_1	For OT Asset Protection
<input type="checkbox"/>	IPS_Rule_2	For HMI Asset Protection

<

When configuring an IPS pattern rule, you can specify the rule's default action and add it to the IPS profile.



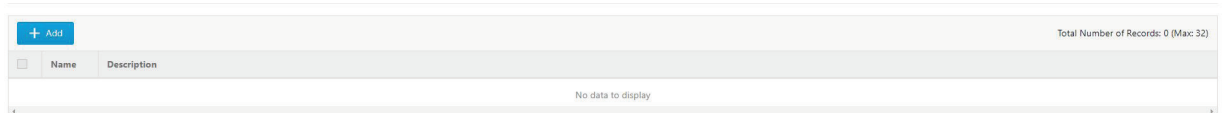
Refer to the table below for an overview of each field.

Task	Action
Status	The operational status of the pattern rule
ID	The pattern rule ID
Name	The pattern name of the intrusion
Category	The threat category of the intrusion
Risk Level	The suggested security level for the intrusion
Impact	The expected impact the intrusion will have on the target network device if the intrusion succeeds
Reference	The vulnerability ID of the intrusion (e.g. CVE-2017-0147)
Actions	The preset action when responding to intrusion
Keyword	The keyword(s) used for searching the pattern rule

Steps:

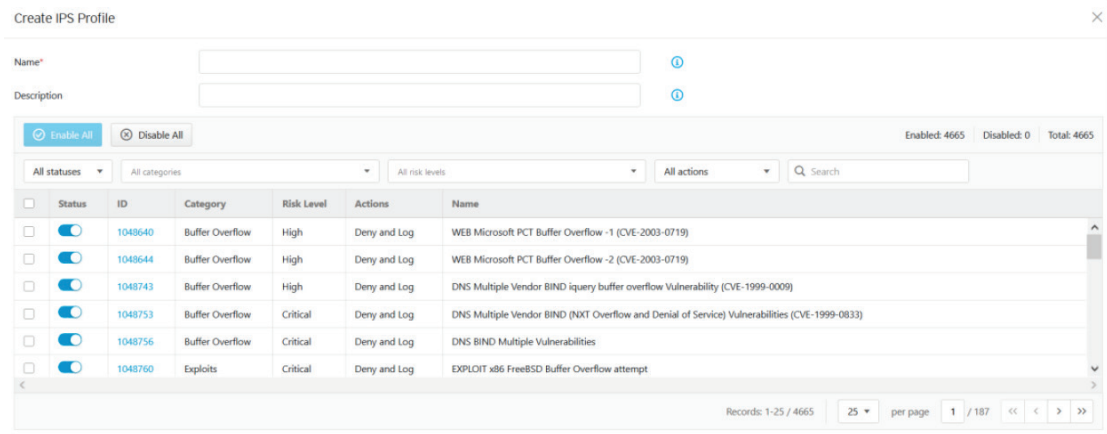
1. Go to [Object Profile] > [IPS Profile].

Object Profiles > IPS Profile

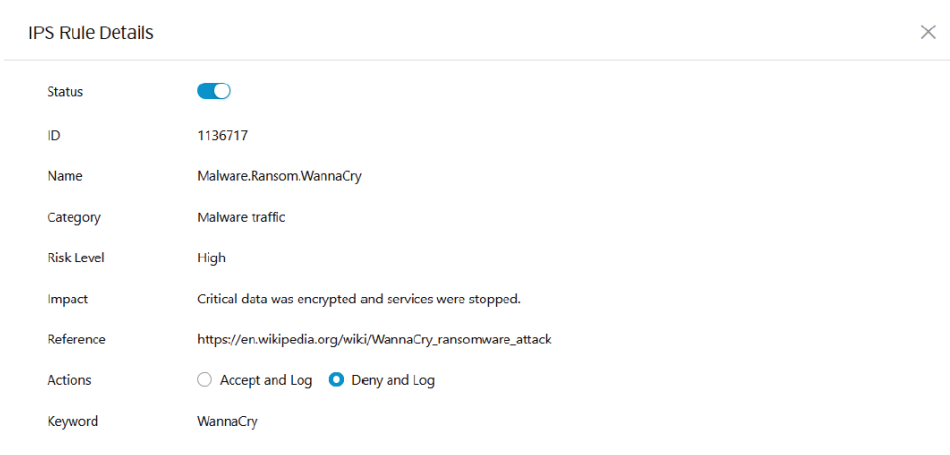


2. Click **Add** to add an IPS profile.
The [Create IPS Profile] screen will appear.

3. Configure the following settings:



- a. **Name:** Enter a name for the profile.
 - b. (Optional) **Description:** Enter a description for the profile.
4. Select the pattern rule you want to configure by clicking the rule ID. The [IPS Rule Details] screen will appear.
5. Configure the following settings:



- a. **Status:** Enable or disable the pattern rule.
 - b. **Actions:** Select the pattern rule's default action
 - i. **Accept and Log:** When an intrusion is detected, the intrusion will be accepted and logged for monitoring.
 - ii. **Deny and Log:** When an intrusion is detected, the intrusion will be rejected and logged for monitoring.
6. When you are done configuring the pattern rule, click **Save**.

9. The Security Screens

This chapter describes the cybersecurity and policy enforcement features.

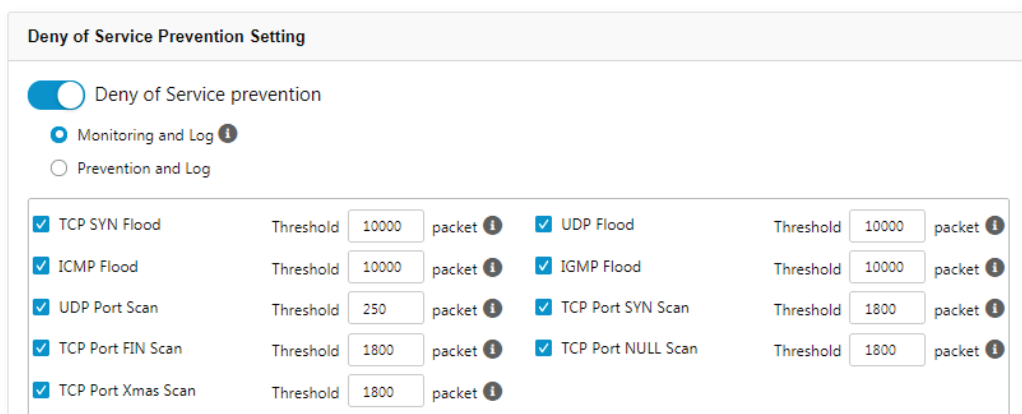
Cybersecurity

This device features cybersecurity mechanisms, which cover both intrusion prevention and denial of service (Dos) attack prevention. The signature rules of intrusion prevention are called DPI (Deep Packet Inspection) patterns. These patterns can be regularly updated through SDC or by manually importing new patterns via the device's web management UI.

Configuring Cybersecurity – Denial of Service Prevention

Steps:

1. Go to [Security] > [Cyber Security].
The [Denial of Service Prevention] screen will appear.



Rule Name	Threshold	Unit	Enabled
TCP SYN Flood	10000	packet	Yes
ICMP Flood	10000	packet	Yes
UDP Port Scan	250	packet	Yes
TCP Port FIN Scan	1800	packet	Yes
TCP Port Xmas Scan	1800	packet	Yes
UDP Flood	10000	packet	Yes
IGMP Flood	10000	packet	Yes
TCP Port SYN Scan	1800	packet	Yes
TCP Port NULL Scan	1800	packet	Yes

2. Use the toggle to enable or disable the Denial of Service prevention feature.
3. Select the default action if the feature is enabled:
 - a. **Monitoring and Log:** The IEF-G9010 device will actively monitor and log DoS attacks but will not act.
 - b. **Prevention and Log:** The IEF-G9010 device will detect, block, and log DoS attacks.
4. Check the DoS prevention rules to enable.
5. (Optional) Configure the threshold values of the enabled DoS service rules.
6. Click **Save**.



NOTE

Flood/Scan Attack Protection rules utilize the detection period and threshold mechanisms to detect an attack. During a detection period (typically every 5 seconds), if the number of anomalous packets reaches the specified threshold, an attack detection occurs. If the rule action is set to **Prevention and Log**, the security node blocks subsequent anomalous packets until the end of the detection period. After the detection period, the security node will continue to allow anomalous packets to go through until the threshold is reached again.

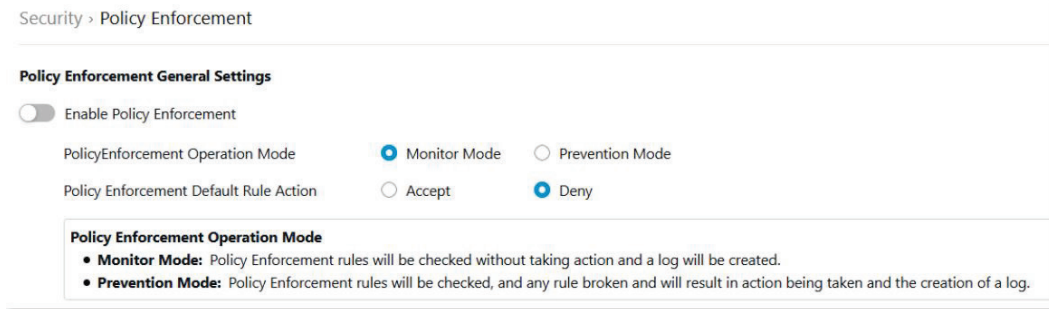
Policy Enforcement

Policy enforcement allows you to define custom protocol rules that match to an industrial protocol and will subsequently allow or deny traffic matching these protocol rules.

Configuring Policy Enforcement

Steps:

1. Go to [Security] > [Policy Enforcement].
The [Policy Enforcement General Setting] screen will appear.



2. Use the toggle to enable or disable the Policy Enforcement feature.
3. Select the operation mode if the feature is enabled:
 - a. **Monitor Mode:** The IEF-G9010 detects and logs abnormal protocol access to OT assets but does not block network attacks.
 - b. **Prevention Mode:** The IEF G-9010 detects, blocks, and logs abnormal access to OT assets.
4. Using the [Policy Enforcement Default Rule Action] radio buttons, select a default action for when no pattern is matched.

The following table summarizes the settings:

Mode (Policy Enforcement)	Action Performed
Monitor Mode	<ul style="list-style-type: none">• Detect and monitor abnormal protocol access to OT assets, without blocking network attacks.• Generate logs.
Prevention Mode	<ul style="list-style-type: none">• Block abnormal protocol access to OT assets.• Generate logs.

Adding Policy Enforcement Rules (For Gateway Mode Only)



Note

Before creating policy enforcement rules, make sure the required objects and profiles are created.

- **IP object profiles:** For more information, see [Configuring IP Object Profiles](#).
- **Service object profiles:** For more information, see [Configuring Service Object Profiles](#).
- **Protocol filter profiles:** For more information, see [Configuring Protocol Filter Profiles](#).

Steps:

1. Go to [Security] > [Policy Enforcement].
The [Policy Enforcement Rule List] screen will appear.

Policy Enforcement Rule List

Maximum Number of Records: 512

<input type="checkbox"/>	Rule No	Status	Rule Name	Source IP / Object	Source IP/ Object Info	Destination IP / Object	Destination IP/ Object Info	Service Object Profile	Service List Info	VLAN	Action
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Rule_1	Any	Any	Any	Any	Any	Any	Disabled	Deny
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Rule_2	Any	Any	Any	Any	Any	Any	Disabled	Advanced

Records: 1-2 / 2 25 per page 1 / 1 << < > >>

2. Click the **Add** button to add a new policy rule. The [Create Policy Enforcement Rule] screen will appear.

Create Policy Enforcement Rule

Status

Rule Name*

Description

Direction Selection

Interface Direction

Source and Destination Selection

Source IP / IP Object Profile

Destination IP / IP Object Profile

Service Object Selection

Service Object

Action Accept Deny Advanced Filter

3. Configure the following settings:
 - a. **Status**: Click to toggle to enable or disable the rule.
 - b. **Rule Name**: Enter a name for the rule.
 - c. (Optional) **Description**: Enter a description for the rule.
4. In the [Direction Selection] section, configure the following settings:
 - a. Select the network traffic direction between interface from the drop-down menu.
 - i. Any
 - ii. WAN to LAN
 - iii. LAN to WAN
 - iv. WAN to DMZ
 - v. DMZ to WAN
 - vi. LAN to DMZ
 - vii. DMZ to LAN
 - viii. LAN to LAN



NOTE

The network interfaces listed in the drop-down menu do not correspond with specific network interfaces on the device. Instead, these refer to types of interfaces. For example, if you select [WAN to LAN], the policy enforcement rule will apply to traffic from the WAN1 interface to the LAN1 interface or from the WAN1 interface to the LAN2 interface. If you select [LAN to LAN], then the policy enforcement rule will apply to traffic from the LAN1 interface to the LAN2 interface or from the LAN2 interface to the LAN1 interface.



NOTE

If you select **Any**, the policy enforcement rule will apply to traffic from all network interfaces.

5. In the [Source and Destination Selection] section, configure the following settings:
 - a. Select the source and destination IP or IP object profile from the drop-down menu.
 - i. Any
 - ii. Single IP
 - iii. IP Range
 - iv. IP Subnet
 - v. Object



NOTE

If you select **Object**, you will need to select the IP object from a previously created IP object profile.

6. In the [Service Object Selection] section, configure the following settings:
 - a. Select the Layer 4 criteria from the drop-down menu.
 - i. TCP: Specify the port range for this protocol.
 - ii. UDP: Specify the port range for this protocol.
 - iii. ICMP: Specify the type and code for this protocol.
 - iv. Custom: Specify the protocol number for this protocol as defined in the Internet protocol suite.
 - v. Service Object



NOTE

If you select **Service Object**, you will need to select the service object from a previously created service object profile.

7. In the [Action] section, configure the following settings:
 - a. Select the rule action.
 - i. Accept: Allow network traffic that matches this rule.
 - ii. Deny: Block network traffic that matches this rule.
 - iii. Advanced Filter: The node will act based on the selected protocol filter and protocol filter action.
8. Click **Save** to save the configuration.



NOTE

Policy enforcement rules in Gateway Mode only work on the network interface level, not on the physical port level. Policy enforcement rules cannot inspect the traffic between the physical ports under the same network interface.

Adding Policy Enforcement Rules (For Bridge Mode Only)



Note

Before creating policy enforcement rules, make sure the required objects and profiles are created.

- **IP object profiles:** For more information, see [Configuring IP Object Profiles](#).
- **Service object profiles:** For more information, see [Configuring Service Object Profiles](#).

- **Protocol filter profiles:** For more information, see [Configuring Protocol Filter Profiles](#).

Steps:

1. Go to [Security] > [Policy Enforcement].
The [Policy Enforcement Rule List] screen will appear

Policy Enforcement Rule List Maximum Number of Records: 512

<input type="checkbox"/>	Rule No.	Status	Rule Name	Source IP / Object	Source IP / Object Info	Destination IP / Object	Destination IP / Object Info	Service Object Profile	Service List Info	VLAN	Action	Pro
No data to display												

2. Click the **Add** button to add a new policy rule.

Create Policy Enforcement Rule

Status

Rule Name*

Description

Source and Destination Selection

Source IP / IP Object Profile

Destination IP / IP Object Profile

Service Object Selection

Service Object

VLAN ID

Action Accept Deny Advanced Filter

3. Configure the following settings:
 - a. **Status:** Click the toggle to enable or disable the rule.
 - b. **Rule Name:** Enter a name for the rule.
 - c. (Optional) **Description:** Enter a description for the rule.
4. In the [Source and Destination Selection] section, configure the following settings:
 - a. Select the source and destination IP or IP object profile from the drop-down menu.
 - i. Any
 - ii. Single IP
 - iii. IP Range
 - iv. IP Subnet
 - v. IP Object



NOTE

If you select **Object**, you will need to select the IP object from a previously created IP object profile.

5. In the [Service Object Selection] section, configure the following settings:
 - a. Select the Layer 4 criteria from the drop-down menu.
 - i. TCP: Specify the port range for this protocol.
 - ii. UDP: Specify the port range for this protocol.
 - iii. ICMP: Specify the type and code for this protocol.
 - iv. Custom: Specify the protocol number for this protocol as defined in the Internet protocol suite.
 - v. Service Object



NOTE

If you select **Service Object**, you will need to select the service object from a previously created service object profile.

6. Click the VLAN ID toggle to enable or disable VLAN ID tagging. If enabled, enter one or multiple VLAN IDs.



NOTE

Each policy enforcement rule supports up to 5 VLAN IDs.

7. In the [Action] section, configure the following settings:
 - a. Select the rule action.
 - i. Accept: Allow network traffic that matches this rule.
 - ii. Deny: Block network traffic that matches this rule.
 - iii. Advanced Filter: The node will act based on the selected protocol filter and protocol filter action.

The screenshot shows the 'Action' configuration section of a network device. At the top, there are three radio buttons for selecting the rule action: 'Accept', 'Deny', and 'Advanced Filter'. The 'Advanced Filter' option is selected. Below this, there are two main sections, each with a toggle switch and a dropdown menu. The first section is 'Protocol Filter Profile Selection', which is toggled on. It contains a 'Protocol Filter Profile' dropdown menu with the text 'Please select a profile'. The second section is 'Protocol Filter Action', which is also toggled on. It contains a 'Protocol Filter Action' dropdown menu with radio buttons for 'Accept' and 'Deny', where 'Deny' is selected. Below this is the 'IPS Profile' section, which is toggled on. It contains an 'IPS Profile' dropdown menu with the text 'Please select a profile'.

8. Click **Save** to save the configuration.

Managing Policy Enforcement Rules

The following table lists the common tasks that are used to manage the policy enforcement rules.

Task	Action
To delete a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the Delete button.
To duplicate a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the Copy button.
To edit a policy enforcement rule	Click the name of the rule and the [Edit Policy Rule] windows will appear.
To change the priority of a policy enforcement rule	Click the check box in front of the policy enforcement rule, click the Change Priority button, and specify a new priority for this rule.



NOTE

When more than one policy enforcement rule is matched, the IEF-G9010 Series takes the action of the rule with the highest priority and ignores the rest of the rules. The rules are listed in the table by priority with the highest priority rule listed in the top row of the table.

10. The Pattern Screens

This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the IEF-G9010 Series device.

The DPI pattern contains signatures to enable the intrusion prevention feature on the device. The intrusion prevention feature detects and prevents behaviors related to network intrusion attempts or targeted attacks at the network level.

Viewing Device Pattern Information

Steps:

1. Go to [Pattern] > [Pattern Update].
The [Pattern Update] screen will appear.
2. The [Device Pattern Information] pane will show the [Current Pattern Version] and [Pattern Build Date].

Device Pattern information	
Pattern Version:	MX_200120_14
Pattern Build Date:	2020-01-20T06:45:02Z

Manually Updating the Pattern

Steps:

1. Go to [Pattern] > [Pattern Update].
The [Pattern Update] screen will appear.
2. Click **Select** and navigate to the pattern file.
3. Click **Upload** to deploy the pattern to the device.

Pattern Update	
Manually Update	
Pattern File Path	<input type="text"/>
	<input type="button" value="Select"/> <input type="button" value="Upload"/>

4. Click **OK**.



NOTE

The patterns can be downloaded at <https://netsecuritylicense.moxa.com>.



NOTE

SDC can only keep a maximum of 5 versions of each pattern. When exceeded, you will need to manually manage which version(s) to keep.

11. The Log Screens

This chapter describes the system event logs and security detection logs you can view from the management console.

Viewing Cybersecurity Logs

The cybersecurity logs include logs detected by both the intrusion prevention and denial of service prevention features.

Steps:

1. Go to [Logs] > [Cyber Security Logs].

The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Event ID	The ID of the matched signature.
Security Category	The category of the matched signature.
Security Severity	The severity level assigned to the matched signature.
Security Rule Name	The name of the matched signature.
Direction	The direction flow of the connection.
Interface	The network interface which received the connection.
Attacker	The IP address of the host device that initiated the cyberattack.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection.
Destination MAC Address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.
Count	The number of detected network packets within the detection period after the detection threshold was reached.

Viewing Policy Enforcement Logs

The policy enforcement logs cover logs created when policy enforcement rules are triggered based on the configured rule setting (allow, deny, or protocol filter profile).

Steps:

1. Go to [Logs] > [Policy Enforcement Logs].

The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Direction	The direction flow of the connection.
Interface	The network interface which received the connection.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection if the selected protocol is TCP/UDP. The ICMP type if the selected protocol is ICMP.
Destination MAC Address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection if the selected protocol is TCP/UDP. The ICMP type if the selected protocol is ICMP.
VLAN ID	The VLAN ID of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.

Viewing Protocol Filter Logs

The protocol filter logs cover logs detected by the [Protocol Filter] feature. Protocol filters are advanced [Policy Enforcement] configurations.

Steps:

1. Go to [Logs] > [Protocol Filter Logs].

The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
Direction	The direction flow of the connection.
Interface	The network interface which received the connection.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection if the selected protocol is TCP/UDP. The ICMP type if the selected protocol is ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection if the selected protocol is TCP/UDP. The ICMP type if the selected protocol is ICMP.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No	The command or the function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing Asset Detection Logs

The asset detection logs cover system status changes of managed assets.

Steps:

1. Go to [Logs] > [Assets Detection Logs].

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Event Type	The log event description.
Interface	The network interface which received the asset information.
Asset MAC Address	The source MAC address of the asset.
Asset IP Address	The source IP address of the asset.

Viewing System Logs

System logs record details about system events occurring on the device.

Steps:

1. Go to [Logs] > [System Logs].

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Severity	The severity level of the log.
Message	The log event description.

12. The Administration Screens

This chapter describes the administrative settings for the IEF-G9010 Series device.

Account Management



NOTE

Log in to the management console using the default administrator account ("admin") to access the Accounts screens.

The system uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to user accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users can log in to the management console using custom user accounts.

The following table outlines the tasks available on the [Account Management] screen.

Task	Description
Add account	Click Add to create a new user account. For more information, see Adding a User Account .
Delete existing accounts	Select one or more existing user accounts and click Delete .
Edit existing accounts	Click on the name of an existing user account to view or modify the current account settings.

User Roles

The following table describes the permissions matrix for user roles.

Configuration Screen	Action	User Roles			
		Admin	Operator	Visitor	Auditor
System	View	Yes	Yes	Yes	Yes
	All operations	Yes	Yes	Yes	Yes
Visibility	View	Yes	Yes	Yes	No
	All operations	Yes	Yes	Yes	No
Device	View	Yes	Yes	No	No
	All operations	Yes	No	No	No
Object Profiles	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Security	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Pattern	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Logs (excluding Audit Log)	View	Yes	Yes	Yes	No
Audit Log	View	No	No	No	Yes
Administration	View	Yes	No	No	No
	All operations	Yes	No	No	No

Built-in User Accounts

The following table lists the built-in user accounts on the device.

Built-in Account ID	Default Password	User Role
admin	moxa	Admin
auditor	moxa	Auditor



NOTE

The built-in user accounts cannot be deleted.



NOTE

For security reasons, it is highly recommended to change the password of the built-in accounts when logging in for the first time.

Adding a User Account

When you log in using the administrator account ("admin"), you can create additional user accounts to access the system.

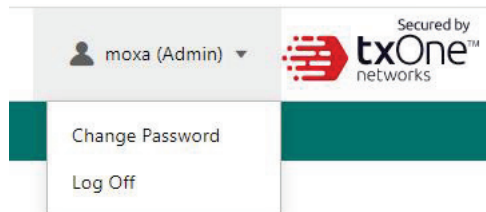
Steps:

1. Go to [Administration] > [Account Management].
2. Click **Add**.
The [Add User Account] screen will appear.
3. Configure the following settings:
 - a. **ID**: Enter the user ID used to log in to the management console.
 - b. **Name**: Enter the name of the user of this account.
 - c. **Password**: Enter the account password.
 - d. **Confirm Password**: Enter the account password again to confirm.
 - e. **Role**: Select a user role for this account. For more information, see [User Roles](#).
4. Click **Save**.

Changing Your Account Password

Steps:

1. On the management console banner, click your account name.



2. Click **Change Password**.
The [Change Password] screen will appear.
3. Configure the following settings:
 - a. **Old password**: Enter your current password.
 - b. **New password**: Enter your new password.
 - c. **Confirm password**: Enter your new password again.
4. Click **Save**.

Configuring Password Policy Settings

The IEF-G9010 Series provides the following password policy settings to enhance web console access security:

- Password complexity

Password complexity settings are used to enforce stronger passwords. For example, you can require users to create passwords that must be at least eight characters long and must contain a combination of both uppercase and lowercase letters, numbers, and symbols.



NOTE

When password complexity settings are configured and a user creates a new password, the system will determine if the password meets the specified requirements. While strict password policies improve security, they may sometimes increase the cost to an organization when users create passwords that are too difficult to remember. Users may call the help desk when they forget their passwords or keep passwords in easily accessible locations where they are vulnerable to theft. When establishing a password policy, consider balancing the need for strong security with manageability for users.

Steps:

1. Go to [Administration] > [Account Management].
2. Click the [Password Policy] tab.
The [Password Policy] screen will appear.
3. Select the option(s) to apply to the password policy.

The screenshot shows a dialog box titled "Password Policy" with a close button (X) in the top right corner. The dialog contains the following settings:

- Minimum password length: (8 - 32)
- Must not include user's account ID
- Must not include user's account name
- Include at least one uppercase letter (A - Z)
- Include at least one lowercase letter (a - z)
- Include at least one number (0 - 9)
- Include at least one non-alphanumeric character (~!@#\$%^&*_-+=`\|0{};'"<>.,?/)
- New password must not be the same as the last password

At the bottom right of the dialog, there are two buttons: "Confirm" (highlighted in blue) and "Cancel".

4. Click **Confirm**.

System Management

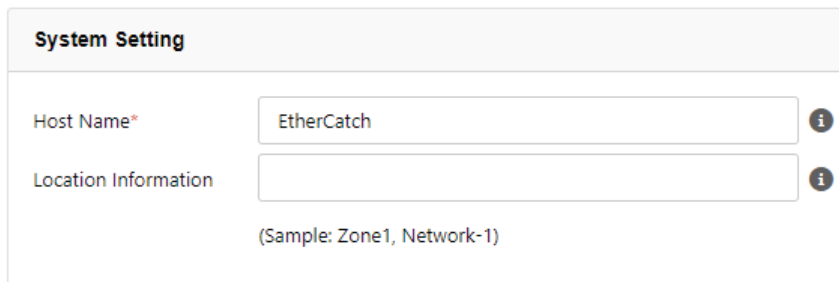
Use the [System Management] screens to do the following:

- Configure the host name and location information of the device.
- Configure the IP addresses that are allowed to manage the device.
- Choose the protocols and ports that can be used to manage the device.

Configuring the Device Name and Device Location Information

Steps:

1. Go to [Administration] > [System Management].
2. In the [System Setting] pane, enter the host name and location information for the device.

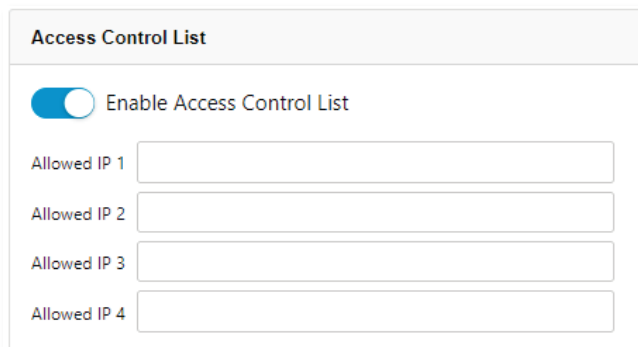


The screenshot shows the 'System Setting' configuration pane. It has a title bar 'System Setting'. Below it, there are two input fields. The first is labeled 'Host Name*' and contains the text 'EtherCatch'. The second is labeled 'Location Information' and is empty. Both fields have an information icon (i) to their right. Below the fields, there is a sample text: '(Sample: Zone1, Network-1)'.

Configuring the Management Client Access Control List

Steps:

1. Go to [Administration] > [System Management].
2. In the [Access Control List] pane, configure the following setting:



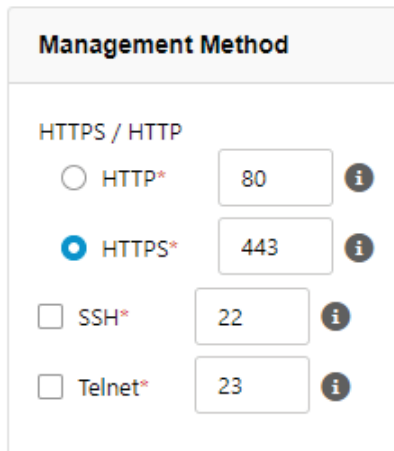
The screenshot shows the 'Access Control List' configuration pane. It has a title bar 'Access Control List'. Below it, there is a toggle switch labeled 'Enable Access Control List' which is currently turned on. Below the toggle, there are four input fields labeled 'Allowed IP 1', 'Allowed IP 2', 'Allowed IP 3', and 'Allowed IP 4', all of which are empty.

- a. Use the toggle to enable or disable access control for the specified management clients.
- b. Provide the IP address(es) that are allowed to manage the device.

Configuring Management Protocols and Ports

Steps:

1. Go to [Administration] > [System Management].
2. In the [Management Method] pane, configure the following settings:



The screenshot shows the 'Management Method' configuration pane. It has a title bar 'Management Method' and a section header 'HTTPS / HTTP'. Below this, there are four rows of settings, each with a radio button or checkbox, a protocol name, a port number input field, and an information icon (i). The first row is 'HTTP*' with port '80'. The second row is 'HTTPS*' with port '443'. The third row is 'SSH*' with port '22'. The fourth row is 'Telnet*' with port '23'. The 'HTTPS*' radio button is selected.

- a. Select the protocols that are allowed to be used to access the device.
- b. Enter the protocol port numbers.



NOTE

The HTTP and HTTPS protocols are used for connecting to the web management console. The SSH and Telnet protocols are used for connecting to the command line interface (CLI).

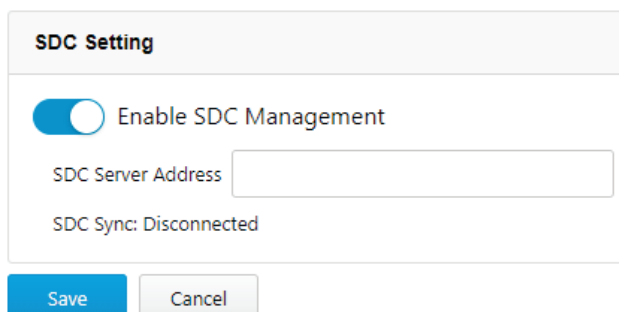
The Sync Setting Screen

The IEF-G9010 Series can be managed by Moxa's SDC (Security Dashboard Console). Use this screen to register the IEF-G9010 Series to an SDC instance.

Enabling SDC Management

Steps:

1. Go to [Administration] > [Sync Setting].
2. In the [SDC Setting] pane, configure the following settings:



The screenshot shows the 'SDC Setting' configuration pane. It has a title bar 'SDC Setting'. Below this, there is a toggle switch for 'Enable SDC Management' which is currently turned on. Below the toggle is an input field for 'SDC Server Address'. Below that, it says 'SDC Sync: Disconnected'. At the bottom, there are two buttons: 'Save' and 'Cancel'.

- a. Use the toggle to enable or disable SDC management.
- b. Enter the IP address of the SDC server.

The Syslog Screen

The IEF-G9010 Series maintains Syslog events that provide a summary of security and system events in Common Event Format (CEF).

Configure the Syslog settings to enable the device to send system logs to a Syslog server.

Configuring Syslog Settings

Steps:

1. Go to [Administration] > [Syslog].
The [Syslog Settings] screen will appear.
2. Configure the following settings:

Syslog Settings

Send logs to a syslog server

Server address:
1.2.3.4

Port:
514

Protocol:
 TCP UDP

Facility Level:
local 4

Log Level:
INFO

Available logs:

Selected logs:
CYBER_SECURITY_LOG
PROTOCOL_FILTER_LOG
POLICY_ENFORCEMENT_LOG
ASSET_LOG
SYSTEM_LOG

- a. Check **Send logs to a syslog server** to enable the syslog server.
 - b. **Server address**: Enter the syslog server address.
 - c. **Port**: Enter the syslog server port.
 - d. **Protocol**: Select the communication protocol.
 - e. **Facility Level**: Select a facility level to determine the source and priority of the logs.
 - f. **Log Level**: Select a syslog severity level. The device will only send logs of the selected severity level or higher to the syslog server. For more information, see [Syslog Severity Levels](#).
 - g. **Available Logs/Selected Logs**: From the Available Logs box, select which types of logs will be sent to the syslog server.
3. Click **Save**.

Syslog Severity Levels

The syslog severity level specifies the type of messages to be sent to the syslog server.

Level	Severity	Description
0	Emergency	Complete system failure. Take immediate action.
1	Critical	Primary system failure. Take immediate action.
2	Alert	Urgent failures. Take immediate action.
3	Error	Non-urgent failures. Resolve issues quickly.
4	Warning	Error pending. Take action to avoid errors.
5	Notice	Unusual events. Immediate action is not required.
6	Information	Normal operational messages useful for reporting, measuring throughput, and other purposes. No action is required.
7	Debug	Useful information when debugging the application. Note: Setting the debug level can generate a large amount of Syslog traffic in a busy network. Use with caution.

Syslog Severity Level Mapping Table

Policy Enforcement / Protocol Filter Action	Cybersecurity Severity Level	Syslog Severity Level
		0 - Emergency
	Critical	1 - Critical
	High	2 - Alert
		3 - Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

The System Time Screen

The Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system time.

Configuring System Time

Steps:

1. Go to [Administration] > [System Time].

Administration > System Time

Date and Time

Current Time: 2019-10-22T14:54:13+08:00

Synchronize system time with an NTP server

NTP Server: (Default time server: pool.ntp.org)

Time Zone

Time Zone:

2. In the [Date and Time] pane, do one of the following:
 - a. Synchronize the system time with an NTP server.
 - i. Check the **Synchronize system time with an NTP server** box.
 - ii. Specify the domain name or IP address of the NTP server.
 - iii. Click **Synchronize now**.
 - b. Manually set the system time.
 - i. Click the calendar to select the date and time.
 - ii. Set the hour, minute, and second.
 - iii. Click **Apply**.
3. From the [Time Zone] drop-down list, select the time zone.
4. Click **Save**.



NOTE

SDC synchronizes the system time with its managed instances.

The Back Up/Restore Screen

You can export settings from the management console to back up the configuration of your IEF-G9010 Series device. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

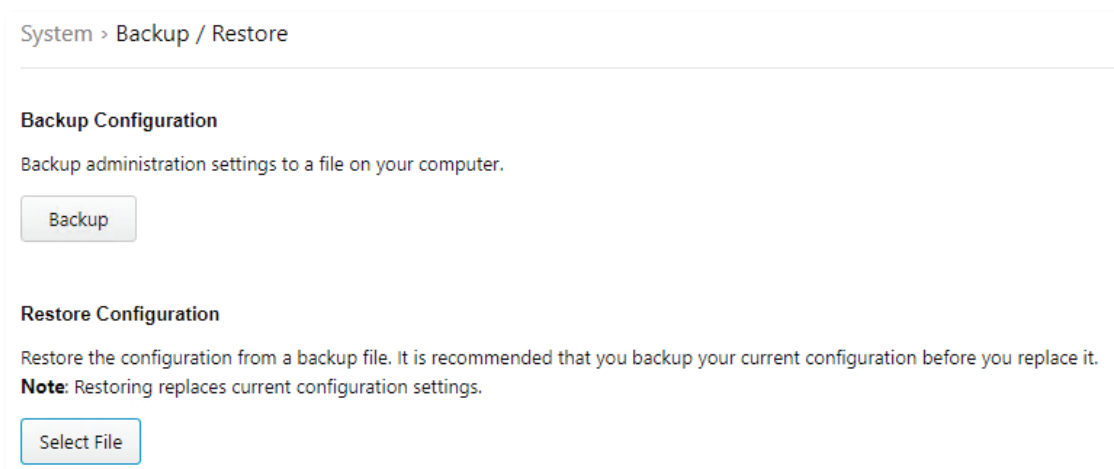
We recommend the following actions:

- Always back up the current configuration before importing a configuration file.
- Import or export configurations while the IEF-G9010 Series is idle, as this will affect the device's performance.

Backing Up a Configuration

Steps:

1. Go to [Administration] > [Back Up / Restore]. The [Backup / Restore] screen will appear.



2. Click **Backup**. The system will automatically create and save a configuration backup file to your computer.

Restoring a Configuration

Steps:

1. Go to [Administration] > [Back Up / Restore].
2. In the [Restore Configuration] section, click **Select File** and navigate to the configuration backup file you want to import. All services will restart. This process may take some time.

The Firmware Management Screen

Use the [Firmware Management] screen to:

- View the firmware information of the device.
- Upgrade the device firmware.

Viewing Device Firmware Information

Steps:

1. Go to [Administration] > [Firmware Management].
2. The [Firmware Management] pane shows information for the two partitions including [Partition #], [Partition Name], [Partition Status], [Firmware Version], and [Firmware Build Date].

No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Standby	IEC_G02_0.9.2	2019-12-16T13:14:05Z	
2	boot2	Running	IEC_G02_1.0.5	2020-02-05T07:16:40Z	



NOTE

The IEF-G9010 Series can have up to two firmware versions installed at any time. Each firmware is installed on its own separate partition. At any given point in time, one partition will be designated as [Running], which indicates it is the currently active firmware. The other partition will have the [Standby] status, acting as the standby partition. To make the standby firmware the running firmware, refer to [Rebooting and Applying Firmware](#) for more information.

Updating the Firmware

Steps:

1. Go to [Administration] > [Firmware Management].



NOTE

When upgrading the firmware, the firmware will always be installed to the [Standby] partition. Therefore, firmware upgrading is only available for the [Standby] partition.

2. Click the **Upgrade Firmware** button in the Actions column of the [Standby] partition.

No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Standby	IEC_G02_0.9.2	2019-12-16T13:14:05Z	
2	boot2	Running	IEC_G02_1.0.5	2020-02-05T07:16:40Z	

3. In the [Firmware Update] window, click **Select** to navigate to the location of the firmware file and click **Upload** to begin the upgrade process.

Firmware Update

Local Firmware Update

4. Once successfully updated, you can make the standby firmware the running firmware. Refer to [Rebooting and Applying Firmware](#).



NOTE

Firmware can be downloaded at <https://netsecuritylicense.moxa.com>.

Rebooting and Applying Firmware

To boot into an upgraded firmware or to revert to a previous firmware, you will need to boot from the [Standby] partition and load the firmware from there.

Steps:

1. Go to [Administration] > [Firmware Management].
2. Click the **Reboot and Apply Firmware** button in the Actions column of the [Standby] partition.

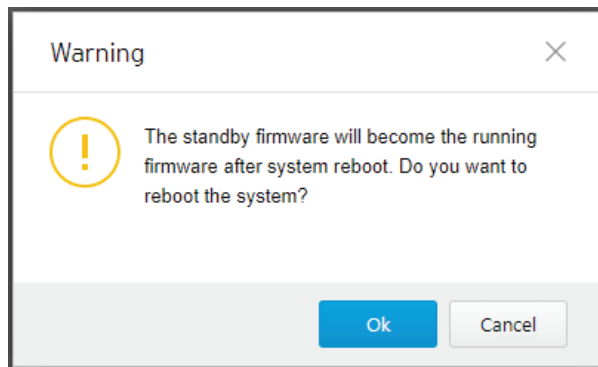
No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Standby	IEC_G02_0.9.2	2019-12-16T13:14:05Z	 
2	boot2	Running	IEC_G02_1.0.5	2020-02-05T07:16:40Z	



NOTE

This function is only available if both partitions have a separate firmware installed onto them.

3. Click **Ok** to reboot the device and make the [Standby] partition the [Running] partition.



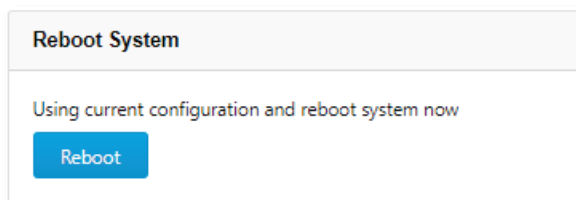
The Reboot System Screen

Use the [Reboot System] screen to reboot the system.

Rebooting the System

Steps:

1. Go to [Administration] > [Reboot System].
2. In the [Reboot System] window, click **Reboot** to reboot the system.



13. Supported USB Devices

This chapter describes the USB devices that can be used with the IEF-G9010-2MGSFP Series to extend or support additional functionalities.

To ensure optimal operation, only use the USB devices listed below.

#	Model	Device Type
1	Moxa Backup Configurator (ABC-02 Series) Model: ABC-02-USB-T	USB Disk Drive

Loading Pattern Files

A DPI pattern file can be loaded onto the device quickly and easily via a USB device. This allows for floor operators to update the pattern file on the physical floor of an ICS environment without the need for a client computer to log in to the device.



NOTE

Pattern files can be downloaded at <https://netsecuritylicense.moxa.com>.



NOTE

Given that this feature allows anyone with a supported USB device to update the pattern file, carefully consider the physical security of the IEF-G9010 Series device.



NOTE

Only supported USB devices can be used for this feature.

Steps:

1. Save the pattern file to a USB disk device under the path `"/TXone/pattern/"`. The pattern file should be named `pattern.acf`. The full file path on the USB drive should be `"/TXone/pattern/pattern.acf"`.



NOTE

Folder names are case-insensitive. Saving pattern files in another location or in an incorrectly named folder will cause the file to not be detected during the pattern load process.

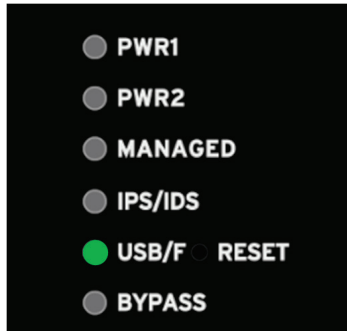


NOTE

If multiple pattern files exist in the folder, the newest will be selected in subsequent steps.

2. Plug the USB disk device into the IEF-G9010 Series device's USB port.

- If the USB drive is detected by the system, the "USB/F" LED will turn solid green. You can also check the system log to confirm that a supported USB disk device was detected.



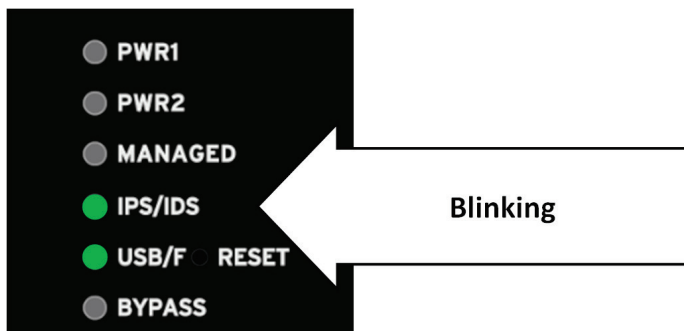
NOTE

If an unsupported USB device is plugged in, it will not be recognized, and no further action will be taken.

- The functionality of the reset button will change while the USB device is plugged in. Use the reset button to cycle through the available actions that can be taken when the USB device is plugged in. By default, no action is selected. The LEDs will indicate which action is currently selected.

Action	LED	COLOR/STATE
Default (No action is selected)	IPS/IDS LED	Solid amber
Load/Restore Pattern from USB Disk Device	IPS/IDS LED	Blinking green (Every second)

- From the default state, press the reset button once to select "Load/Restore Pattern from USB Disk Device". The IPS/IDS LED will start blinking green.



- After ensuring the correct action is selected, press down the reset button for more than 3 seconds to confirm the action.



NOTE

The action must be confirmed within 10 seconds after selecting it. If the action is not confirmed within 10 seconds, the LEDs will return to their default state (no action selected) and the action must be selected again.

- If data is being transferred from the USB device, the following LED will indicate this state. The LED will return to their previous state once completed.

Action	LED	COLOR/STATE
Data Transfer Indication	IPS/IDS LED	Blinking amber/green (Every 0.5 seconds)

- If any error occurs during an action, the LED will indicate this state.

Action	LED	COLOR/STATE
Error Indication (While an action was in progress)	Fault LED	Solid red



NOTE

The error can be cleared if: (1) the reset button is pressed again (LEDs return to default state with no action selected) or (2) the USB device is unplugged.

9. Relevant system logs can be checked to verify whether an action was completed successfully or not. If an action was successful, the LEDs will be restored to their default state when the USB disk device was first plugged in and no action was selected.
10. If the USB disk device is unplugged, the LEDs will return to their state prior to the USB device being plugged in, and a system log will be generated.