# **IEC-G102-BP Series User's Manual**

Version 1.1, June 2021

www.moxa.com/product



# **IEC-G102-BP Series User's 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**

© 2021 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

<u>Moxa Am</u>	<u>iericas</u>	<u>Moxa Ch</u>	<u>ina (Shanghai office)</u>
Toll-free:	1-888-669-2872	Toll-free:	800-820-5036
Tel:	+1-714-528-6777	Tel:	+86-21-5258-9955
Fax:	+1-714-528-6778	Fax:	+86-21-5258-5505
Moxa Eu	rope	<u>Moxa As</u>	ia-Pacific
Tel:	+49-89-3 70 03 99-0	Tel:	+886-2-8919-1230
Fax:	+49-89-3 70 03 99-99	Fax:	+886-2-8919-1231
Moxa Ind	lia		

+91-80-4172-9088

+91-80-4132-1045

Tel: Fax:

### **Table of Contents**

1.	About IEC-G102-BP Series Introduction	<b>1-1</b>
_		1-5
2.	Getting Started	2-1
	Getting Started Task List	2-2
	Changing the Administrator's Password	2-3
2		
3.	The System Screen	3-1
	System Information	3-2 3_2
	Resource Monitor	
4		
4.	Viewing Accet Information	<b>1-4</b>
	Viewing Real-time Network Application Traffic	4-2 /_3
	Enable Active Query	
F	The Davies Screen	E_1
5.	Configuring Notwork Sottings	<b>3-1</b> 5_2
	Configuring Interface Link Mode for Ports	
~		
ο.	Configuring ID Object Ductile	0-1
	Configuring IP Object Profile	6-2
	Configuring Protocol Filter Profiles	0-3 6-4
	Specifying Commands Allowed in an ICS Protocol	0 4 6-5
	Enabling the Drop Malformed Option for an ICS Protocol	6-5
	Advanced Settings for the Modbus Protocol	6-6
	Advanced Settings for the CIP Protocol	6-7
	Advanced Settings for S7Comm	6-10
	Advanced Settings for S7Comm Plus	6-13
	Advanced Settings for SLMP	6-16
	Advanced Settings for TOYOPIC	0-19 6-22
	Configuring IPS Profiles	6-25
7	The Security Screens	7_1
/.	Security General Settings	
	Configuring Security Operation Mode	7 2
	Cybersecurity	
	Configuring Cybersecurity – Denial of Service Prevention	7-4
	Policy Enforcement	
	,	/-5
	Configuring Policy Enforcement	7-5 7-5
	Configuring Policy Enforcement	7-5 7-5 7-6
	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules	7-5 7-5 7-6 7-7
8.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens	7-5 7-5 7-6 7-7 <b>8-1</b>
8.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens Viewing Device Pattern Information	7-5 7-5 7-6 7-7 8-1
8.	Configuring Policy Enforcement	7-5 7-5 7-6 7-7 8-1 8-2 8-2
8. 9.	Configuring Policy Enforcement	7-5 7-5 7-6 7-7 8-1 8-2 8-2 8-2
8. 9.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules <b>The Pattern Screens</b> Viewing Device Pattern Information Manually Updating the Pattern <b>The Log Screens</b> Viewing Cybersecurity Logs	7-5 7-5 7-6 7-7 <b>8-1</b> 8-2 8-2 8-2 
8. 9.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens Viewing Device Pattern Information Manually Updating the Pattern The Log Screens Viewing Cybersecurity Logs Viewing Policy Enforcement Logs	7-5 7-5 7-6 7-7 <b>8-1</b> 8-2 8-2 8-2 9-1 9-2 9-2
8. 9.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens Viewing Device Pattern Information Manually Updating the Pattern The Log Screens Viewing Cybersecurity Logs Viewing Policy Enforcement Logs Viewing Protocol Filter Logs	7-5 7-6 7-7 <b>8-1</b> 8-2 8-2 9-1 9-2 9-3 9-3
8. 9.	Configuring Policy Enforcement	7-5 7-5 7-6 7-7 <b>8-1</b> 8-2 8-2 9-1 9-2 9-3 9-3 9-4 9-4
8. 9.	Configuring Policy Enforcement	7-5 7-5 7-7 <b>8-1</b> 8-2 8-2 9-1 9-2 9-3 9-4 9-4 9-4
8. 9.	Configuring Policy Enforcement Rules         Adding Policy Enforcement Rules         Managing Policy Enforcement Rules         The Pattern Screens         Viewing Device Pattern Information         Manually Updating the Pattern         The Log Screens         Viewing Cybersecurity Logs         Viewing Policy Enforcement Logs         Viewing System Logs         Viewing System Logs         Viewing Audit Logs	7-5 7-5 7-6 7-7 8-1 8-2 8-2 9-1 9-2 9-3 9-3 9-4 9-4 9-4 9-4
8. 9. 10.	Configuring Policy Enforcement Rules         Adding Policy Enforcement Rules         Managing Policy Enforcement Rules         The Pattern Screens         Viewing Device Pattern Information         Manually Updating the Pattern         The Log Screens         Viewing Cybersecurity Logs         Viewing Policy Enforcement Logs         Viewing Protocol Filter Logs         Viewing System Logs         Viewing Audit Logs         The Administration Screens	7-5 7-5 7-7 <b>8-1</b> 8-2 8-2 9-1 9-2 9-3 9-3 9-4 9-4 9-4 9-4 9-4
8. 9. 10.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens	7-5 7-5 7-7 <b>8-1</b> 8-2 9-2 9-3 9-3 9-3 9-4 
8. 9. 10.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens Viewing Device Pattern Information Manually Updating the Pattern The Log Screens Viewing Cybersecurity Logs Viewing Policy Enforcement Logs Viewing Policy Enforcement Logs Viewing Asset Detection Logs Viewing Asset Detection Logs Viewing System Logs Viewing System Logs Viewing Audit Logs The Administration Screens Account Management Built-in User Accounts Adding a User Account	7-5 7-5 7-7 <b>8-1</b> 8-2 8-2 9-1 9-2 9-3 9-3 9-4 9-4 9-4 9-4 9-4 9-4 9-4 9-4 10-6 10-7 10-7
8. 9. 10.	Configuring Policy Enforcement	7-5 7-5 7-7 <b>8-1</b> 8-2 9-1 9-2 9-3 9-3 9-4 9-1 9-7 9-1 
8. 9. 10.	Configuring Policy Enforcement	7-5 7-5 7-7 <b>8-1</b> 8-2 9-1 9-2 9-3 9-3 9-4 9-7 9-7 9-4 9-4 
8. 9. 10.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules The Pattern Screens	7-5 7-5 7-7 <b>8-1</b> 8-2 9-1 9-2 9-3 9-3 9-4 9-7 10-6 10-7 10-7 10-8 10-8 10-8
8. 9. 10.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules <b>The Pattern Screens</b> Viewing Device Pattern Information Manually Updating the Pattern <b>The Log Screens</b> Viewing Cybersecurity Logs Viewing Policy Enforcement Logs Viewing Policol Filter Logs Viewing Asset Detection Logs Viewing Asset Detection Logs Viewing System Logs Viewing Audit Logs Viewing Audit Logs Account Management Built-in User Accounts Adding a User Account Configuring Password Policy Settings System Management Configuring Device Name and Device Location Information	7-5 7-5 7-7 <b>8-1</b> 8-2 9-1 9-2 9-3 9-3 9-4 9-7 10-6 10-7 10-7 10-8 10-8 10-8 10-9
8. 9. 10.	Configuring Policy Enforcement Adding Policy Enforcement Rules Managing Policy Enforcement Rules <b>The Pattern Screens</b> Viewing Device Pattern Information Manually Updating the Pattern. <b>The Log Screens</b> Viewing Cybersecurity Logs Viewing Policy Enforcement Logs Viewing Protocol Filter Logs Viewing Asset Detection Logs Viewing Asset Detection Logs Viewing System Logs Viewing Audit Logs. <b>The Administration Screens</b> Account Management Built-in User Accounts Adding a User Account Changing Your Password Configuring Password Policy Settings. System Management. Configuring Device Name and Device Location Information Configuring Control List Access from Management Clients Configuring Control List Access from Management Clients	
8. 9. 10.	Configuring Policy Enforcement Rules         Adding Policy Enforcement Rules         Managing Policy Enforcement Rules         The Pattern Screens         Viewing Device Pattern Information         Manually Updating the Pattern         The Log Screens         Viewing Cybersecurity Logs.         Viewing Policy Enforcement Logs         Viewing Protocol Filter Logs.         Viewing System Logs         Viewing System Logs         Viewing Audit Logs.         The Administration Screens         Account Management         Built-in User Accounts         Adding a User Account         Changing Your Password         Configuring Password Policy Settings.         System Management.         Configuring Device Name and Device Location Information         Configuring Control List Access from Management Clients         Configuring Control List Access from Management Clients         Configuring Screen (Pro Vercion)	
8. 9. 10.	Configuring Policy Enforcement Rules         Adding Policy Enforcement Rules         Managing Policy Enforcement Rules         The Pattern Screens         Viewing Device Pattern Information         Manually Updating the Pattern         Menaging Policy Enforcement Logs         Viewing System Logs         Viewing System Logs         Viewing Audit Logs         The Administration Screens         Account Management         Built-in User Accounts         Adding a User Account         Changing Your Password         Configuring Device Name and Device Location Information         Configuring Control List Access from Management Clients         Configuring Management Protocols and Ports         The Sync Setting Screen (Pro Version)         Enabling Management by SDC	7-5 7-5 7-7 <b>8-1</b> 8-2 9-1 9-2 9-3 9-3 9-4 9-4 9-4 9-4 10-5 10-7 10-7 10-7 10-7 10-8 10-9 10-9 10-10 10-10 10-10

	Configuring Syslog Settings	
	Syslog Severity Levels	
	Syslog Severity Level Mapping Table	
	The System Time Screen	
	Configuring System Time	
	The Back Up/Restore Screen	
	Backing Up a Configuration	
	Restoring a Configuration	
	The Firmware Management Screen	
	Viewing Device Firmware Information	
	Updating Firmware	
	Rebooting and Applying Firmware	
	The Reboot System Screen	
	Rebooting the System	
11.	Supported USB Devices	
	Pattern Loading Function	
	Procedure	

### **Terms and Acronyms**

Term/Acronym	Definition
CEF	Common Event Format
DPI	Deep Packet Inspection
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
SDC	Security Dashboard Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition

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

1

# **About IEC-G102-BP Series**

The following topics are covered in this chapter:

- □ Introduction
- Main Functions

### Introduction

The IEC-G102-BP Series is an industrial next-generation IPS device that delivers deliver a palm-sized platform that is fitted with dual Ethernet LAN ports. Users can access its web-based management console that provides a graphical user interface for policy management. The whole management process is designed to comply with the manufacturing SOP of the industry. The IEC-G102-BP Series protects your individual assets with OT visibility, cybersecurity, and OT protocol whitelisting.

Traditionally, IT and OT operate separately, each with its own network, transportation team, goals, and needs. In addition, each industrial environment is equipped with tools and devices that were not designed to connect to a corporate network, thus making provisioning security updates or patches in a timely manner difficult. Therefore, the requirements for security products that provide proper security protection and visibility are on the rise.

Moxa 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 comply with size, power consumption, durability for OT environments and have the ability to tolerate a wide range of temperature variations
- Threat detection and interception against the spread of worms
- Intrusion Prevention System and Denial-of-Service (DoS) that target legacy vulnerable devices
- Virtual patch protection against OT device exploits

## **Main Functions**

The IEC-G102-BP Series is a transparent network security device. Below are the main functions of the product:

### **Extensive Support for Industrial Protocols**

The IEC-G102-BP 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 allows 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 IEC-G102-BP 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 executes filtering of control commands within the 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 IEC-G102-BP Series comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant 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 IEC-G102-BP Series flexibly switches between '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 IEC-G102-BP 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 operations 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

This chapter describes the IEC-G102-BP Series and how to get started with configuring the initial settings.

The following topics are covered in this chapter:

- Getting Started Task List
- Opening the Management Console
- Changing the Administrator's Password

## **Getting Started Task List**

This task list provides a high-level overview of all procedures required to get the IEC-G102-BP Series up and running as quickly as possible. Each step links to more detailed instructions later in the document.

#### **Steps Overview:**

- Open the management console.
   For more information, see *Opening the Management Console*.
- Change the administrator password.
   For more information, see *Changing the Administrator's Password*.
- Configure the system time.
   For more information, see *Configuring System Time*.
- (Optional) Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings*.
- Configure Object Profiles.
   For more information, see *The Object Profiles Screens*.
- Configure security policies.
   For more information, see *The Security Screens*.
- Configure the device name and device location information.
   For more information, see *Configuring Device Name and Device Location Information*.
- 8. (Optional) Configure access control list from management clients. For more information, see *Configuring Control List Access from Management Clients*.
- Configure management protocols and ports.
   For more information, see *Configuring Management Protocols and Ports*.
- 10. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device. For more information, see *Manually Updating the Pattern*.
- (Optional) Enabling Management by SDC.
   For more information, see *Enabling Management by SDC*.
- 12. Configure the network settings and network interface link modes for the device. For more information, see *The Device Screen*

### **Opening the Management Console**

The IEC-G102-BP Series provides a built-in management web console that you can use to configure and manage the product. View the management console using a web browser.

Note: View the management console using 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 IEC-G102-BP Series in the following format: https://192.168.127.254, and the login screen appears.
- **NOTE** The default IP address of the IEC-G102-BP Series is **192.168.127.254** with subnet **255.255.255.0**. Before connecting a PC/Laptop to the IEC-G102-BP 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 IEC-G102-BP Series using an Ethernet cable.
- **NOTE** The IEC-G102-BP 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.
  - 2. Enter the login credentials (user ID and password). Use the default administrator login credentials when logging in for the first time:
    - User ID: admin
    - Password: moxa

admin	
••••	

- 3. Click Log On.
- 4. When you log in for the first time, the IEC-G102-BP Series will request you to create a new admin account and change the default password for security reasons.

🙁 Login Ir	nformation Setup
Change the default l unauthorized access	login name and password to prevent ; your account
New Login Name*	
New Password*	
Retype Password*	
	Confirm

5. The login screen will pop out again. Please use the new admin account and password to log in.

## **Changing the Administrator's Password**

To change the password of the IEC-G102-BP Series, you have to log in to a web browser with proper credentials first.

#### Steps:

- 1. In a web browser, type the address of the IEC-G102-BP Series in the following format: https://192.168.127.254, and the login screen will appear.
- 2. Log in as the administrator.
- 3. Click the admin account icon at the top-right corner and select [Change Password].
- 4. Proceed to change the password.

MO	× Ethe	erCatch						💄 Admin01 (Admin) 🔻	EXCORE DAY
System	Visibility 🔻	Device 🔻	Object Profiles 🔻	Security 🔻	Pattern 🔻	Logs 🔻	Administration 🔻	Change Password	
System								Log Off	

**NOTE** If you accidentally forget the administrator account and password, the only way to retrieve your administration access is to reset the IEC-G102-BP to factory defaults. To reset the IEC-G102-BP to factory defaults, press and hold 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 when loading default settings.

# **The System Screen**

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

VOX/	🔨 Ethe	rCatch						💄 moxa (Admir	• 🗐	networ
stem Vis	sibility 🔻	Device 🔻	Object Profiles 🔻	Security 🔻	Pattern 🔻	Logs 🔻	Administration 🔻	About		
stem										
								Refresh Time	10 Sec	
MOXA		s	System information							
	USB		System Boo	ot Time	2019-11-10T08:00:03Z	!	Device Name:	EtherCatch		
PWR1			Device IP A	ddress	192.168.127.254		Model:	IEC-G102-BP-P	ro	
PWR2     MANAGED			Gateway IP	Address	192.168.127.1		Firmware Version:	IEC_G02_1.0.5		
			DNS Server				FW Build Date / Time:	2020-02-05T07	:16:40Z	
BYPASS		s	System Status							
	<sup>2</sup> 7		Cyber Secu	rity:	Disabled		Throug	hput / Connecti	on	
	- SS		Policy Enfor	rcement:	Disabled		-			
10	BYP/		Signature V	ersion:	MX_200120_14		Real Time Throughput	Co	onnection Usage	
	ן ר י		SDC Sync:	I	Disconnected		0 bps		2 / 10000	
» EtherCa	antch 🚟	txOne	Resource Monitor							
IEC-G102-B	P	networks		CPU Utilizatio	n		Mer	nory Utilization		
							0.11			
				Realtime Usage:	2%		Keal	time Usage: 10%		

The following topics are covered in this chapter:

- System Information
- System Status
- Resource Monitor

## **System Information**

This widget shows the time when the system started, name of the device, model name of the device, version of the firmware on the device, firmware build date/time, and the IP address settings of the device.

System info	ormation			
	System Boot Time	2019-11-10T08:00:03Z	Device Name:	EtherCatch
	Device IP Address	192.168.127.254	Model:	IEC-G102-BP-Pro
	Gateway IP Address	192.168.127.1	Firmware Version:	IEC_G02_1.0.5
	DNS Server	-	FW Build Date / Time:	2020-02-05T07:16:40Z

## **System Status**

The widget shows whether cybersecurity is enabled, whether the policy enforcement is enabled, signature version on the device, whether the device is managed by SDC (Pro Version), current network throughput on the device, and current network connection usage on the device.

/stem Stat	tus			
	Cyber Security:	Disabled	Throughput /	Connection
	Policy Enforcement:	Disabled		
$\mathbf{V}$	Signature Version:	MX_200120_14	Real Time Throughput	Connection Usage
	SDC Sync:	Disconnected	0 bps	1 / 10000

## **Resource Monitor**

This widget shows resource usage on the device.

esource Monitor				
CPU Utilization			Memory Utilization	
0 %	100 %	0 %	Keartime Usage: 13%	100 %

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

# **The Visibility Screen**

The Visibility screen gives you an overview of asset visibility of your managed assets. The screens provide you with timely and accurate information on the assets that are managed by the IEC-G102-BP Series.

Active Query in Inline Node						C 10 Sec
Name: PLC Example Nr 0	Assets Int	formation		IP Addrose	102 168 1 10	
MAC: b5:96:60:1a:1c:50 Interface: Port1	Model Nam	e LOGIX5561		MAC Address	00:1d:9c:11:22:33	
	Vendor Nar	ne Rockwell		Interface	Port1	
Name: PLC Example Nr 1	Assets Typ	e PLC		First Seen	2019-11-22T07:51:49+08:00	
MAC: 90:8d:ce:da:71:db Interface: Port1	Serial Num OS	ber S/N 123.456-7890 Windows 2000		Last Seen	2020-07-28T07:51:49+08:00	
Name: PLC Example Nr 2	Real Time	Network Application Traffic				C 10 Sec
MAC: b3:80:da:10:46:74	No	Application Name	тх		RX	
Interface: Porti	1	Modbus	984.94 GB		655.53 GB	
Name: PLC Example Nr 2	2	SLMP	673.36 GB		766.10 GB	
MAC: b3:80:da:10:46:74	3	100	541.82 GB		482.64 GB	
Interface: Port1	4	-	640.75 GB		432.98 GB	
	-		612 72 CP		E20.22 CP	

The assets, listed on the screen, are automatically detected by the IEC-G102-BP Series devices.

**NOTE** The term **asset** in this chapter refers to the devices or hosts that are protected by the IEC-G102-BP Series.

The following topics are covered in this chapter:

- Viewing Asset Information
- Viewing Real-time Network Application Traffic
- Enable Active Query

# **Viewing Asset Information**

### Steps:

- 1. Go to [Visibility]  $\rightarrow$  [Assets View].
- 2. Click an asset icon and view its detailed information.

	Name: PLC Example Nr 0 IP Addr: 192.168.112.151 MAC: 84:ef:a3:7c:c8:87
	Name: PLC Example Nr 1 IP Addr: 192.168.240.72 MAC: f3:df:1d:37:89:e1
	Name: PLC Example Nr 2 IP Addr: 192.168.100.38 MAC: 33:b9:44:ea:24:85
-	Name: PLC Example Nr 3 IP Addr: 192.168.7.115 MAC: 7d:4d:2f:f9:f4:15
	Name: PLC Example Nr 4 IP Addr: 192.168.134.119 MAC: 06:8c:24:43:14:b2

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]  $\rightarrow$  [Assets View].
- 2. Click an asset icon and view its 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.
ТХ	The amount of traffic transmitted for this traffic.
RX	The amount of traffic received for this traffic.

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

**NOTE** Specify the refresh time under the [Refresh Time] dropdown menu.

## **Enable 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]  $\rightarrow$  [Assets View].
- 2. Click the [Active Query in Inline Mode] toggle in the top-left.

# **The Device Screen**

Network Setting				
Device IP Address	192.16	58.127.254		
Netmask	255.25	55.255.0		
Sateway	192.16	58.127.1		
DNS				
Network VLAN-ID	0		1	
Port Configuratoin				
Physical interface link mode	PORT1	Auto Negotiation	•	i
	PORT2	Auto Negotiation	•	

This chapter describes how to set up the network settings and port configurations for the device.

The following topics are covered in this chapter:

- **Configuring Network Settings**
- Configuring Interface Link Mode for Ports

## **Configuring Network Settings**

**NOTE** Access to the [Network Settings] pane depends on the current device operation mode set in the [Configuring Security Operation Mode] section. If the device is set to the Inline Mode, [Network Settings] can be accessed through either physical Port 1 or Port 2. If the device is set to Offline, [Network Settings] can only be accessed through the selected management port. The default access port for Offline mode is Port 1.

### Steps:

- 1. Go to [Device]  $\rightarrow$  [Device Setting]
- 2. In the [Network Setting] pane, configure the network settings for the device:

Task	Action
Device IP Address	IP Address of the device
Netmask	Netmask of the device
Gateway	Gateway of the device
DNS	DNS address of the device
Enable VLAN-ID	Enable/Disable VLAN ID
VLAN-ID	Network VLAN-ID of the device

# **Configuring Interface Link Mode for Ports**

**NOTE** Access to the [Network Settings] pane depends on the current device operation mode set in the [Configuring Security Operation Mode] section. If the device is set to the Inline Mode, [Network Settings] can be accessed through either physical Port 1 or Port 2. If the device is set to Offline, [Network Settings] can only be accessed through the selected management port. The default access port for Offline mode is Port 1.

### Steps:

- 1. Go to [Device]  $\rightarrow$  [Device Setting]
- 2. In the [Port Configuration] pane, configure the link modes for the ports of the device:

Task	Action
Port 1 and Port 2	Choose [Auto Negotiation] to specify that the interface should automatically negotiate the highest speed that both sides can work with or specify the configured speed value of the interface. Auto Negotiation          10 Mbps Full Duplex         10 Mbps Half Duplex         10 Mbps Half Duplex

# **The Object Profiles Screens**

Object profiles simplify policy management by storing configurations that can be used by the IEC-G102-BP 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. Details of ICS (Industrial Control System) protocols are defined here.

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 a profile name to edit the settings.
Delete a profile	Select one or more profiles and click [Delete].
Copy a profile	Select on profile and click [Copy].

The following topics are covered in this chapter:

- Configuring IP Object Profile
- Configuring Service Object Profile
- Configuring Protocol Filter Profiles
  - > Specifying Commands Allowed in an ICS Protocol
  - > Enabling the Drop Malformed Option for an ICS Protocol
  - > Advanced Settings for the Modbus Protocol
  - > Advanced Settings for the CIP Protocol
  - Advanced Settings for S7Comm
  - Advanced Settings for S7Comm Plus
  - Advanced Settings for SLMP
  - Advanced Settings for MELSOFT
  - Advanced Settings for TOYOPUC
  - > Configuring IPS Profiles

## **Configuring IP Object Profile**

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]  $\rightarrow$  [IP Object Profile].
- 2. Do one of the following:
  - Click [Add] to create a profile.
  - Click a profile name to edit settings.

Create IP Object	Profile	
IP Object Name*		0
Description		0
IP Profile List		(Max: 8 IP list)
No.1* Single	p •	+

- 3. Type a descriptive name for the IP Object Name field.
- 4. Type a description.
- 5. Under the [IP Object List], specify an IP address, an IP range, or an IP subnet.
- 6. If you want to add another entry, click the + button.
- 7. Click [OK].

## **Configuring Service Object Profile**

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 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]  $\rightarrow$  [Service Object Profile].
- 2. Do one of the following:
  - Click [Add] to create a profile.
  - Click a profile name to edit settings.

Create Servio	e Object Profile						
Service Object Name*							0
Description							0
Service Object Li	st						(Max: 8 service list)
No.1*	тср 🔹	Protocol Number	6	Service Port	0 ~	0	+

- 3. Type a descriptive name for the Service Object Profile.
- 4. Type a description.
- 5. Provide one of the following definitions:
- 6. TCP protocol and its port range
- 7. UDP protocol and its port range
- 8. ICMP protocol and its type and code
- 9. Custom protocol with specified protocol number
- 10. If you want to add another entry, click the + button.
- 11. 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

Crea	te Protocol Filter Profi	le			×
roto	ol Filter Profile Name*			(	D
Descri	ption			C	D
* IC	S Protocol				Selected 0 / Total 11 Items
	Factory	Automation		Power & Electricity	
	Protocol Name	Advanced Settings	Information		Drop Malformed ()
	Modbus	Settings	Any		
	CIP	Settings	Any		
	S7Comm	Settings	Any		
	S7Comm Plus	Settings	Any		
	PROFINET	Settings	Any		
	SLMP	Settings	Any		
	MELSOFT	Settings	Any		
	FINS	Settings	Any		
	SECS/GEM	Settings	Any		
	TOYOPUC	Settings	Any		
• G	eneral Protocol				Selected 0 / Total 5 Items
	elect All SMB	RDP	MQTT	HTTP	FTP
					Ok Cancel

rotocol Filter Profile Name*				0
escription				0
* ICS Protocol				Selected 0 / Total 11 Item
Factory	y Automation		Power & Electricity	1
Protocol Name	Advanced Settings	Information		
EC61850-MMS	Settings	Any		
General Protocol				Selected 0 / Total 5 Item
Select All MQTT	HTTP	FTP	SMB	RDF

### **Specifying Commands Allowed in an ICS Protocol**

When configuring an ICS protocol, you can specify which commands will be included in the protocol profile, as the following picture shows.



### **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, EtherCatch will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, EtherCatch 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 ()
Modbus	Settings	Any	
CIP	Settings	Any	
S7Comm	Settings	Any	
S7Comm Plus	Settings	Any	
PROFINET	Settings	Any	
SLMP	Settings	Any	
MELSOFT	Settings	Any	
FINS	Settings	Any	
SECS/GEM	Settings	Any	
TOYOPUC	Settings	Any	

### **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 acc	ess permissior	n ()			
🔿 Any						
O Basic						
Read Only	Read / Wri	te 🗌 Adm	in Config	Others		
• Professional Setting	9					
Function list	0x01:	Read Coils				•
Function Code	0x01	0				
Unit ID	0	1				
Address	Any	•		0		
Add De	lete				Max: 8 fu	nction code list
No Funct	ion Code	Function Co	ode List		Unit ID	Address
		No d	ata to displa	у		

#### Steps:

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

	0			ol Filter Profile Name*	otod
	0			ption	escri
cted 0 / Total 11 Ite	Selecte			S Protocol	IC
	Power & Electricity		ry Automation	Facto	
op Malformed 🕕	Drop	Information	Advanced Settings	Protocol Name	
		Any	Settings	Modbus	
		Any	Settings	CIP	
		Any	Settings	S7Comm	
		Any	Settings	S7Comm Plus	
		Any	Settings	PROFINET	
		Any	Settings	SLMP	
		Any	Settings	MELSOFT	
		Any	Settings	FINS	
		Any	Settings	SECS/GEM	
		Any	Settings	TOYOPUC	
ected 0 / Total 5 Ite	Select			eneral Protocol	Ge
F	HTTP		RDP	elect All SMB	S
ected 0 / To	Select	_ ΜΩΤ	RDP	eneral Protocol	▼ Ge

- 3. Type a protocol filter profile name.
- 4. Type a description.

- 5. 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:
    - 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 [Modbus] protocol to configure advanced settings for this protocol:
    - Click [Settings] besides [Modbus], and select [Advanced Matching Criteria].
    - From the [Function list] drop-down menu, select a function for this protocol.

0x05	5: Write Single Coil	
	0x02: Read Discrete Inputs	*
	0x03: Read Holding Registers	
	0x04: Read Input Registers	
~	0x05: Write Single Coil	
	0x06: Write Single Register	
	0x07: Read Exception Status	
	0x08: Diagnostics	
	0x0b: Get Comm Event Counter	
	0x0c: Get Comm Event Log	
	0x0f: Write Multiple Coils	
	0x10: Write Multiple Registers	
	0x11: Report Slave ID	
	0x14: Read File Record	
	0x15: Write File Record	
	0x16: Mask Write Register	
	0x17: Read/Write Multiple Registers	
	0x18: Read FIFO Queue	
	0x2b: Encapsulated Interface (MEI) Transport	
	Custom	

- If you want to specify a custom function code, select [Custom] and input a function code in the [Function Code] field.
- Type a unit ID in the [Unit ID] field.
- Type the address or range of addresses against which the function will operate.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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.

 $\times$ 

CIP Advanced Settings

Command / Function Category Access Permission 🏠	
O Any	
O Basic	
Read Only Read / Write Admin Config Others	
Advanced Matching Criteria	
Object Class List Any -	
Object Class ID* Any	
Any Service Code	
O Preset Service Code	
Available Service Code 28 Selected Service Code 0	
(0x01) Get_Attribute_All	
(0x02) Set_Attribute_All	
(0x03) Get_Attribute_List	
(0x04) Set_Attribute_List <	
(0x05) Reset	
(0x06) Start	
O Custom Service Code	
Add Clear	_
	•
OK Cancel	

#### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

otoo	ol Filter Profile Name*				0
escri	ption				0
IC	S Protocol				Selected 0 / Total 11 Items
	Factory	Automation		Power & Electricity	
	Protocol Name	Advanced Settings	Information		Drop Malformed ()
	Modbus	Settings	Any		
	CIP	Settings	Any		
	S7Comm	Settings	Any		
	S7Comm Plus	Settings	Any		
	PROFINET	Settings	Any		
	SLMP	Settings	Any		
	MELSOFT	Settings	Any		
	FINS	Settings	Any		
	SECS/GEM	Settings	Any		
	TOYOPUC	Settings	Any		
Ge	neral Protocol				Selected 0 / Total 5 Items
5	elect All SMB	RDP	MQTT	HTTP	FTP
		<ul> <li>Soport</li> </ul>			
					Ok Cancel

- 3. Type a protocol filter profile name.
- 4. Type a description.

(0x004B) Safety Dual Channel Analog...

(0x004C) SERCOS III Link

- 5. 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:
    - 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 [CIP] protocol to configure advanced settings for this protocol:
    - Click [Settings] besides [CIP], and select [Advanced Matching Criteria].
    - From the [Object Class List] drop-down menu, select a function for this protocol.

			(0x004D) Target Connection List
~	Any	(0x002B) Acknowledge Handler	(0x004E) Base Energy
	(0x0001) Identity	(0x002C) Overload	(0x004F) Electrical Energy
	(0x0002) Message Router	(0x002D) Softstart	(0x0050) Non-Electrical Energy
	(0x0003) DeviceNet	(0x002E) Selection	(0x0051) Base Switch
	(0x0004) Assembly	(0x0030) S-Device Supervisor	(0x0052) SNMP
	(0x0005) Connection	(0x0031) S-Analog Sensor	(0x0053) Power Management
	(0x0006) Connection Manage	(0x0032) S-Analog Actuator	(0x0054) RSTP Bridge
	(0x0007) Register	(0x0033) S-Single Stage Controller	(0x0055) RSTR Port
	(0x0008) Discrete Input Point	(0x0034) S-Gas Calibration	
	(0x0009) Discrete Output Point	(0x0035) Trip Point	(0.0057) PBP No doo Table
	(0x000A) Analog Input Poing	(0x0037) File	(0x0057) PRP Nodes Table
	(0x000B) Analog Output Point	(0x0038) S-Partial Pressure Object	(0x0058) Safety Feedback
	(0x000E) Presence Sensing	(0x0039) Safety Supervisor	(0x0059) Safety Dual Channel Feedba
	(0x000F) Parameter	(0x003A) Safety Validator	(0x005A) Safety Stop Functions
	(0x0010) Parameter Group	(0x003B) Safety Discrete Output Point	(0x005B) Safety Limit Functions
	(0x0012) Group	(0x003C) Safety Discrete Output Group	(0x005C) Power Curtailment
	(0x001D) Discrete Input Group	(0x003D) Safety Discrete Input Point	(0x005D) CIP Security
	(0x001E) Discrete Output Group	(0x003E) Safety Discrete Input Group	(0x005E) EtherNet/IP Security
	(0x001F) Discrete Group	(0x003F) Safety Dual Channel Output	(0x005F) Certificate Management
	(0x0020) Analog Input Group	(0x0040) S-Sensor Calibration	(0x0067) PCCC Class
	(0x0021) Analog Output Group	(0x0041) Event Log	(0x00F0) ControlNet
	(0x0022) Analog Group	(0x0042) Motion Device Axis	(0x00F1) ControlNet Keeper
	(0x0023) Position Sensor	(0x0043) Time Sync	(0x00F2) ControlNet Scheduling
	(0x0024) Position Controller Supervisor	(0x0044) Modbus	(0x00F3) Connection Configuration
	(0x0025) Position Controller	(0x0045) Originator Connection List	(0x00F4) Port
	(0x0026) Block Sequencer	(0x0046) Modbus Serial Link	(0x00F5) TCP/IP Interface
	(0x0027) Command Block	(0x0047) Device Level Ring	(0x00F6) Ethernet Link
	(0x0028) Motor Data	- (0x0048) QoS	(0x00F7) CompoNet
	(0x0029) Control Supervisor	(0x0049) Safety Analog Input Point	(0x00F8) CompoNet Repeater
	(0x002A) AC/DC Drive	(0x004A) Safety Analog Input Group	Custom

- If you want all service codes within the specified function to be applied, select [Any Service Code].
- 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.

- If you want to specify a custom service code, select [Custom Service Code] and input a service code in the [Custom Service Code] field. .
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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.

Advanced Matching Criteria	iyə			~
dot.				
Function List	Any			
Function Code*	Any	<b>(</b> )		
🔿 User Data				
Function Group List	Any		Υ.	
Function Group Code*	Any	()		
Any Sub-function C	ode			
Preset Sub-function     Available Sub-function	Code	Colortad Sub d	unstian Cada	
Available Sub-Turict	Ion Code	Selected Sub-I	unction Code	
		>>		
		>		
		<		
		~~		
Custom Sub-function	on Code		(1)	

S7Comm Advanced Setting	<u>js</u>			$\times$
Function List	Any		Y	^
Function Code*	Апу	(i)		
🗿 User Data				
Function Group List	0x0: Mode-tran	sition	•	
Function Group Code*	0x0	i		
Any Sub-function Code	de			
Preset Sub-function C	lode			
Available Sub-functio	n Code 🧿	Selected Sub-functi	on Code 이	
(0x00) Stop	^			
(0x01) Warm restar	t			
(0x02) Run		>		
(0x03) Hot restart		<		
(0x04) Hold		<<		
(0x06) Cold restart	~			
O Custom Sub-function	Code		<b>(</b> )	
	Add	Clear		
	Aud	Clear		<b>_</b>
			Ok	ancel

### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

otocol Filter Profile Name*				J
escription				Ð
ICS Protocol				Selected 0 / Total 11 Item
Fe	ctory Automation		Power & Electricity	
Protocol Name	Advanced Settings	Information		Drop Malformed ()
Modbus	Settings	Any		
CIP	Settings	Any		
S7Comm	Settings	Any		
S7Comm Plus	Settings	Any		
PROFINET	Settings	Any		
SLMP	Settings	Any		
MELSOFT	Settings	Any		
FINS	Settings	Any		
SECS/GEM	Settings	Any		
Тоуорис	Settings	Any		
General Protocol				Selected 0 / Total 5 Item
Select All SMB	RDP	MQTT	HTTP	FTP
Select All SMB	C RDP	_ ΜΩΤΤ	☐ HTTP	

3. Type a protocol filter profile name.

- 4. Type a description.
- 5. 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:
    - 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] protocol to configure advanced settings for this protocol:
    - Click [Settings] besides [S7Comm], and select [Advanced Matching Criteria].
    - 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.

~	Any
	0x00: CPU services
	0x04: Read Var
	0x05: Write Var
	0x1A: Request download
	0x1B: Download block
	0x1C: Download ended
	0x1D: Start upload
	0x1E: Upload
	0x1F: End upload
	0x28: PLC Control; PI services
	0x29: PLC Stop
	0xF0: Setup communication
	Custom

• 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.

~	Any
	(0x0) Mode-transition
	(0x1) Programmer commands
	(0x2) Cyclic data (read data from PLC without a request)
	(0x3) Block functions
	(0x4) CPU functions
	(0x5) Security functions (e.g. PLC password)
	(0x6) PBC (Programmable Block Comm) BSEND/BRECV
	(0x7) Time functions

• If you want all sub-function codes within the specified function group code to be applied, select [Any Sub-function Code].

- 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.
- If you want to specify a custom sub-function, select [Custom Sub-function Code] and input a sub-function code in the [Custom Sub-function Code] field. .
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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 Advar	nced Settings	×
Command / Function Cate Any Basic Read Only R Advanced Matching Cri	ead / Write Admin Config Others	
Function Code list Function Code*	(0x04B1) Error	
	Add	
	Total Number of Records: 0 (Max: 32)	
No Fun	tion	
	No data to display	
	Ok Canc	el

#### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

			i i	O	
escription					
· ICS	Protocol				Selected 0 / Total 11 Items
	Factory	Automation		Power & Electricity	
	Protocol Name	Advanced Settings	Information		Drop Malformed ()
	Modbus	Settings	Any		
	CIP	Settings	Any		
	\$7Comm	Settings	Any		
	S7Comm Plus	Settings	Any		
	PROFINET	Settings	Any		
	SLMP	Settings	Any		
	MELSOFT	Settings	Any		
	FINS	Settings	Any		
	SECS/GEM	Settings	Any		
	TOYOPUC	Settings	Any		
Ge	neral Protocol				Selected 0 / Total 5 Items
S	elect All SMB	RDP		HTTP	FTP

- 3. Type a protocol filter profile name.
- 4. Type a description.
- 5. 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:
    - 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:
    - Click [Settings] besides [S7Comm], and select [Advanced Matching Criteria].
    - From the [Function List] drop-down menu, select a function for this protocol.



- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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 Set	tings	$\times$
Command / Function Cate	gory Access Permission (i)	
Any		
O Basic		
Read Only     Read Only     Read Only     Advanced Matching Crit	ead / Write Admin Config Others	
Command Code list	(0x0101) Read Type Name	
Command Code*	0x0101 (j)	
	Add Clear	
	Total Number of Records: 0 (Max: 32	)
No Com	mand	
	No data to display	
	Ok Car	ncel

### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

roto	col Filter Profile Name*	(	D		
Jescription				0	
- IC	S Protocol				Selected 0 / Total 11 Items
	Factory	Automation		Power & Electricity	
	Protocol Name	Advanced Settings	Information		Drop Malformed ()
	Modbus	Settings	Any		
	CIP	Settings	Any		
	S7Comm	Settings	Any		
	S7Comm Plus	Settings	Any		
	PROFINET	Settings	Any		
	SLMP	Settings	Any		
	MELSOFT	Settings	Any		
	FINS	Settings	Any		
	SECS/GEM	Settings	Any		
	TOYOPUC	Settings	Any		
G	eneral Protocol				Selected 0 / Total 5 Item
	Select All SMB	RDP		HTTP	FTP

- 3. Type a protocol filter profile name.
- 4. Type a description.
- 5. 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:
    - 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:
    - Click [Settings] besides [S7Comm], and select [Advanced Matching Criteria].
    - From the [Command Code List] drop-down menu, select a function for this protocol.
(0x0101) Read Type Name (0x0401) Device Batch Read (0x0403) Device Random Read (0x0406) Device Read Block (0x041A) Array Label Read (0x041C) Label Random Read (0x0601) Extend Unit Read (0x0613) Memory Read (0x0619) Self Test (0x0801) Device Monitor Regist... (0x0802) Device Monitor (0x1001) Remote Run (0x1002) Remote Stop (0x1003) Remote Pause (0x1005) Remote Latch Clear (0x1006) Remote Reset (0x1401) Device Batch Write (0x1402) Device Random Write (0x1406) Device Write Block (0x141A) Array Label Write (0x141B) Label Random Write (0x1601) Extend Unit Write (0x1613) Memory Write (0x1630) Remote Password Unl... (0x1631) Remote Password Lock (0x1810) Read Directory/File Info (0x1811) Search Directory/File I... (0x1820) Create File (0x1822) Delete File (0x1824) Copy File (0x1826) Change File Date (0x1827) Open File (0x1828) Read File (0x1829) Write File (0x182A) Close File Custom

- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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	$\times$
Command / Function Cate Any Basic Read Only Re Advanced Matching Crit	gory Access Permission 🚯 ead / Write 📄 Admin Config 📄 Others eria	
Command Code list Command Code*	(0x0101) Read CPU Model Name 0x0101  Add Clear	
	Total Number of Records: 0 (Max: 32)	
No Com	mand	
	No data to display	
	Ok Canc	el

#### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

roto	col Filter Profile Name*				J
escri	ption				J
IC	S Protocol				Selected 0 / Total 11 Item
	Factory	Automation		Power & Electricity	
	Protocol Name	Advanced Settings	Information		Drop Malformed ()
	Modbus	Settings	Any		
	CIP	Settings	Any		
	S7Comm	Settings	Any		
	S7Comm Plus	Settings	Any		
	PROFINET	Settings	Any		
	SLMP	Settings	Any		
	MELSOFT	Settings	Any		
	FINS	Settings	Any		
	SECS/GEM	Settings	Any		
	TOYOPUC	Settings	Any		
Ge	eneral Protocol				Selected 0 / Total 5 Item
5	Select All SMB	RDP	MQTT	HTTP	FTP

- 3. Type a protocol filter profile name.
- 4. Type a description.
- 5. 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:
    - 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 [MELSOFT] protocol to configure advanced settings for this protocol:
    - Click [Settings] besides [MELSOFT], and select [Advanced Matching Criteria].
    - From the [Command Code List] drop-down menu, select a function for this protocol.

(0x0101) Read CPU Model Na... (0x0114) Authentication (0x0121) Read CPU Model - R ... (0x0401) Device Batch Read (0x0403) Device Random Read (0x0801) Device Monitor Regs... (0x0802) Device Monitor (0x0B05) Read Info - Q Series (0x0B11) Auto Search - Q Series (0x0B20) Auto Search - R Series (0x0B2A) Read Info - R Series (0x1001) Remote RUN (0x1002) Remote STOP (0x1003) Remote Pause (0x1005) Remote Latch Clear (0x1006) Remote RESET (0x1401) Device Batch Write (0x1402) Device Random Write (0x1640) Password Unlock (0x1641) Password Lock (0x1810) Read DIR/File Info (0x1811) Search Directory File (0x1820) Create File (0x1826) Modify File Time (0x1827) Open File (0x1828) Read File (0x1829) Write File (0x182A) Close File (0x1836) Write to Storage (0x1837) Close File SP (0x1838) Delete a File Custom

- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].
- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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 Confi	ig 🔲 Others
Command Code List (0x32) Function Call Command Code 0x32 (1) Preset Sub-cmd Code Available Sub-cmd Code (1)	▼ Selected Sub-cmd Code
(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	
Custom Sub-cmd Code	Clear
No Command	Total Number of Records: 0 (Max: 32) Sub-cmd
	ОК Сапсеі

#### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [Protocol Filter Profile].
- Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

	Selected 0 / Total 11 Items tricity  Drop Malformed
	Selected 0 / Total 11 Items tricity Drop Malformed ()
Factory Automation     Power & Elect       Protocol Name     Advanced Settings     Information       Modbus     Settings     Any       CIP     Settings     Any       S7Comm     Settings     Any       S7Comm Plus     Settings     Any       PRDEINET     Conv     Any	tricity Drop Malformed ③
Protocol Name         Advanced Settings         Information           Modbus         Settings         Any           CIP         Settings         Any           S7Comm         Settings         Any           S7Comm Plus         Settings         Any           PRDENET         Settings         Any	Drop Malformed ()
Modbus     Settings     Any       CIP     Settings     Any       S7Comm     Settings     Any       S7Comm Plus     Settings     Any	
CIP     Settings     Any       S7Comm     Settings     Any       S7Comm Plus     Settings     Any       PROFINET     Settings     Any	
S7Comm     Settings     Any       S7Comm Plus     Settings     Any       PROFINIT     Cettings     Any	
STComm Plus Setting: Any	
DROEINET Cuttions Any	
Settings Any	
SLMP Settings Any	
MELSOFT Settings Any	
FINS Settings Any	
SECS/GEM Settings Any	
TOYOPUC Settings Any	
r General Protocol	Selected 0 / Total 5 Items
Select All SMB RDP MQTT HT	TP TP

- 3. Type a protocol filter profile name.
- 4. Type a description.
- 5. 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:
    - 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 [TOYOPUC] protocol to configure advanced settings for this protocol:
    - Click [Settings] besides [TOYOPUC], and select [Advanced Matching Criteria].
    - From the [Command Code List] drop-down menu, select a function for this protocol.

- ✓ (0x18) Read Sequence Program Word (0x19) Write Sequence Program Word (0x1C) Reading IO Register Word (0x1D) Writing IO Register Word (0x1E) Reading IO Register Byte (0x1F) Writing IO Register Byte (0x20) Reading IO Register Bit (0x21) Writing IO Register Bit (0x22) Reading IO Register Multi-poin... (0x23) Writing IO Register Multi-point... (0x24) Reading IO Register Multi-poin... (0x25) Writing IO Register Multi-point... (0x26) Reading IO Register Multi-poin... (0x27) Writing IO Register Multi-point... (0x30) Reading Parameter (0x31) Writing Parameter (0x32) Function Call (0x60) Relay Command (0x90) Reading Program Expansion W... (0x91) Writing Program Expansion W... (0x92) Reading Parameter Expansion (0x93) Writing Parameter Expansion (0x94) Reading Data Expansion Word (0x95) Writing Data Expansion Word (0x96) Reading Data Expansion Byte (0x97) Writing Data Expansion Byte (0x98) Reading Data Expansion Multi-... (0x99) Writing Data Expansion Multi-... (0xA0) Expansion Function Call (0xC2) PC10 data byte reading (0xC3) PC10 data byte writing (0xC4) PC10 multi-point reading (0xC5) PC10 multi-point writing (0xCA) PC10 FR register registration Custom
- 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.
- 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.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- 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.

- 6. In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
- 7. 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
  - Denny and Log

**Object Profiles > IPS Profile** 

+	Add	
	Name	Description
	IPS_Rule_1	For OT Asset Protection
	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.

0	Enable All	( ) Disable	IIA									Enabled: 4665	Disabled: 0	Total: 4665
All	statuses 💌	All categor	es		•	All risk level	8		All actions	٠	Q, wanna	×		
	Status	ID	Category	Risk Level	Actions		Name							
		1133637	Exploits	Critical	Deny and	d Log	SMB Microsoft Windows MS17-010 S	MB Remote	Code Execution -3					^
		1133638	Exploits	Critical	Deny and	d Log	SMB Microsoft Windows MS17-010 S	MB Remote	Code Execution -4					
		1133710	Buffer Overflow	High	Deny and	d Log	SMB Microsoft Windows SMB Server	SMBv1 CV8	-2017-0147 Informa	tion Disclo	isure -1			
		1133713	Buffer Overflow	Critical	Deny and	d Log	SMB Microsoft Windows MS17-010 E	ternalBlue	SMB Remote Window	vs Kernel P	Pool Corruption -1 (C	VE-2017-0146)		
		1133812	Buffer Overflow	High	Deny and	d Log	SMB Microsoft Windows SMB Server	SMBv1 CV8	-2017-0144 Memory	Corruptio	on -1			
		1136717	Malware traffic	High	Deny and	d Log	Malware.Ransom.WannaCry							~
<		d'	)											>
										Recor	rds: 1-6 / 6 2	5 • per page 1	/1 << <	> >>

IPS Rule Details

PS Rule Details		×
Status		
ID	1136717	
Name	Malware.Ransom.WannaCry	
Category	Malware traffic	
Risk Level	High	
Impact	Critical data was encrypted and services were stopped.	
Reference	https://en.wikipedia.org/wiki/WannaCry_ransomware_attack	
Actions	Accept and Log O Deny and Log	
Keyword	WannaCry	

#### Steps

- 1. Go to [Object Profile]  $\rightarrow$  [IPS Profile].
- 2. Click [Add] to add an IPS profile.

The [Create IPS Profile] screen will appear.

Create	e IPS Profil	e														×
Name*								0								
Descript	tion							0								
$\odot$	Enable All	🛞 Disable	e All									Enabled	: 4665	Disabled: 0	Total:	4665
All	statuses 💌	All catego	pries		•	All risk levels	*	All actions	*	Q Sear	ch					
	Status	ID	Category	Risk Level	Actions	Name										
		1048640	Buffer Overflow	High	Deny and	Log WEB Microsoft PCT	Buffer Overflow -1 (CVE-20	03-0719)								^
		1048644	Buffer Overflow	High	Deny and	Log WEB Microsoft PCT	Buffer Overflow -2 (CVE-20	03-0719)								
		1048743	Buffer Overflow	High	Deny and	Log DNS Multiple Vendo	r BIND iquery buffer overfl	ow Vulnerability	(CVE-1999-000	09)						
		1048753	Buffer Overflow	Critical	Deny and	Log DNS Multiple Vendo	r BIND (NXT Overflow and	Denial of Servic	e) Vulnerabilitie	es (CVE-199	9-0833)					
		1048756	Buffer Overflow	Critical	Deny and	Log DNS BIND Multiple	/ulnerabilities									
		1048760	Exploits	Critical	Deny and	Log EXPLOIT x86 FreeBSI	D Buffer Overflow attempt									~
¢																>
									Records: 1-25	5 / 4665	25 *	per page	1/	187 <<	c >	"

- 3. Type a name for the IPS profile.
- 4. Type a description.
- 5. Select the pattern rule you want to configure by clicking the rule ID.
- 6. The IPS rule details will appear. Configure the following:
  - a. Status Enable or disable the pattern rule.
  - b. Actions Select the pattern rule's default action.
    - Accept and Log: When an intrusion is detected, the intrusion will be accepted and logged for monitoring.
    - Deny and Log: When an intrusion is detected, the intrusion will be rejected and logged for monitoring.

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

When you are done configuring the pattern rule, click [Save].

7

# **The Security Screens**

This chapter describes the security general setting, cybersecurity, and policy enforcement.

The following topics are covered in this chapter:

- Security General Settings
- Configuring Security Operation Mode
- Cybersecurity
  - > Configuring Cybersecurity Denial of Service Prevention

#### Policy Enforcement

- > Configuring Policy Enforcement
- > Adding Policy Enforcement Rules
- > Managing Policy Enforcement Rules

# **Security General Settings**

Use the [Security General Setting] screens to configure the security operation mode of the device. The IEC-G102-BP Series offers two operation modes:

- Inline Mode
- Offline Mode

The following sections describe these two modes in detail.

#### **Inline Mode**

The IEC-G102-BP Series deploys in the direct communication path between source and destination, actively analyzing, filtering, and taking actions on all traffic that passes through it.



#### **Offline Mode**

Data packets are mirrored from a core or other type of switch to **port 2** of the IEC-G102-BP Series, which keeps detecting, monitoring, as well as outputting detection logs if threat events are detected.



**NOTE** By default, **Port 1** of the IEC-G102-BP Series functions as the management port, which connects to another switch, allowing the IEC-G102-BP Series to be managed by SDC.

# **Configuring Security Operation Mode**

#### Steps:

- 1. Go to [Security]  $\rightarrow$  [Security General Setting]
- 2. On the [Security General Setting] screen you will see the following.

Inline Mode	selection			
Offline Mode				
Management Port 🛈	PORT1	Ψ.		
ecurity Operation Mode D Inline Mode: EdgelPS w	efinition orks in the direct	communication path between source ar	nd destination, actively analyzing, fi	Itering and running automated actions on a

3. Choose a desired security operation mode for this device.

Mode	Description
Inline Mode	EtherCatch is placed in the direct communication path between
	the source and destination and will actively analyze, filter, and run
	automated actions for all traffic
Offline Mode	EtherCatch will mirror data packets from the core or other switch
	to monitor traffic and generate log if threats are detected

- **NOTE** Access to the [Network Settings] pane depends on the selected device operation mode. If the device is set to the Inline Mode, [Network Settings] can be accessed through either physical Port 1 or Port 2. If the device is set to Offline, [Network Settings] can only be accessed through the selected management port. The default access port for Offline mode is Port 1.
- **NOTE** Starting from firmware v1.1, EtherCatch can log the OT protocol activity from the mirror port of the switch if a protocol filter profile is configured and applied on the policy enforcement rule.
  - 4. If you selected Offline Mode, choose the device ports.
- **NOTE** When you switch from Inline Mode to Offline Mode for the first time, please note that you MUST connect to the physical port 1 for device management in case you are unable to access the web console. After successfully switching back to Inline Mode, you can specify Port 1 or Port 2 as the port to receive the traffic from the network device for monitoring and logging.
  - 5. Click [Save].



#### WARNING

Ensure that the operation mode is correctly selected. If the IEC-G102-BP Series is deployed as inline network topology with the [Security Operation Mode] being set to [Offline Mode], then devices that connect to **port 2** cannot get through.

# Cybersecurity

This device features cybersecurity, which covers both intrusion prevention and denial of service attack prevention. The signature rules of intrusion prevention are called 'DPI (Deep Packet Inspection) Pattern'. This pattern can be regularly updated through SDC as well by manual import via the device's web management UI.

### **Configuring Cybersecurity – Denial of Service Prevention**

#### Steps:

- 1. Go to [Security]  $\rightarrow$  [Cyber Security].
- 2. At the [Cyber Security] screen you will see the [Denial of Service Prevention] pane.

Deny of Service Prevention Setting											
Deny of Service	prevention										
<ul> <li>Monitoring and Log</li> </ul>	•										
O Prevention and Log											
TCP SYN Flood	Threshold	10000	packet 🚺	UDP Flood	Threshold	10000	packet 🚺				
ICMP Flood	Threshold	10000	packet 🕕	✓ IGMP Flood	Threshold	10000	packet 🕚				
UDP Port Scan	Threshold	250	packet 🕕	✓ TCP Port SYN Scan	Threshold	1800	packet 🚯				
TCP Port FIN Scan	Threshold	1800	packet 🕕	✓ TCP Port NULL Scan	Threshold	1800	packet 🕚				
TCP Port Xmas Scan	Threshold	1800	packet 🕕								

- 3. Use the toggle to enable or disable the denial of service prevention feature.
- 4. Select an action ([Monitor and Log] or [Prevent and Log]) for the feature.
- 5. You can optionally configure the thresholds of the denial of 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 [Block], the security node blocks subsequent anomalous packets until the end of the detection period. After the detection period, the security node will again allow anomalous packets until the threshold is reached.

IEC-G102-BP Series	Action Settings	Action Performed
<b>Operation Mode (Security</b>		
General Setting)		
Inline Mode	Monitor and Log	<ul> <li>Detects and monitors network attacks, but</li> </ul>
		does not block network attacks.
		Generates logs.
	Prevent and Log	Blocks network attacks.
		Generates logs.
Offline Mode	Monitor and Log	Passively detects and monitors network
		attacks.
		Generates logs.

The following table summarizes the settings:

# **Policy Enforcement**

Policy enforcement allows you to define a custom protocol that matches to an industrial protocol, and then whitelist or blacklist activities fitting that protocol in your network environment.

### **Configuring Policy Enforcement**

#### Steps:

- 1. Go to [Security]  $\rightarrow$  [Policy Enforcement].
- 2. On the [Policy Enforcement] screen you will see the [Policy Enforcement General Setting] pane.
- 3. Use the toggle to enable or disable the policy enforcement feature.
- 4. Select a mode ([Monitor Mode], or [Prevent Mode]) for the feature.
- 5. At the [Policy Enforcement Default Rule Action] drop-down menu, select a default action for when no pattern is matched.

Policy Enforcement General Settings		
Enable Policy Enforcement		
PolicyEnforcement Operation Mode	<ul> <li>Monitor Mode</li> </ul>	O Prevention Mode
Policy Enforcement Default Rule Action	<ul> <li>Accept</li> </ul>	O Deny
Policy Enforcement Operation Mode  Monitor Mode: Policy Enforcement ru  Prevention Mode: Policy Enforcemen	iles will be checked without t rules will be checked, an	ut taking action and a log will be created. d any rule broken and will result in action being taken and the creation of a log

The following table summarizes the settings:

IEC-G102-BP Series Operation Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	<ul> <li>Detect and monitor abnormal protocol access to OT assets, without blocking network attacks.</li> <li>Generate logs.</li> </ul>
	Prevention Mode	<ul><li>Block abnormal protocol access to OT assets.</li><li>Generate logs.</li></ul>
Offline Mode	Monitor and Log	Not supported.

### **Adding Policy Enforcement Rules**

#### Steps:

- 1. Configure the required object or objects.
  - IP object profiles For more information, see Configuring IP Object Profile.
  - Service object profiles For more information, see Configuring Service Object Profile.
  - Protocol filter profiles For more information, see Configuring Protocol Filter Profile.
- 2. Go to [Security]  $\rightarrow$  [Policy Enforcement]
- 3. Under the [Policy Enforcement] screen you will see the following panes.

+	Add								Maxim	um Number of Re	cords: 512
	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
	1		Rule_1	Any	Any	Any	Any	Any	Any	Disabled	Deny
	2		Rule_2	Any	Any	Any	Any	Any	Any	Disabled	Advance

- 4. Click the [Add] button to add a new policy rule.
- 5. Toggle to enable or disable the policy rule.

Create Policy	y Enforcement	Rule				$\times$
Status						
Rule Name*	Rule_1		3			
Description	PE Rule for O	Γ Asset			0	
Source and Des	tination Selection					
Source IP / IP Ob	oject Profile	Any				
Destination IP / IP Object Profile		Any	•			
Service Object	Selection					
Service Object		Any	•			
VLAN ID				3		
Action		🔿 Accept 🗿 De	ny 🔿 Advan	ced Filter		
						_
					Ok	Cancel

- 6. Input a descriptive [Rule Name].
- 7. Input a descriptive [Description] for the rule.
- At the [Source IP / IP Object Profile] drop-down menu, select either one of the following for the source IP address(es):
  - Any
  - Single IP
  - IP Range
  - IP Subnet
  - Object

**NOTE** If you select [Object], then you need to select the IP object from an IP object profile that has been created previously.

- 9. At the [Destination IP / IP Object Profile] drop-down menu, select either one of the following for the destination IP address(es):
  - Any
  - Single IP
  - IP Range
  - IP Subnet
  - Object
- 10. At the [Service Object] drop-down menu, select either one of the following for the layer 4 criteria:
  - TCP You can further specify the port range for this protocol.
  - UDP You can further specify the port range for this protocol.
  - ICMP You can further specify the Type and Code for this protocol.
  - Custom You can further specify the protocol number for this protocol. The term protocol number refers to the one defined in the internet protocol suite.
  - Service Object

**NOTE** You need to select the service object from a service object profile that has been created previously.

- 11. At the [Action] drop-down menu, select one of the following:
  - Accept: Select this option to allow network traffic that matches this rule.
  - Deny: Select this option to block network traffic that matches this rule.
  - Advanced Filter: The node will take further actions based on the protocol filter:
    - a. Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
    - b. Under the [Protocol Filter Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.
    - c. Under the [IPS Profile] drop-down menu, select an IPS profile you have defined beforehand.

1	○ Accept ○ Deny ○ Advance	ed Filter
Protocol Filter Profile Se	lection	
Protocol Filter Profile	Please select a profile	•
Protocol Filter Action	O Accept O Deny	
IPS Profile		
IPS Profile	Please select a profile	*

12. [Optional] Specify a VLAN ID for VLAN network scanning. The maximum VLAN number for scanning in one policy enforcement is 5.

**NOTE** The maximum number of VLANs for scanning per policy enforcement is 5.

13. Click [Save] to save the configurations.

### 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, the [Edit Policy Rule] window will
	appear.
To change the priority of a policy	Click the check box in front of the policy enforcement rule, click
enforcement rule	the [Change Priority] button, and specify a new priority for this
	rule.

**NOTE** When more than one policy enforcement rule is matched, the IEC-G102-BP Series takes the action of the rule with the highest priority, and ignores the rest of the rules. The rules are listed on the table of the UI screen by priority with the highest priority rule listed on the first row of the table.

# **The Pattern Screens**

This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the IEC-G102-BP 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.

The following topics are covered in this chapter:

- Viewing Device Pattern Information
- Manually Updating the Pattern

# **Viewing Device Pattern Information**

#### Steps:

- 1. Go to [Pattern]  $\rightarrow$  [Pattern Update]
- 2. At the [Pattern Update] screen you will see the following pane.
- 3. The [Device Pattern Information] pane shows 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]  $\rightarrow$  [Pattern Update].
- 2. At the [Pattern Update] screen you will see the following pane.
- 3. Click [File Selection] or [Upload].
- 4. Manually select the pattern to be deployed to the device.

Pattern Update			
Manually Update Pattern File Path		Select	Upload

5. Click [Ok]

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

**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.

# **The Log Screens**

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

You can view the following logs on the operational technology defense console:

- Viewing Cybersecurity Logs
- Viewing Policy Enforcement Logs
- Viewing Protocol Filter Logs
- Viewing Asset Detection Logs
- Viewing System Logs
- Viewing Audit Logs
- Account Management
  - Built-in User Accounts
  - Adding a User Account
  - Changing Your Password
- **Configuring Password Policy Settings**
- System Management
  - > Configuring Device Name and Device Location Information
  - Configuring Control List Access from Management Clients
  - > Configuring Management Protocols and Ports

#### The Sync Setting Screen (Pro Version)

Enabling Management by SDC

#### The Syslog Screen

- Configuring Syslog Settings
- Syslog Severity Levels
- > Syslog Severity Level Mapping Table

#### The System Time Screen

Configuring System Time

#### □ The Back Up/Restore Screen

- Backing Up a Configuration
- Restoring a Configuration

#### The Firmware Management Screen

- > Viewing Device Firmware Information
- Updating Firmware
- > Rebooting and Applying Firmware

#### The Reboot System Screen

Rebooting the System

# **Viewing Cybersecurity Logs**

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

#### Steps:

Go to [Logs]  $\rightarrow$  [Cyber Security Logs].

The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule ID	The ID of the policy enforcement rule.
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.
Port	The physical port interface on which the cyberattack was detected.
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 is reached.

# **Viewing Policy Enforcement Logs**

The policy enforcement logs cover logs created by the [Policy Enforcement] feature without [Protocol Filter] being enabled, i.e., the [Action] of the policy enforcement rule is either to allow or to deny. The protocol filter is not used in the policy rule.

#### Steps:

Go to [Logs]  $\rightarrow$  [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.
Rule ID	The ID of the policy enforcement rule.
Source MAC Address	The source MAC address of the connection.
Port	The physical port interface through which incoming traffic was checked
	against policy enforcement rules and activity was recorded.
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.
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 filter is the advanced configuration when you configure the [Policy Enforcement] settings.

#### Steps:

Go to [Logs]  $\rightarrow$  [Protocol Filter Logs].

The following table describes the log table.

Field	Description	
Time	The time the log entry was created.	
Policy Enforcement 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.	
Port	The physical port interface that received traffic that matched the protocol	
	filter profile criteria.	
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.	

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	he 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 the system status changes of the managed assets.

#### Steps:

Go to [Logs]  $\rightarrow$  [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.	
Port	The physical port interface that received the asset information.	
Asset MAC Address	The MAC address of the asset.	
Asset IP Address	The source IP address of the asset.	

# **Viewing System Logs**

You can view details about system events on the device.

#### Steps:

Go to [Logs]  $\rightarrow$  [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 logs.
Message	The log event description.

# **Viewing Audit Logs**

You can view details about user access, configuration changes, and other events that occurred when using the device.

#### Steps:

Go to [Logs]  $\rightarrow$  [Audit Logs].

The following table describes the log's fields.

Field	Description	
Time	The time the log entry was created.	
User ID	ne user account used to execute the task.	
Client IP	The IP address of the host used to access the management console.	
Severity	The severity level of the logs.	
Message	The log event description.	

**NOTE** To view the audit logs, please log in with the default "audit" account.

# 10

# **The Administration Screens**

This chapter describes the available administrative settings for the IEC-G102-BP Series device.

The following topics are covered in this chapter:

#### Account Management

- > Built-in User Accounts
- Adding a User Account
- > Changing Your Password

#### Configuring Password Policy Settings

#### System Management

- > Configuring Device Name and Device Location Information
- > Configuring Control List Access from Management Clients
- > Configuring Management Protocols and Ports

#### The Sync Setting Screen (Pro Version)

Enabling Management by SDC

#### The Syslog Screen

- Configuring Syslog Settings
- > Syslog Severity Levels
- > Syslog Severity Level Mapping Table

#### □ The System Time Screen

Configuring System Time

#### □ The Back Up/Restore Screen

- Backing Up a Configuration
- Restoring a Configuration

#### The Firmware Management Screen

- > Viewing Device Firmware Information
- Updating Firmware
- Rebooting and Applying Firmware

#### The Reboot System Screen

> Rebooting the System

# **Account Management**

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

This system uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the 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 on 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 preexisting user accounts and click Delete.	
Edit existing accounts	Click the name of a preexisting user account to view or modify the current	
	account settings.	

#### **User Roles:**

The following table describes the permissions matrix for user roles.

		User Roles			
Sub-Screen	Action	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 – not including	View	Yes	Yes	Yes	No
audit log					
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 in the device.

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

**NOTE** The built-in user accounts cannot be deleted from the device.

**NOTE** Ensure that the passwords of the built-in accounts are changed when you first set up the device.

### Adding a User Account

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

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Account Management].
- 2. Click [Add], and the Add User Account screen appears.
- 3. Configure the account settings.

Field	Description	
ID	Type the user ID to log on to the management console.	
Name	Type the name of the user for this account.	
Password	Type the account password.	
Confirm password	Type the account password again to confirm.	
Role	Select a user role for this account.	
	For more information, see User Roles.	

4. Click [Save].

### **Changing Your Password**

#### Steps:

- 1. On the management console banner, click your account name.
- 2. Click [Change Password], and the Change Password screen will appear.
- 3. Specify the password settings.
  - Old password
  - New password
  - Confirm password
- 4. Click [Save].

# **Configuring Password Policy Settings**

The IEC-G102-BP Series provides the following password policy settings to enhance web console access security:

• Password complex settings

Specify password complexity settings to enforce strong passwords. For example, you can specify that users must create strong passwords that contain a combination of both uppercase and lowercase letters, numbers, and symbols, and which are at least eight characters in length.

**NOTE** When strong passwords are required, a user submits a new password, and the password policy determines whether the password meets your company's established requirements. Strict password policies may sometimes increase costs to an organization when users select passwords that are too difficult to remember. Users call the help desk when they forget their passwords, or keep passwords in easily accessible locations and increase their vulnerability to threats. When establishing a password policy, balance your need for strong security against the need to make the policy easy for users to follow.

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Account Management].
- 2. Click the [Password Policy] tab, and the [Password Policy] screen will appear.
- 3. Select one or more options that meet your required password policy.
- 4. Click Save.

Password Policy	×
Minimum password length:       8       (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	
Confirm	2

# 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 Device Name and Device Location Information**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [System Management].
- 2. In the [System Setting] pane, provide the host name and location information for the device.

System Setting		
Host Name*	EtherCatch	6
Location Information		6
	(Sample: Zone1, Network-1)	

### **Configuring Control List Access from Management Clients**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [System Management].
- 2. In the [Access Control List] pane, use the toggle to enable or disable access control from the management clients.
- 3. Provide the IP addresses that are allowed to manage the device.

Access Control List		
Ena	ble Access Control List	
Allowed IP 1		
Allowed IP 2		
Allowed IP 3		
Allowed IP 4		

### **Configuring Management Protocols and Ports**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [System Management].
- 2. In the [Management Method] pane:
  - a. Select the protocols that are allowed to be used.
  - b. Input the port numbers for the protocols.

Management Method						
HTTPS / HTTP						
○ HTTP* 80 3						
HTTPS*	443	6				
SSH*	22	6				
Telnet*	23	6				

**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 CLI commands.

# The Sync Setting Screen (Pro Version)

The IEC-G102-BP Series can be managed by Moxa SDC (Security Dashboard Console). Use this screen to register the IEC-G102-BP Series to a Moxa SDC.

### **Enabling Management by SDC**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Sync Setting].
- 2. In the [ODC Setting] pane:
  - a. Use the toggle to enable management by ODC.
  - b. Input the IP address of the ODC server.

SDC Setting			
Enable SDC Management			
SDC Server Address			
SDC Sync: Disconnected			
Save Cancel			

# **The Syslog Screen**

The IEC-G102-BP Series system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) syslog messages are used in the IEC-G102-BP Series.

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

### **Configuring Syslog Settings**

#### Steps:

1. Go to [Administration]  $\rightarrow$  [Syslog].

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	<b>^</b>
	_	PROTOCOL_FILTER_LOG	
	÷	POLICY_ENFORCEMENT_LOG	
		ASSET_LOG	
		SYSTEM_LOG	-

- 2. Select [Send logs to a syslog server] to set the ODC system to send logs to a Syslog server.
- 3. Configure the following settings.

Field	Description		
Server address	Type the IP address of the Syslog server.		
Port	Type the port number.		
Protocol	Select the protocol for the communication.		
Facility level	Select a facility level to determine the source and priority of the logs.		
Severity level Select a Syslog severity level.			
	This device only sends logs with the selected severity level or higher to the		
	Syslog servers.		
	For more information, see Syslog Severity Levels.		

- 4. Select the types of logs to send.
- 5. Click Save.

### **Syslog Severity Levels**

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		Error pending	
		Take action to avoid errors.	
5	Notice	Unusual events	
		Immediate action is not required.	
6	Informational	• 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.	

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

# Syslog Severity Level Mapping Table

Policy Enforcement /	Cybersecurity Severity Level	Syslog Severity Level
<b>Protocol Filter Action</b>		
		0 - Emergency
	Critical	1 - Alert
	High	2 - Critical
		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]  $\rightarrow$  [System Time].

Administratio	n > System Time
Date and Ti	me
Current Time:	2019-10-22T14:54:13+08:00
Synchroniz	ze system time with an NTP server
NTP Server:	pool.ntp.org Synchronize now (Default time server: pool.ntp.org)
Time Zone	
Time Zone:	(GMT+08:00) Asia/Taipei 🔹

- 2. In the [Date and Time] pane, select one of the following:
  - Synchronize system time with an NTP server
    - a. Specify the domain name or IP address of the NTP server.
    - b. Click Synchronize Now.
  - Set system time manually
    - a. Click the calendar to select the date and time.
    - b. Set the hour, minute, and second.
    - c. Click Apply.
- 2. From the [Time Zone] drop-down list, select the time zone.
- 3. Click Save.

**NOTE** SDC system synchronizes the system time with its managed instances.

# The Back Up/Restore Screen

Export settings from the management console to back up the configuration of your IEC-G102-BP Series. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

We recommend the following:

- Backing up the current configuration before each import operation.
- Performing the operation when the IEC-G102-BP Series is idle. Importing and exporting configuration settings affects the performance of the IEC-G102-BP Series.

### **Backing Up a Configuration**

#### Steps:

1. Go to [Administration]  $\rightarrow$  [Back Up / Restore], and the [Backup / Restore] screen will appear.

System > Backup / Restore
Backup Configuration
Backup administration settings to a file on your computer.
Backup
Restore Configuration
Restore the configuration from a backup file. It is recommended that you backup your current configuration before you replace it.
Note: Restoring replaces current configuration settings.
Select File

2. Click the [Backup] button, and a configuration backup file will automatically save in your computer.

### **Restoring a Configuration**

Follow the steps to restore the configurations of the IEC-G102-BP Series device.

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Back Up / Restore].
- 2. Under the [Restore Configuration] section, click the [Select File] button, and proceed to import the file.

All services will restart. It can take some time to restart services after applying imported settings and rules.

# **The Firmware Management Screen**

Use the [Firmware Management] screen to:

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

### **Viewing Device Firmware Information**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Firmware Management].
- 2. The [Firmware Management] pane lists the two partitions available. It shows the [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 IEC-G102-BP Series can have up to two firmware versions installed. Each firmware is installed in its own and separate partition. At any given point in time, one partition will have the status of [Running], which indicates the currently running and active firmware. The other partition will have the status of [Standby] which indicates an alternative or standby partition.

### **Updating Firmware**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Firmware Management].
- **NOTE** During a firmware upgrade, firmware will always be installed to the [Standby] partition. As such, the firmware upgrade button is only available in the [Standby] partition row.
  - 2. Click on the Upgrade Firmware button to install it to the [Standby] partition.

N	lo	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1		boot1	Standby	IEC_G02_0.9.2	2019-12-16T13:14:05Z	<b>1</b> ≓
2		boot2	Running	IEC_G02_1.0.5	2020-02-05T07:16:40Z	

3. In the [Update Firmware] pane provide the location of the firmware and click [Upload] to install the firmware to the [Standby partition].

Firmware Update		
Local Firmware Update	Select	Upload

- 4. After successfully installing the required firmware to [Standby] partition, click on the [Reboot and Apply firmware] button as shown in the next section.
- **NOTE** Various versions of the firmware can be downloaded at <u>https://netsecuritylicense.moxa.com</u>.

# **Rebooting and Applying Firmware**

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

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Firmware Management].
- 2. Click on the [Reboot and Apply firmware] button that is available in the [Standby] partition row.

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** Only when 2 partitions have their own firmware, and the switch icon appears.

3. Click [OK] to proceed with rebooting into the [Standby] partition and making it the [Running] partition.

Warning	×
The standby firmware will become the runn firmware after system reboot. Do you want reboot the system?	ing to
Ok Car	icel

# **The Reboot System Screen**

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

### **Rebooting the System**

#### Steps:

- 1. Go to [Administration]  $\rightarrow$  [Reboot System].
- 2. In the [Reboot System] pane, click [Reboot] to reboot the system.

Reboot Sys	tem	
Using current	configuration and reboot system now	1
Reboot		1
	•	
## **Supported USB Devices**

This chapter describes the USB devices that can be used with the IEC-G102-BP device for extended or supporting functionality.

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

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

## **Pattern Loading Function**

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

**NOTE** Given that this feature allows anyone with a supported USB disk device to update the pattern file, the physical security of the IEC-G102-BP device must be considered carefully.

**NOTE** Only supported USB disk devices can be used for this feature.

## Procedure

- Save the pattern file in a USB disk device under the path "/TXone/pattern/". Assuming a pattern file has the name pattern.acf, as its file path on the USB disk device the path would be "/TXone/pattern/pattern.acf".
- **NOTE** Saving pattern files under other paths or incorrect folder names will cause the file to not be detected during the pattern load process. Folder names are case-insensitive.

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

2. Plug the supported USB disk device into the IEC-G102-BP device's USB port.

 Upon successful detection of the USB disk device, the "USB" LED will change to steady green. The system log can also be checked to confirm that a supported USB disk device was properly detected when inserted.



**NOTE** If a USB device is plugged in that is not supported, it will be ignored and no further action will be taken.

- 4. The functionality of the reset button will also change to support this function until the USB device is unplugged. The reset button will at this time not serve as a reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken when a USB device is plugged in.
- 5. The user can use the reset button to cycle through a set of possible actions. By default, no action is selected. The user must press the reset button at least once to make a selection. The LEDs will indicate which action is currently selected.

Action	LED	COLOR/STATE
Default – No action selected but USB plugged in	USB LED	Green – Steady
Load/Restore Pattern from USB Disk Device	IPS/IDS LED	Green – Blinking (1/sec)

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



7. After ensuring the correct action is selected, the action must be confirmed by holding down the reset button for more than 3 seconds.

**NOTE** The action must be confirmed within 10 seconds. If the action is not confirmed within 10 seconds, the LEDs will return to their default state (no action selected) and an action must be selected once again if desired.

8. While attempting an action, if there is a USB disk data transfer, the following LEDs will indicate it as shown below. After the transfer is complete, it will return to its previous state.

Action	LED	COLOR/STATE	
Data Transfer Indication	LED	COLOR/STATE	
	USB LED	Green – Blinking (Once every 0.5 sec)	
	IPS/IDS LED	Green – Blinking (Once every 0.5 sec)	

9. If any error occurs when an action is being attempted, the following LEDs will indicate it as shown below:

Action	LED	COLOR/STATE
Error Indication (any error while action was being	LED	COLOR/STATE
processed)	Fault LED	Red – Steady

**NOTE** The error can only be cleared if: (1) the reset button is pressed once more (LEDs return to default state with no action selected) or (2) the USB disk is unplugged.

- 10. Relevant system logs can be checked to verify whether an action was completed successfully or not. If an action is successful, LEDs will be restored to their default state when the USB disk device was first plugged in and no action was selected.
- 11. The USB disk device may be unplugged, after which LEDs will return to their state prior to the USB disk device being plugged in (USB LED off), and a log will be available in system logs.

**NOTE** Various versions of the pattern files can be downloaded at <u>https://netsecuritylicense.moxa.com</u>.