IEC-G102-BP Series User's Manual

Version 1.1, June 2021

www.moxa.com/product

IEC-G102-BP Series User's Manual

Copyright Notice

Trademarks

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

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

Terms and Acronyms

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

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

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

2

Getting Started

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:

1. Open the management console.
   For more information, see *Opening the Management Console*.
2. Change the administrator password.
   For more information, see *Changing the Administrator's Password*.
3. Configure the system time.
   For more information, see *Configuring System Time*.
4. (Optional) Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings*.
5. Configure Object Profiles.
   For more information, see *The Object Profiles Screens*.
6. Configure security policies.
   For more information, see *The Security Screens*.
7. 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*.
9. 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*.
11. (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.

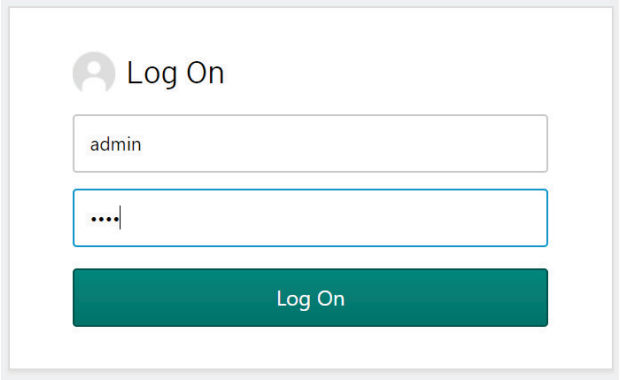
Steps:

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.

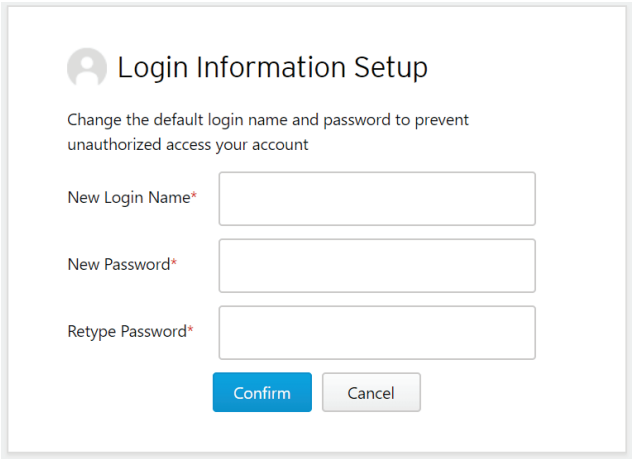
NOTE The default IP address of the IEC-G102-BP Series is **192.168.127.254** with subnet **255.255.255.0**. Before connecting a PC/Laptop to the IEC-G102-BP Series, the PC's IP address should be set to an IP address that is able to access the default IP address. After that, connect the PC and the IEC-G102-BP 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



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.



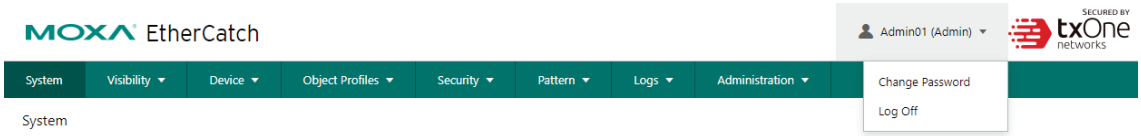
5. The login screen will pop out again. Please use the new admin account and password to log in.

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.

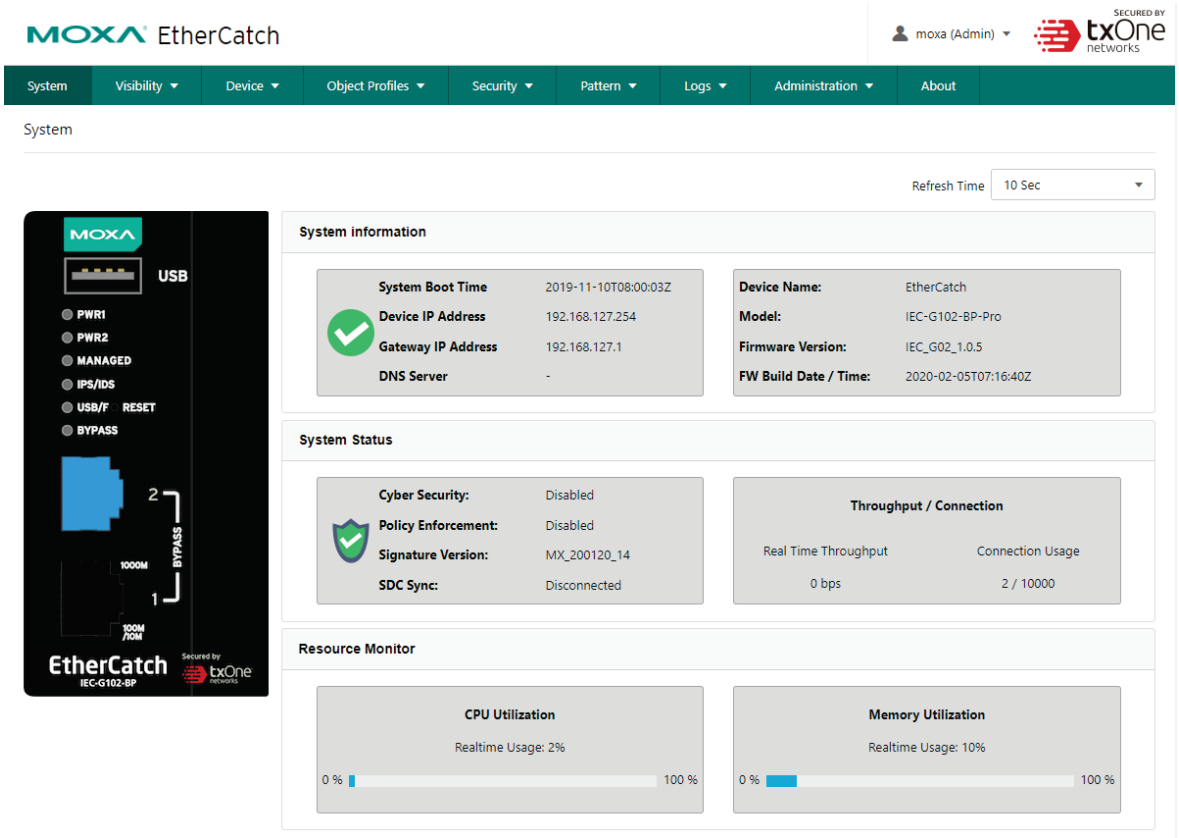


NOTE If you accidentally forget the administrator account and password, the only way to retrieve your administration access is to reset the IEC-G102-BP to factory defaults. To reset the IEC-G102-BP to factory defaults, press and hold the reset button for more than 10 seconds. The MANAGED LED will begin 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.

3

The System Screen

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

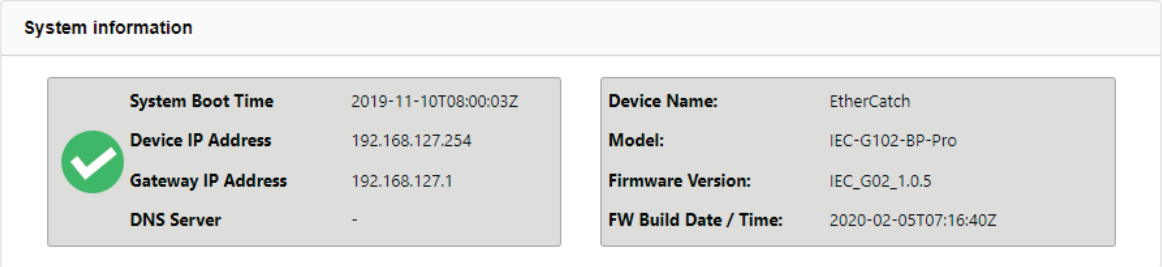


The following topics are covered in this chapter:

- **System Information**
- **System Status**
- **Resource Monitor**

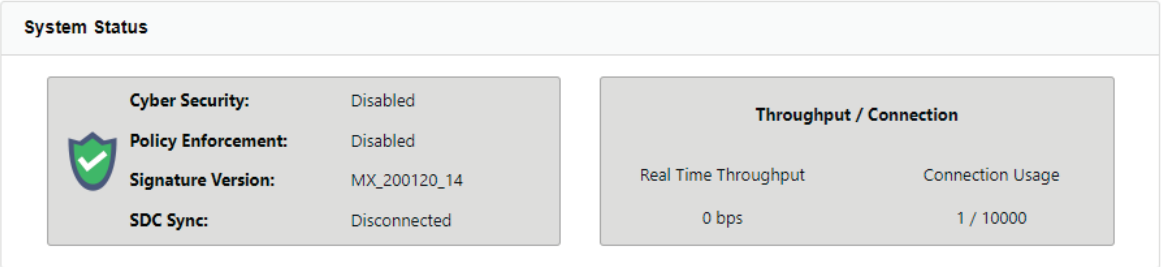
System Information

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.



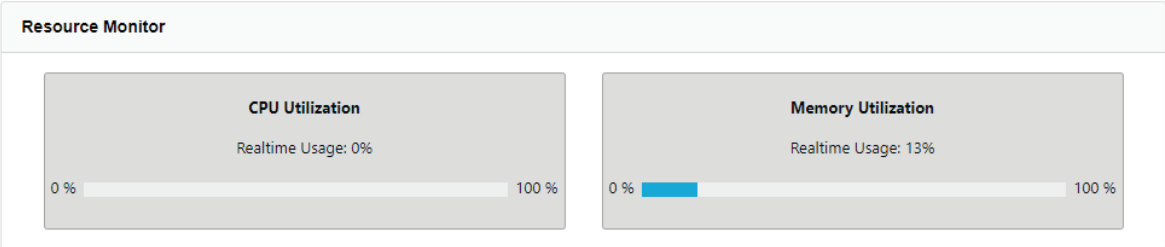
System Status

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.



Resource Monitor

This widget shows resource usage on the device.

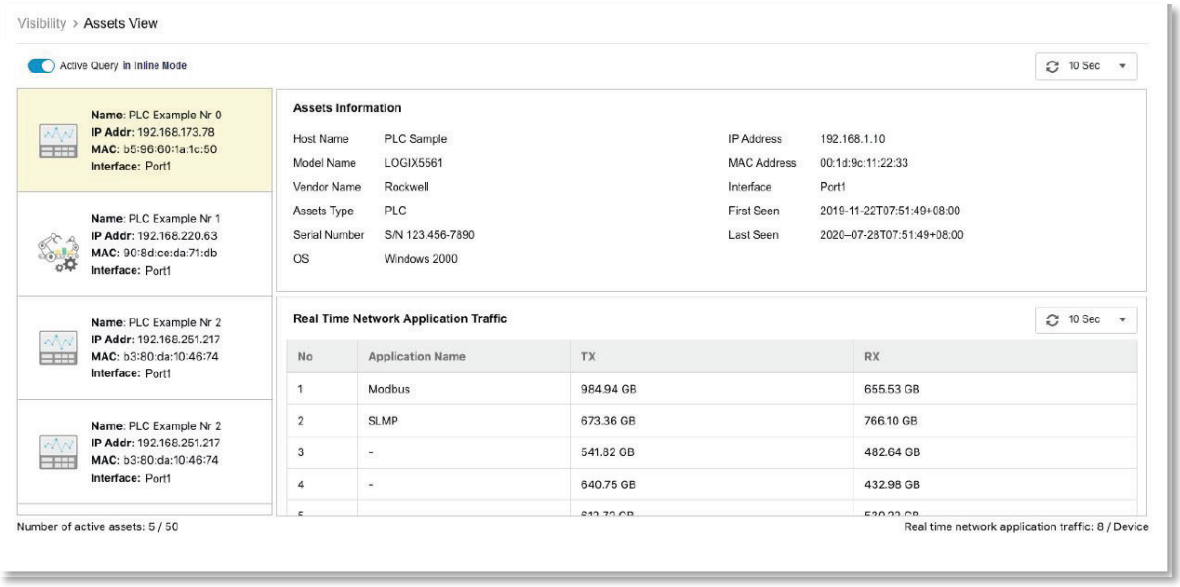


Item	Description
CPU Utilization	Real-time CPU utilization % (according to the refresh time settings)
Memory Utilization	Real-time memory utilization % (according to the refresh time settings)

4

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.



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.

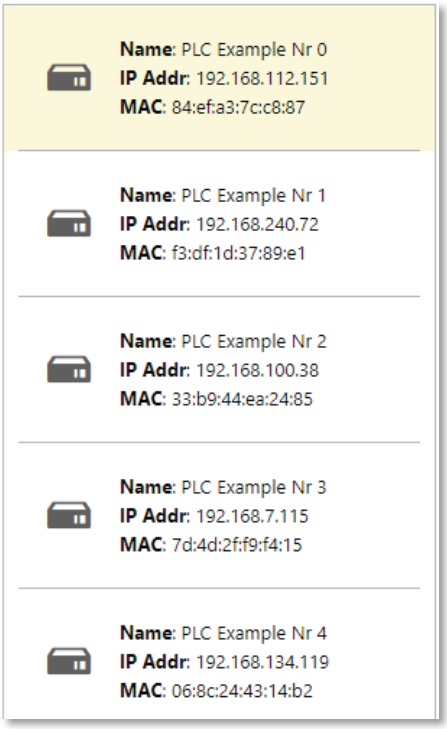
The following topics are covered in this chapter:

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

Viewing Asset Information

Steps:

1. Go to [Visibility] → [Assets View].
2. Click an asset icon and view its detailed information.



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

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

Viewing Real-time Network Application Traffic

Steps:

1. Go to [Visibility] → [Assets View].
2. Click an asset icon 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.
TX	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).

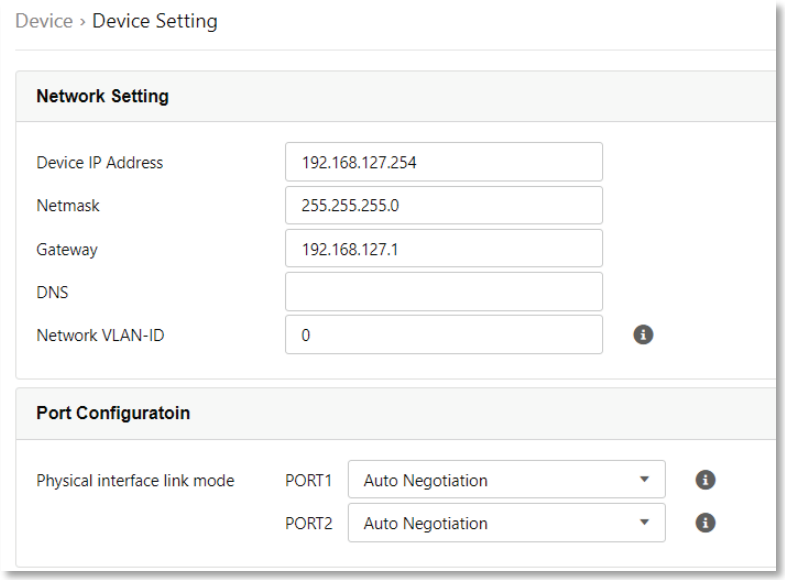
Steps

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

5

The Device Screen

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] → [Device Setting]
2. In the [Network Setting] pane, configure the network settings for the device:

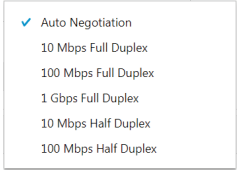
Task	Action
Device IP Address	IP Address of the device
Netmask	Netmask of the device
Gateway	Gateway of the device
DNS	DNS address of the device
Enable VLAN-ID	Enable/Disable VLAN ID
VLAN-ID	Network VLAN-ID of the device

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] → [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. 

6

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:

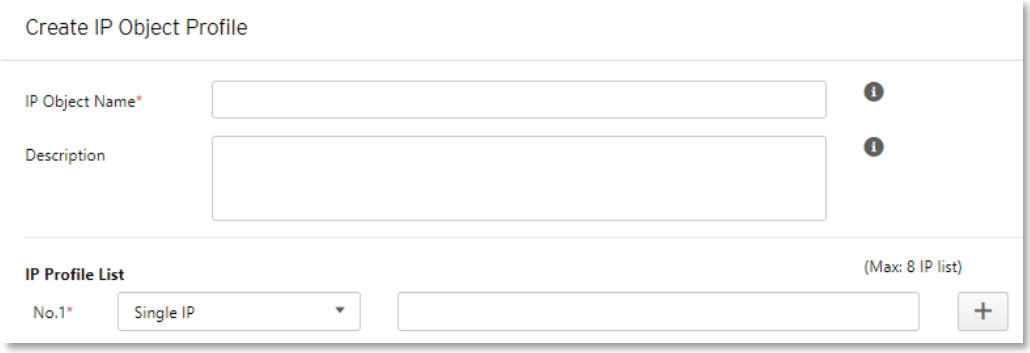
Configuring IP Object Profile

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

- Single IP address
- IP ranges
- IP Subnets

Steps:

1. Go to [Object Profile] → [IP Object Profile].
2. Do one of the following:
   - Click [Add] to create a profile.
   - Click a profile name to edit settings.



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

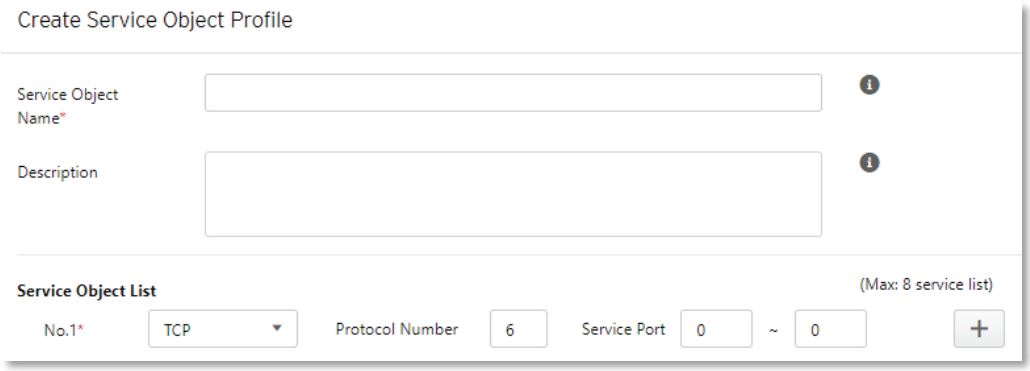
In a service object profile, you can define the following:

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



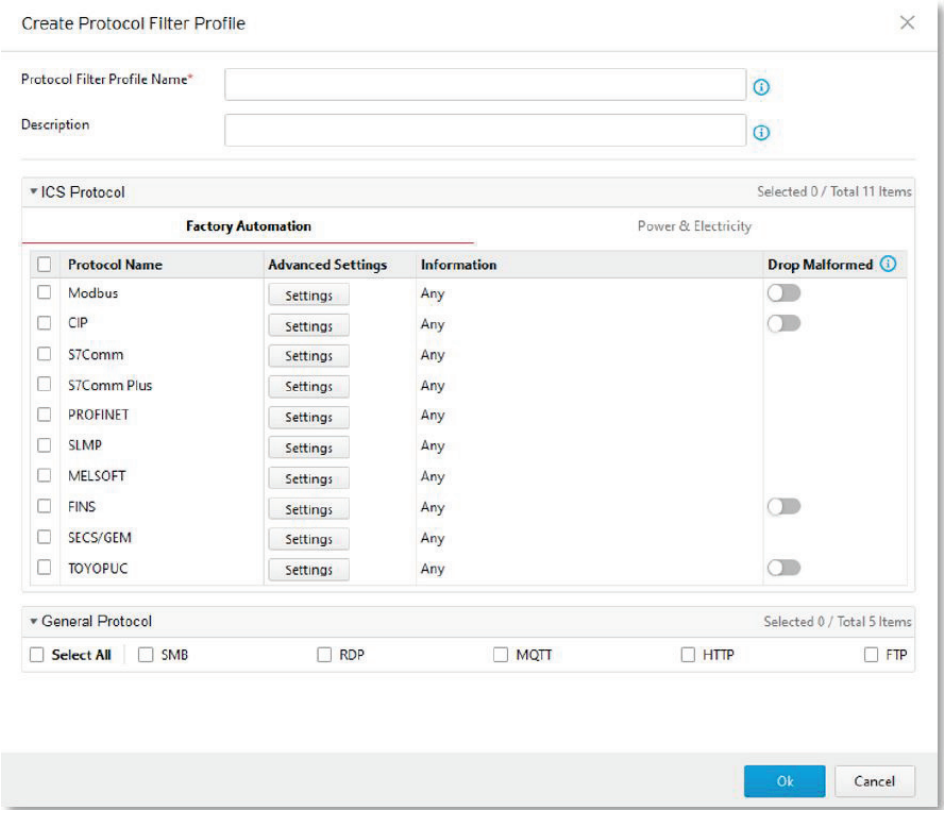
3. Type a descriptive name for the Service Object Profile.
4. Type a description.
5. Provide one of the following definitions:
6. TCP protocol and its port range
7. UDP protocol and its port range
8. ICMP protocol and its type and code
9. Custom protocol with specified protocol number
10. If you want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

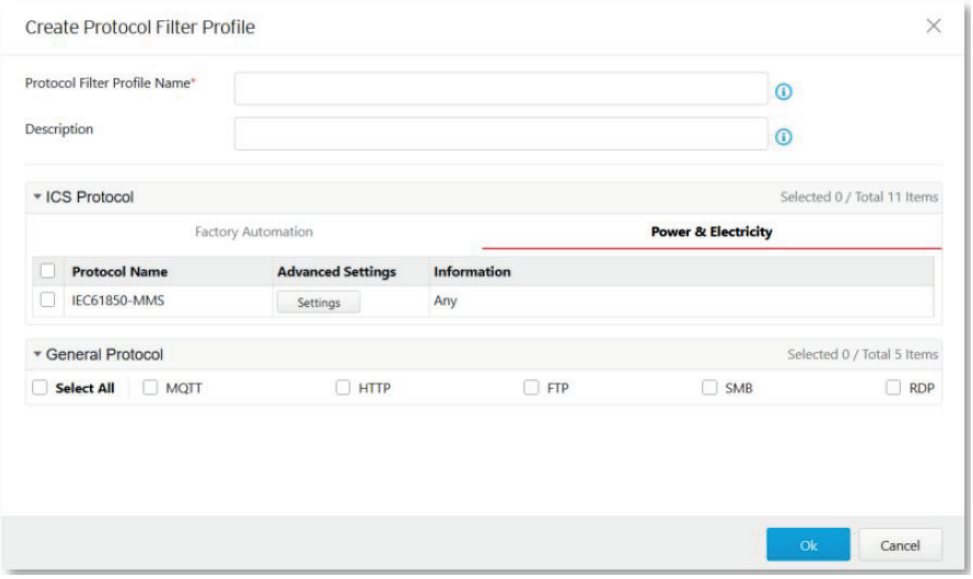
Configuring Protocol Filter Profiles

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:

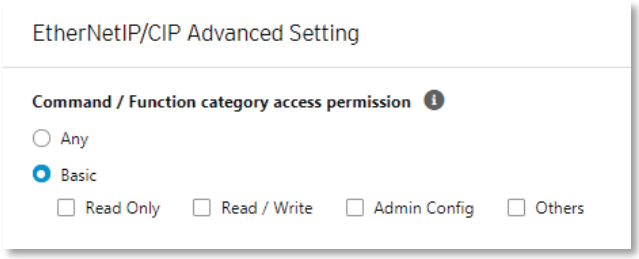
- Details of ICS protocols, including:
  - Modbus
  - CIP
  - S7COMM
  - S7COMM_PLUS
  - PROFINET
  - SLMP
  - FINS
  - MELSOFT
  - SECS/GEM
  - TOYOPUC
  - IEC61850-MMS
- General Protocols, including:
  - HTTP
  - FTP
  - SMB
  - RDP
  - MQTT





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.

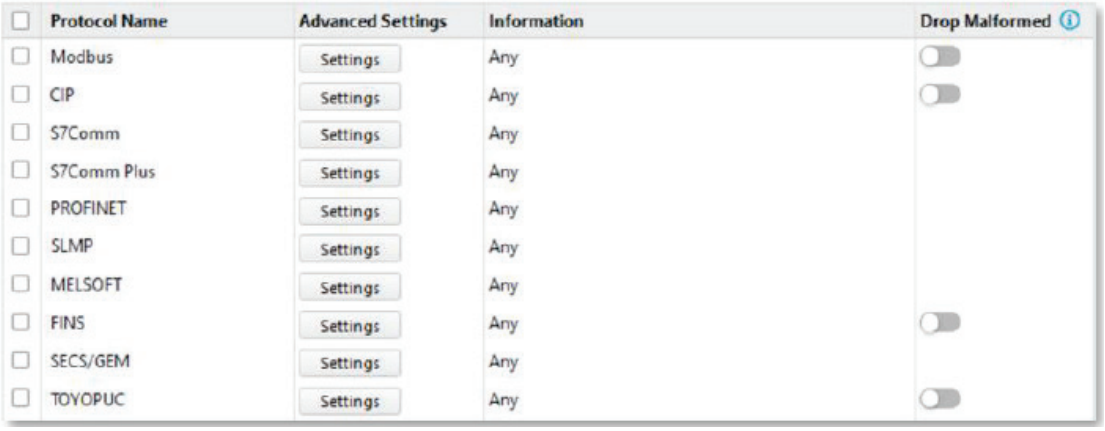


Enabling the Drop Malformed Option for an ICS Protocol

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

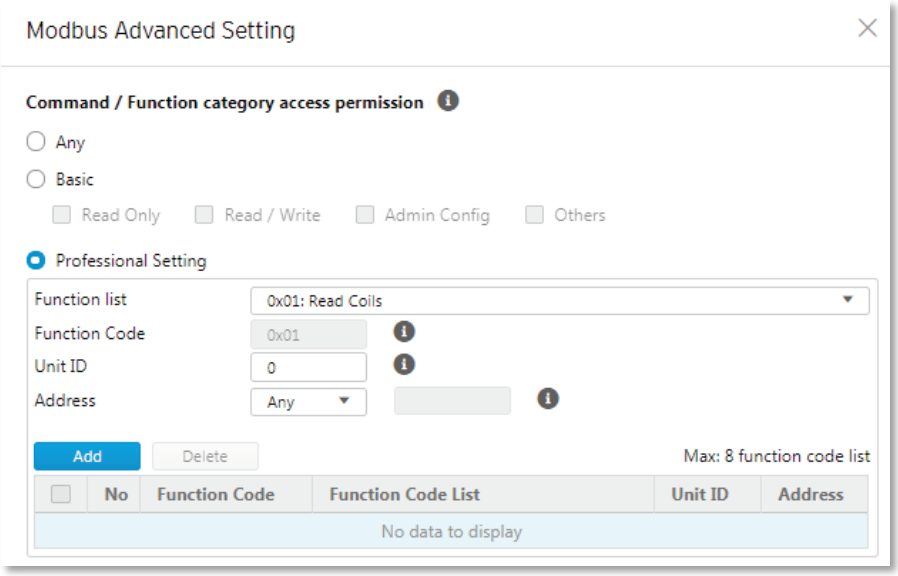
If the [Drop Malformed] option is enabled, EtherCatch will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, EtherCatch will drop the packets of that ICS protocol.

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



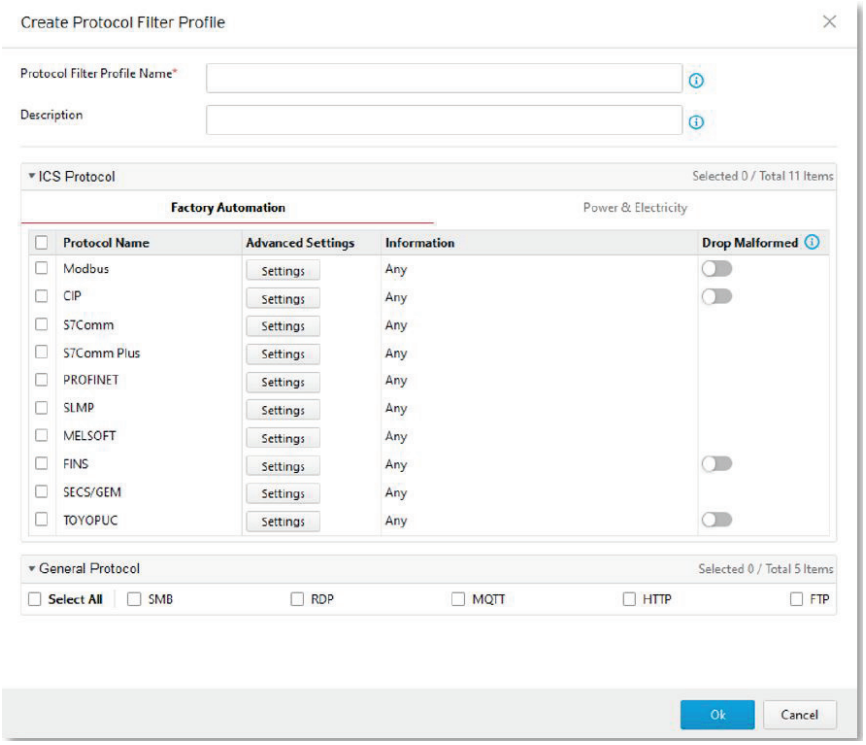
Advanced Settings for the Modbus Protocol

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.



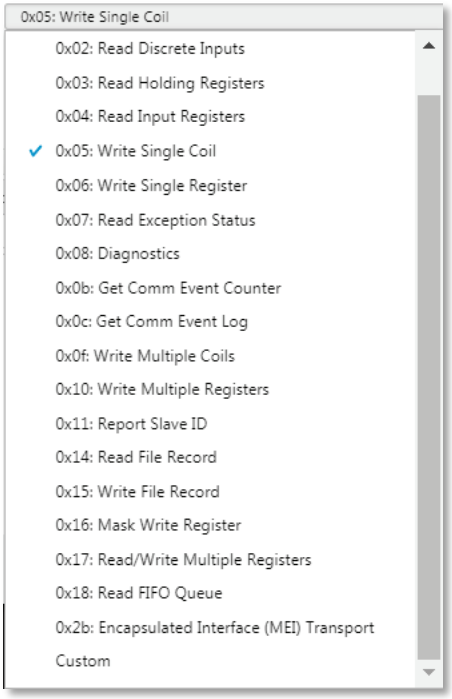
Steps:

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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

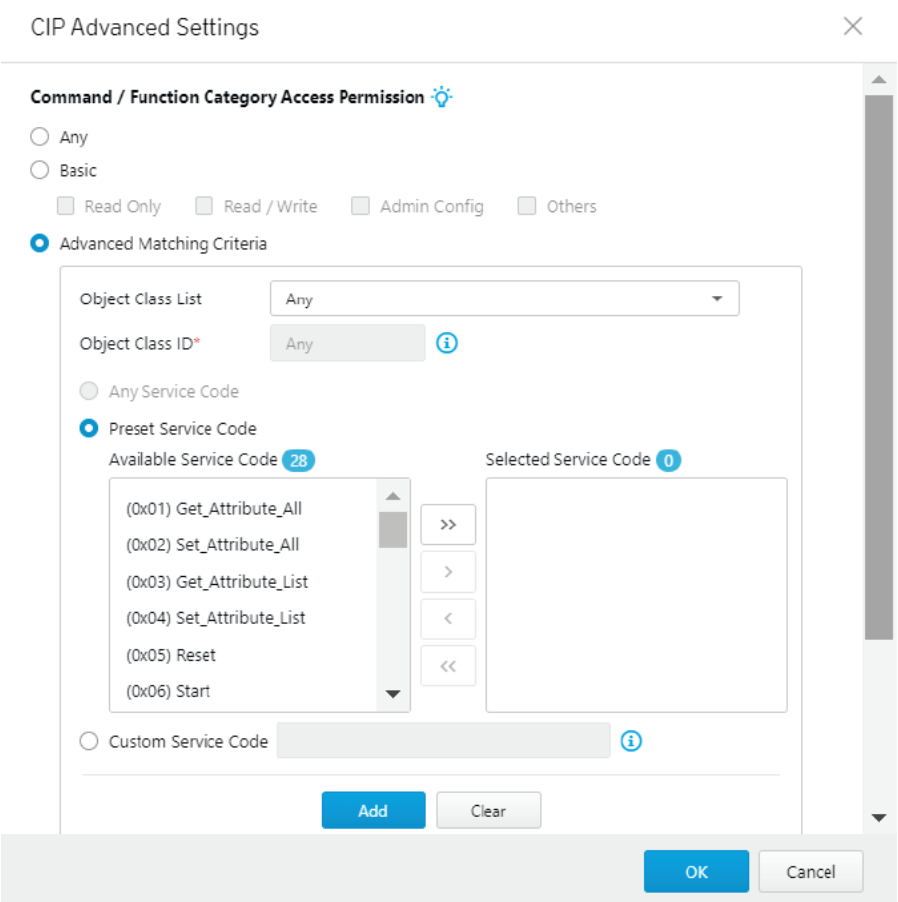
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
   a. Click [Settings] next to a protocol, and select one of the following:
      - **Any** - Specify all available commands or function access in this protocol.
      - **Basic** - Multiple selections of 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.



      - 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].

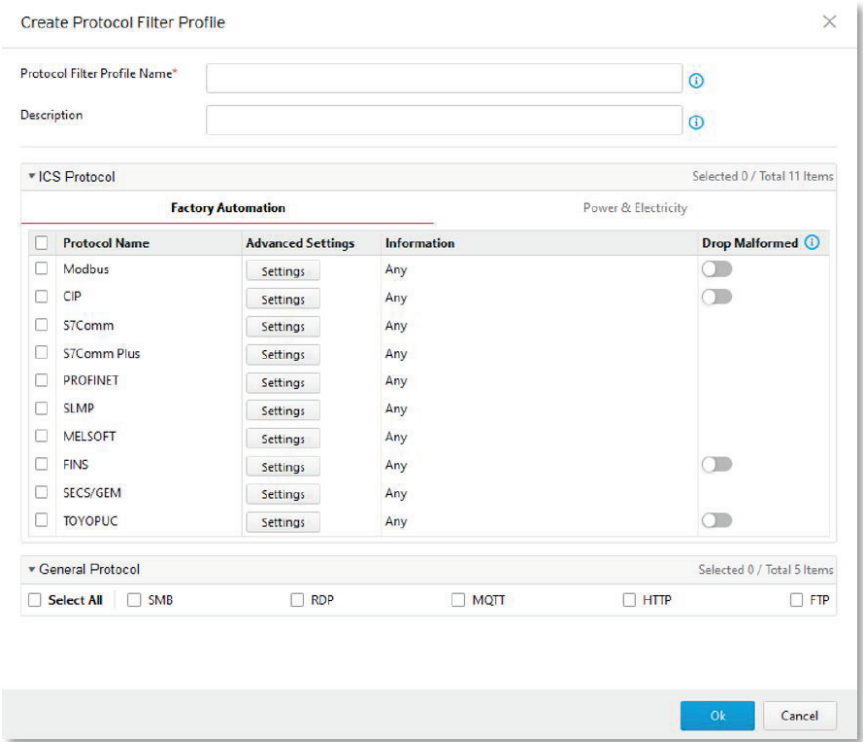
Advanced Settings for the CIP Protocol

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.



Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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 [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.

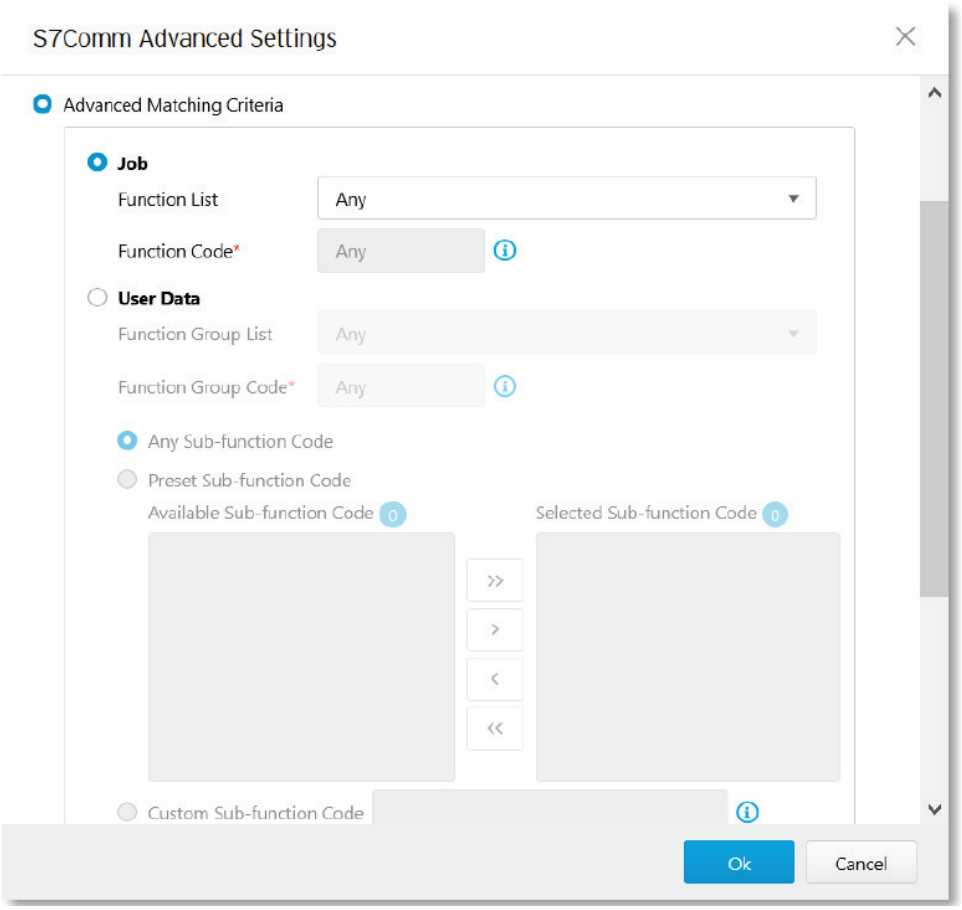
      - If you want all service codes within the specified function to be applied, select [Any Service Code].
      - If you want to specify one or more function codes, move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.

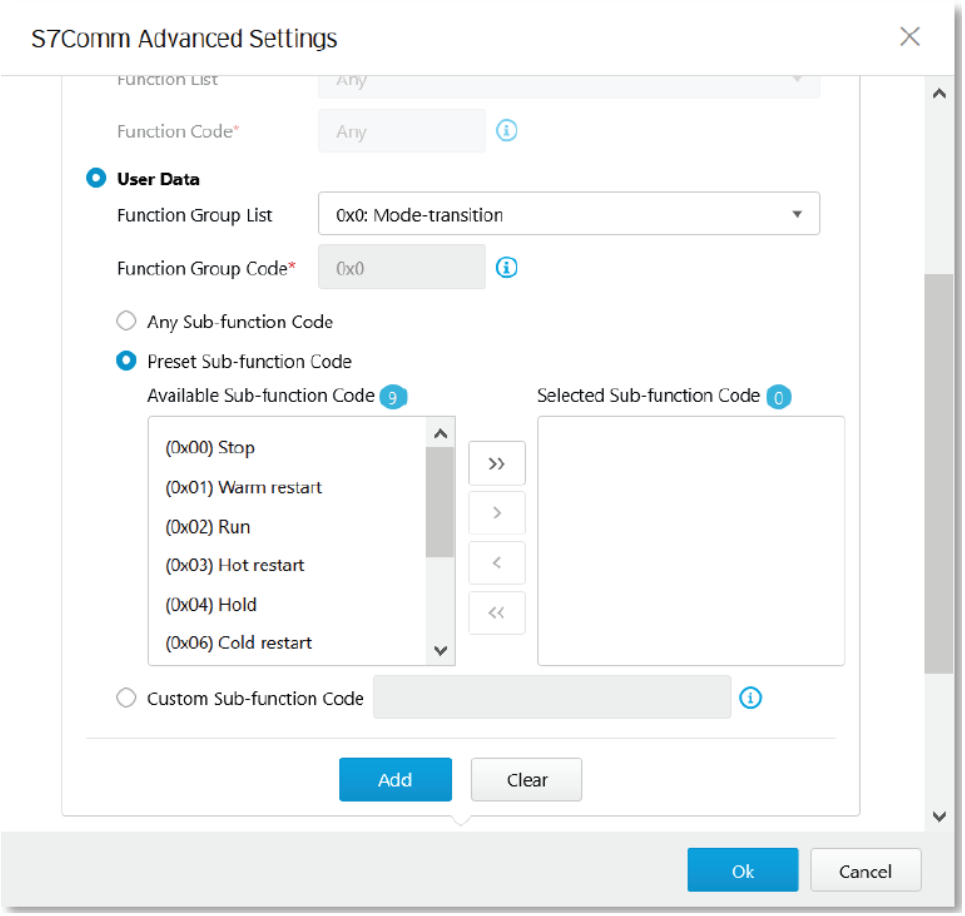
- If you want to specify a custom service code, select [Custom Service Code] and input a service code in the [Custom Service Code] field. .
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

Advanced Settings for S7Comm

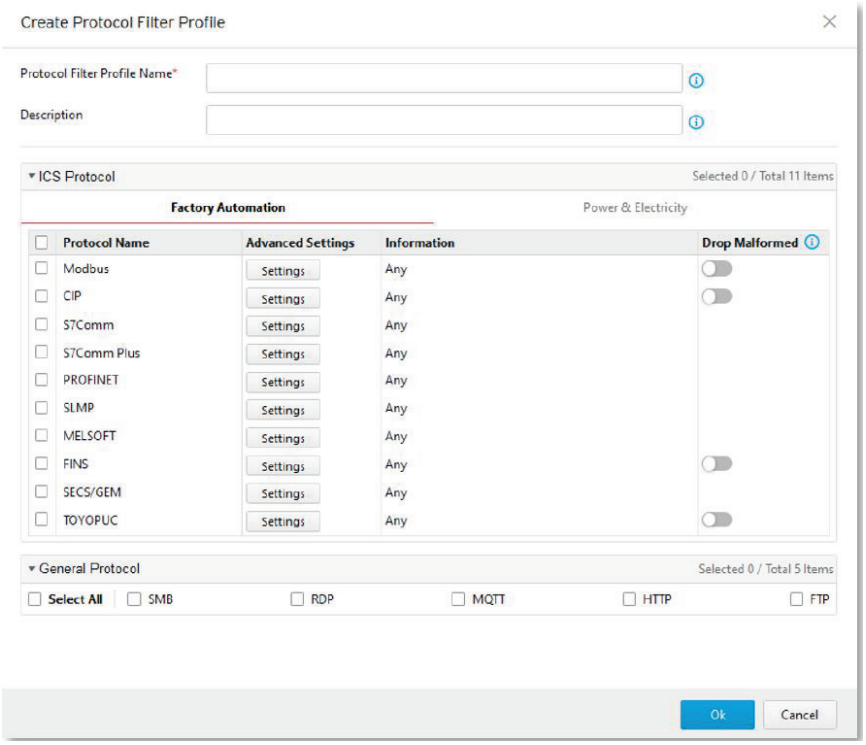
The device features more detailed configurations for the S7Comm ICS protocol. Through the [Advanced Settings] pane, you can further specify the function code, function group code, and sub-function code against which the function will operate.





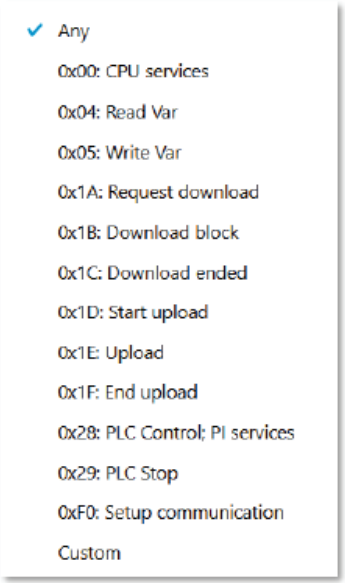
Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.

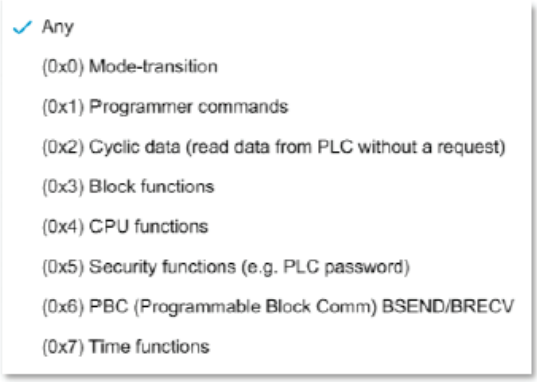


3. Type a protocol filter profile name.

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.



      - 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.



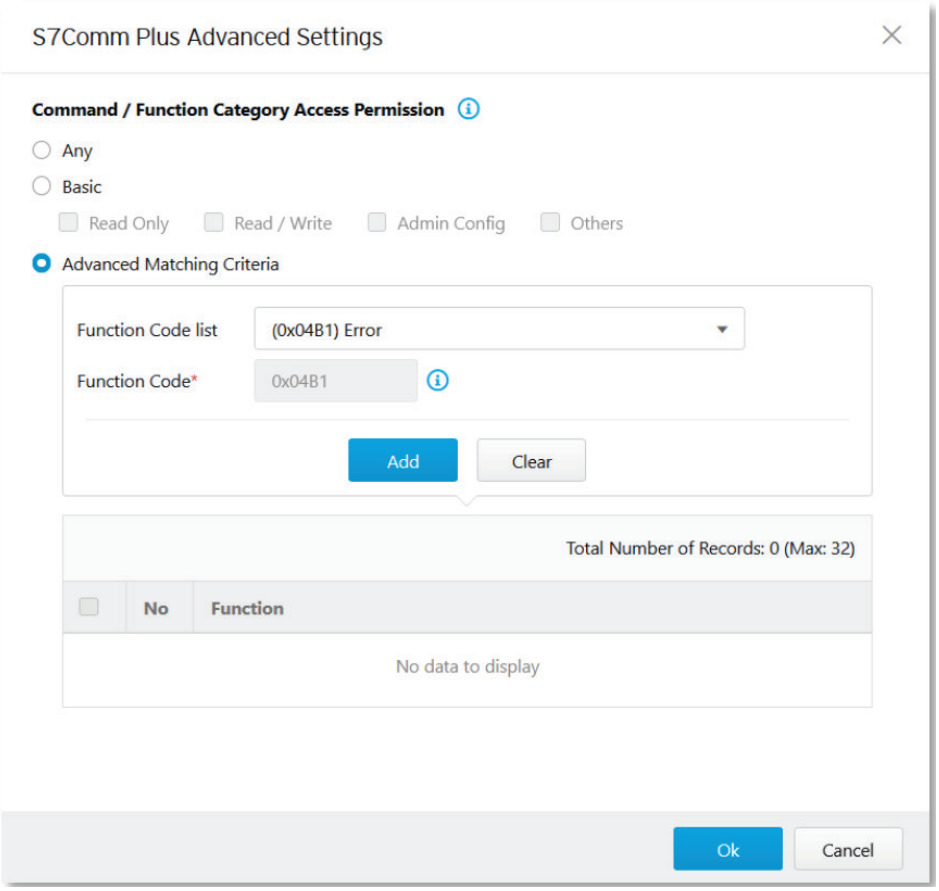
      - If you want all sub-function codes within the specified function group code to be applied, select [Any Sub-function Code].

- 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].

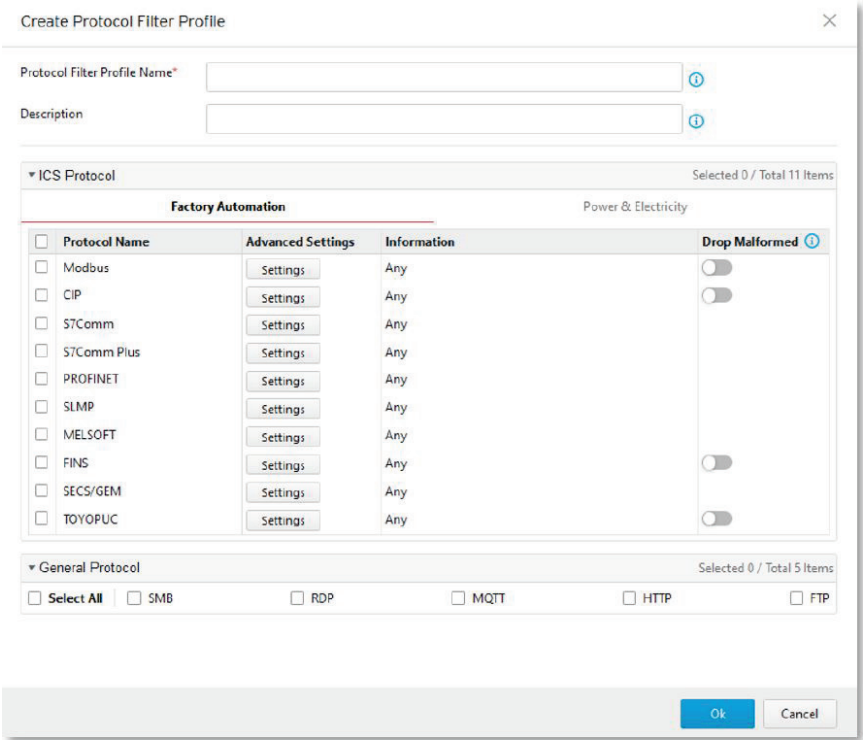
Advanced Settings for S7Comm Plus

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.

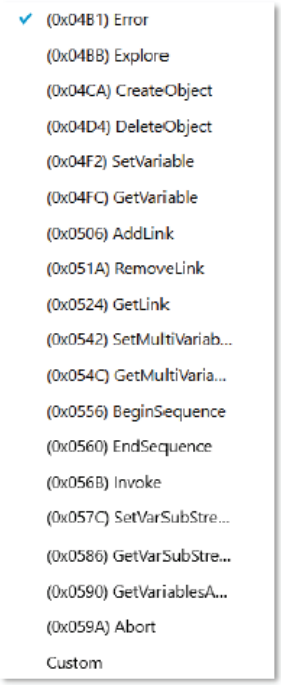


Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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.

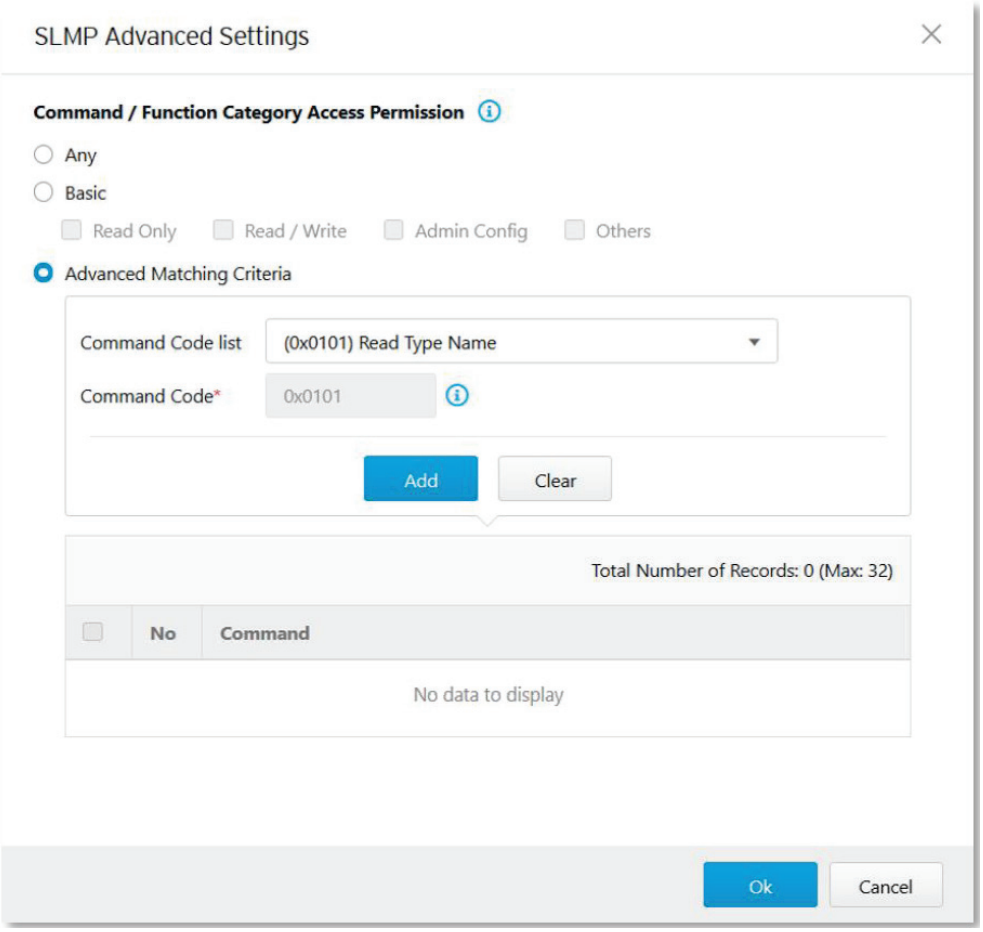


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

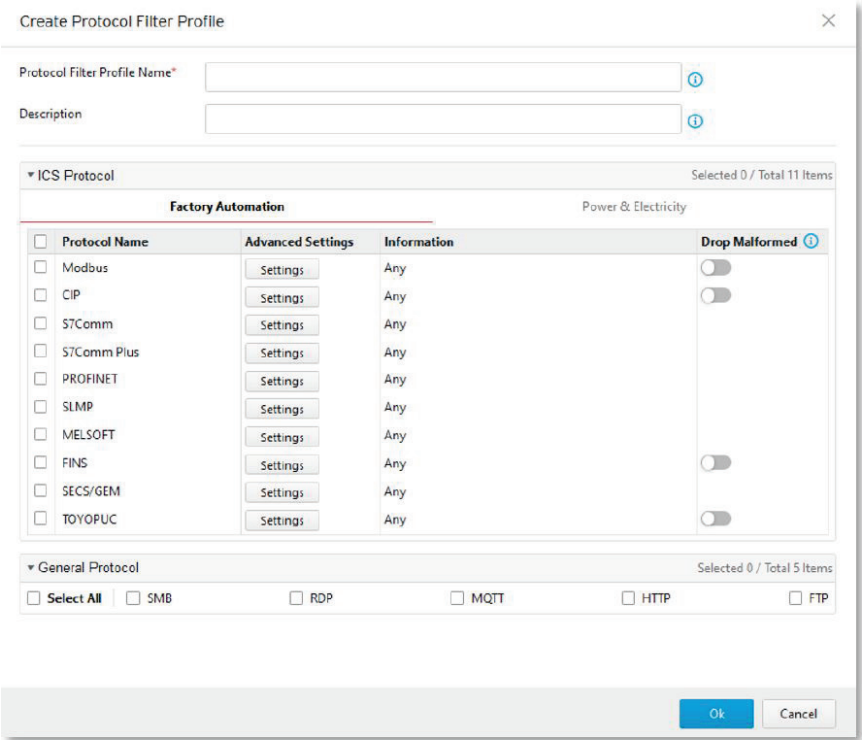
Advanced Settings for SLMP

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.

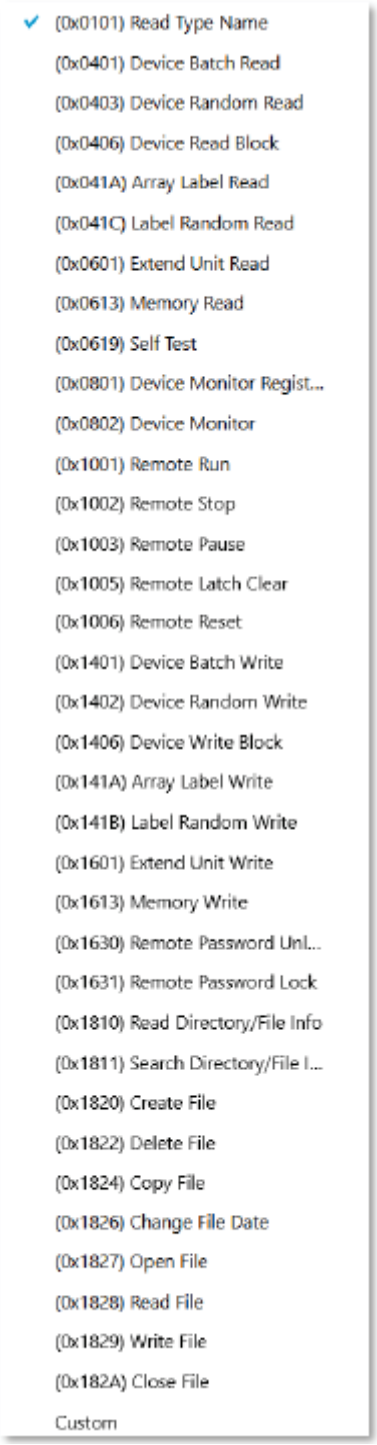


Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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.

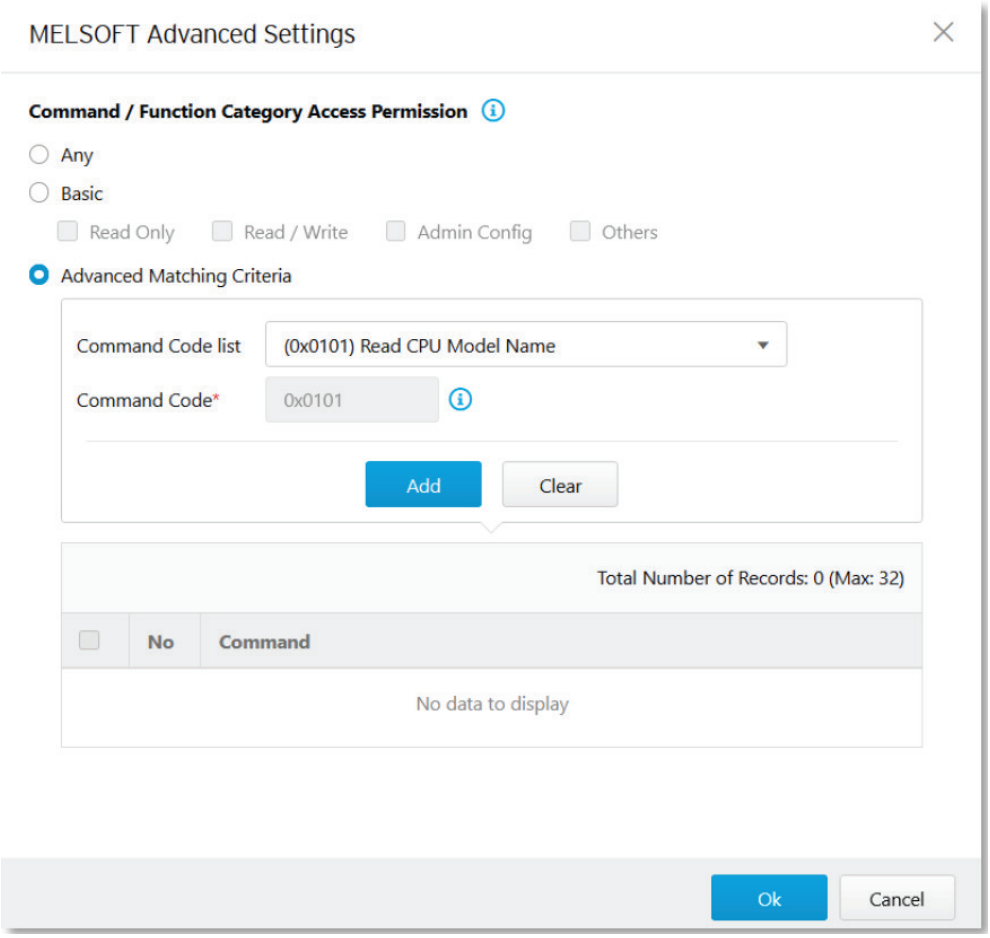


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

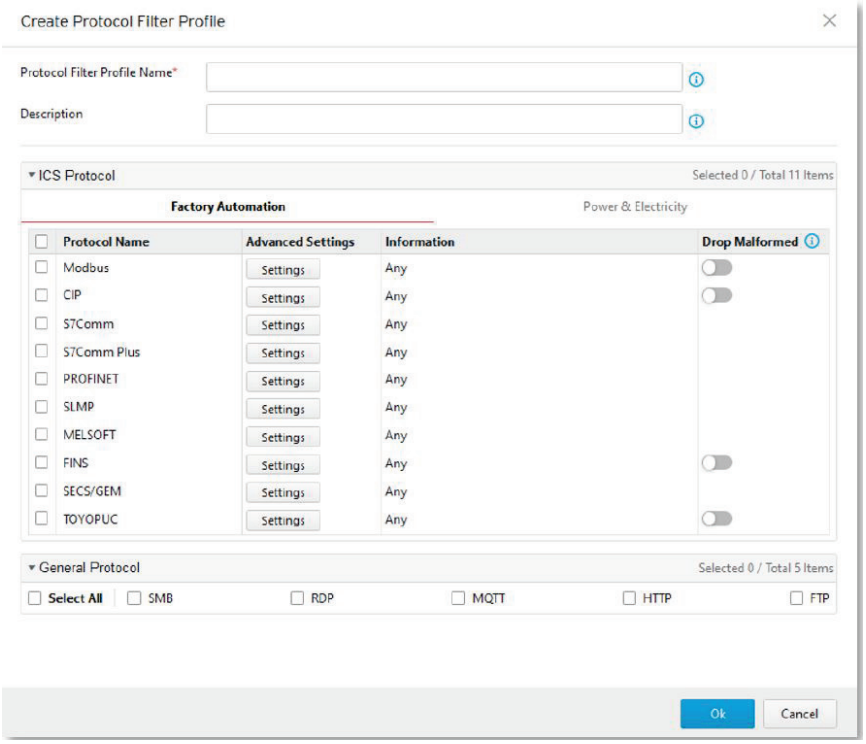
Advanced Settings for MELSOFT

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.



Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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

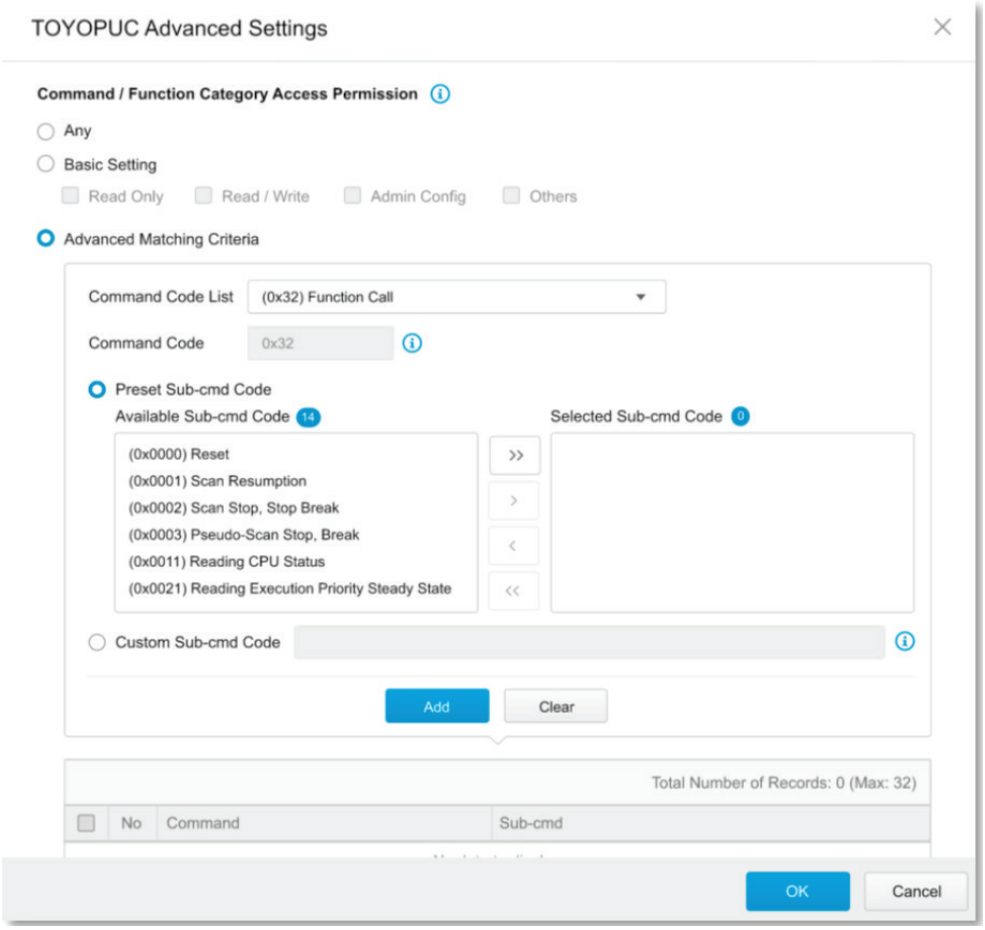
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
   a. Click [Settings] next to a protocol, and select one of the following:
      - **Any** - Specify all available commands or function access in this protocol.
      - **Basic** - Multiple selections of 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.

- 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].

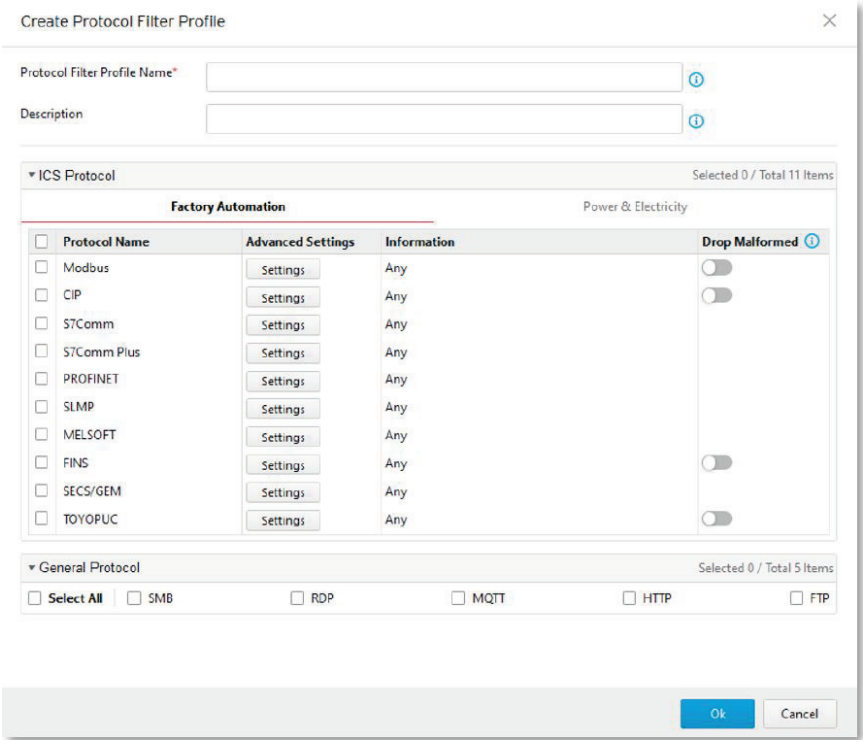
Advanced Settings for TOYOPUC

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.

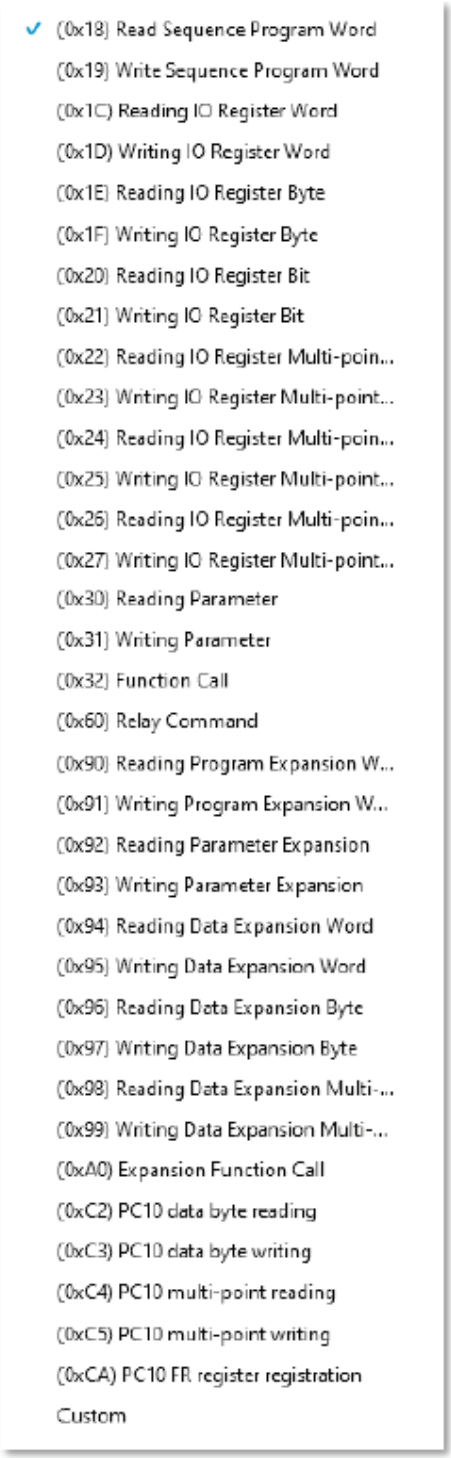


Steps

1. Go to [Object Profile] → [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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.



- 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].

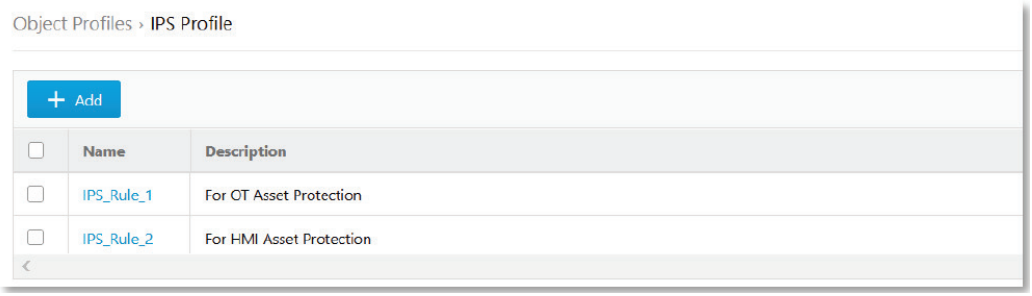
NOTE The [Preset Sub-cmd code] and [Custom Sub-cmd] functions do not support all command codes. Only the "(0x32) Function Call" and "(0xA0) Expansion Function Call" command codes are supported.

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

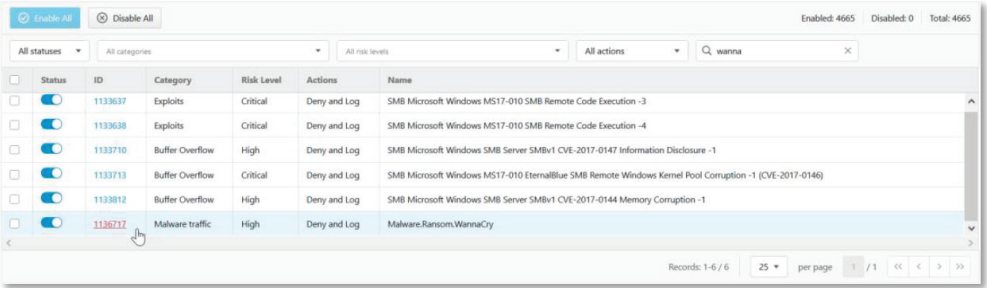
Configuring IPS Profiles

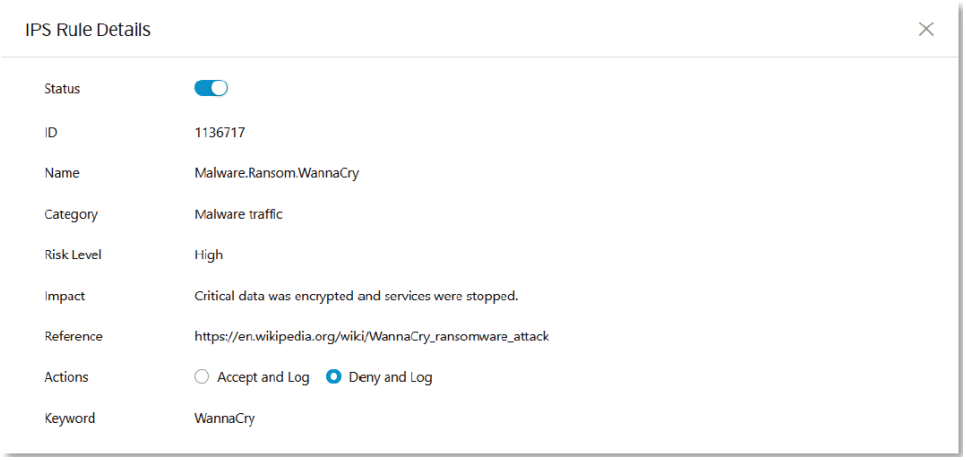
An IPS profile contains more sophisticated pattern rules for more granular control and can be applied to policy rules. The following can items be configured in an IPS profile:

- 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



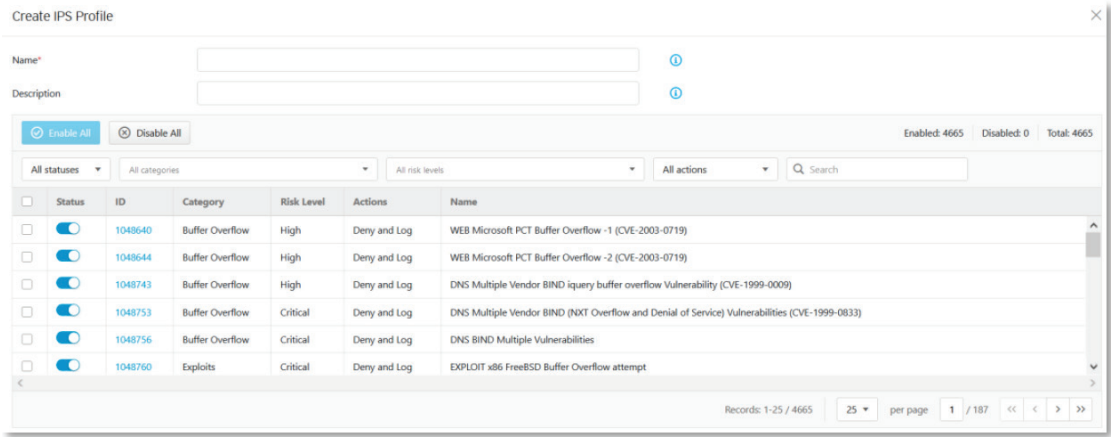
When configuring an IPS pattern rule, you can specify the rule's default action and add it to the IPS profile.





Steps

1. Go to [Object Profile] → [IPS Profile].
2. Click [Add] to add an IPS profile.
   The [Create IPS Profile] screen will appear.



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

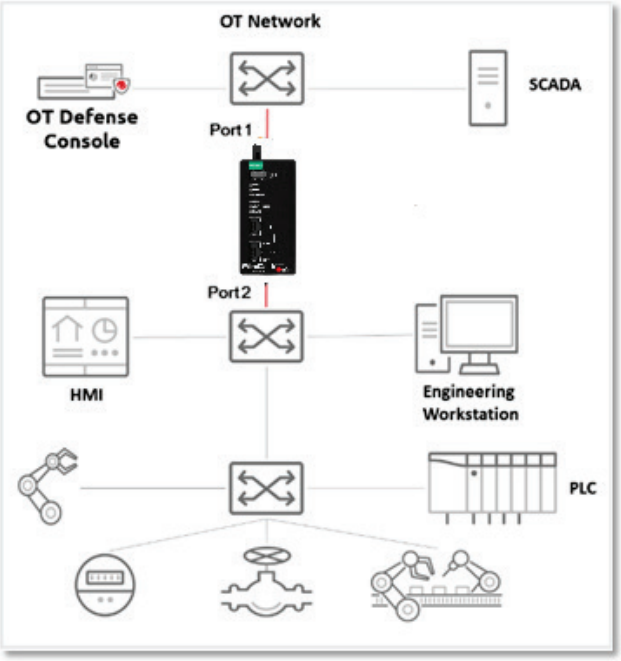
Use the [Security General Setting] screens to configure the security operation mode of the device. The IEC-G102-BP Series offers two operation modes:

- **Inline Mode**
- **Offline Mode**

The following sections describe these two modes in detail.

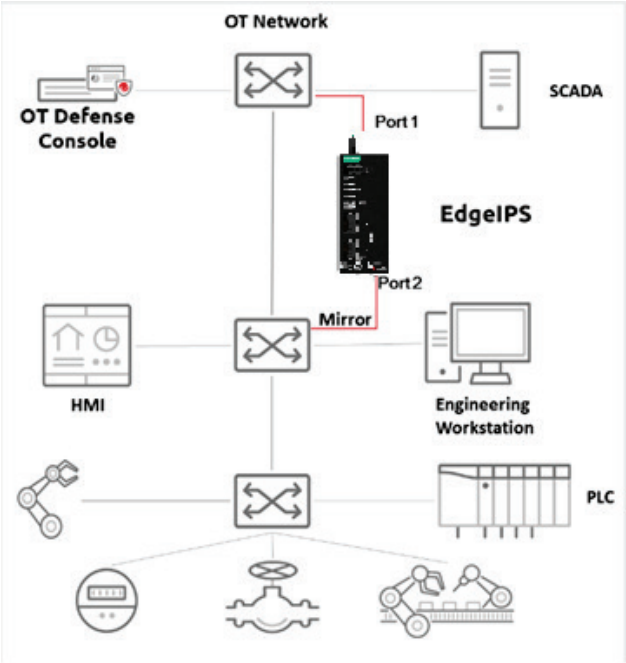
Inline Mode

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.

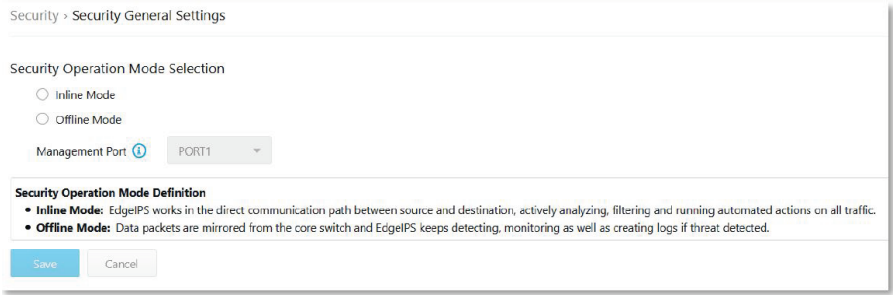


NOTE By default, **Port 1** of the IEC-G102-BP Series functions as the management port, which connects to another switch, allowing the IEC-G102-BP Series to be managed by SDC.

Configuring Security Operation Mode

Steps:

1. Go to [Security] → [Security General Setting]
2. On the [Security General Setting] screen you will see the following.



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.

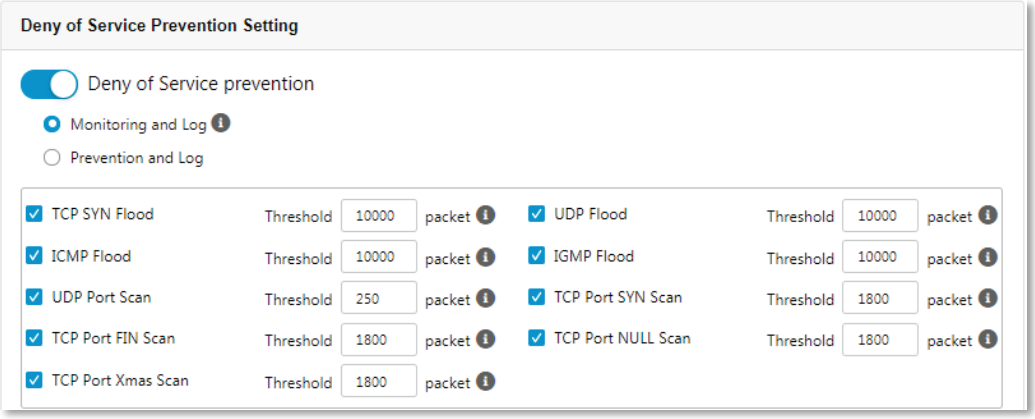
Cybersecurity

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] → [Cyber Security].
2. At the [Cyber Security] screen you will see the [Denial of Service Prevention] pane.



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.

The following table summarizes the settings:

IEC-G102-BP Series Operation Mode (Security General Setting)	Action Settings	Action Performed
Inline Mode	Monitor and Log	• Detects and monitors network attacks, but 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.

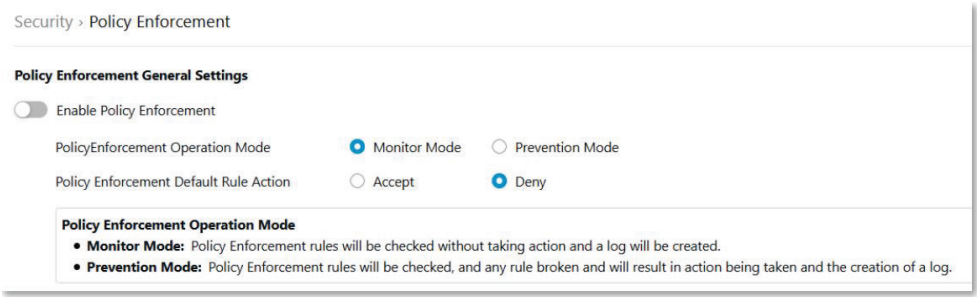
Policy Enforcement

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] → [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.



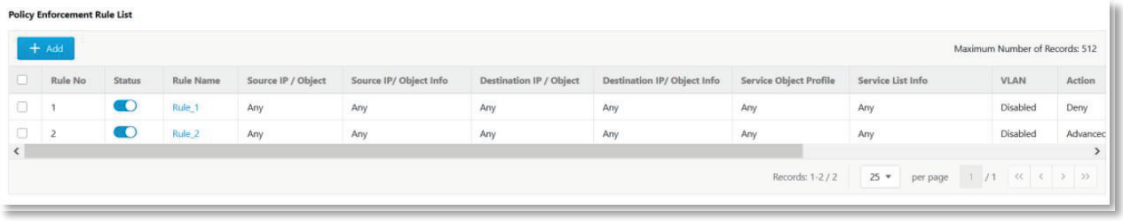
The following table summarizes the settings:

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

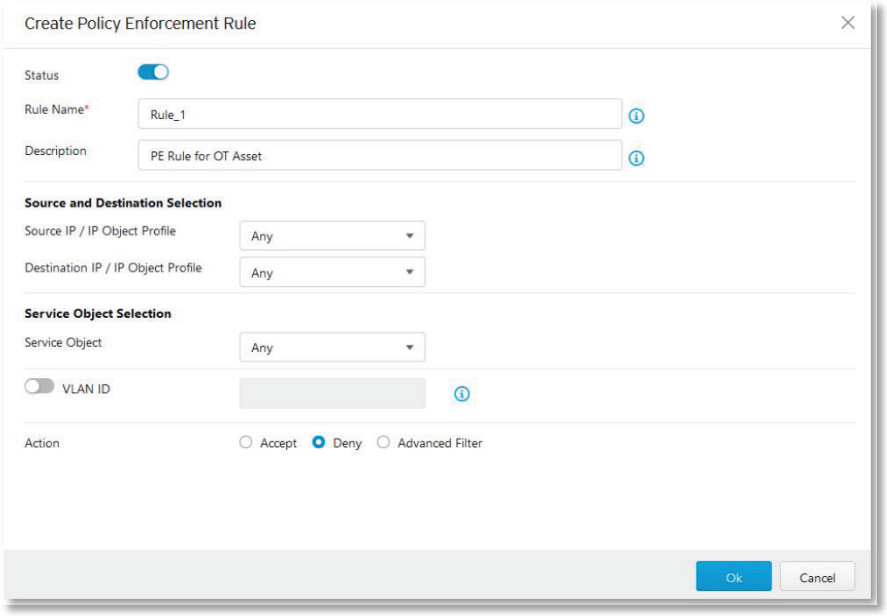
Adding Policy Enforcement Rules

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] → [Policy Enforcement]
3. Under the [Policy Enforcement] screen you will see the following panes.



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



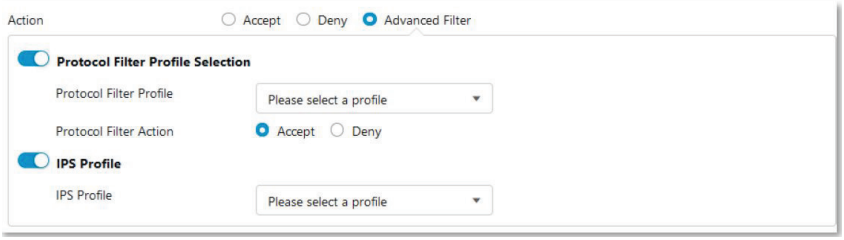
6. Input a descriptive [Rule Name].
7. Input a descriptive [Description] for the rule.
8. At the [Source IP / IP Object Profile] drop-down menu, select either one of the following for the source IP address(es):
   - Any
   - Single IP
   - IP Range
   - IP Subnet
   - Object

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.



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 enforcement rule	Click the check box in front of the policy enforcement rule, click the [Change Priority] button, and specify a new priority for this rule.

NOTE When more than one policy enforcement rule is matched, the 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.

8

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.

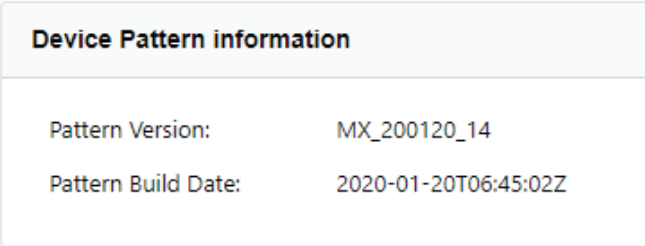
The following topics are covered in this chapter:

- **Viewing Device Pattern Information**
- **Manually Updating the Pattern**

Viewing Device Pattern Information

Steps:

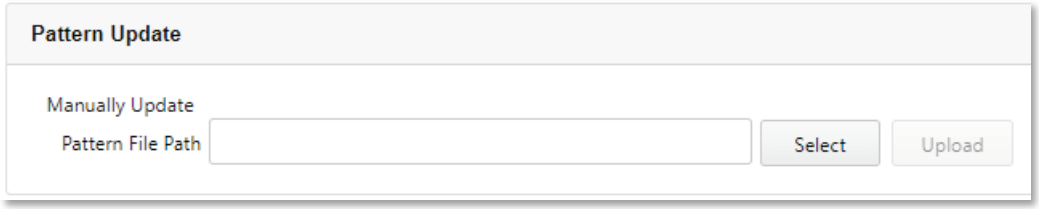
1. Go to [Pattern] → [Pattern Update]
2. At the [Pattern Update] screen you will see the following pane.
3. The [Device Pattern Information] pane shows the [Current Pattern Version] and [Pattern Build Date]



Manually Updating the Pattern

Steps:

1. Go to [Pattern] → [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.



5. Click [Ok]

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

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

9

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] → [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] → [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] → [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	The command or the function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing Asset Detection Logs

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

Steps:

Go to [Logs] → [Assets Detection Logs].

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Event Type	The log event description.
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] → [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] → [Audit Logs].

The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
User ID	The 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 audit log	View	Yes	Yes	Yes	No
Audit Log	View	No	No	No	Yes
Administration	View	Yes	No	No	No
	All operations	Yes	No	No	No

Built-in User Accounts

The following table lists the built-in user accounts 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] → [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:

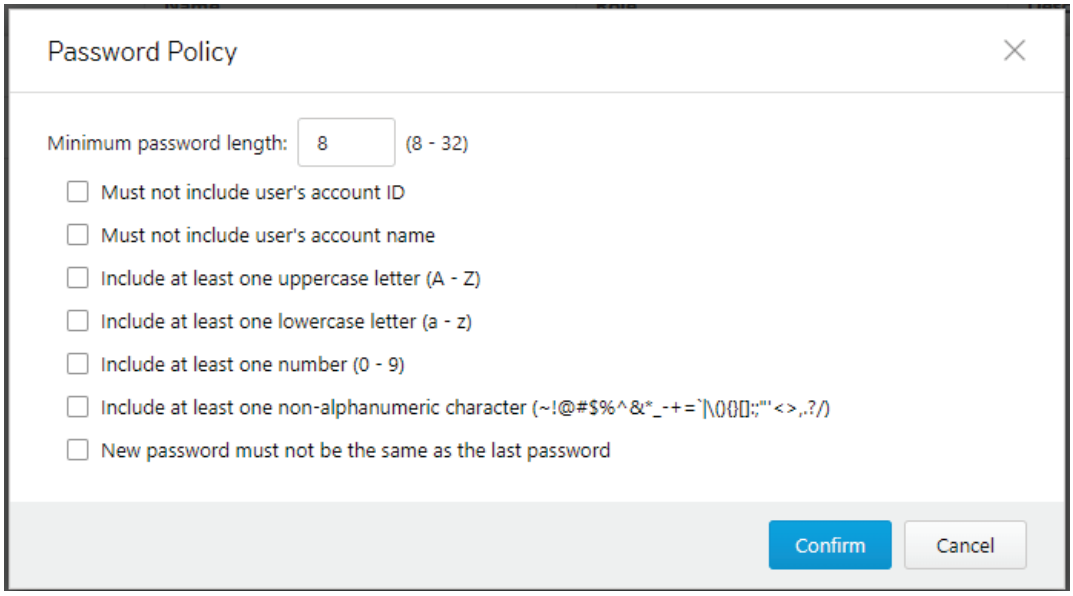
- Password complex settings

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] → [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.



System Management

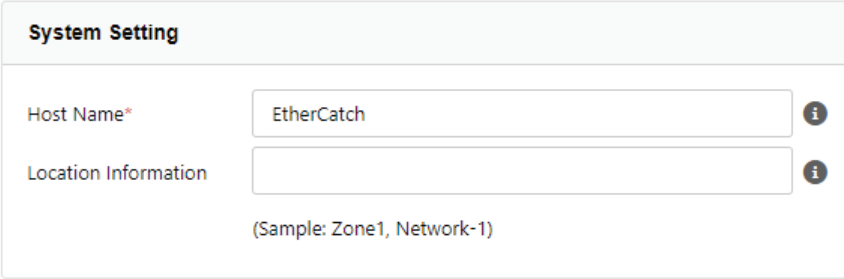
Use the [System Management] screens to do the following:

- 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:

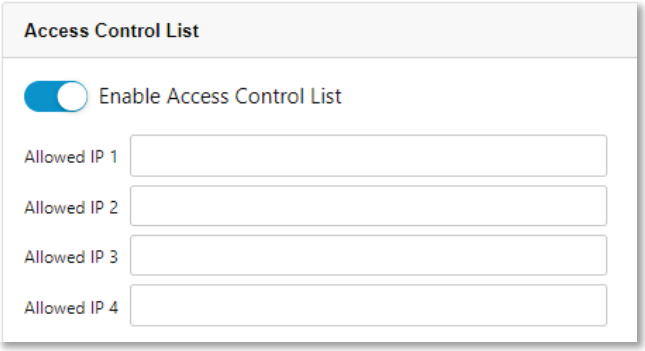
1. Go to [Administration] → [System Management].
2. In the [System Setting] pane, provide the host name and location information for the device.



Configuring Control List Access from Management Clients

Steps:

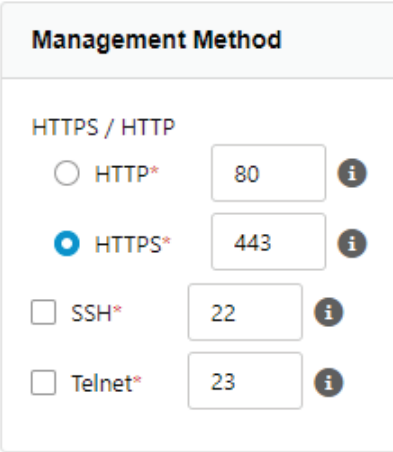
1. Go to [Administration] → [System Management].
2. In the [Access Control List] pane, use the toggle to enable or disable access control from the management clients.
3. Provide the IP addresses that are allowed to manage the device.



Configuring Management Protocols and Ports

Steps:

1. Go to [Administration] → [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.



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.

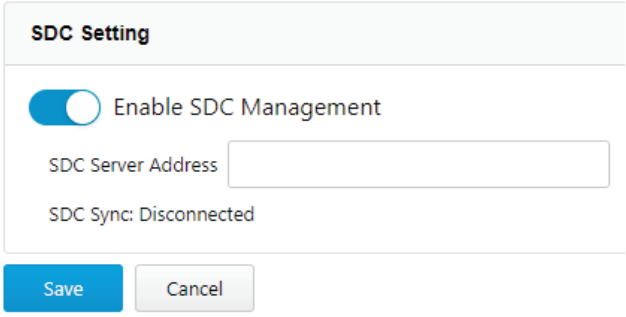
The Sync Setting Screen (Pro Version)

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] → [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.



The Syslog Screen

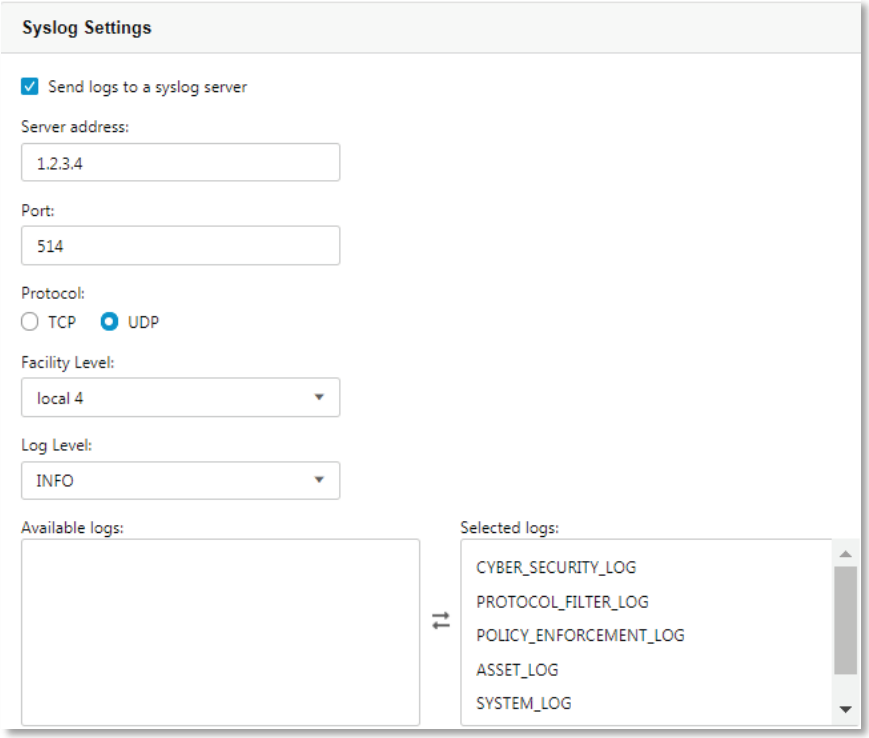
The IEC-G102-BP Series system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) syslog messages are used in the IEC-G102-BP Series.

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

Configuring Syslog Settings

Steps:

1. Go to [Administration] → [Syslog].



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

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

Level	Severity	Description
0	Emergency	• Complete system failure Take immediate action.
1	Critical	• Primary system failure Take immediate action.
2	Alert	• Urgent failures Take immediate action.
3	Error	• Non-urgent failures Resolve issues quickly.
4	Warning	• Error pending Take action to avoid errors.
5	Notice	• Unusual events Immediate action is not required.
6	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.

Syslog Severity Level Mapping Table

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

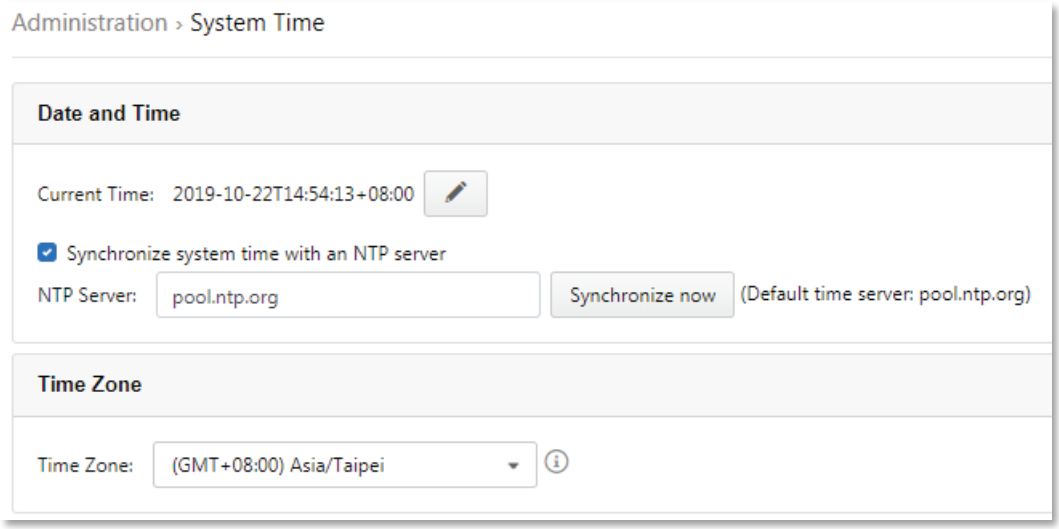
The System Time Screen

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] → [System Time].



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.

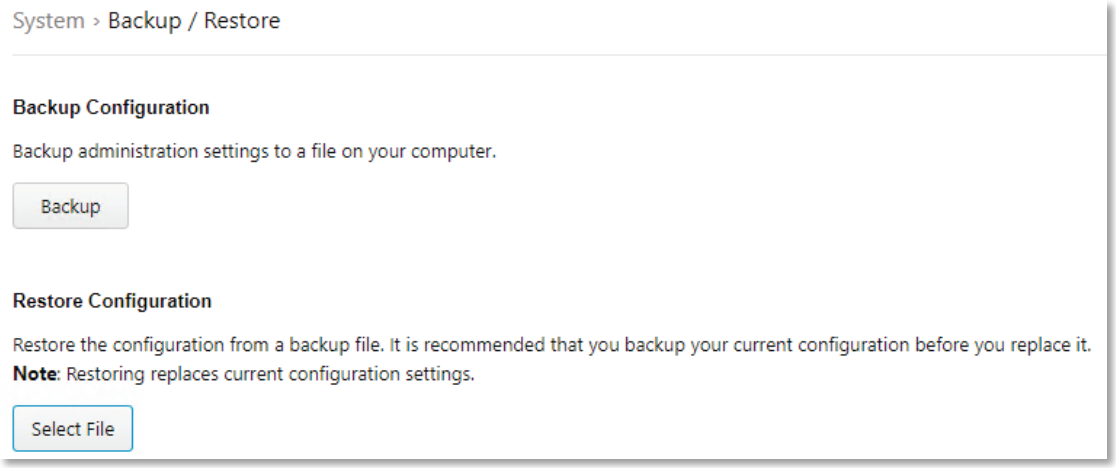
We recommend the following:

- 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] → [Back Up / Restore], and the [Backup / Restore] screen will appear.



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] → [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] → [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:

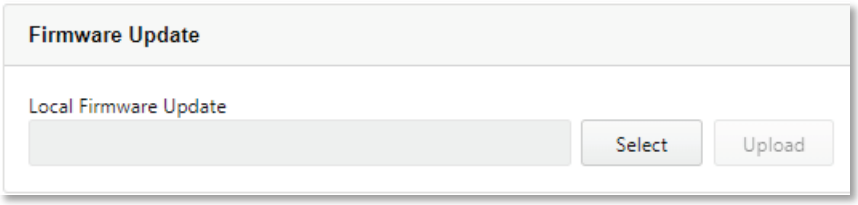
1. Go to [Administration] → [Firmware Management].

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.

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

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



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 https://netsecuritylicense.moxa.com.

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.

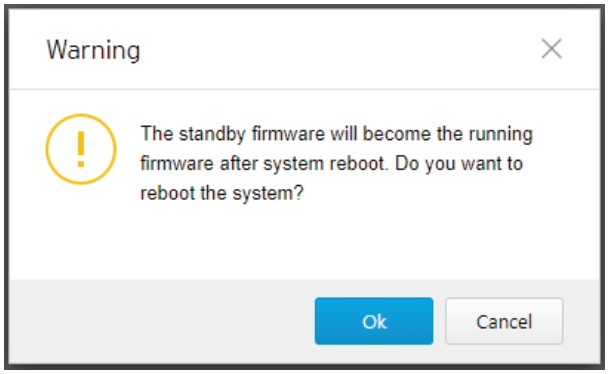
Steps:

1. Go to [Administration] → [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.



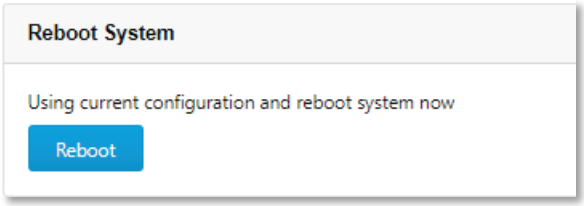
The Reboot System Screen

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

Rebooting the System

Steps:

1. Go to [Administration] → [Reboot System].
2. In the [Reboot System] pane, click [Reboot] to reboot the system.



11

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) Model: ABC-02-USB-T	USB Disk Drive

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

1. 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.

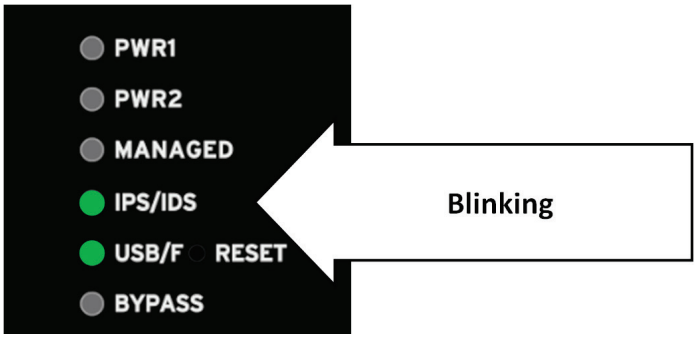
3. Upon successful detection of the USB disk device, the "USB" LED will change to steady green. The system log can also be checked to confirm that a supported USB disk device was properly detected when inserted.

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 processed)	LED	COLOR/STATE
	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 https://netsecuritylicense.moxa.com.