EdgeIPS™

Administrator's Guide

2021-05-10

Copyright © 2021 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/home.aspx

Trend Micro, the Trend Micro t-ball logo, and TXOne Networks are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Table of Contents

Table of Contents 3

Chapter 1 7

About EdgeIPS™ 7

Introduction 7

Main Functions 8

Extensive Support for Industrial Protocols 8

Policy Enforcement for Mission-Critical Machines 8

Improve Shadow OT Visibility by Integrating IT and OT Networks 8

Intrusion Prevention and Intrusion Detection 8

Switch Between Two Flexible Modes, 'Monitor' & 'Prevention' 8

Top Threat Intelligence and Analytics 8

Centralized Management 8

Chapter 2 10

Getting Started 10

Getting Started: Task List 10

Opening the Management Console 11

Changing the Administrator's Password 12

Chapter 3 13

The System Tab 13

Network Information & Device Information 13

Service Status & Throughput Connection 13

Resource Monitor 14

Chapter 4 15

The Visibility Tab 15

Active Query 15

Viewing Asset Information 15

Viewing Real Time Network Application Traffic 16

Chapter 5 17

The Device Tab 17

Configuring Network Settings 17

Configuring Interface Link Mode for Ports 18

Chapter 6 19
The Object Profiles Tab 19
Configuring IP Object Profile 19
Configuring Service Object Profile 20
Configuring Protocol Filter Profile 21
Specifying Commands Allowed in an ICS Protocol 22
Applying the Drop Malformed Option to an ICS Protocol 23
Advanced Settings for Modbus Protocol 23
Advanced Settings for CIP Protocol 26
Advanced Settings for S7COMM 29
Advanced Settings for S7COMM_PLUS 32
Advanced Settings for SLMP 35
Advanced Settings for MELSOFT 38
Advanced Settings for TOYOPUC 42
Configuring IPS Profile 45
Configuring a Pattern Rule for Granular Control 46
Chapter 7 49
The Security Tab 49
Security General Settings 49
Inline Mode 49
Offline Mode 50
Configuring Security Operation Mode 50
Cyber Security 51
Configuring Cyber Security – Denial of Service Prevention 51
Policy Enforcement 53
Configuring Policy Enforcement 53
Adding Policy Enforcement Rules 53
Managing Policy Enforcement Rules 55
Suspicious Objects 56
Configuring Suspicious Objects 56
Chapter 8 58
The Pattern Tab 58

Viewing Device Pattern Information 58
Manually Updating the Pattern 58
Chapter 9 59
The Logs Tab 59
Viewing Cyber Security Logs 59
Viewing Policy Enforcement Logs 60
Viewing Protocol Filter Logs 60
Viewing Suspicious Object Logs 61
Viewing Assets Detection Logs 62
Viewing System Logs 62
Viewing Audit Logs 62
Chapter 10 63
The Administration Tab 63
Account Management 63
User Roles 64
Built-in User Accounts 64
Adding a User Account 64
Changing Your Password 65
Configuring Password Policy Settings 65
Auth Service 66
Configuring TACACS+ 66
System Management 67
Configuring Device Name and Device Location Information 68
Configuring Control List Access from Management Clients 68
Configuring Management Protocols and Ports 68
The Sync Setting Tab 69
Enabling Management by ODC 69
The Syslog Tab 70
Configuring Syslog Settings 70
Syslog Severity Levels 72
Syslog Severity Level Mapping Table 72
The System Time Tab 73

Configuring System Time 73
The Back Up / Restore Tab 74
Backing Up a Configuration 74
Restoring a Configuration 74
The Firmware Management Tab 75
Viewing Device Firmware Information 75
Updating Firmware 75
Rebooting and Applying Firmware 76
The Reboot System Tab 77
Rebooting the System 77
Chapter 11 78
Supported USB Devices 78
Supported actions via USB Disk 78
On-demand Configuration backup 80
Load Pattern from Disk 80
Load Configuration from Disk 81
Load Firmware from Disk 81
Appendix A 83
Terms and Acronyms 83

About EdgeIPS™

Introduction

EdgeIPS™ is 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 device configuration and security policy settings. The whole management process is designed to comply with the manufacturing SOPs of the industry. The EdgeIPS™ protects your individual assets with OT visibility, cybersecurity, and OT protocol allow-listing/deny-listing.

IT and OT traditionally are operated 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 provisioning timely security updates or patches can be difficult. Therefore, the need for security products that provide proper security protection and visibility is on the rise.

Trend Micro provides a wide range of security products that cover both your IT and OT layers. These easy-to-build solutions provide an active and immediate protection to Industrial Control System (ICS) environments with the following features:

- Certified industrial grade hardware with size, power consumption, and durability tailored for OT environments, as well as the ability to tolerate a wide range of temperature variations
- Threat detection and interception, with safeguards against the spread of worms
- Protection against Advanced Persistent Threats (APTs) and Denial of Service (DoS) attacks that target vulnerable legacy devices
- Virtual patch protection against OT device exploits

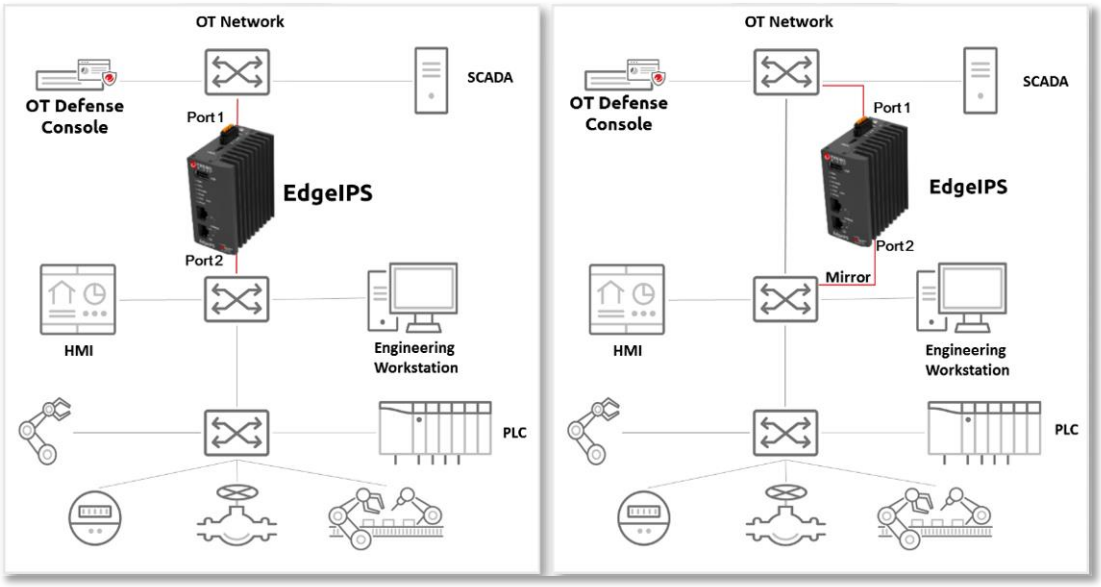


Figure 1. TXOne Networks security solutions for an OT network

Main Functions

EdgeIPS[tm] is a transparent network security device. The main functions of the product are as follows:

Extensive Support for Industrial Protocols

EdgeIPS supports the identification of a wide range of industrial control protocols, including Modbus and other protocols used by well-known international companies such 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

EdgeIPS's core technology TXODI 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 operational traffic, block unknown network attacks, and block other activity that matches a defined policy.

Improve Shadow OT Visibility by Integrating IT and OT Networks

EdgeIPS 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 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'

EdgeFire flexibly switches between 'Monitor' and 'Prevention' modes. '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

EdgeIPS provides advanced protection against unknown threats with its up-to-date threat information. With the help of the Zero Day Initiative (ZDI) vulnerability reward program, EdgeIPS offers your systems exclusive protection from undisclosed and zero-day threats.

Centralized Management

TXOne's OT Defense Console (ODC) provides a graphical user interface for policy management in compliance with manufacturing SOP. It centrally monitors operations information, edits network protection policies, and sets patterns for attack behaviors.

All 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 configuration 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

Getting Started

This chapter describes the EdgeIPS™ and how to get started with configuring the initial settings.

Note: For an overview of the physical hardware and characteristics, or a more condensed manual to help with initial setup of the device, please refer to the document "EdgeIPS - Quick Setup Guide"

Getting Started: Task List

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

Procedure

1. Open the management console.
   For more information, see *Opening the Management Console on page 11*.
2. Change the administrator password.
   For more information, see *Changing the Administrator's Password on page 12*.
3. Configure the system time.
   For more information, see *Configuring System Time on page 73*.
4. (Optional) Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings on page 70*.
5. Configure Object Profiles.
   For more information, see *The Object Profiles on page 19*.
6. Configure security policies.
   For more information, see *The Security on page 49*.
7. Configure the device name and device location information.
   For more information, see *Configuring Device Name and Device Location Information on page 68*.
8. (Optional) Configure access control list from management clients.
   For more information, see *Configuring Control List Access from Management Clients on page 68*.
9. Configure management protocols and ports.
   For more information, see *Configuring Management Protocols and Ports on page 68*.
10. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device.
    For more information, see *Manually Updating the Pattern on page 58*.
11. (Optional) Enabling Management by ODC.
    For more information, see *Enabling Management by ODC on page 69*.
12. Configure the network settings and network interface link modes for the device.
    For more information, see *The Device on page 17*.

Opening the Management Console

EdgeIPS 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.

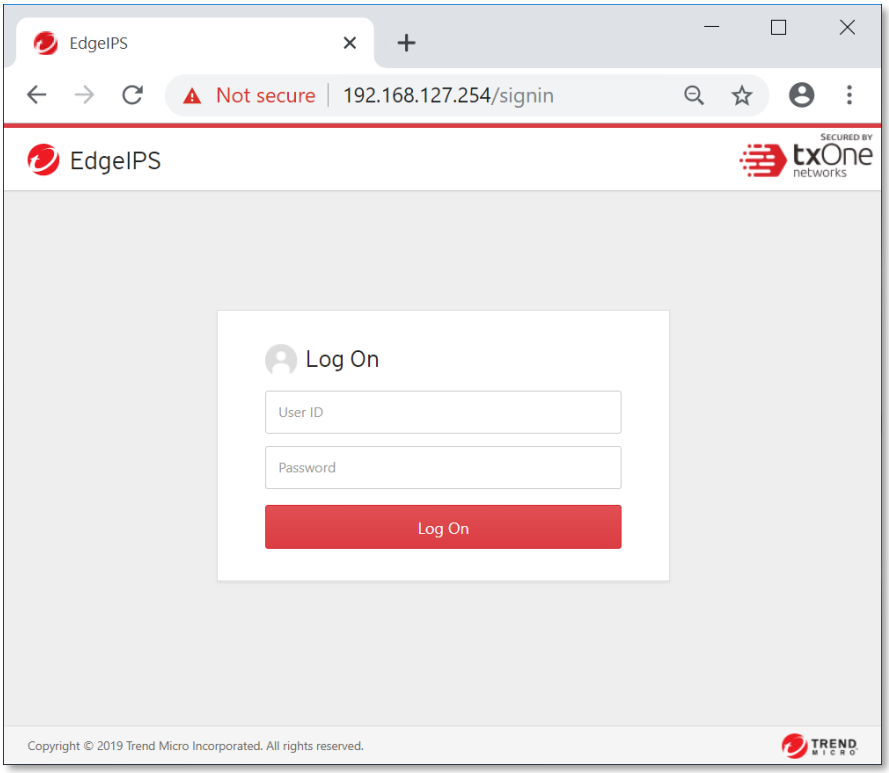
Procedure

1. In a web browser, type the address of the EdgeIPS in the following format:
   https://192.168.127.254

Note: TXONE devices use 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.

The logon screen will appear.

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



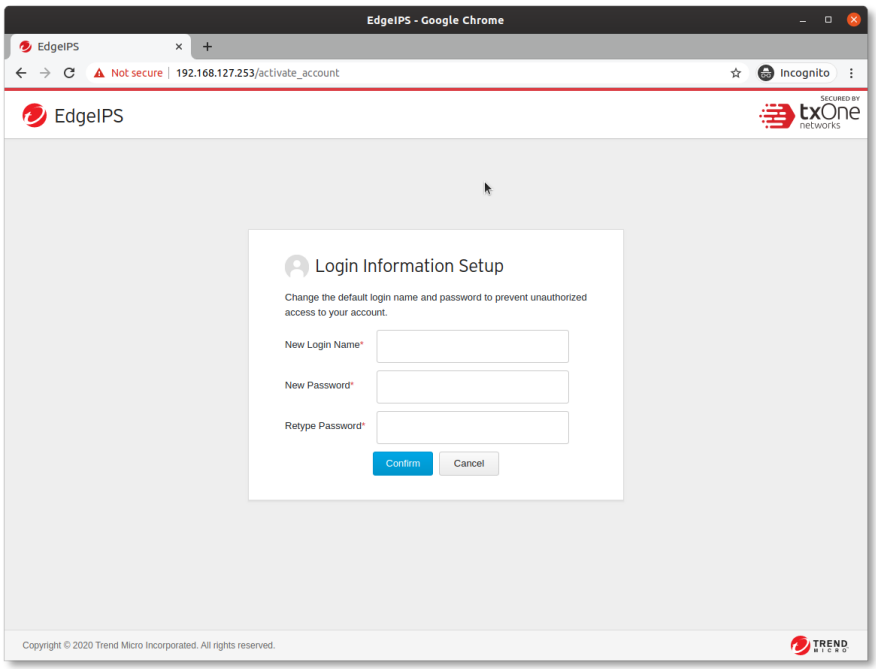
2. Input the logon credentials (user ID and password).

   Use the default administrator logon credentials when logging on for the first time:

   - User ID: `admin`
   - Password: `txone`

3. Click Log On.

4. When logging in for the first time or after a factory reset, you will be prompted to change the default user ID and password. The default user ID and password cannot be used.



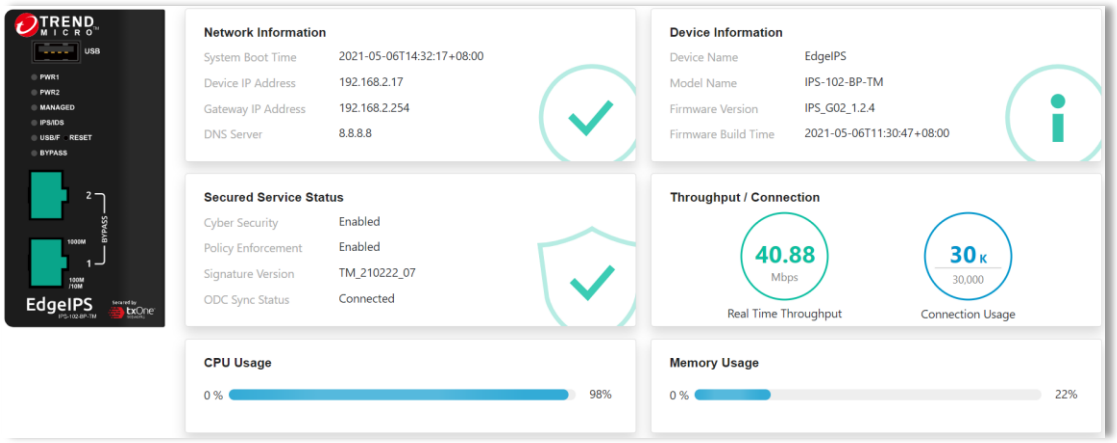
5. Login with newly changed user ID/password credentials.

Changing the Administrator's Password

Refer to chapter "The Administration Tab", under sub-topic Account Management > Changing Your Password.

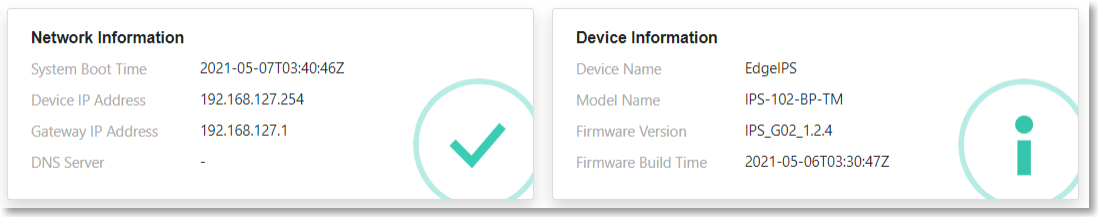
The System Tab

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



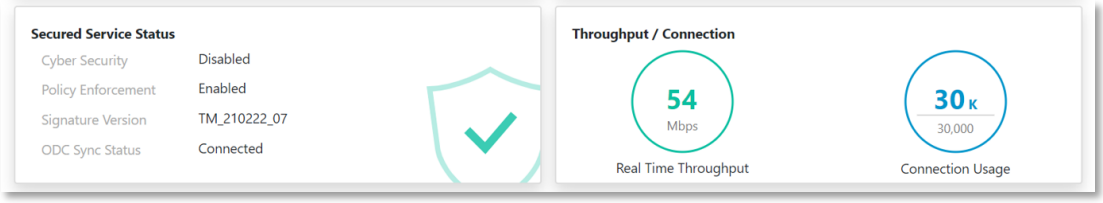
Network Information & Device Information

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.



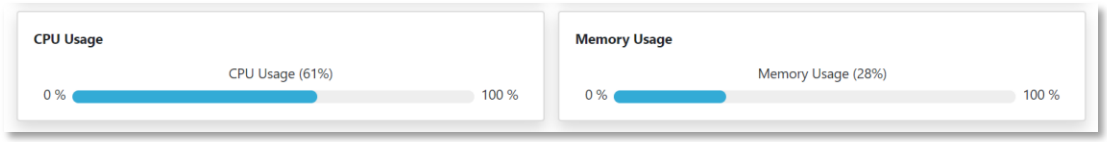
Service Status & Throughput Connection

The widget shows whether cyber security is enabled, whether policy enforcement is enabled, the signature version on the device, if the device is managed by ODC, current network throughput on the device, and current network connection (according to the refresh time settings) usage on the device.



Resource Monitor

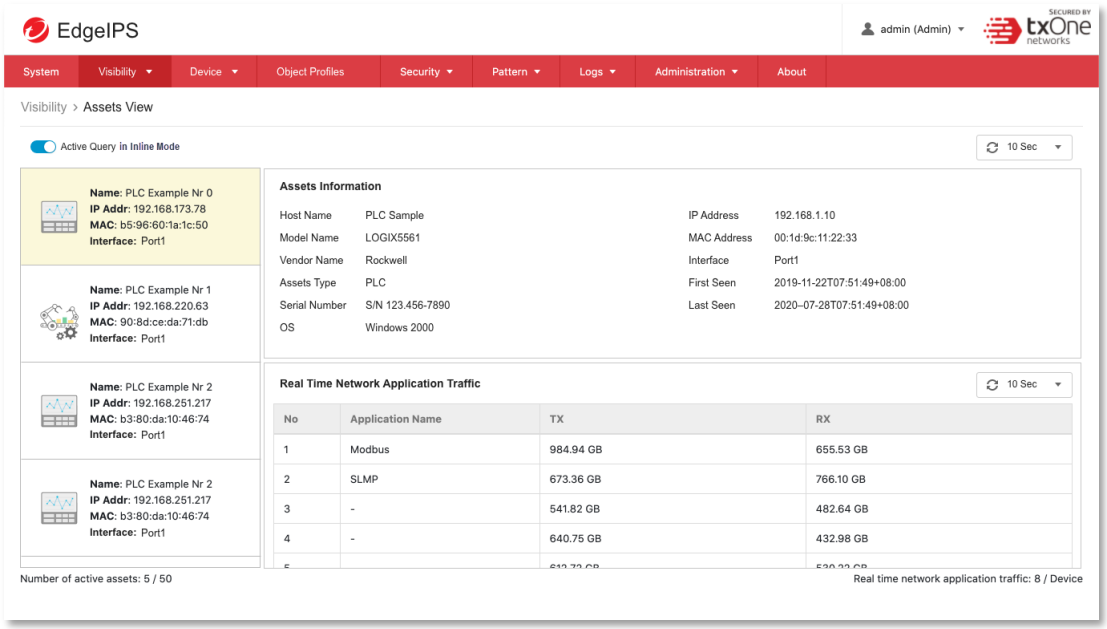
This widget shows resource usage on the device.



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)

The Visibility Tab

The [Visibility] tab gives you an overview of asset visibility for your managed assets. The tab provides you with timely and accurate information on the assets that are managed by EdgeIPS™.



The assets, listed under the tab, are automatically detected by EdgeIPS™ devices.

Note: The term **asset** in this chapter refers to the devices or hosts that are protected by EdgeIPS.

Active Query

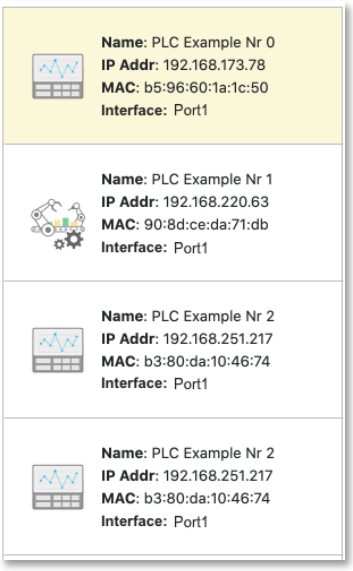
Active query can detect inactive or dormant assets or passive assets in the network.

Note: Active query operates only in Inline Mode. In Offline Mode, the switch button of active query is not configurable. In firmware 1.1, Active query supports 4 protocols (Modbus, CIP, OMRON FINS and SMB)

Viewing Asset Information

Procedure

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
Host Name	The host name of the asset.
Model Name	The model name of the asset.
Vendor Name	The vendor name of the asset.
Asset Type	The asset type of the asset.
Serial Number	The serial number of the asset.
OS	The operating system of the asset.
IP Address	The IP address of the asset.
MAC Address	The MAC address of the asset.
Interface	The physical port of EdgeIPS that detects the connection with 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

Procedure

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

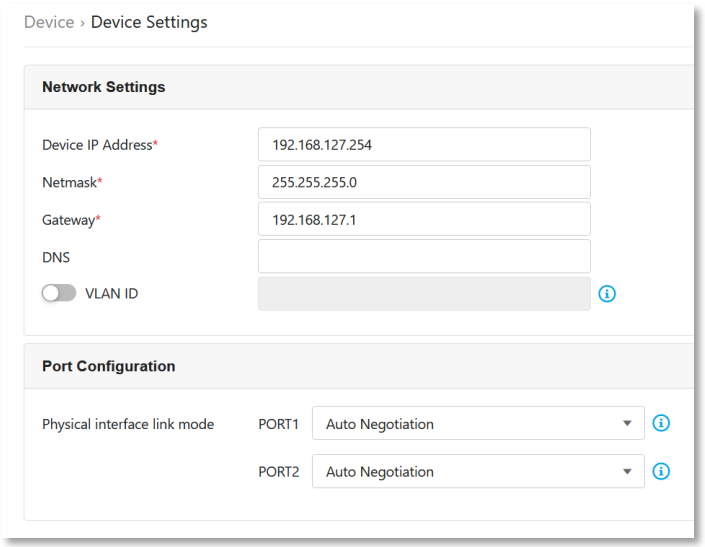
Field	Description
No.	Ordinal number of the application traffic.
Application Name	The application type of the traffic.
TX (Kbytes)	The amount of traffic transmitted for this traffic.
RX (Kbytes)	The amount of traffic received for this traffic.

Note: Click the [Manual Asset Info Refresh] to refresh the information displayed.

Note: Specify the refresh time under the [Refresh Time] dropdown menu.

The Device Tab

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



Configuring Network Settings

Procedure

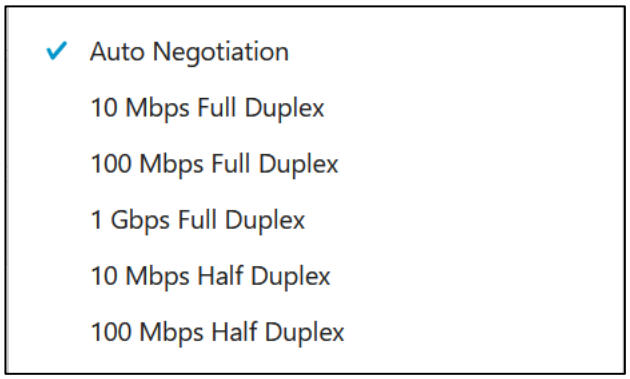
1. Go to [Device] > [Device Settings]
2. In the [Network Settings] pane, configure the network settings for the device:

Field	Description
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

Procedure

1. Go to [Device] > [Device Settings]
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. 

The Object Profiles Tab

Object profiles simplify policy management by storing configurations that can be used by EdgeIPS™.

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 create profiles or edit profiles to apply on 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].

Configuring IP Object Profile

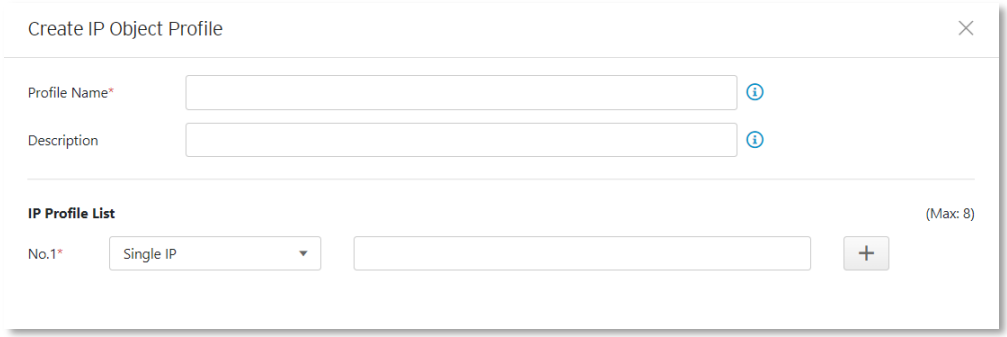
You can configure the IP address in an IP object profile, which can be used by other policy rules.

The types of IP address you can assign are:

- Single IP addresses
  For example: `192.168.1.1`
- IP ranges
  For example: from `192.168.1.1 to 192.168.1.20`
- IP subnets
  For example: `192.168.1.0/24`

Procedure

1. Go to [Object Profiles] > [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 Profile Name field.
4. Type a description.
5. Under the [IP Profile 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

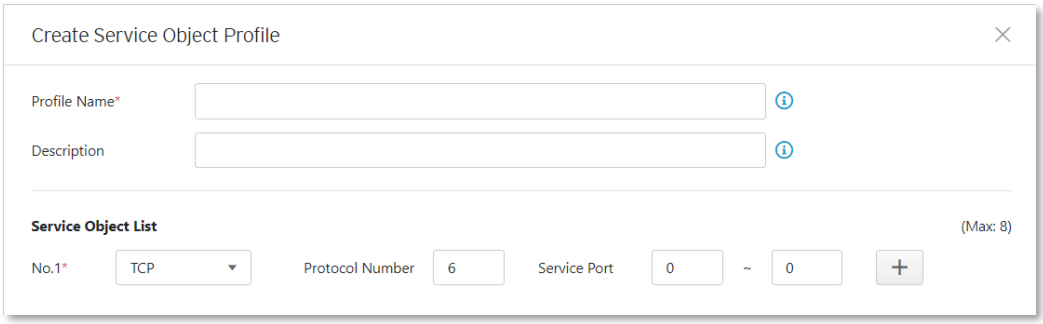
In a service object profile, you can define the following:

- TCP protocol port range
  For example: TCP port 100 ~ 120
- UDP protocol port range
  For example: UDP port 100 ~ 120
- ICMP protocol type and code
  For example: ICMP type 8 code 0
- Custom protocol with specified protocol number
  For example: protocol number = 6 and service ports range from 100 to 120

Note: The term 'protocol number' refers to the protocol number defined in the internet protocol suite.

Procedure

1. Go to [Object Profiles] > [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 Profile Name field.
4. Type a description.

5. Provide one of the following definitions:

a. TCP protocol and its port range

b. UDP protocol and its port range

c. ICMP protocol and its type and code

d. Custom protocol with specified protocol number

6. If you want to add another entry, click the + button.

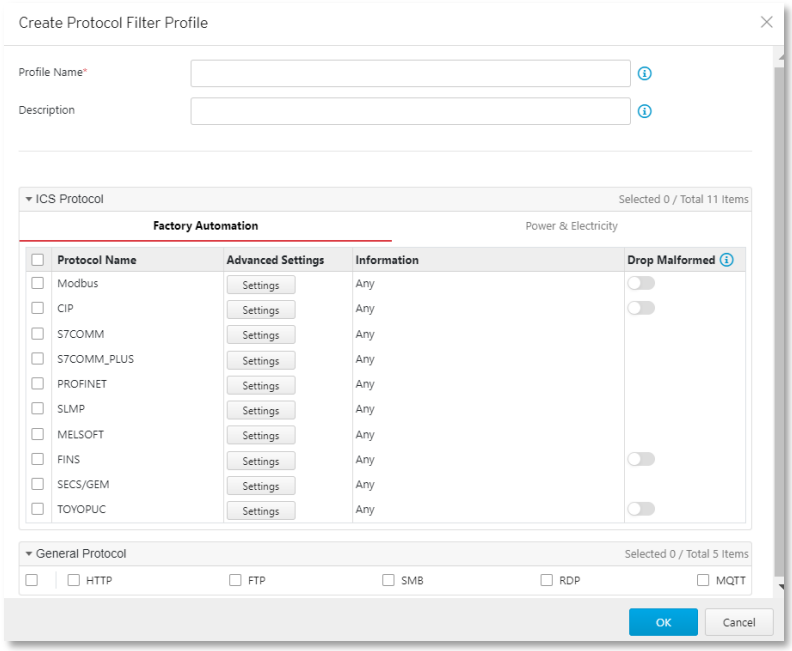
7. Click [OK].

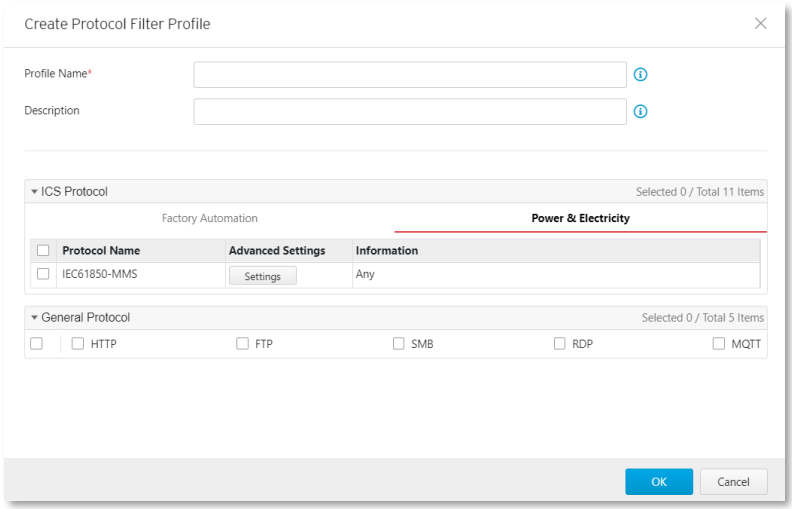
Configuring Protocol Filter Profile

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:

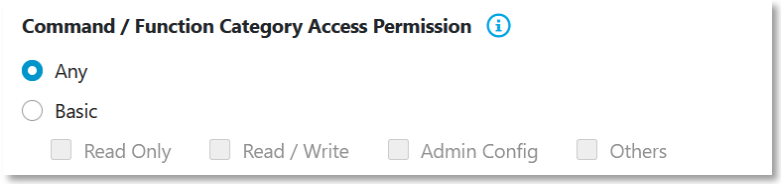
- Details of ICS protocols, including:
  - Modbus
  - CIP
  - S7COMM
  - S7COMM PLUS
  - PROFINET
  - SLMP
  - MELSOFT
  - FINS
  - SECS/GEM
  - TOYOPUC
  - IEC61850-MMS
- General Protocol, including:
  - HTTP
  - FTP
  - SMB
  - RDP
  - MQTT





Specifying Commands Allowed in an ICS Protocol

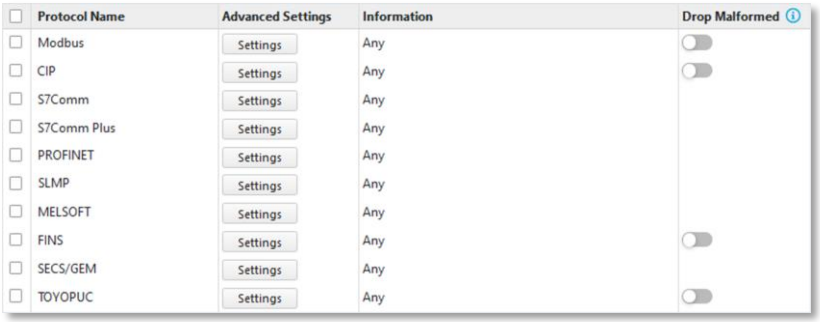
When configuring an ICS protocol, you can specify which commands will be included in the protocol profile, as the following picture shows.



Applying the Drop Malformed Option to an ICS Protocol

When configuring an ICS protocol, you can specify which OT protocols will be applied with the option [Drop Malformed] in the protocol profile, as the following picture shows.

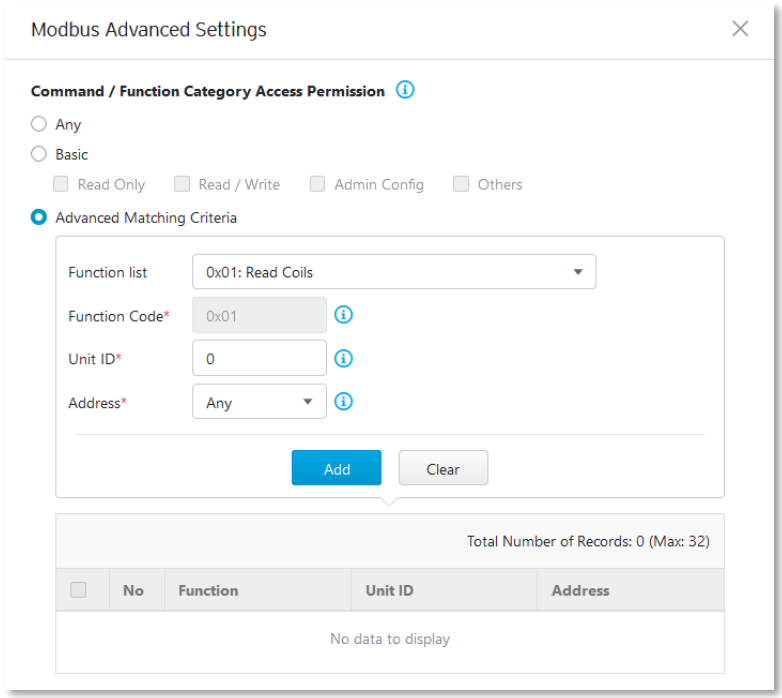
When the option [Drop Malformed] is enabled, EdgeIPS will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, EdgeIPS will drop the packets of the ICS protocol.



Note: In firmware 1.1, Drop Malformed supports 4 protocols (Modbus, CIP, FINS and TOYOPUC)

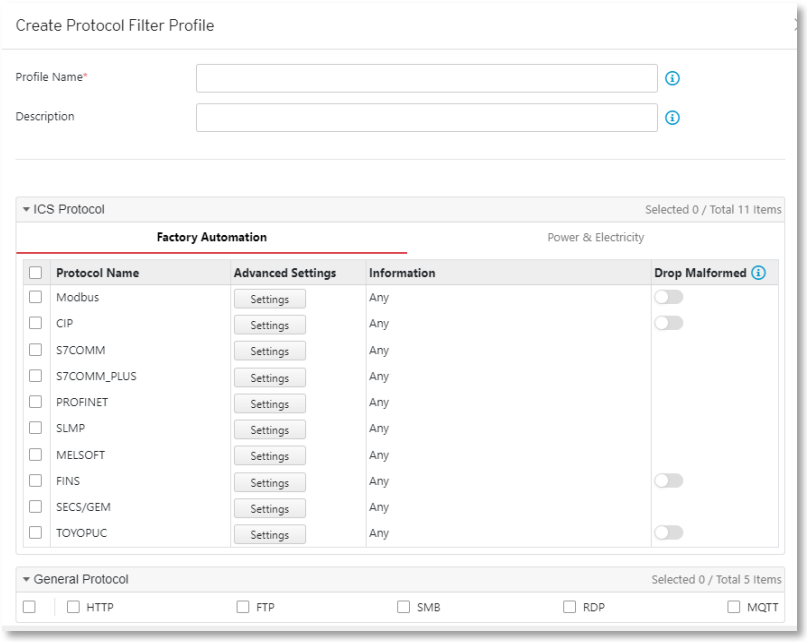
Advanced Settings for Modbus Protocol

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



Procedure

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



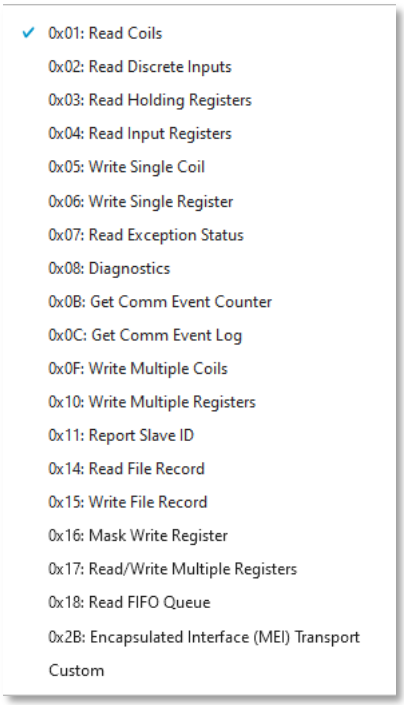
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

b. If you have selected [Modbus], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [Modbus], and select [Advanced Matching Criteria].
- At the [Function list] drop down menu, select a function of this protocol.

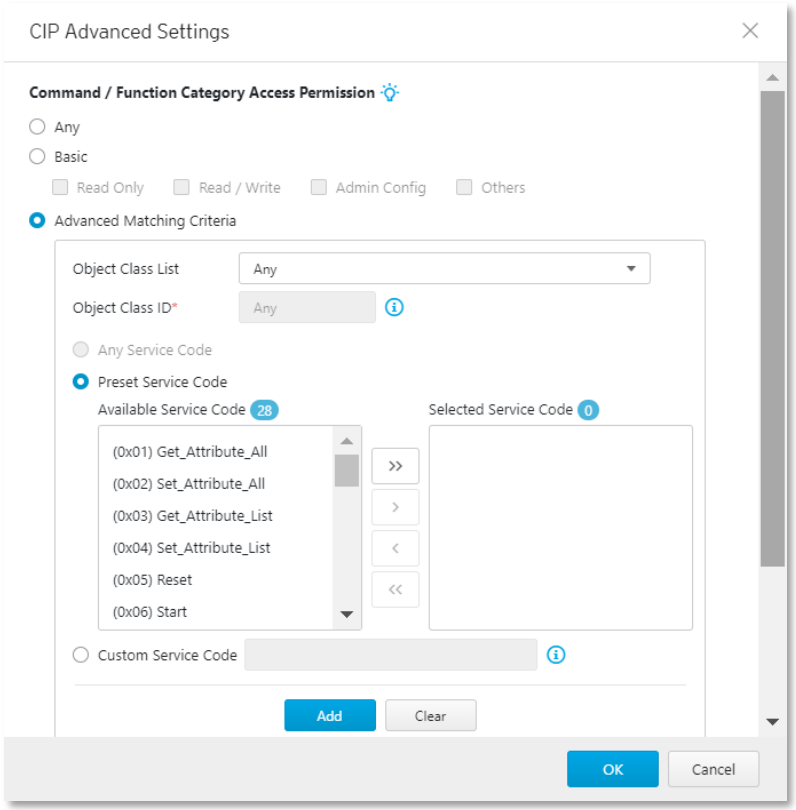


- If you want to specify a function code by yourself, then select [Custom] and input a function code in the [Function Code] field.
- Type a unit ID in the [Unit ID] field.
- Type the address or range of addresses against which the function will operate.
- Click [Add].
- Repeat the above steps if you 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].

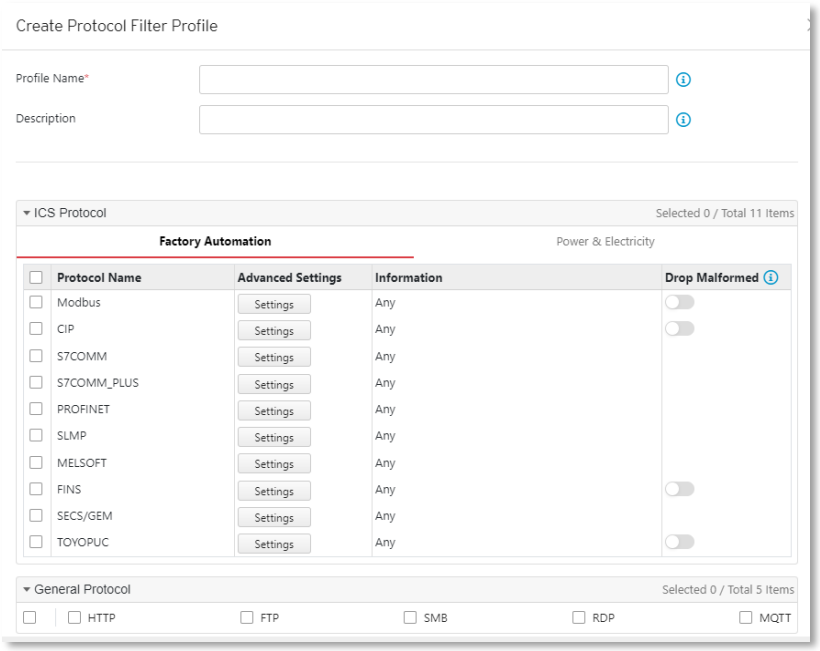
Advanced Settings for CIP Protocol

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.



Procedure

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



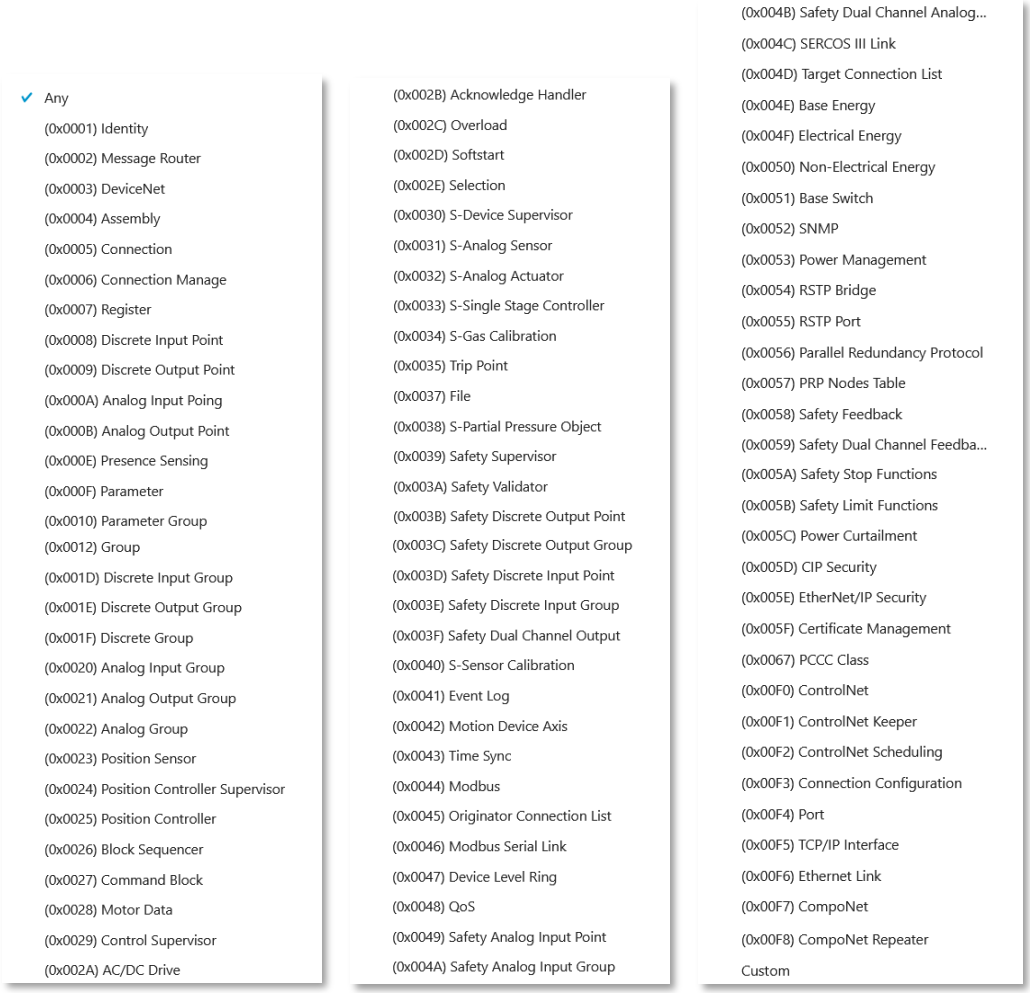
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

c. 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

d. If you have selected [CIP], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [CIP], and select [Advanced Matching Criteria].
- At the [Object Class List] drop down menu, select a function of this protocol.

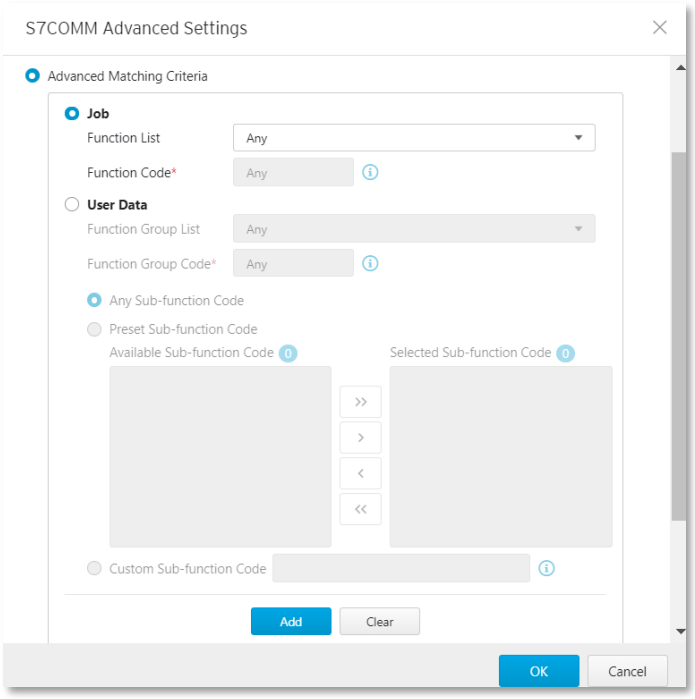


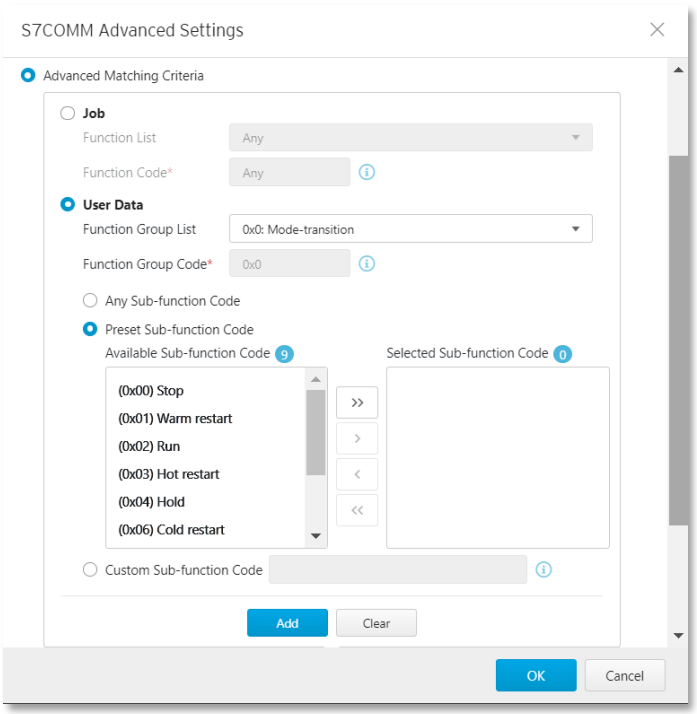
- If you want to all the service codes within the function you specified to be applied, then select [Any Service Code]
- If you want to specify one service code or multiple service codes, then select [Preset Service Code] and move the service code(s) from the [Available Service Code] field to the [Selected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

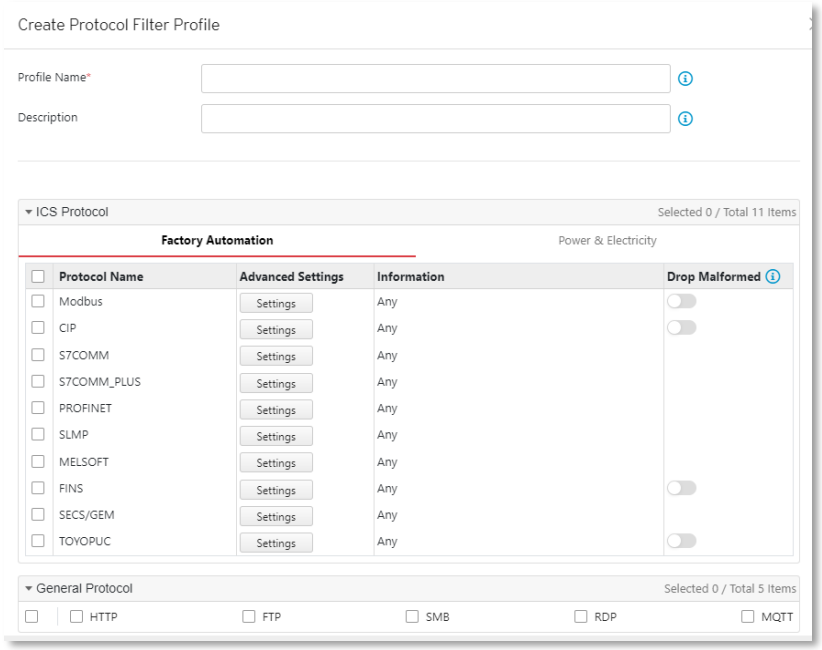




Procedure

1. Go to [Object Profiles] > [Protocol Filter Profile].
2. Click [Add] to add a protocol filter profile.

The [Create Protocol Filter Profile] screen will appear.



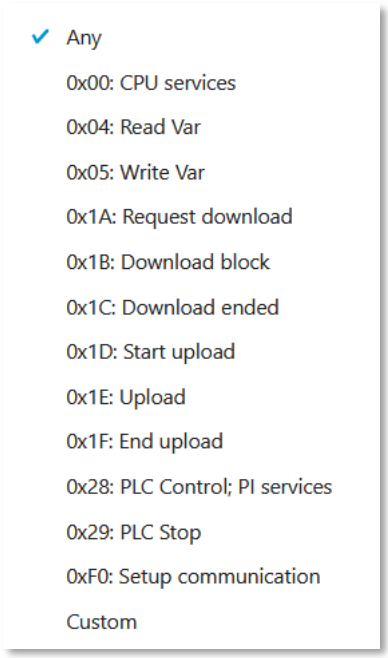
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

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

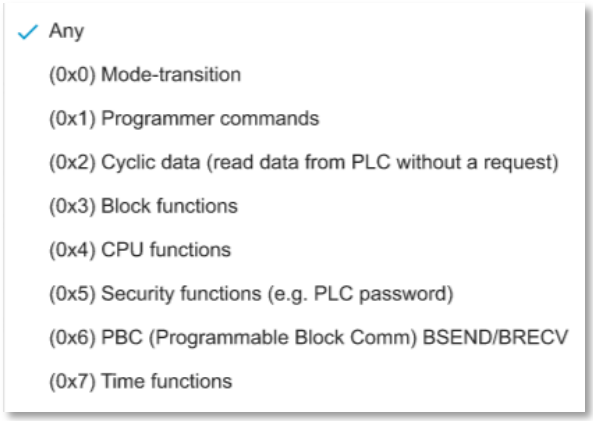
- **Any** - Specify all available commands or function access in this protocol.
- **Basic** - Multiple selections of the following:
  - **Read Only**: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

f. If you have selected [S7COMM], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [S7COMM], and select [Advanced Matching Criteria].
- If you want to specify one function code from the category [Job], then select the category [Job] and select a function at the [Function list] drop down menu.



- If you want to specify one function group code from the category [User Data], then select the category [User Data] and select a function group code at the [Function Group List] drop down menu.



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

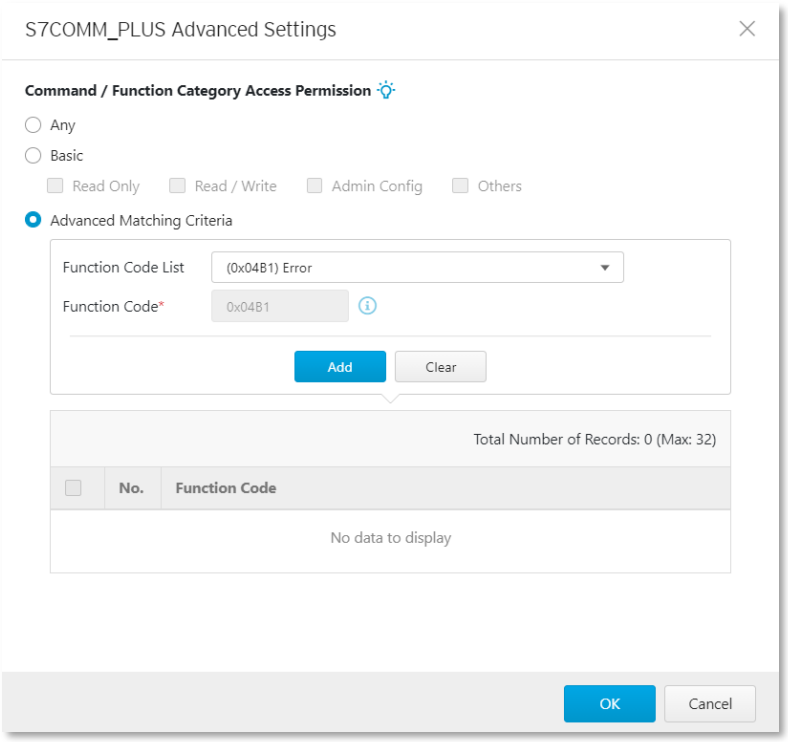
- If you want to specify a service code by yourself, then select [Custom Sub-function Code] and input a sub-function code in the [Custom Sub-function Code] field.

- 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].

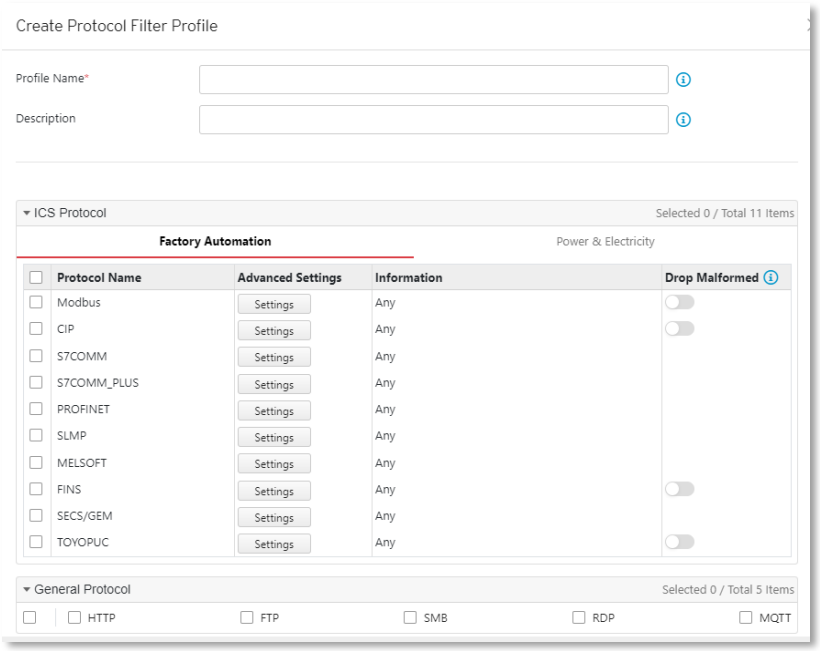
Advanced Settings for S7COMM_PLUS

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.



Procedure

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



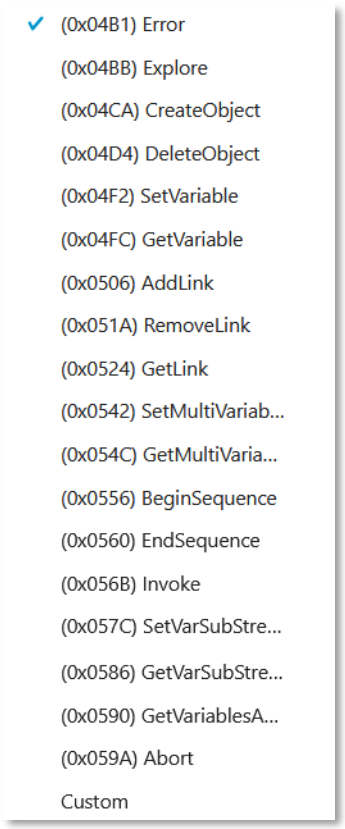
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

g. 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

h. If you have selected [S7COMM_PLUS], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [S7COMM_PLUS], and select [Advanced Matching Criteria].
- At the [Function Code List] drop down menu, select a function of this protocol.

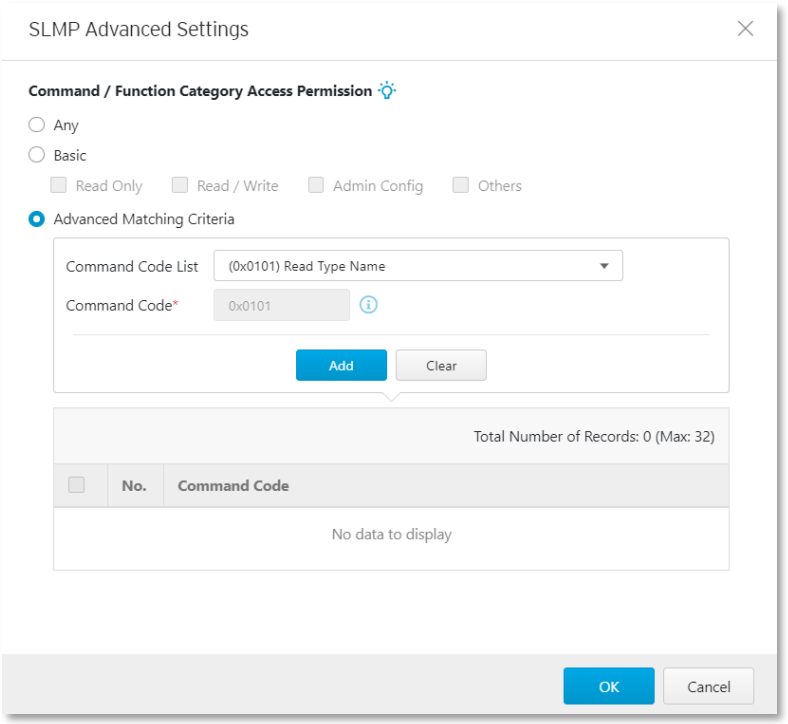


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

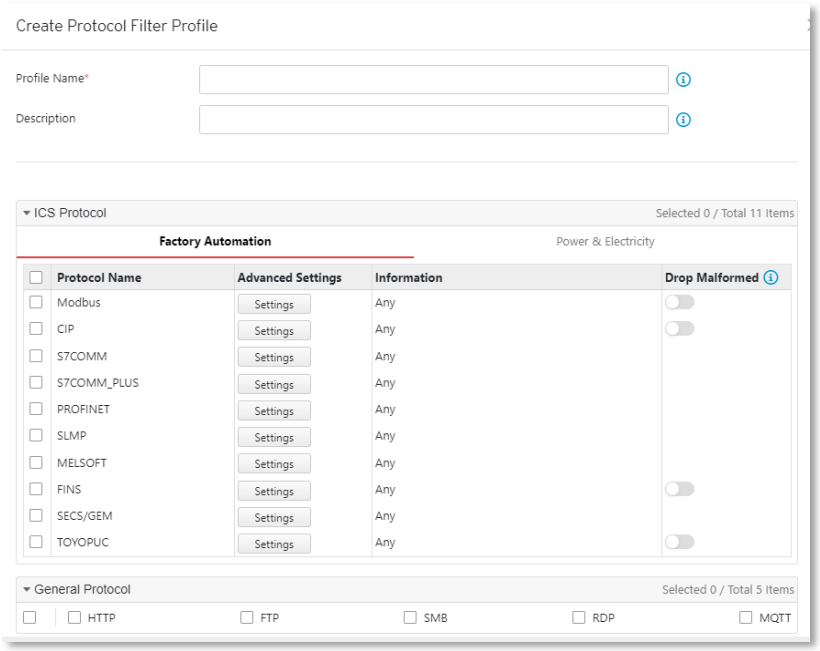
Advanced Settings for SLMP

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.



Procedure

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



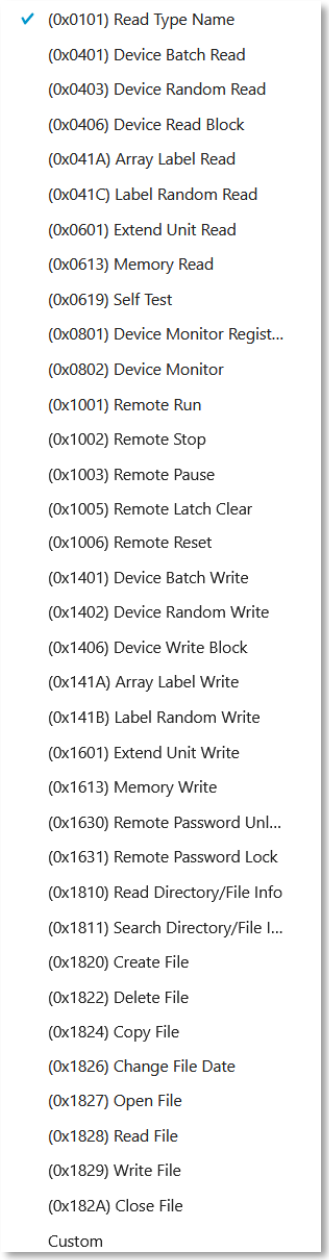
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

i. 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

j. If you have selected [SLMP], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [SLMP], and select [Advanced Matching Criteria].
- At the [Command Code List] drop down menu, select a command code of this protocol.

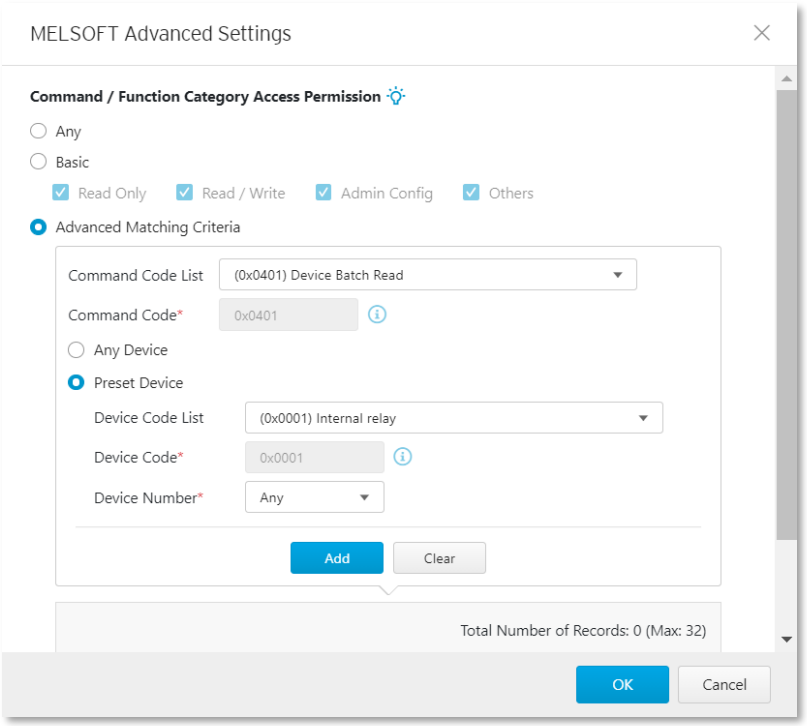


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

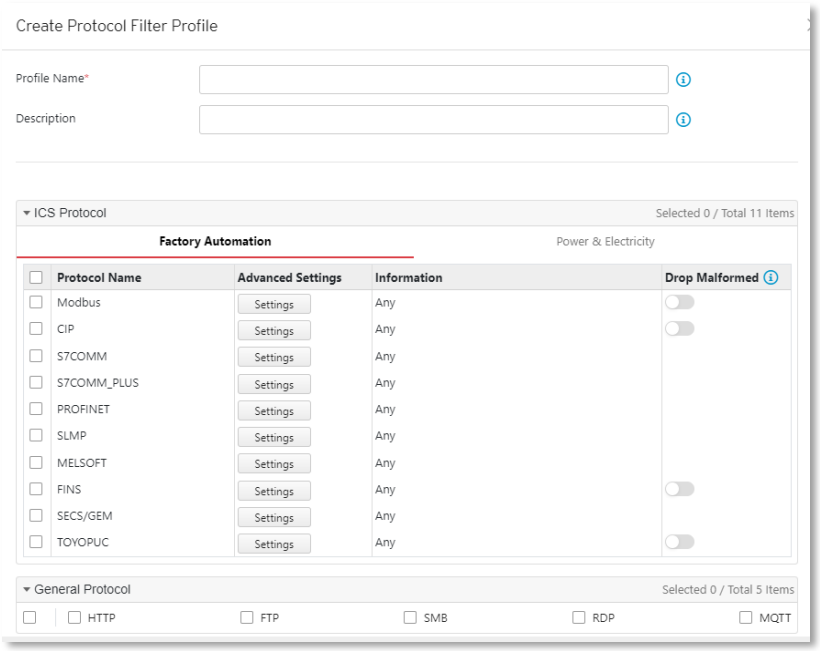
Advanced Settings for MELSOFT

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.



Procedure

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



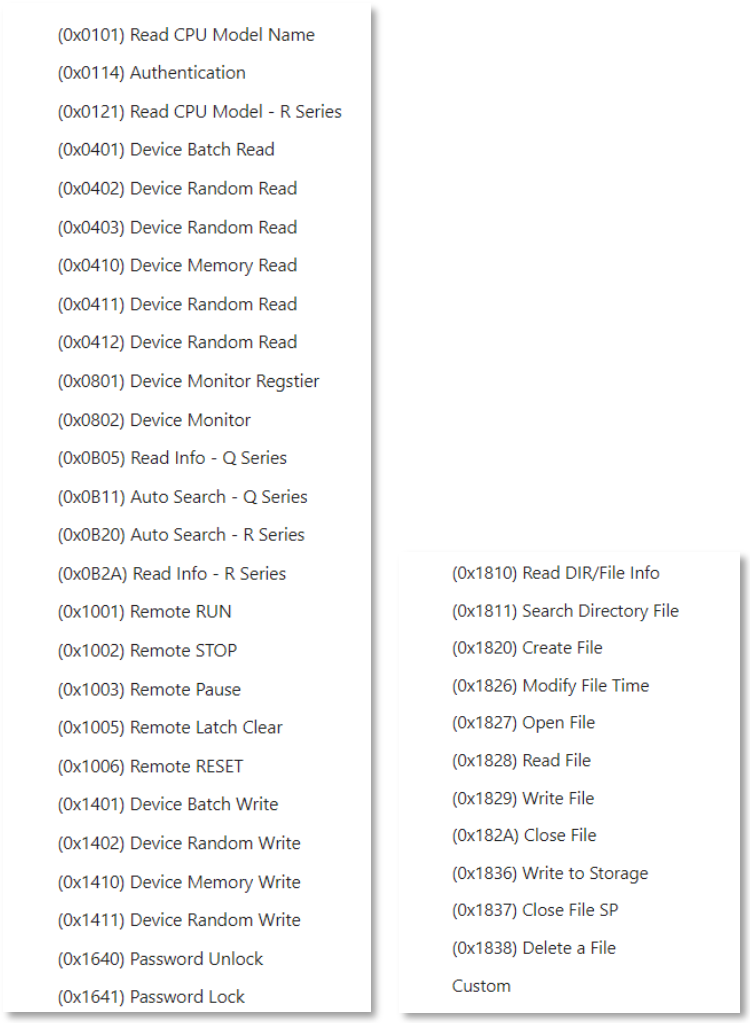
3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

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

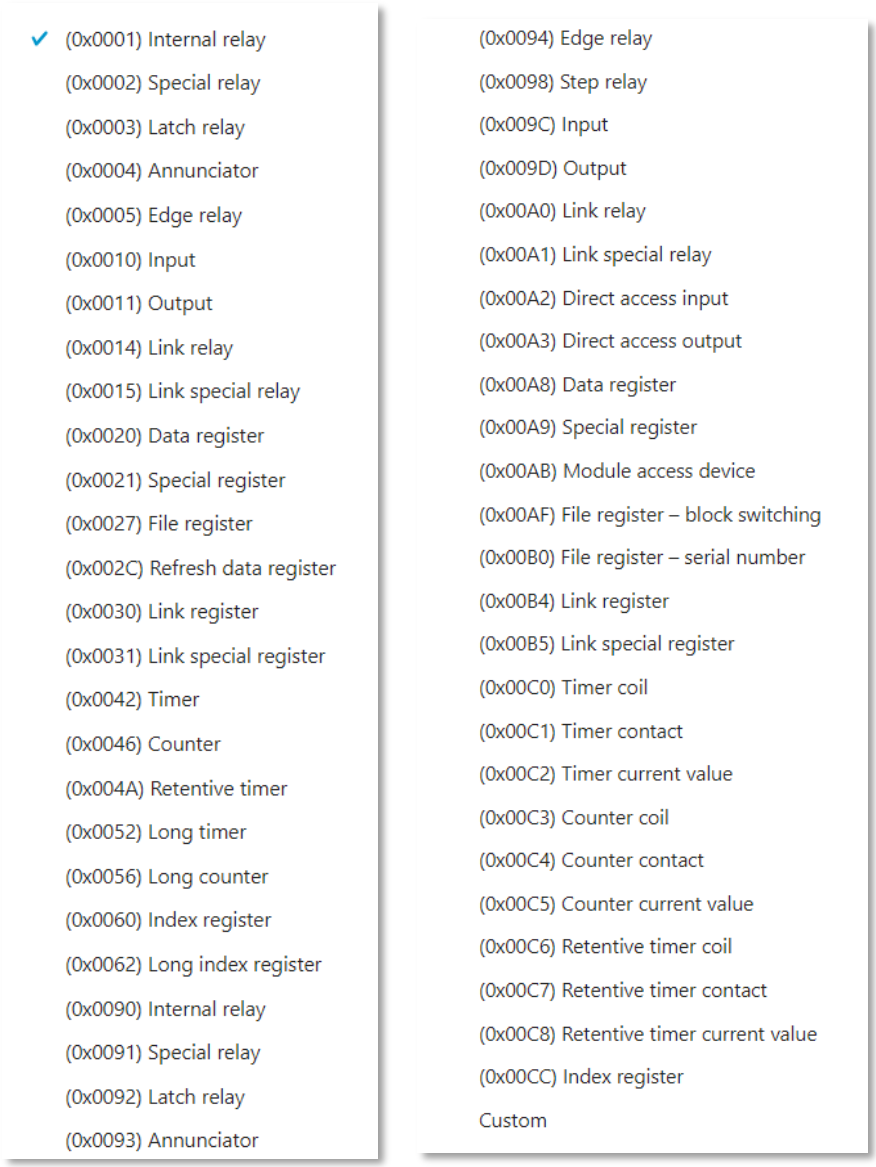
- **Any** - Specify all available commands or function access in this protocol.
- **Basic** - Multiple selections of the following:
  - **Read Only**: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

l. If you have selected [MELSOFT], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [MELSOFT], and select [Advanced Matching Criteria].
- At the [Command Code List] drop down menu, select a function of this protocol.



- If you want to specify one device code, then select [Preset Device] and select one of the device code(s) from the drop list.

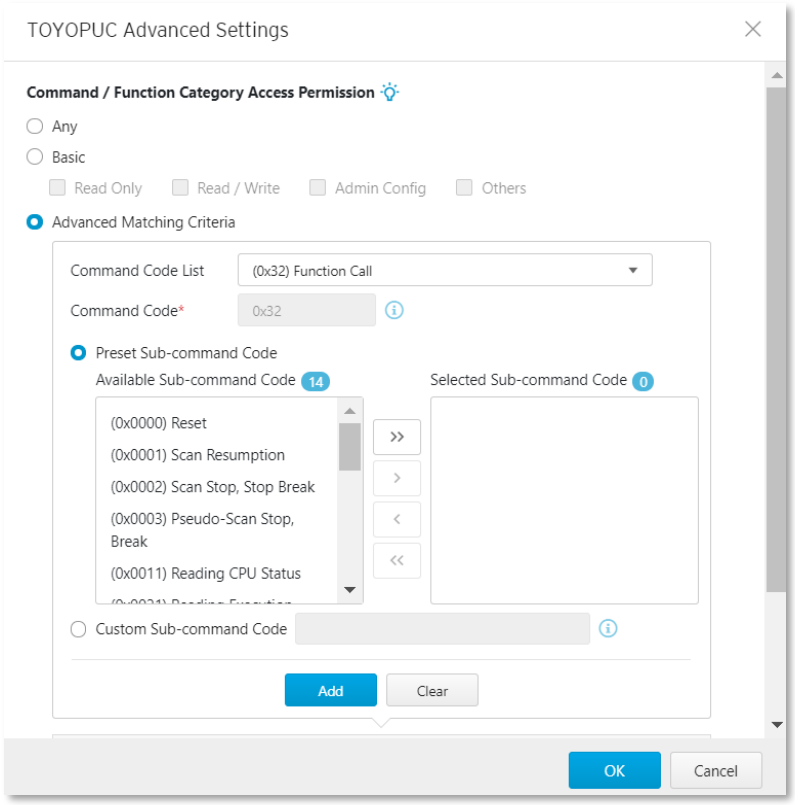


- If you want to include a device number as a filter criteria, then select [Any] from the drop list.
- If you want to specify a device number, then select [Single] from the drop list.
- If you want to specify a range of device numbers, then select [Range] from the drop list.
- Click [Add].
- Repeat the 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].

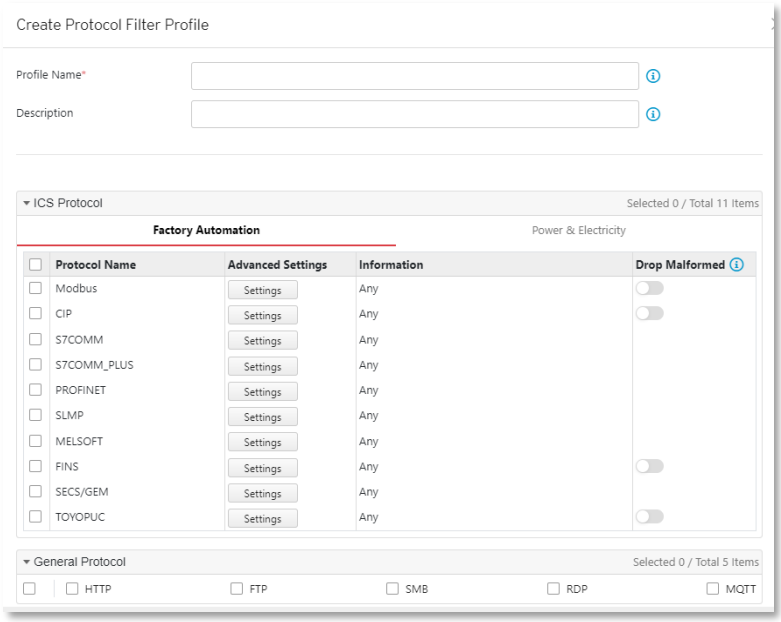
Advanced Settings for TOYOPUC

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.



Procedure

8. Go to [Object Profiles] > [Protocol Filter Profile].
9. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



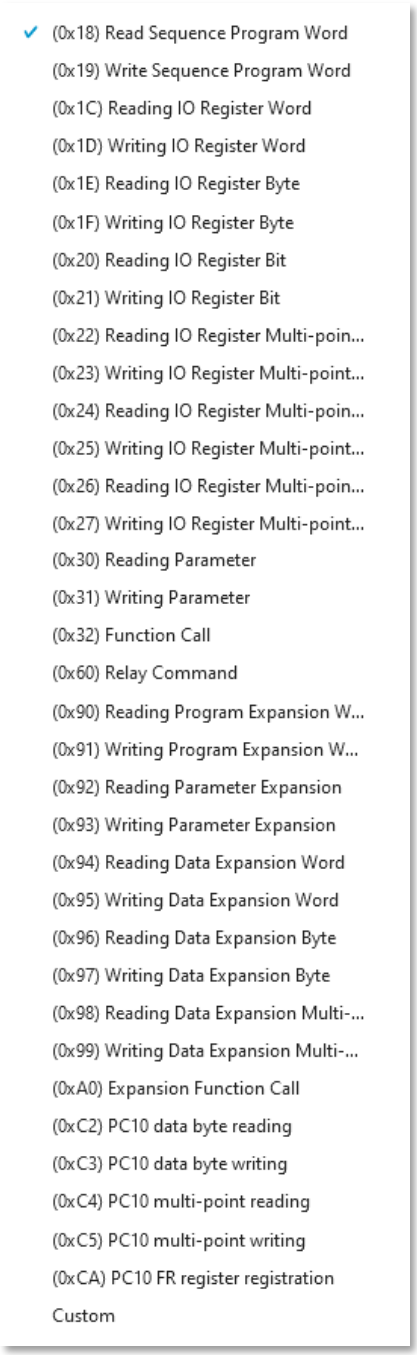
10. Type a profile name for the protocol filter.
11. Type a description.
12. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

m. 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 sent from EWS to PLC.
  - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

n. If you have selected [TOYOPUC], you can optionally configure advanced settings for this protocol:

- Click [Settings] next to [TOYOPUC], and select [Advanced Matching Criteria].
- At the [Command Code List] drop down menu, select a function of 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 sub-command code or multiple sub-command codes, then select [Preset Sub-command Code] and move the sub-function code(s) from the [Available Sub-command Code] field to the [Selected Sub-command Code] field.
- If you want to specify a sub-command code by yourself, then select [Custom Sub-command Code] and input a sub-command code in the [Custom Sub-command Code] field.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

Note: Not all the command codes support the feature of [Preset Sub-cmd code] and [Custom Sub-cmd]. Only the command code "(0x32) Function Call" and "(0xA0) Expansion Function Call" support them.

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

Configuring IPS Profile

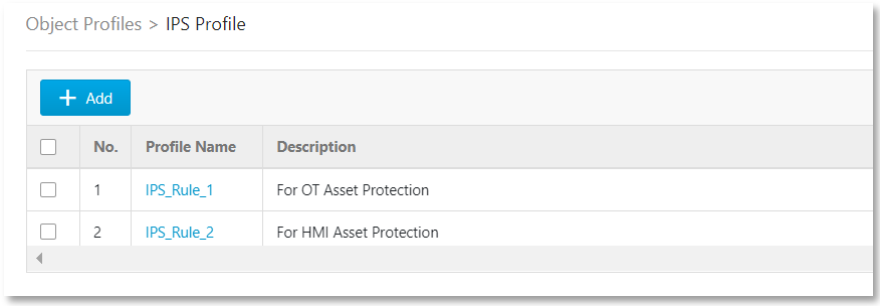
An IPS profile contains more sophisticated pattern rules that you can do granular control and apply to a policy rule.

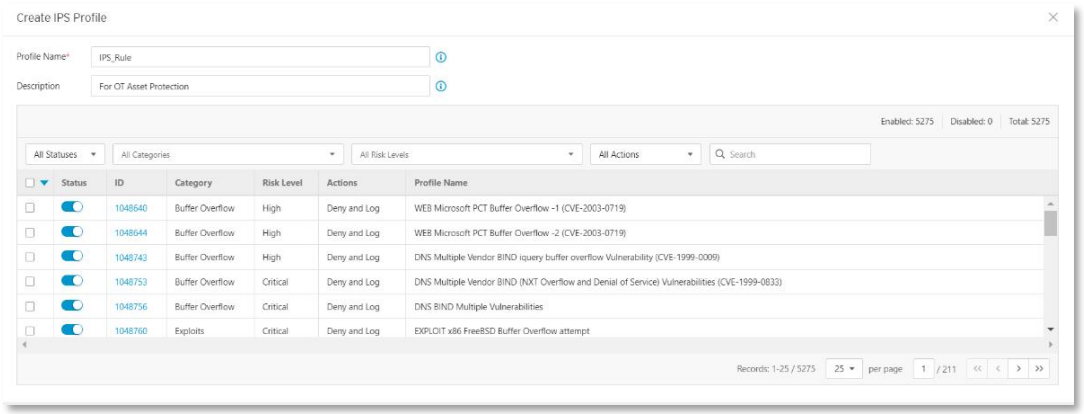
The following can be configured in an IPS profile:

- Details of IPS protocol category, including:
  - File Vulnerabilities
  - Buffer Overflow
  - DoS Attack
  - Exploits
  - Malware Traffic
  - Reconnaissance
  - Web Threats
  - ICS Threats
  - Others
  - Misc

- Details of IPS protocol risk level category, including:
  - Information
  - Low
  - Medium
  - High
  - Critical

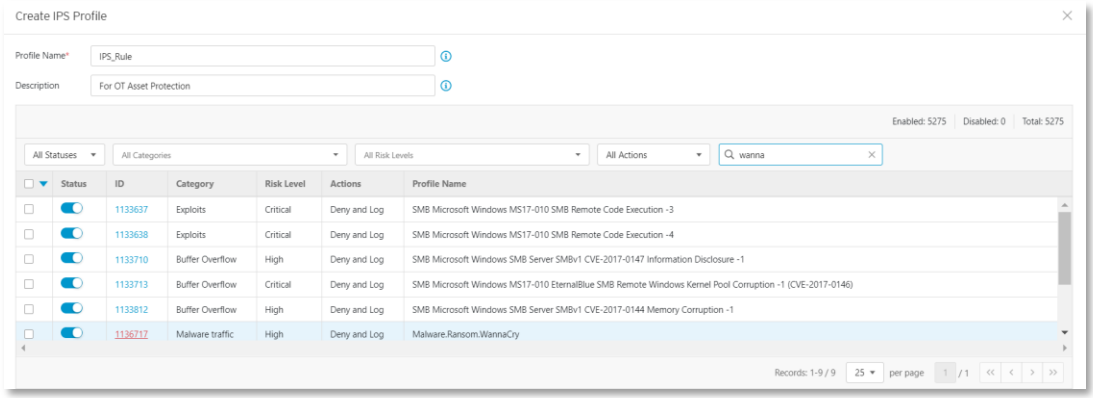
- Details of default action list for IPS patterns, including:
  - Accept and Log
  - Deny and Log

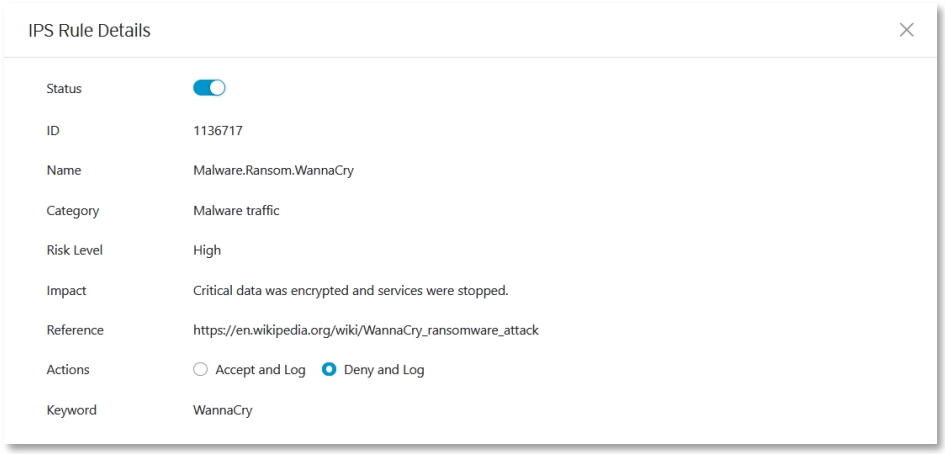




Configuring a Pattern Rule for Granular Control

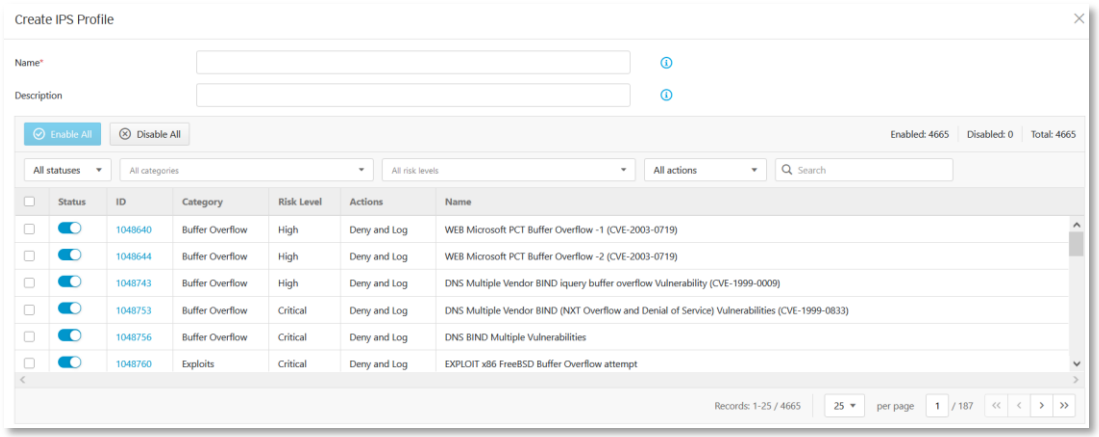
When configuring an IPS pattern rule protocol, you can specify which action should be taken and add it in the IPS profile, as the following picture shows.





Procedure

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



3. Type a profile name for the IPS profile.
4. Type a description.
5. Select a pattern rule you want to configure by clicking on the rule ID.
6. IPS rule details will show up. Select one of the following:
   - **Status** - Specify the pattern rule to be enabled or disabled.
   - **Actions** - Multiple selections of the following:
     - **Accept and Log**: When the attack is detected by EdgeIPS, the attack will be bypassed and logged for monitoring.
     - **Deny and Log**: When the attack is detected by EdgeIPS, the attack will be bypassed and logged for monitoring.

Field	Description
Status	The operational status of the pattern rule
ID	The pattern rule ID
Pattern Name	The pattern name for the cyber attack
Category	The threat category for the cyber attack
Risk Level	The suggested security level for the cyber attack

Field	Description
Impact	The damage that will cause to the target network device if the cyber attack succeeds.
Reference	The vulnerability ID of the cyber attacks (e.g. CVE-2017-0147)
Actions	The preset action for the cyber attacks.
Keyword	The word(s) for searching the pattern rules

7. If you already configure the pattern rule, press [Save].

The Security Tab

This chapter describes security general settings, cyber security, and policy enforcement.

Security General Settings

Use the [Security General Settings] tab to configure the security operation mode of the device.

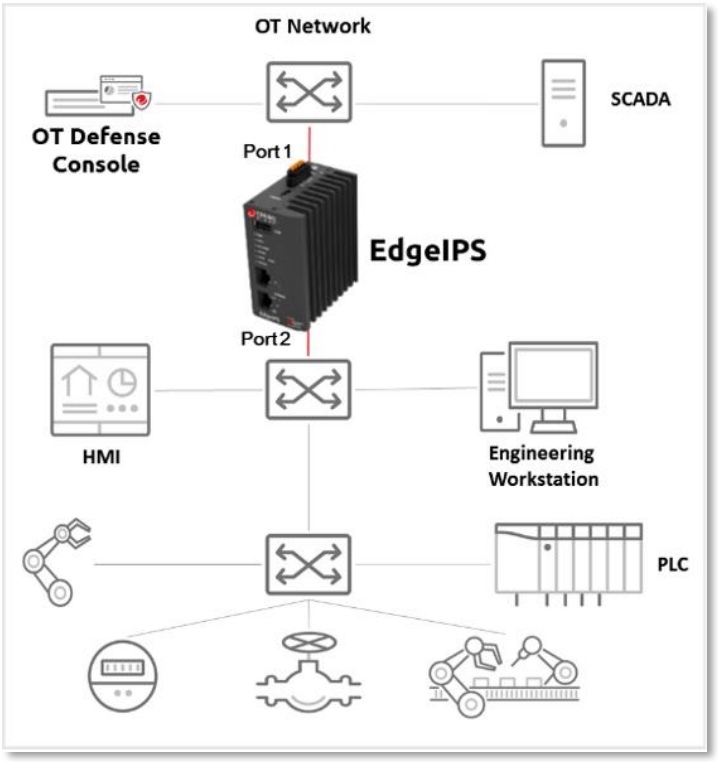
EdgeIPS™ offers two operation modes:

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

The following sections describe these two modes in detail.

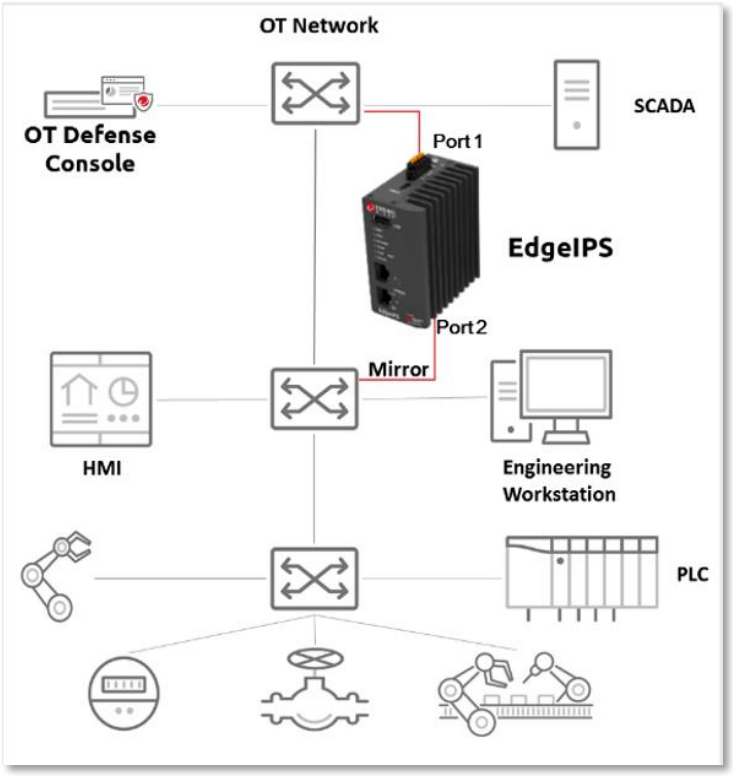
Inline Mode

EdgeIPS sits 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 EdgeIPS, which keeps detecting, monitoring, as well as outputting detection logs if threat events are detected.

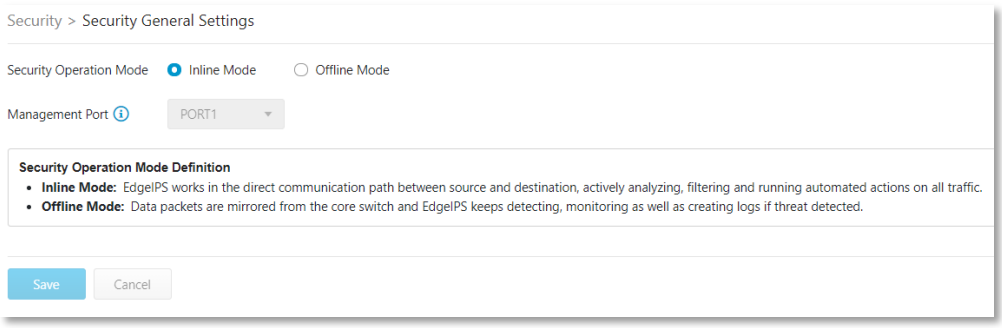


Note: **Port 1** of the EdgeIPS functions as the management port, which connects to another switch, allowing the EdgeIPS to be managed by ODC.

Configuring Security Operation Mode

Procedure

1. Go to [Security] > [Security General Settings]
2. At the [Security General Settings] tab you will see the following screen.



3. Choose a desired operation mode for this device.

Task	Action
Inline Mode	Choose [Inline Mode] to have EdgeIPS operate in Inline Mode. Configured IP setting in [Network Settings] pane can be connected from Port 1 or Port 2 at the same time.
Offline Mode	Choose [Offline Mode] to have EdgeIPS operate in Offline Mode. Configured IP setting in [Network Settings] pane can be connected from the selected physical port. The default port is Port1.

Note: Starting from firmware 1.1, EdgeIPS 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. Choose the management port of the device if you select Offline Mode.

Note: When you switch from Inline Mode to Offline Mode for the first time, please note that you MUST connect to the physical port for device management in case you are unable to access the web console. After successfully switching 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 EdgeIPS is deployed using inline network topology with the [Security Operation Mode] being set to [Offline Mode], then devices that connect to the non-management port cannot get through to outside.

Cyber Security

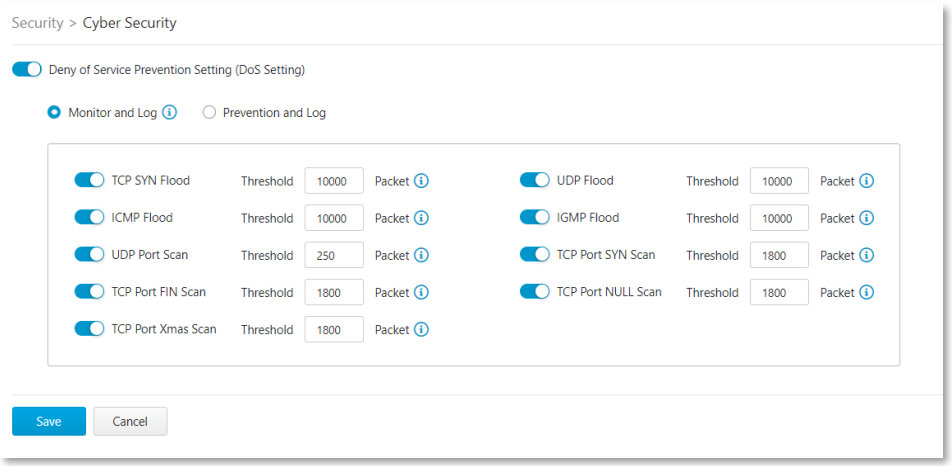
This device features cyber security, which covers denial of service attack prevention. The signature rules of intrusion prevention are called the 'Trend Micro DPI (Deep Packet Inspection) Pattern'. This pattern is provided by Trend Micro and can be regularly updated through ODC as well by manual import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

Configuring Cyber Security – Denial of Service Prevention

Procedure

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

2. At the [Cyber Security] tab you will see the [Denial of Service Prevention Setting (DoS Setting)] pane.



3. Use the toggle to enable or disable the denial of service prevention feature.
4. Select an action ([Monitor and Log] or [Prevention 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 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:

IPS 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.

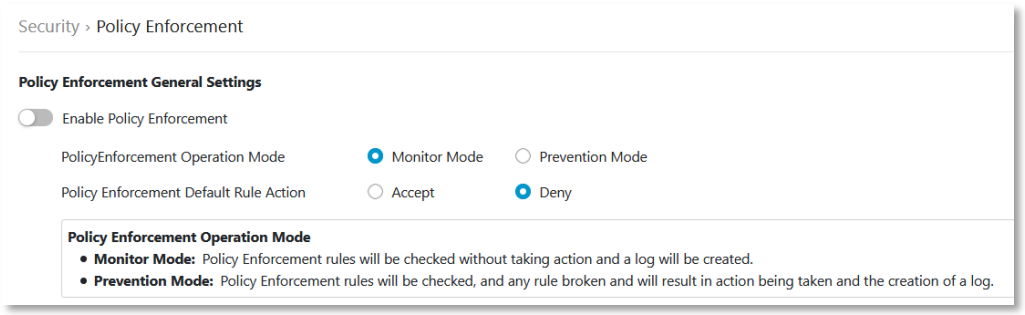
Policy Enforcement

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

Configuring Policy Enforcement

Procedure

1. Go to [Security] > [Policy Enforcement].
2. At the [Policy Enforcement] tab you will see the [Policy Enforcement General Settings] pane.
3. Use the toggle to enable or disable the policy enforcement feature.
4. Select a mode ([Monitor Mode], or [Prevention Mode]) for the feature.



5. At the [Policy Enforcement Default Rule Action] pane, select a default action [Accept], [Accept and Log] or [Deny and Log] for when no policy enforcement rule is matched.

The following table summarizes the settings:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	▪ Detect and monitor abnormal protocol accesses to the OT assets, without blocking network attacks. ▪ Generate logs.
	Prevention Mode	▪ Block abnormal protocol access to OT assets. ▪ Generate logs.
Offline Mode	Monitor and Log	▪ Detect and monitor abnormal protocol accesses to the OT assets ▪ Generate logs

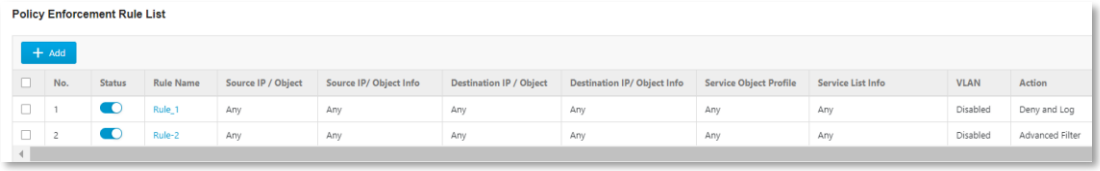
Adding Policy Enforcement Rules

Procedure

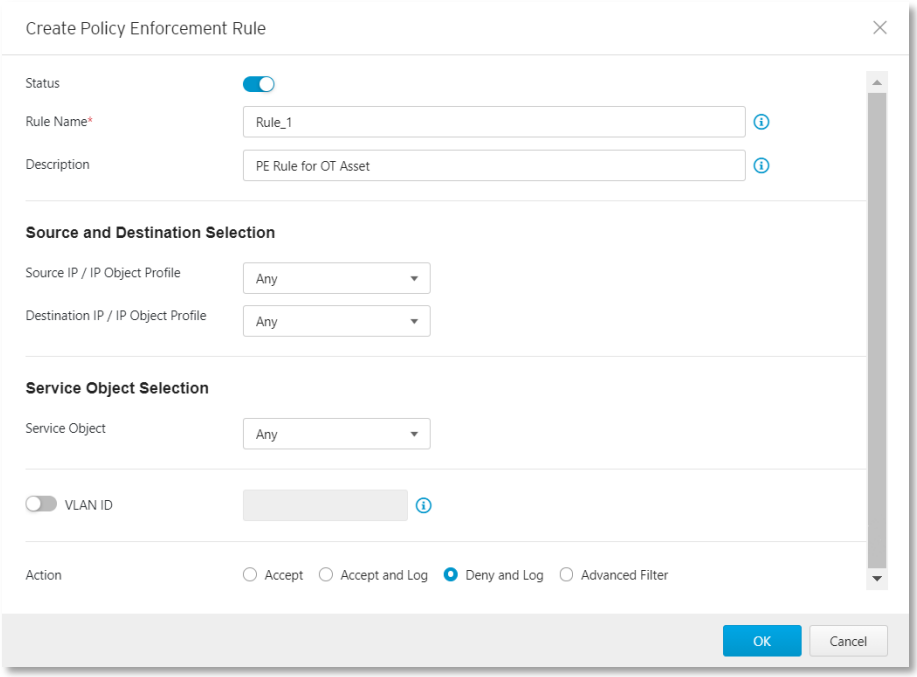
1. Configure the required object or objects.
   - IP object profiles
     For more information, see *Configuring IP Object Profile on page 19*.

- Service object profiles
  For more information, see *Configuring Service Object Profile on page 20*.
- Protocol filter profiles
  For more information, see *Configuring Protocol Filter Profile on page 21*.

2. Go to [Security] > [Policy Enforcement]
3. Under the [Policy Enforcement] tab 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 profiles that have been created beforehand.

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 service object profiles that have been created beforehand.

11. At the [Action] drop-down menu, select one of the following:

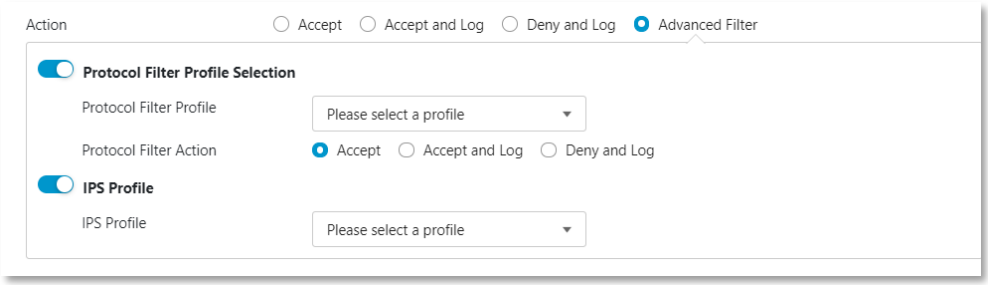
a. Accept: Select this option to allow network traffic that matches this rule.

b. Accept and Log: Select this option to allow network traffic that matches this rule, and generate log

c. Deny: Select this option to block network traffic that matches this rule.

d. Advanced Filter: The node will take further actions based on the protocol filter:

- Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
- Under the [Protocol Filter Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.



- Under the [IPS Profile] drop-down menu, select an IPS profile you have defined beforehand.

12. Click [OK] to save the configuration.

Managing Policy Enforcement Rules

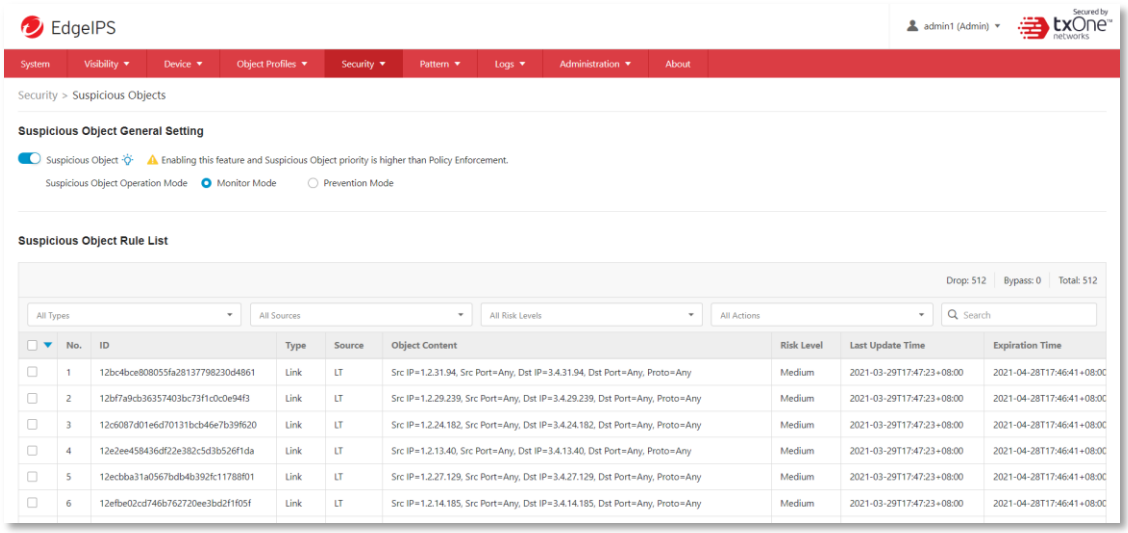
The following table lists the common tasks that are used to manage policy enforcement rules.

Task	Action
To delete a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the [Delete] button.
To duplicate a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the [Copy] button.
To edit a policy enforcement rule	Click the name of the rule, and an [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, EdgeIPS™ 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.

Suspicious Objects

Suspicious Objects allows you to define a custom node-based/link-based list that matches to the hash value of a network node or a network link, and then allow or block activities fitting that network node/network link in your network environment.



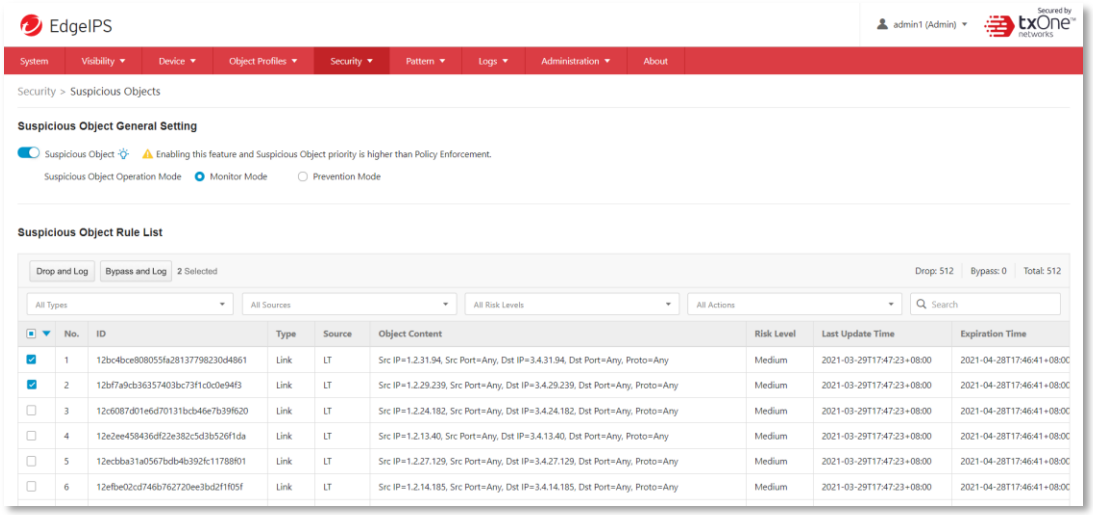
Note: Before you enable suspicious objects feature, please note that the [ODC Setting] pane in [Administration] > [Sync Settings], is properly configured and ODC is connected with 3rd party API from the source of suspicious object.

Configuring Suspicious Objects

Procedure

1. Go to [Security] > [Suspicious Objects].
2. At the [Suspicious Objects] tab you will see the [Suspicious Object General Settings] pane.
3. Use the toggle to enable or disable the suspicious object feature.

4. Select a mode ([Monitor Mode], or [Prevention Mode]) for the feature.



5. If you want to change the action of the specific suspicious object at the [Suspicious Object Rule List] table, select the specific suspicious object and choose the action [Drop and Log] or [Bypass and Log] for when the pattern is matched.

The following table summarizes the settings:

Task	Suspicious Object Operation Mode	Action Settings	Action Performed
Inline Mode	Prevention Mode	Prevent and Log	▪ Blocks network node or network link. ▪ Generates logs.
	Monitor Mode	Monitor and Log	▪ Detects network node or network link, but does not block communication related to the network node or network link. ▪ Generates logs.
Offline Mode	Prevention Mode / Monitor Mode	Monitor and Log	▪ Detects network node or network link ▪ Generates logs.

The Pattern Tab

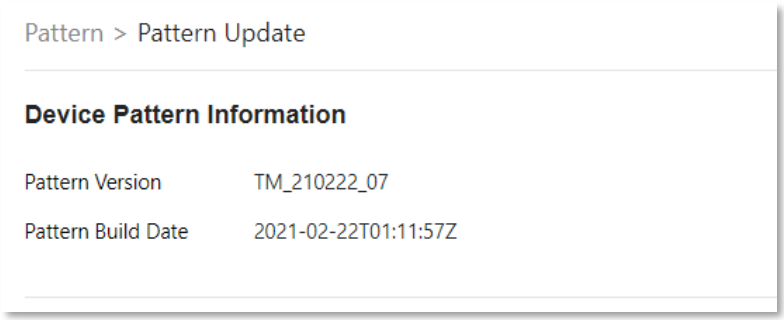
This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the EdgeIPS™ device.

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

Viewing Device Pattern Information

Procedure

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



Manually Updating the Pattern

Procedure

1. Go to [Pattern] > [Pattern Update].
2. At the [Pattern Update] tab you will see the following pane.
3. Click [Select]
4. Manually select the pattern to be deployed to the device.

5. Click [Upload] and then [Confirm].

The Logs Tab

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:

- **Cyber Security Logs**
- **Policy Enforcement Logs**
- **Protocol Filter Logs**
- **Suspicious Object Logs**
- **Assets Detection Logs**
- **System Logs**
- **Audit Logs (Can only be seen by auditor)**

Viewing Cyber Security Logs

'Cyber Security Logs' will include logs detected by both intrusion prevention and denial of service prevention features.

Procedure

1. Go to [Logs] > [Cyber Security Logs].
   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the IPS profile that was used to generate the log.
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.
Interface	The physical port interface which receives the cyber attack
Attacker	The IP address of host device which initiates the cyber attack
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 packet, if protocol is TCP/UDP. The ICMP type of the packet, if protocol is ICMP
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the packet, if protocol is TCP/UDP. The ICMP type of the packet, if protocol is ICMP
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the IPS profile settings.

Field	Description
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.

Procedure

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

   The following table describes the log table.

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

Viewing Protocol Filter Logs

The protocol filter logs cover logs detected by the [Protocol Filter] feature. Protocol filter is the advanced configuration when you configure the [Policy Enforcement] settings.

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
Interface	The physical port interface which receives the traffic and the traffic matches the setting of protocol filter profile.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.

Field	Description
Source Port	The source port, if protocol is TCP/UDP. The ICMP type, if protocol is ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No.	The command or 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 Suspicious Object Logs

The suspicious object logs will include logs detected by the [Suspicious Objects] feature.

Procedure

1. Go to [Logs] > [Suspicious Object Logs].

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
ID	The hash ID of the matched suspicious object.
Type	The suspicious object type, which is node type or link type.
Source	The source of suspicious object
Risk Level	The threat level of suspicious object
Expiration Time	The Expiration Time of suspicious object. When the expiration time reaches, the suspicious object will be deleted.
Interface	The physical port interface which receives the suspicious object
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 suspicious object settings.
Count	The number of detected suspicious object within the detection threshold.

Viewing Assets Detection Logs

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

Procedure

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

   The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Event Type	The log event description.
Port	The physical port interface which receives 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.

Procedure

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

   The following table describes the log's fields.

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

Procedure

1. 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 login with the default "audit" account.

The Administration Tab

This chapter describes the available administrative settings for EdgeIPS™ device.

Account Management

Note: Log onto the management console with an administrator account to access the Accounts tab.

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 log on to the management console using custom user accounts.

The following table outline the tasks available on the [Account Management] tab.

Task	Description
Add account	Click Add to create a new user account. For more information, see *Adding a User Account on page 642*.
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-Tab	**Action**	**Admin**	**Operator**	**Viewer**	**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 default Account ID	User Role	Default Password
admin	Admin	txone
auditor	Auditor	txone

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, you can create new user accounts to access the system.

Procedure

1. Go to [Administration] > [Account Management].
2. Click [Add].
   The Add User Account screen will appear.
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.
Authentication Source	Type the authentication source for this account
Local Password	Type the account password.
Confirm password	Type the account password again to confirm.
Description	Add a description for this account
Role	Select a user role for this account. For more information, see User Roles *on page 642*.

4. Click [Save].

Changing Your Password

Procedure

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

Configuring Password Policy Settings

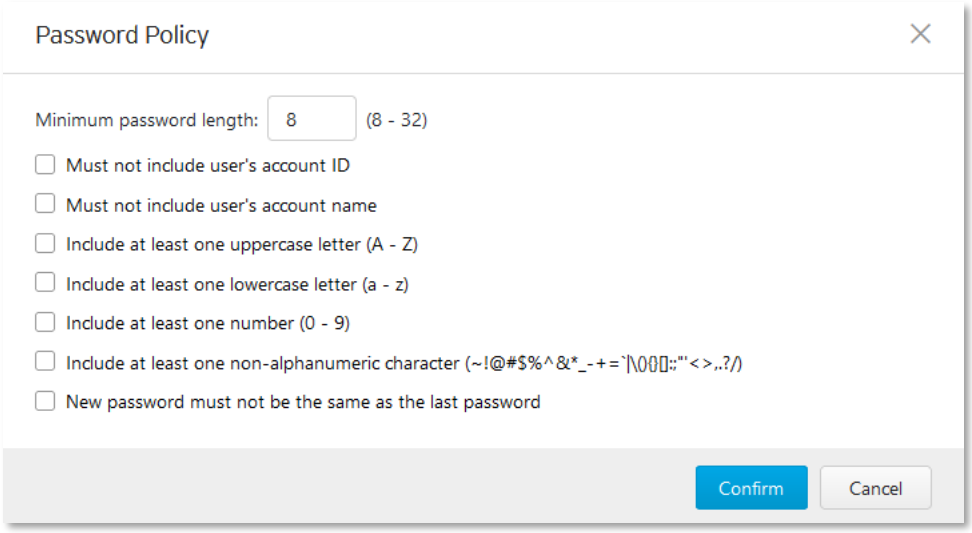
EdgeIPS™ provides the following password policy settings to enhance web console access security:

- **Password complexity settings**
  Specify password complexity settings to enforce strong passwords. For example, you can specify users 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.

Procedure

1. Go to [Administration] > [Account Management].
2. Click the [Password Policy] tab.
   The [Password Policy] screen will appear.



3. Select one or more options that meet your required password policy.
4. Click Save.

Auth Service

Use the [Auth Service] tab to do the following:

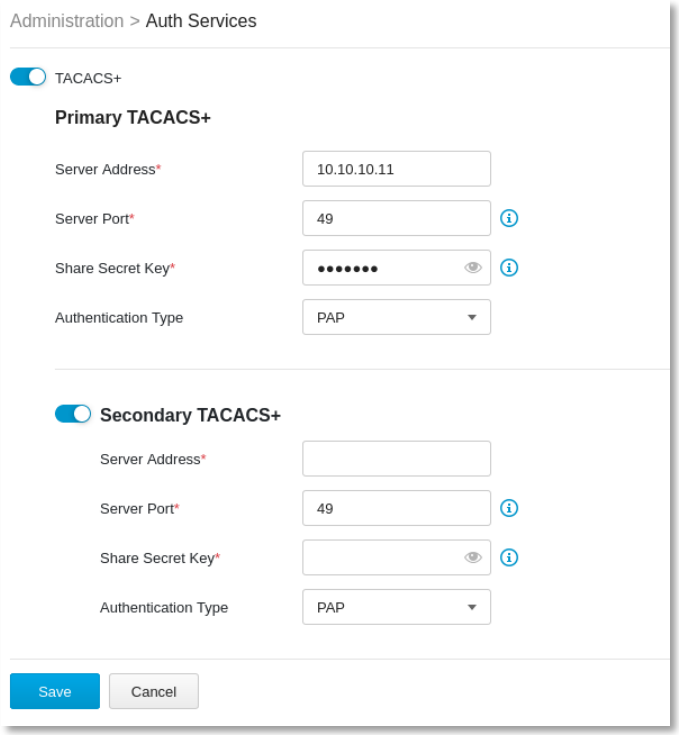
- Configure the TACACS+ of the device.

Configuring TACACS+

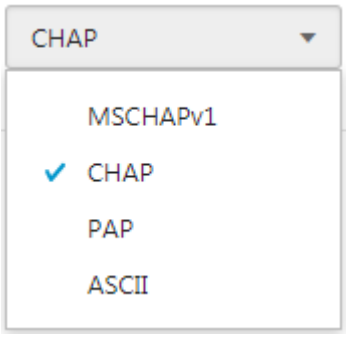
Procedure

1. Go to [Administration] > [Auth Services].

2. In the [TACACS] pane, provide the Primary and Secondary TACACS+ Server for the device.



3. Enable Primary TACACS+ and configure setting
   e. Configure Server address.
   f. Configure Server Port (Default port: 49)
   g. Configure Share Secret Key (MAX: 64 characters)
   h. Select Authentication type, includes list as follows



   i. Enable Secondary TACACS+ Server if you need

System Management

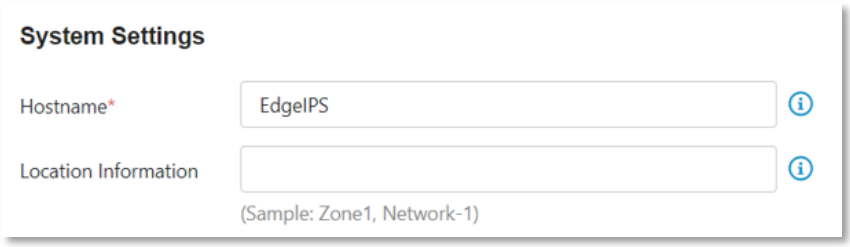
Use the [System Management] tab to do the following:

- 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

Procedure

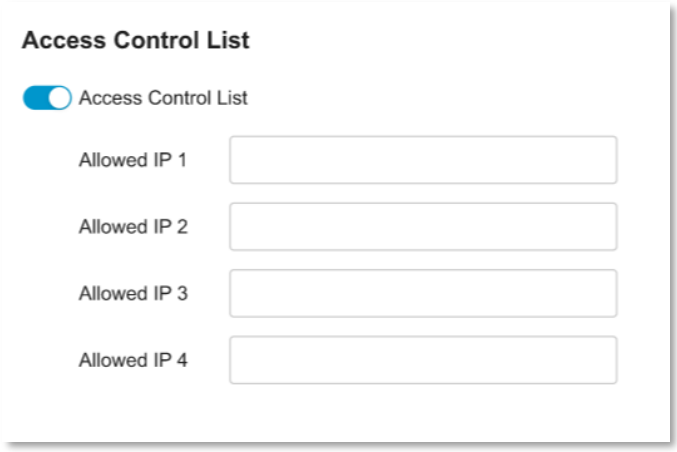
1. Go to [Administration] > [System Management].
2. In the [System Settings] pane, provide the host name and location information for the device.



Configuring Control List Access from Management Clients

Procedure

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.



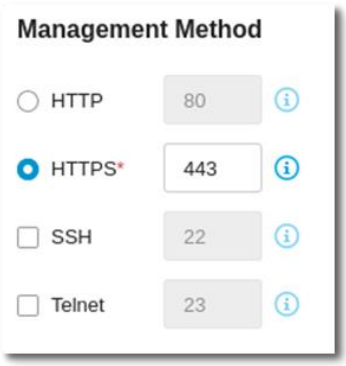
Configuring Management Protocols and Ports

Procedure

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 Tab

EdgeIPS™ can be managed by a TXOne ODC (Operational Technology Defense Console). Use this tab to register the EdgeIPS™ to a TXOne ODC.

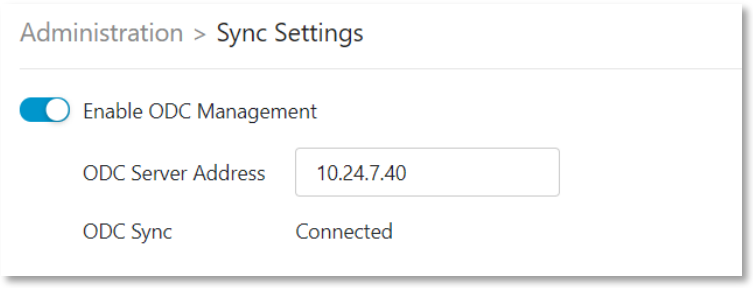
Enabling Management by ODC

Procedure

1. Go to [Administration] > [Sync Settings].

a. Use the toggle to enable management by ODC.

b. Input the IP address of the ODC server.



The Syslog Tab

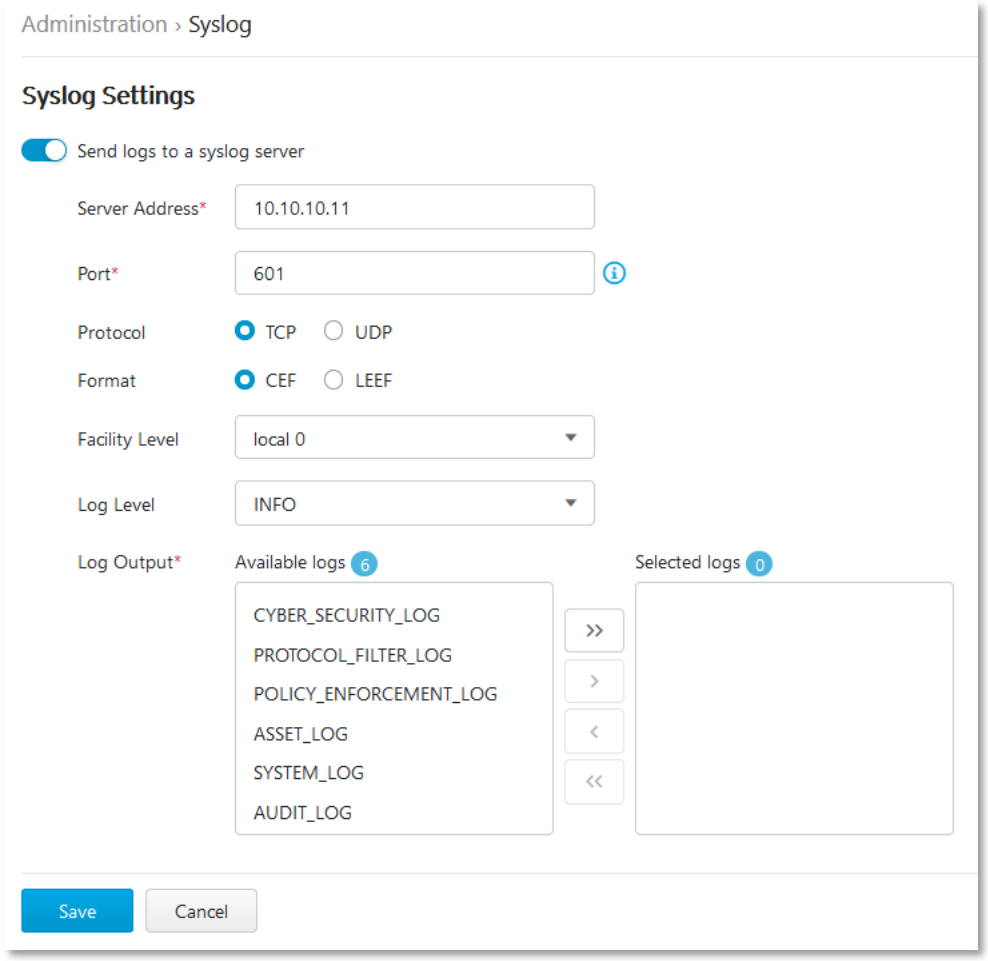
The EdgeIPS™ system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) and Log Event Extended Format (LEEF) syslog messages are used in EdgeIPS.

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

Configuring Syslog Settings

Procedure

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.
Format	Select the syslog format: CEF or LEEF
Facility Level	Select a facility level to determine the source and priority of the logs.
Log level	Select a Syslog severity level.

Field	Description
	This device only sends logs with the selected severity level or higher to the Syslog servers. For more information, see *Syslog Severity* Levels *on page 72*.

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	Alert	▪ Primary system failure Take immediate action.
2	Critical	▪ Urgent failure Take immediate action.
3	Error	▪ Non-urgent failure 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

The following table summarizes the logs of Policy Enforcement/Protocol Filter/Cyber Security and their equivalent Syslog severity levels.

Policy Enforcement / Protocol Filter Action	Cyber Security 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

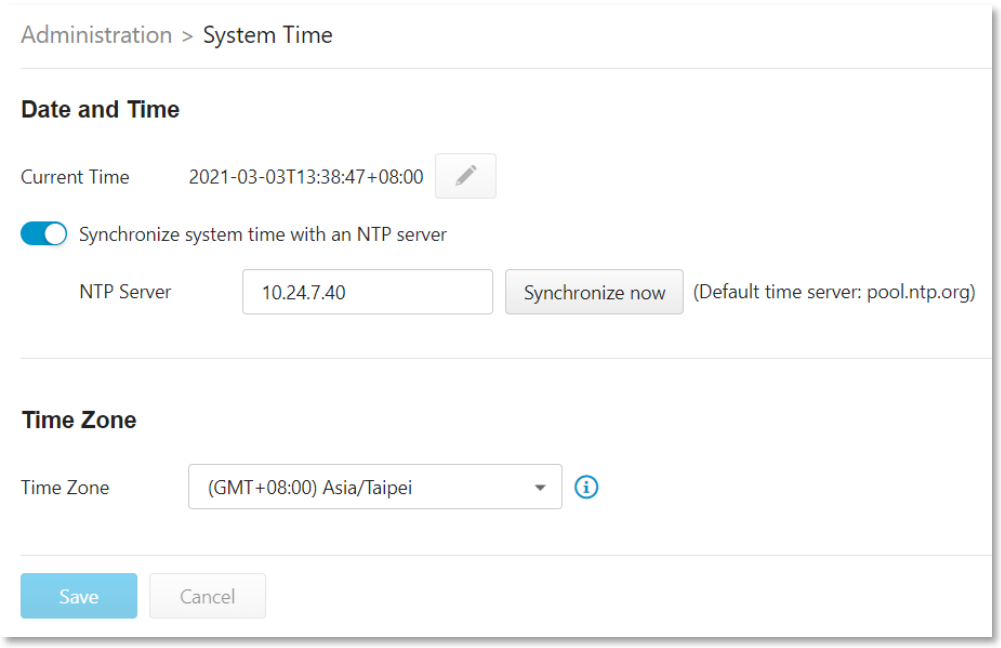
The System Time Tab

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

Procedure

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 elect the date and time.
     b. Set the hour, minute, and second.
     c. Click Apply.
3. From the [Time Zone] drop-down list, select the time zone.
4. Click Save.

Note: ODC system synchronizes the system time with its managed instances.

The Back Up / Restore Tab

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

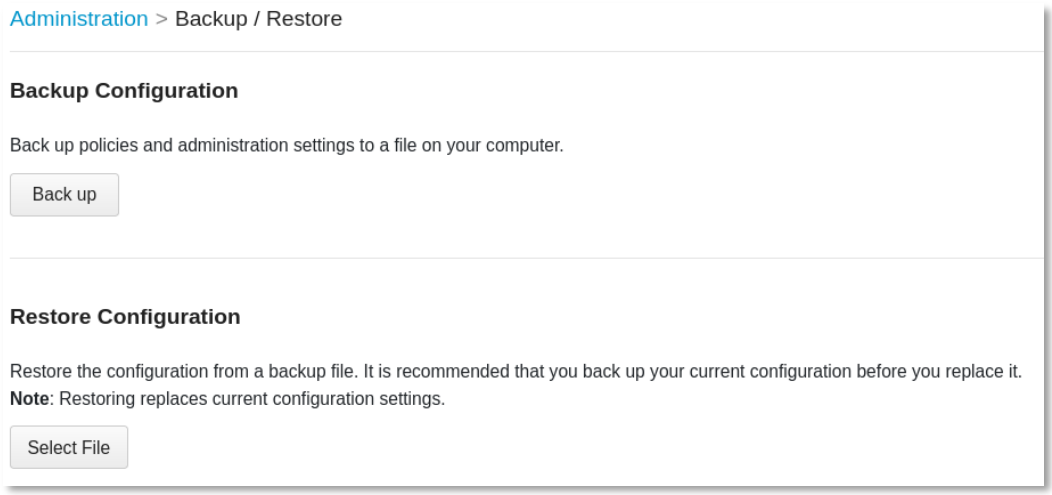
We recommend the following:

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

Backing Up a Configuration

Procedure

1. Go to [Administration] > [Backup / Restore].
   The [Backup / Restore] tab will appear.



2. Click the [Back Up] button.
   A configuration backup file will automatically be saved in your computer.

Restoring a Configuration

Follow the steps to restore the configurations of the EdgeIPS.

Procedure

1. Go to [Administration] > [Backup / 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 Tab

Use the [Firmware Management] tab to:

- View the firmware information for the device
- Upgrade the firmware of the device
- Boot into standby partition and firmware

Viewing Device Firmware Information

Procedure

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 Time].

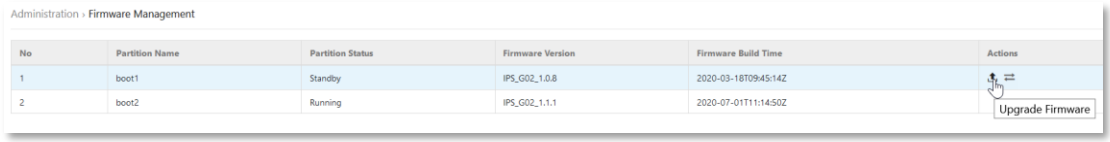
Note: EdgeIPS can have up to two firmwares installed. Each firmware is installed in its own separate partition. At any given point in time, one partition will have the status [Running], which indicates the currently running and active firmware. The other partition will have the status [Standby] which indicates an alternative or standby partition.

Updating Firmware

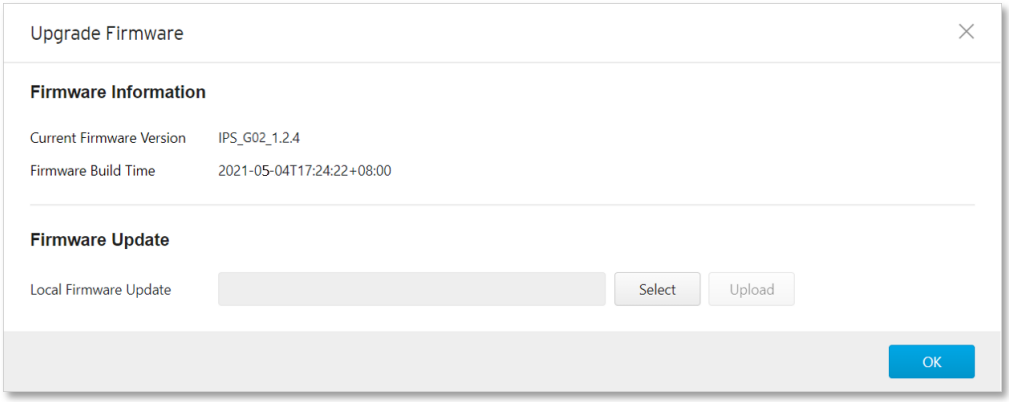
Procedure

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.
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 required firmware to [Standby] partition, click on the [Reboot and Apply Firmware] button as shown in the next section.

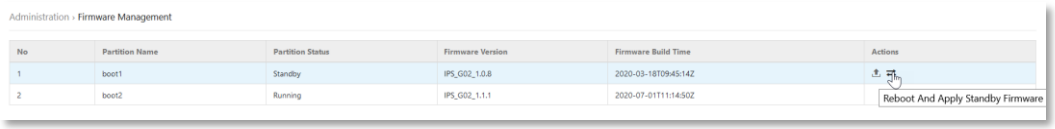
Note: Various versions of the firmware can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

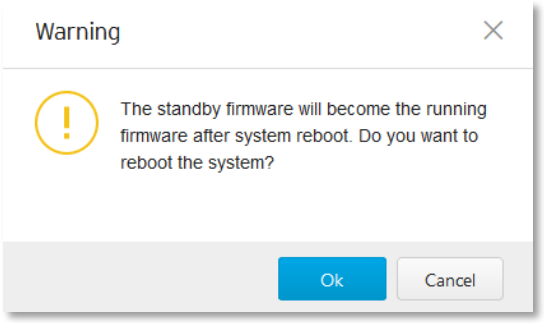
Rebooting and Applying Firmware

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

Procedure

1. Go to [Administration] > [Firmware Management].
2. Click on the [Reboot and Apply Firmware Button] that is available in the [Standby] partition row





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

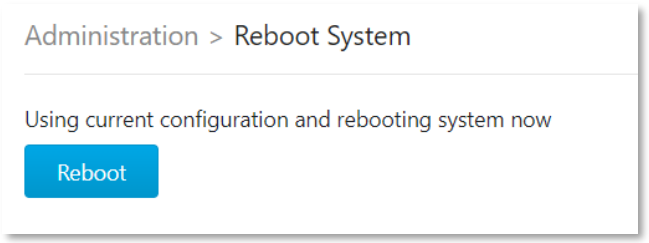
The Reboot System Tab

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

Rebooting the System

Procedure

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



Supported USB Devices

This chapter describes the use of supported USB devices with the EdgeIPS™ device for extended or supporting functionality.

To ensure optimal operation, only the below list of USB devices is currently supported. This list may be updated from time to time. Please visit TrendMicro's support page for a more updated list.

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

Supported actions via USB Disk

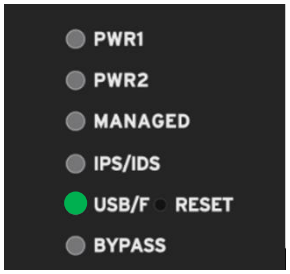
1. On-demand configuration for disk backup
2. Load pattern from disk
3. Load configuration from disk
4. Load firmware from disk

Given that this feature allows anyone with a supported USB disk device to perform various operation via USB, the physical security of the EdgeIPS device must be considered carefully.

Only supported USB disk devices may be used for this feature.

To perform any of these actions:

1. Plug the supported USB disk device into the EdgeIPS Pro device's USB port.
2. Upon successful detection of the USB disk device, the "USB/F" LED will change to a steady green. The system log can also be checked to confirm that a supported USB disk device was detected when inserted. This state is referred to as the "Default Action" state.



Note: If an unsupported USB device is plugged in, it will simply be ignored and no further action will be taken.

The functionality of the reset button will also change until the USB device is unplugged. The reset button will at this time not serve the as the 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.

The user can use the reset button to cycle through a set of possible actions. The LEDs will indicate which action is currently selected. Each quick press of the Reset button will toggle through the next possible action.

Possible Actions to Toggle Through

State/Action	LED	COLOUR/STATE
Default State – USB Plugged in Backup Configuration	USB/F LED	Green – Steady
Load/Restore Pattern	IPS/IDS LED	Green – Blinking (1/sec)
Load/Restore Configuration	MANAGED LED	Green – Blinking (1/sec)
Load/Restore Firmware	IPS/IDS & MANAGED LED	Green – Blinking (1/sec)

1. After selecting an action, it must be confirmed by pressing the Reset button for more than 3 seconds. (a long, steady press).

Note: The action must be confirmed within 10 seconds. If the action is not confirmed within 10 seconds, the LEDs will be return to their default state.

2. While an action is being attempted, if there is a USB disk data transfer, the following LEDs will indicate it as shown here and then return to previous state after data transfer is complete.

Data Transfer Indication	LED	COLOUR/STATE
	USB/F LED & IPS/IDS LED	Green – Blinking (Once every 0.5 sec)

3. If any error occurs when action is being attempted, the following LEDs will show it like so:

Error Indication (on any error while action was being processed)	LED	COLOUR/STATE
	USB/F 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.

4. Relevant system logs can be checked to verify whether the action was completed successfully or failed. 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.

5. 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/F LED off), and a log will be available in system logs.

On-demand Configuration backup

1. In the "Default Action" state, on-demand configuration backup to disk can be performed by holding down the reset button for > 10 seconds. During file transfer the USB LED may blink. However, since configuration files are usually not be very large, this process may finish quickly.

2. This action will save the current running configuration to the disk under the path"**/TXone/config/xxxxxx.acf**".

3. After saving the config, if successful, the USB app will return to the "Default Action" state. If any error occurs, the FAULT LED will turn red.

The system logs will also reflect whether the action was successful or not.

Load Pattern from Disk

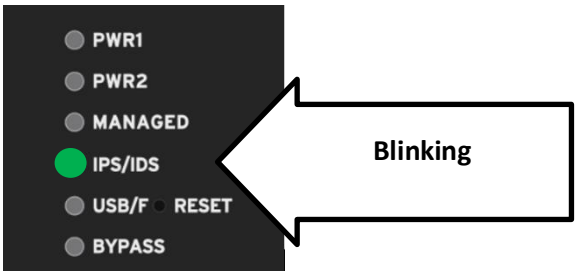
A DPI pattern file may be easily and quickly loaded from a USB disk device. This functionality allows for a floor operator to update the pattern file on the physical floor of the ICS environment without the need of a client computer to log into the device.

1. Save the pattern file in a USB disk device under path "**/TXone/pattern/**". Assuming a pattern file has the name pattern.acf, its file path on the USB disk device 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.

If multiple pattern files exist in the folder, the newest will be used.

2. Plug in the USB disk. Enter the "Default Action" state.
3. In the default action state, give the reset button one short press to toggle it to its "Load Pattern" action state.
4. When in its "Load Pattern" action state, the "IPS/IDS" LED will change to blinking green.



5. The "Load Pattern" action must now be confirmed by holding down the reset button for more than 3 seconds.

6. After confirmation, the selected action will be attempted. If successful, the USB app will return to the "Default Action" state. If any errors occur, the USB/F LED will turn red.

7. The system logs will also reflect whether the action was successful or not.

Load Configuration from Disk

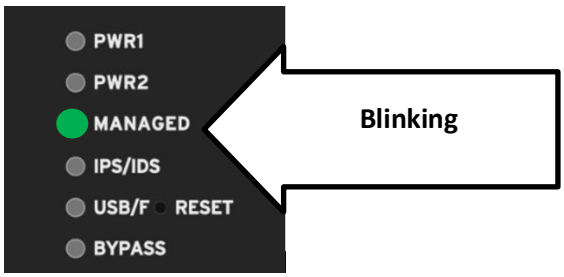
A configuration file may be easily and quickly loaded via a USB disk device. This functionality allows for a floor operator to update/restore the configuration on the physical floor of the ICS environment without the need of a client computer to log into the device.

1. Save the pattern file in a USB disk device under path "**/TXone/config/**". Assuming a pattern file has the name pattern.acf, its file path on the USB disk device would be "**/TXone/config/config.acf**".

Note: Saving config 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.

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

2. Plug in the USB disk. Enter the "Default Action" state.
3. In the default action state, give the reset button one short press to toggle it to its "Load Config" action state.
4. When in its "Load Config" action state, the "MANAGED" LED will change to blinking green.



5. The "Load Config" action must now be confirmed by holding down the reset button for more than 3 seconds.
6. After confirming, the action will be attempted. If successful, the USB app will return to the "Default Action" state. If any error occurs, the USB/F LED will turn red.
7. The system logs will also reflect whether the action was successful or not.

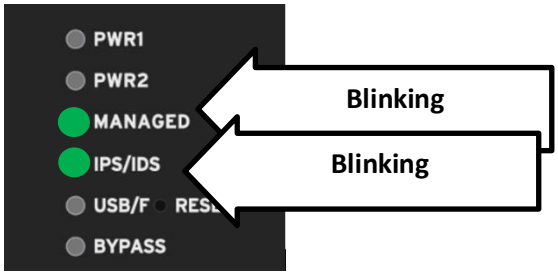
Load Firmware from Disk

Device firmware may be easily and quickly upgraded via a USB disk device. This functionality allows for a floor operator to upgrade/change the firmware of a device on the physical floor of the ICS environment without the need of a client computer to log into the device.

1. Save the pattern file in a USB disk device under path "**/TXone/firmware/**". Assuming a pattern file has the name pattern.acf, its file path on the USB disk device would be "**/TXone/firmware/firmware.acf**".

Note: Saving firmware files under other paths or incorrect folder names will cause the file to not be detected during the firmware load process. Folder names are case-insensitive. If multiple firmware files exist in the folder, the newest will be selected in subsequent steps

1. Plug in the USB disk. Enter the "Default Action" state.
2. In the default action state, give the reset button three short presses to toggle to the "Load Firmware" action state.
3. When in "Load Firmware" action state, the "MANAGED" and "IPS/IDS" LEDs will change to blinking green.



4. The "Load Firmware" action must now be confirmed by holding down the reset button for more than 3 seconds.
5. After confirming, the action will be attempted. If successful, the USB app will return to the "Default Action" state. If any error occurs, the USB/F LED will turn red.
6. The system logs will also reflect whether the action was successful or not.

Note: Latest versions of the firmware files can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

Terms and Acronyms

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

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