EdgeIPS™ Pro

Administrator's Guide

Ver 1.1
2020-12-18

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

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

About EdgeIPS™Pro

Introduction

EdgeIPS Pro is a purpose-built appliance, set up for friendly, rack-mounted deployment and equipped with in-depth OT protocol filtering to enable administrators to easily manage micro-segmentation for a complex environment. Created using the solid ICS security building block EdgeIPS, it's built from the ground up to isolate and protect multi-segment networks. This security solution is designed specifically to fit transparently into the IT-OT convergency network environment.

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
- High availability with fail-safe multi-segmenting

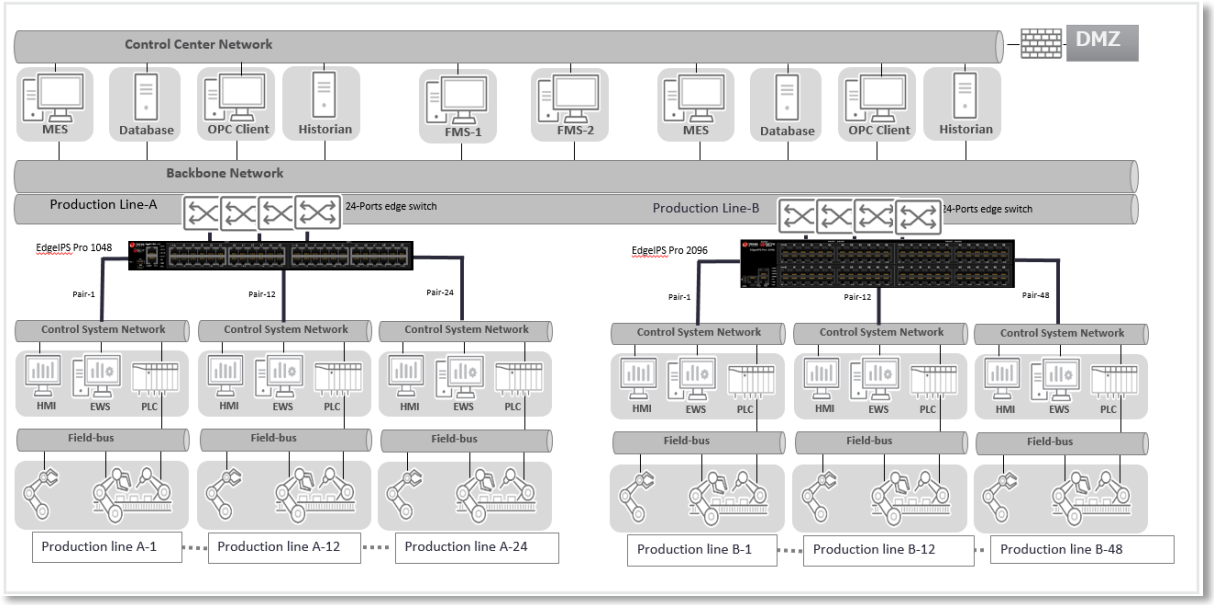


Figure 1. TXOne Networks security solutions for an OT network

Main Functions

EdgeIPS Pro is a transparent network security appliance. The main functions of the product are as follows:

Multi-segmenting with Integrated Security

EdgeIPS Pro is designed for use in levels 1-3, both in front of mission-critical assets and at the network edge. Transparent, as well as prepared to sense your network traffic and production assets, EdgeIPS Pro fits right into your network without disrupting operations.

High Port Density and Flexible Deployment

EdgeIPS Pro 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.

Extensive Support for Industrial Protocols

EdgeIPS Pro 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 Pro'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 Pro 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

EdgeIPS Pro 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'

EdgeIPS Pro 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 Pro 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 Pro offers your systems exclusive protection from undisclosed and zero-day threats.

Easily Centralized Management with Convenient, Consolidated Overview

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 Pro and how to get started with configuring the initial settings.

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 Pro - Quick Setup Guide"

Getting Started: Task List

This task list provides a high-level overview of all procedures required to get EdgeIPS Pro 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 12*.
2. Change the administrator password.
   For more information, see *Changing the Administrator's Password on page 13*.
3. Configure the system time. For more information, see *The System Time Tab on page 79*.
4. (Optional) Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings on page 73*.
5. Configure Object Profiles.
   For more information, see *The Object Profiles on page 22*.
6. Configure security policies.
   For more information, see *The Security on page 51*.
7. Configure the device name and device location information.
   For more information, see *Configuring Device Name and Device Location Information on page 71*.
8. (Optional) Configure the access control list from management clients.
   For more information, see *Configuring Control List Access from Management Clients on page 72*.
9. Configure management protocols and ports.
   For more information, see *Configuring Management Method and Access* Control List Configuring Management Protocols and Ports *on page 71*.
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 72*.
12. Configure the network settings and network interface link modes for the device.
    For more information, see *The Network on page 17*.

Opening the Management Console

EdgeIPS Pro 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.

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.

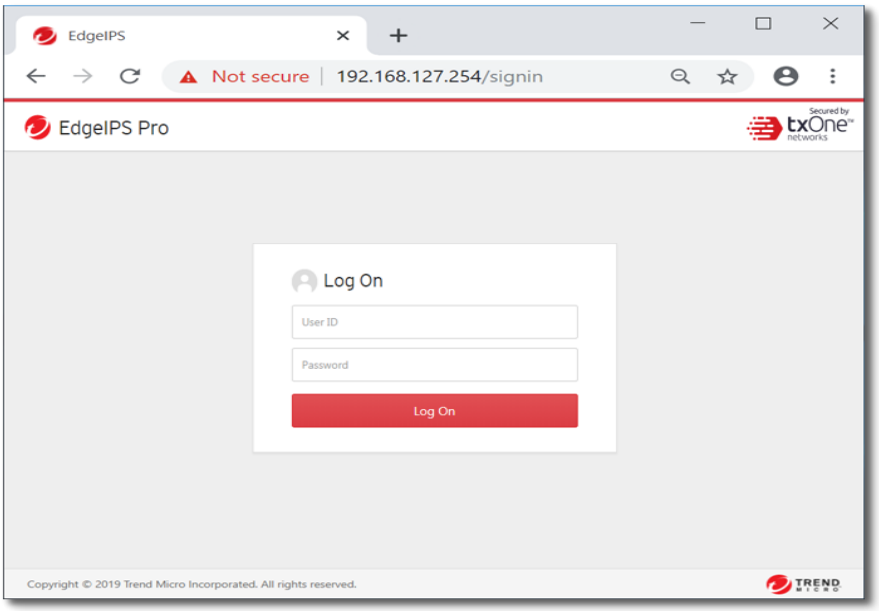
Procedure

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

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.

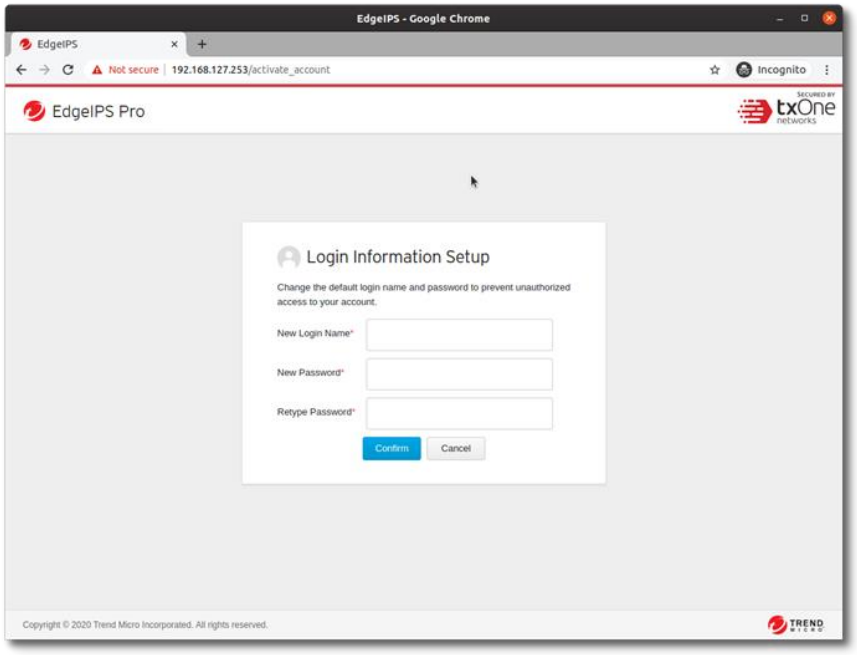
The default IP address of EdgeIPS Pro is 192.168.127.254 with subnet 255.255.255.0. Before connecting a PC/Laptop to EdgeIPS Pro, the PC's IP address should be set to an IP address that is able to access to access the default IP address. After that, connect the PC and EdgeIPS Pro using an Ethernet cable.



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. Log in 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.

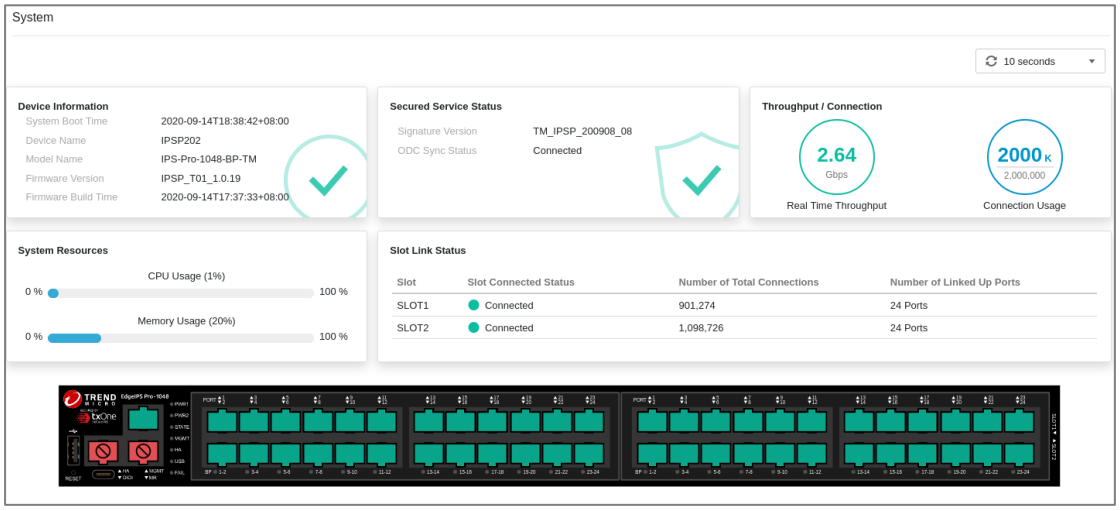


Figure 1: EdgeIPS Pro-1048

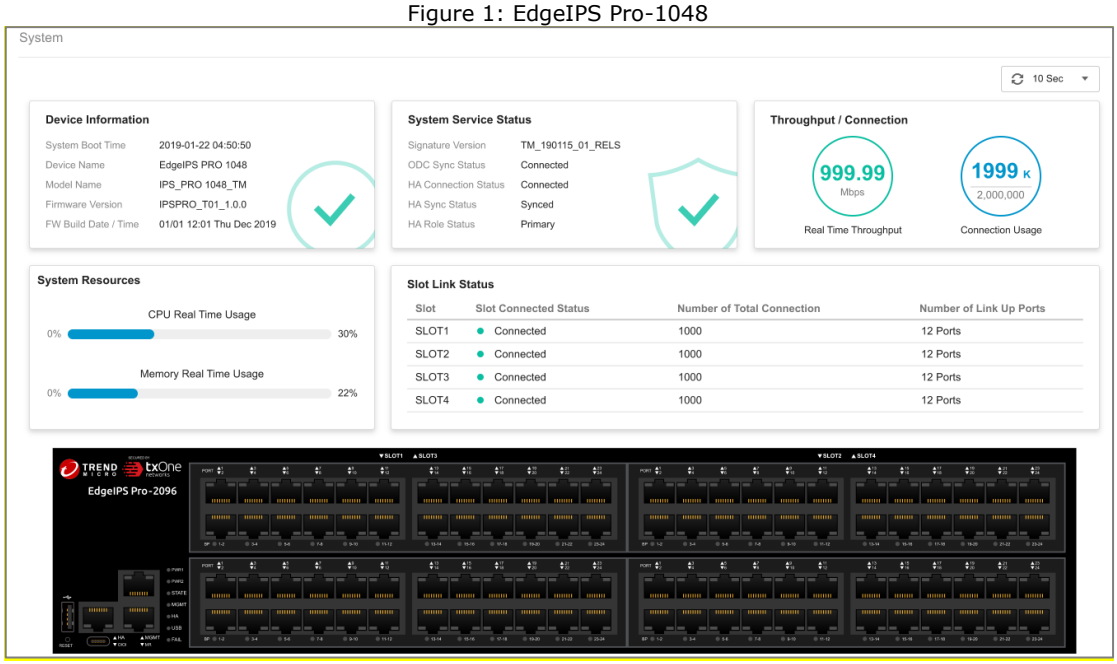
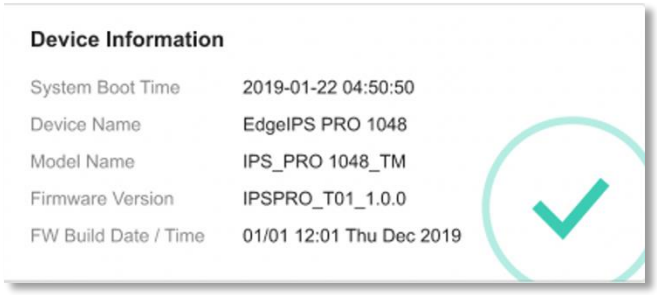


Figure 2: EdgeIPS Pro-2096 (Available firmware V1.1)

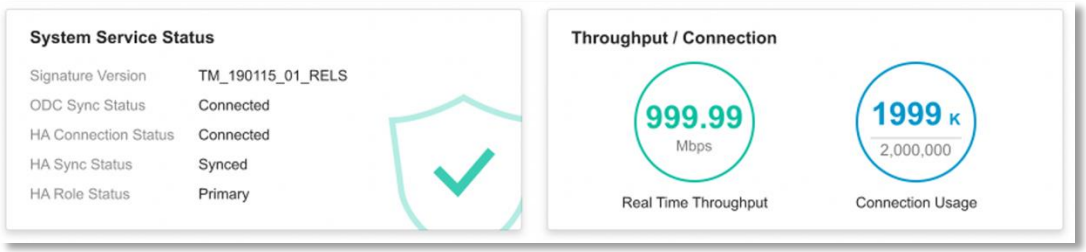
Device Information

This widget shows the time when the system booted up, name of the device, model name of the device, version of the firmware on the device, firmware build date/time.



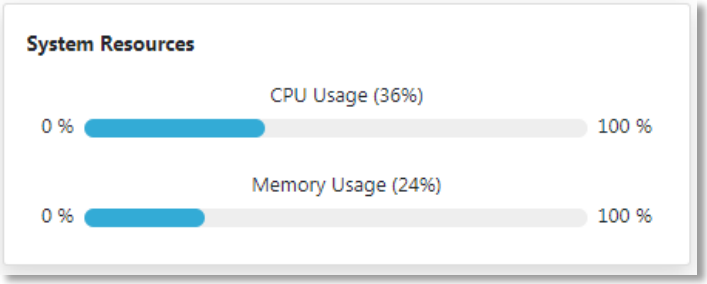
Secured Service Status & Throughput Connection

The widget shows the signature version on the device, if the device is managed by ODC, HA status, 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)

Slot Link Status

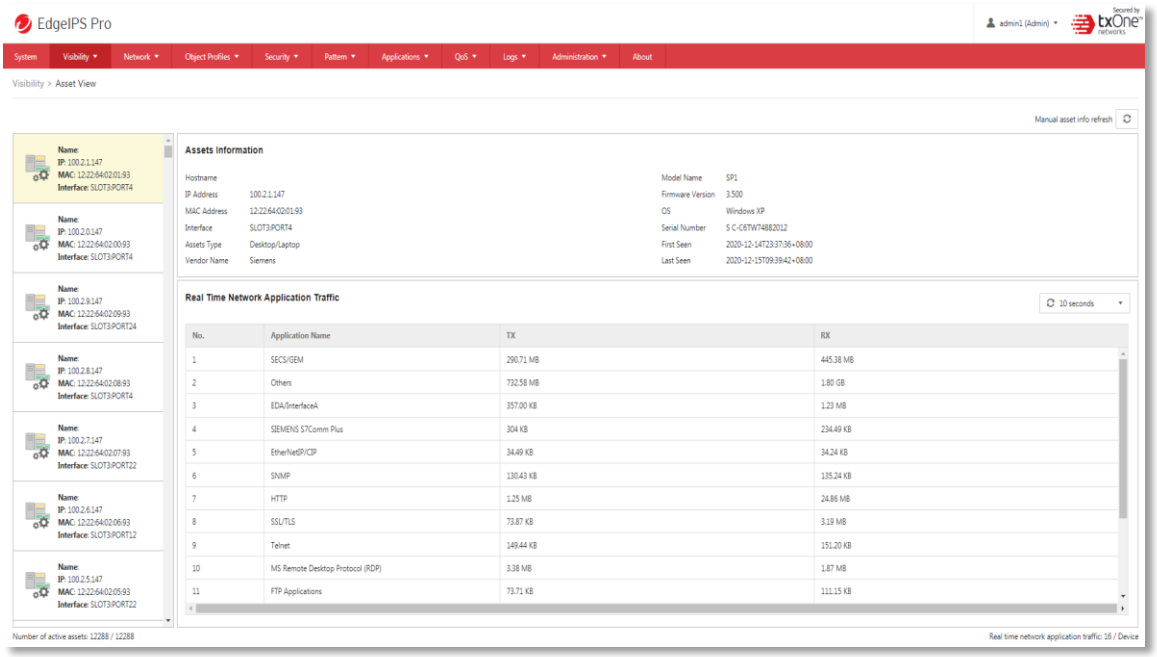
The widget shows the how many module cards have been installed and their connection status. The field includes slot number, slot connection status, total number of connections and number of linked up ports.

Slot Link Status

Slot	Slot Connected Status	Number of Total Connections	Number of Linked Up Ports
SLOT1	Connected	995,578	23 Ports
SLOT2	Connected	983,466	24 Ports

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 Pro.



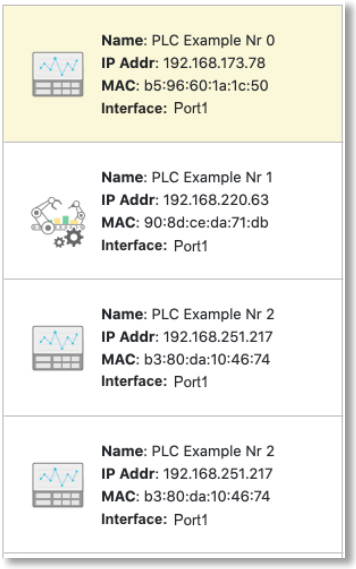
The assets, listed under the tab, are automatically detected by EdgeIPS Pro™ devices.

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

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 hostname 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.
Firmware version	The firmware version of 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 Pro 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 the network traffic statics for the asset.

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

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

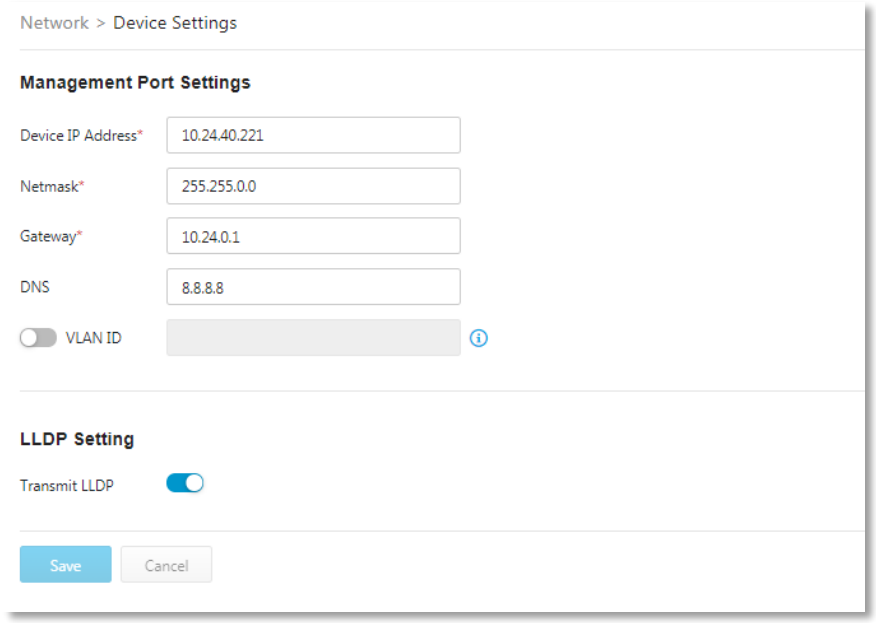
Specify the refresh time under the [Refresh Time] drop-down menu.

The Network Tab

This chapter describes how to configure various network related features and port settings.

Configuring Device Settings

Procedure



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

2. In the [Network Settings] pane, configure the network settings for the device:

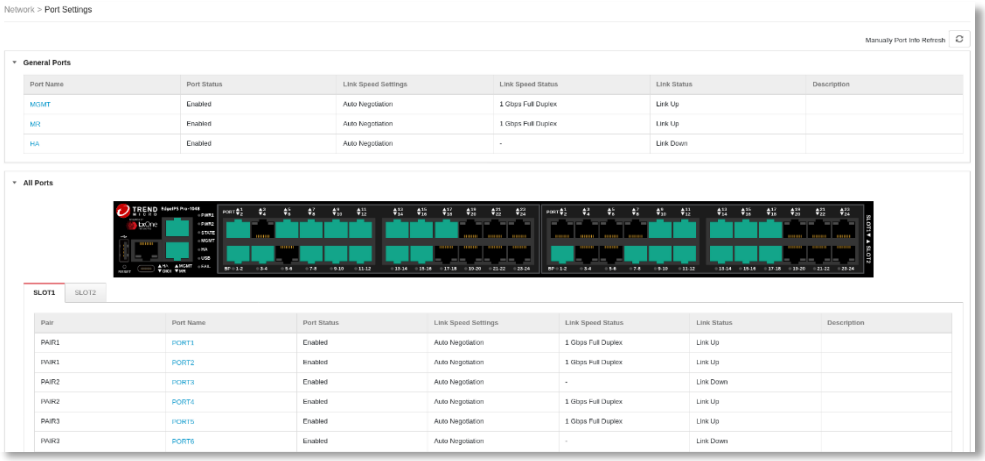
Field	Description
Device IP Address	IP Address of the device
Netmask	Netmask of the device
Gateway	Gateway of the device
DNS	DNS address of the device
Enable VLAN-ID	Enable/Disable VLAN ID
VLAN ID	Network VLAN ID of the device
Transmit LLDP	Enable Transmit LLDP, Link Layer Discovery Protocol (LLDP) for discovery and configuration – allows a network device to advertise its identity and capabilities on the network

Configuring Port Settings

Procedure

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

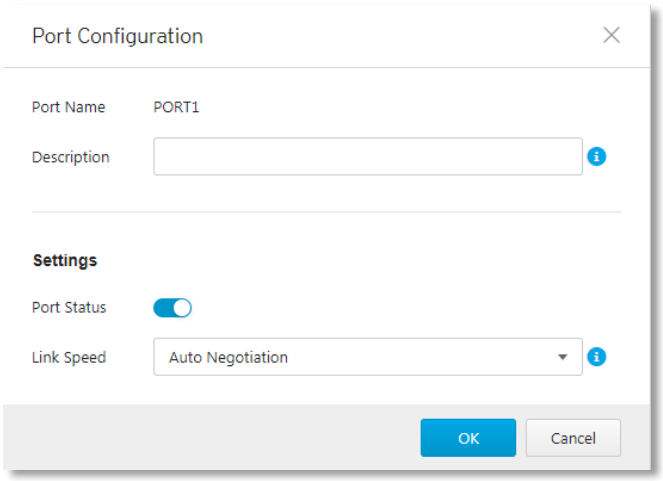
2. Click a port in the [Port Name] column to configure the port:



a. Use the toggle to enable or disable the port.

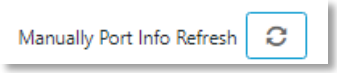
Note. The MGMT port cannot be disabled

b. Under the [Link Speed] drop down menu, select the speed and negotiation method for the port.



Note. The pane picture on the tab shows a graphical depiction of the ports that are connected on the device.

3. (Optional) Click the [Manual Port Refresh] button to refresh the information displayed.



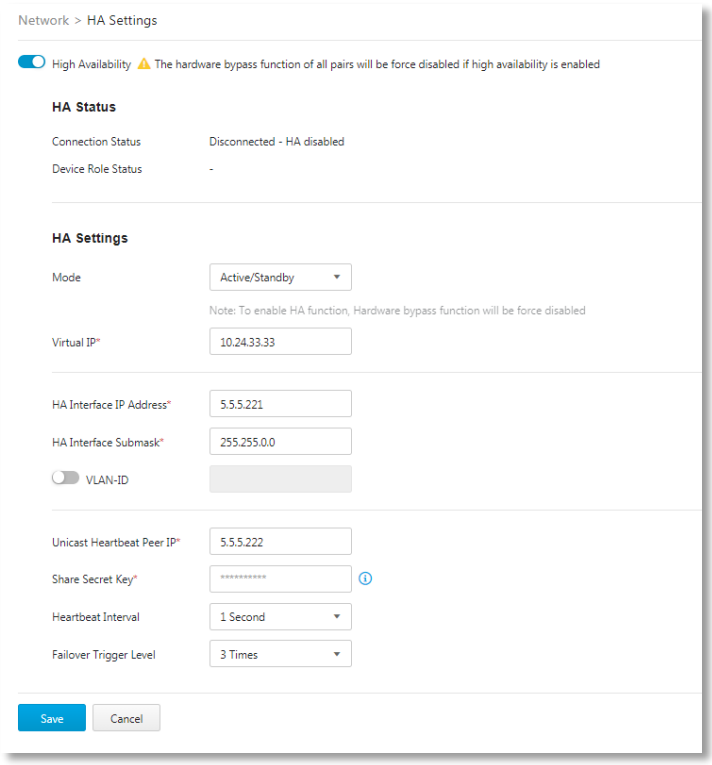
Configuring High Availability Settings

Using a single device for network security and traffic flow can create a single point of failure. IPSP provides a High Availability (HA) feature that enables redundancy by way of the ability to add and synchronize configuration with a secondary backup device. This eliminates the single point of failure and allows for a seamless switchover from primary device to secondary backup in case of primary device failure. It thus allows for the planning and building of a fault-tolerant, resilient, and secure network to minimize any OT operational downtime.

The HA feature allows for the grouping of two devices to form an HA group where configurations of the devices in the group are synchronized to support full fail-over redundancy. This section describes how to configure HA.

Procedure

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



2. In the [HA Settings] pane, configure the network settings for the device

Field	Description
Connection Status	Shows HA sync status between two EdgeIPS Pros in the same HA group. This also displays the sync progress.
HA Modes	Supported stances for HA mode: **Active-Active**: Both devices in the HA group are fully active and online. Traffic may flow via either device. If a single connection's traffic is split across the two devices, it may cause the packet classifier to not be able to classify the traffic and thus not be able to apply any filtering/security policies. A single connection's complete session must pass through a single device. In this stance, the switching/flow of traffic between devices is handled by an external/upper layer that is outside the devices.

	Active-Standby: Only one device in HA group is active and online. The secondary/standby device is only brought online in case of primary device failure. Traffic only flows via the active device. In this stance, the switching of traffic between devices is handled internally on the devices via HA protocol logic set up between the devices.
Virtual IP	A floating IP on the MGMT interface that allows access to the HA primary device
HA Interface Address	IP Address of the HA interface that will send/receive HA heartbeats and data messages to/from its peer
HA Interface Submask	Subnet mask of the HA interface
Enable VLAN-ID	VLAN ID of the HA Interface
Unicast Heartbeat Peer IP	The IP address of the HA peer
Share Secret key	Shared secret key to allow for two HA peers to authenticate and communciate with each other
Heartbeat Interval	Interval between sent heartbeats – supported range of: 1-10 seconds
Failover Trigger Level	Failover retry time – supported range of 1-10 heartbeats: Maximum number of consecutive missed hearbeats before secondary to primary switch is triggered

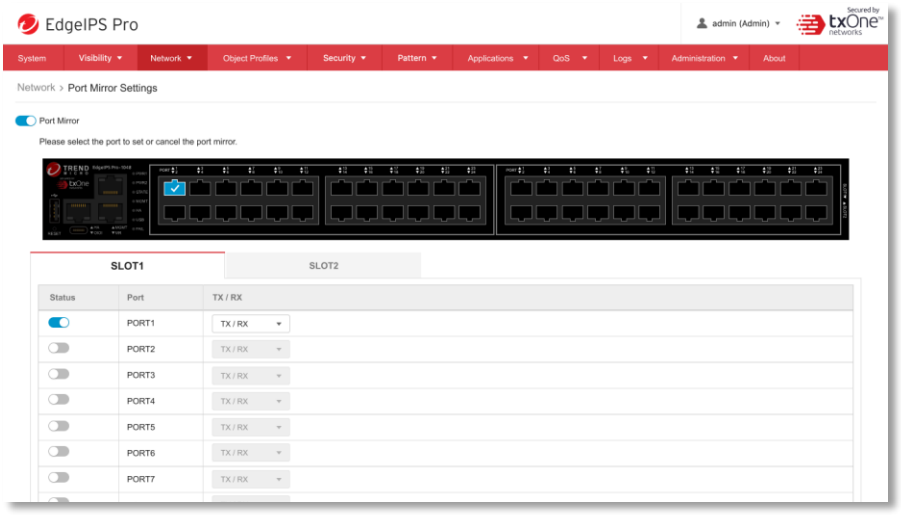
The pane picture on the tab shows a graphical depiction of the ports that are connected on the device.

Configuring Port Mirror Settings

Traffic from any of the protected segments may be mirrored to the MR port for analysis. This section describes the configuration of the same.

Procedure

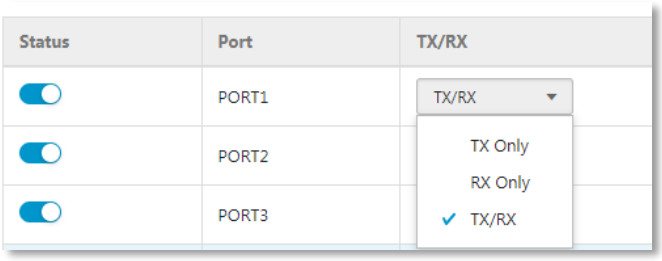
1. Go to [Network] > [Port Mirror Settings]



2. Click on a front panel port to configure it:

a. Use the toggle to enable or disable the port.

b. Under the [TX/RX] drop down menu, select the mirror traffic direction for the port.



The pane picture on the tab shows a graphical depiction of the ports that are connected on the device.

The Object Profiles Tab

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

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.
- **File Filter Profile**: Contains the settings of File filter profile that you can apply on a policy rule. Detail of File filter by protocol 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

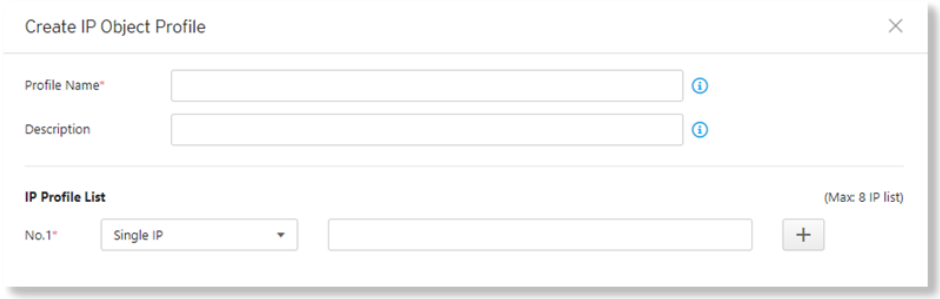
You can configure the IP address in an IP object profile, which can be used by other policy rules.

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 Profiles].
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. 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 Profiles

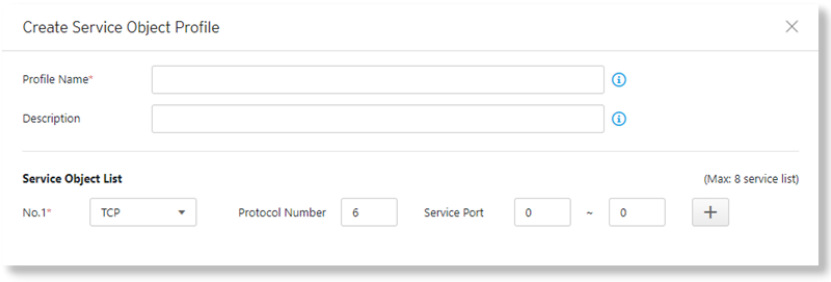
In a service object profile, you can define the following:

- 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

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

Procedure

1. Go to [Object Profiles] > [Service Object Profiles].
2. Do one of the following:
   - Click [Add] to create a profile.
   - Click a profile name to edit settings.



3. Type a descriptive name for the Service Object Profile.
4. Type a description.
5. Provide one of the following definitions:
   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

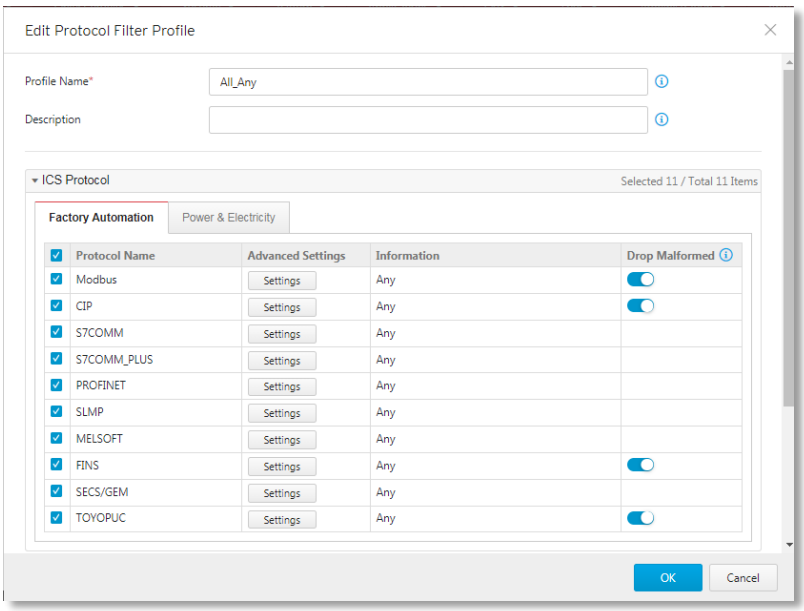
6. If you want to add another entry, click the + button.
7. Click [OK].

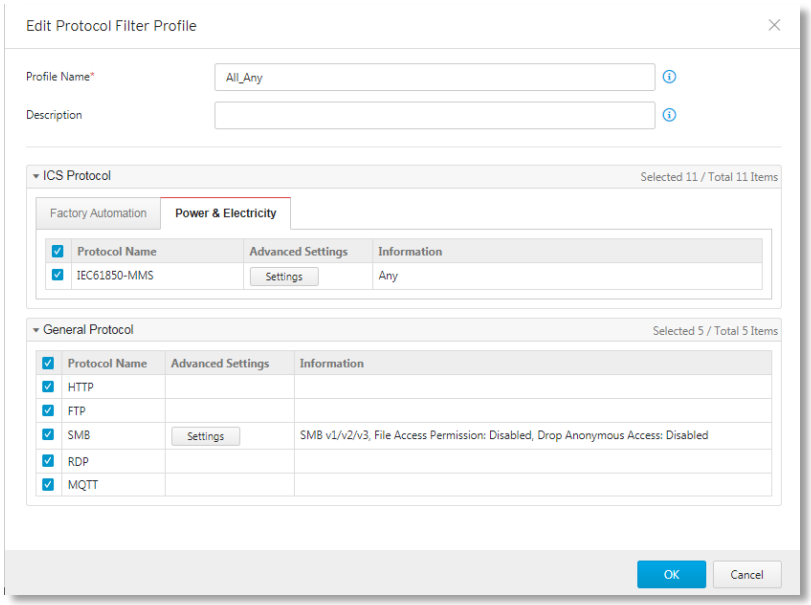
Configuring Protocol Filter Profile

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:

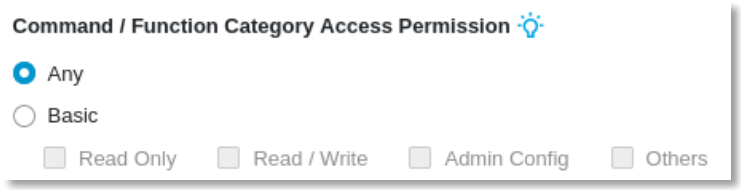
- Details of ICS protocols, including:
  - Modbus
  - CIP
  - S7COMM
  - S7COMM PLUS
  - PROFINET
  - SLMP
  - MELSOFT
  - FINS
  - SECS/GEM
  - TOYOPUC
  - IEC61850-MMS
- General Protocol, including:
  - HTTP
  - FTP
  - SMB
  - RDP
  - MQTT





Specifying Commands Allowed in an ICS Protocol

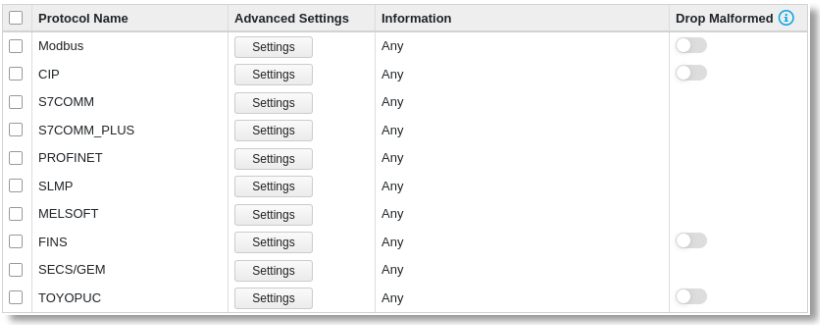
When configuring an ICS protocol, you can specify which commands will be included in the protocol profile, as the following picture shows.



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.

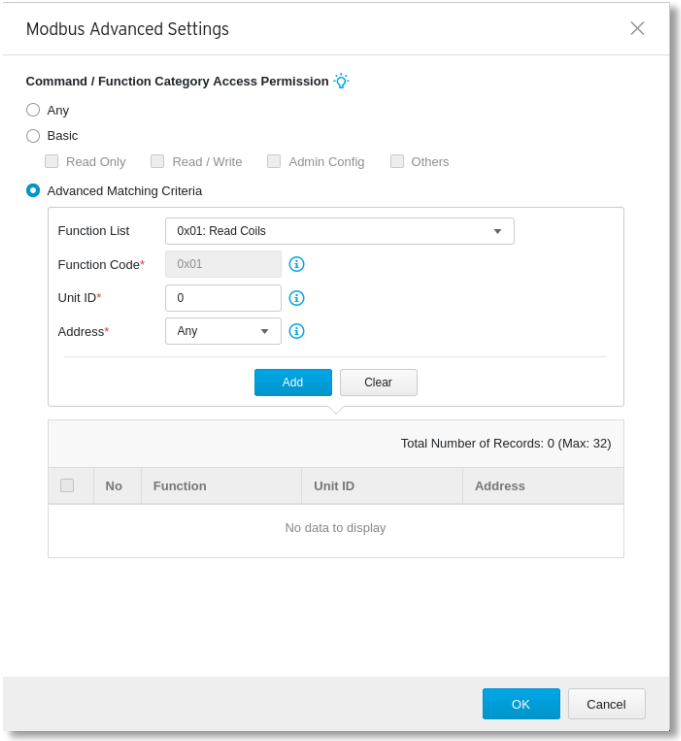
When the option [Drop Malformed] is enabled, EdgeIPS Pro will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, EdgeIPS Pro will drop the packets of the ICS protocol.



In firmware Version 1.0 and 1.1, Drop Malformed supports 4 protocols (Modbus, CIP, FINS and TOYOPUC)

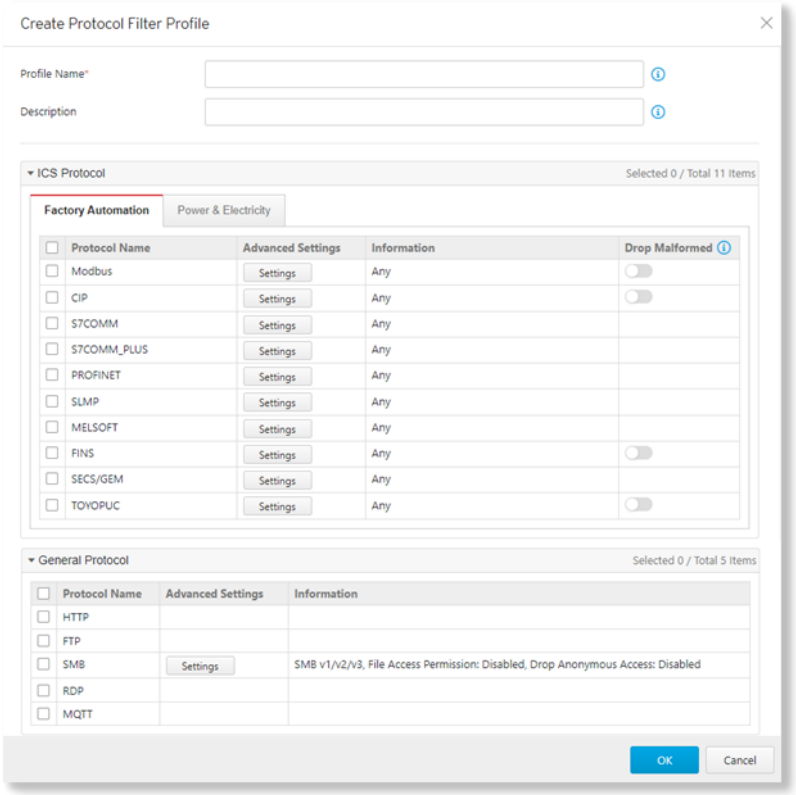
Advanced Settings for Modbus Protocol

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



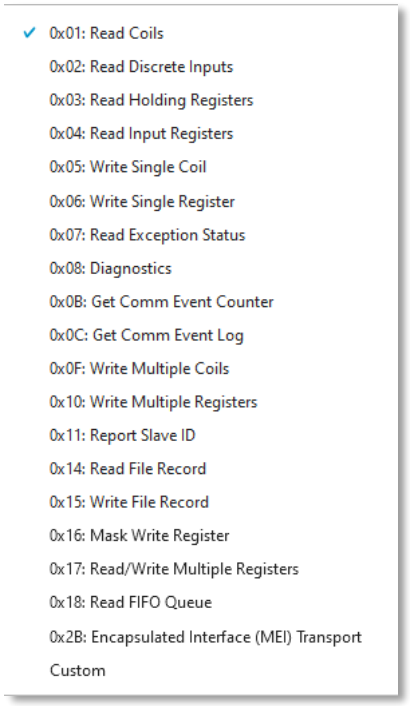
Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles].
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 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 commands relevant to administration configuration 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.

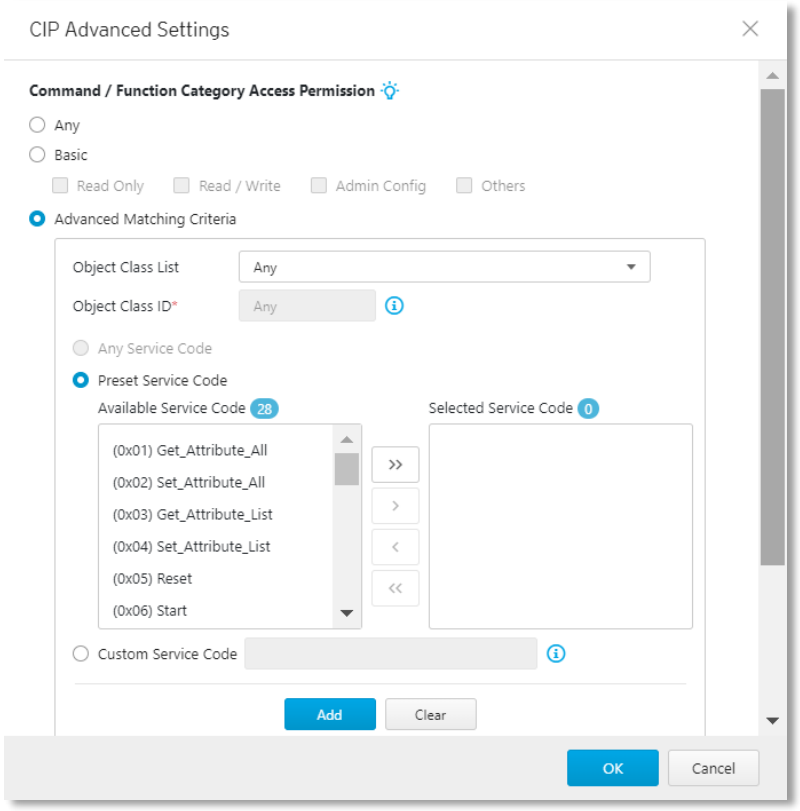


- If you want to specify a function code yourself, then select [Custom] and input a function code in the [Function Code] field.
- Type a unit ID in the [Unit ID] field.
- Type the address or range of addresses against which the function will operate.
- Click [Add].
- Repeat the above steps if you want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

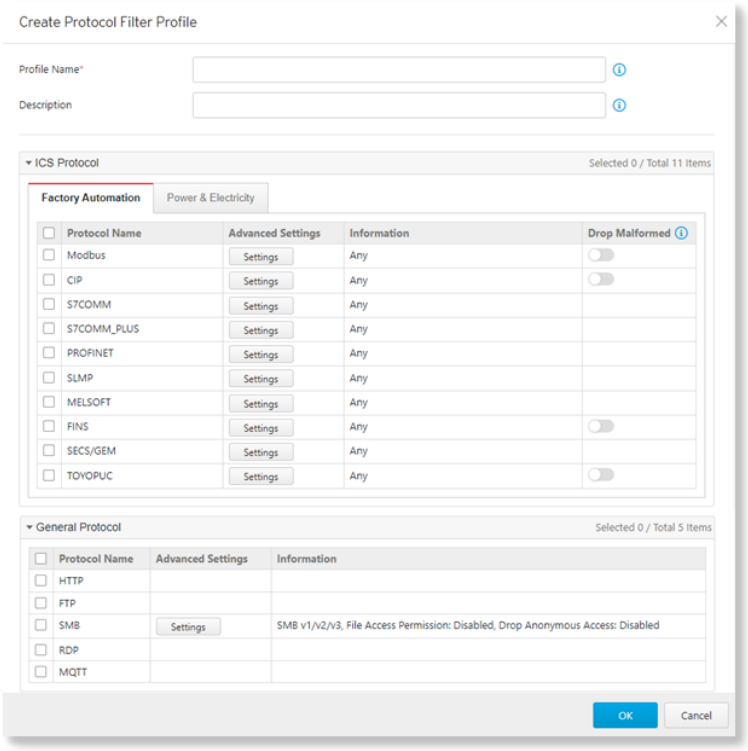
Advanced Settings for CIP Protocol

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



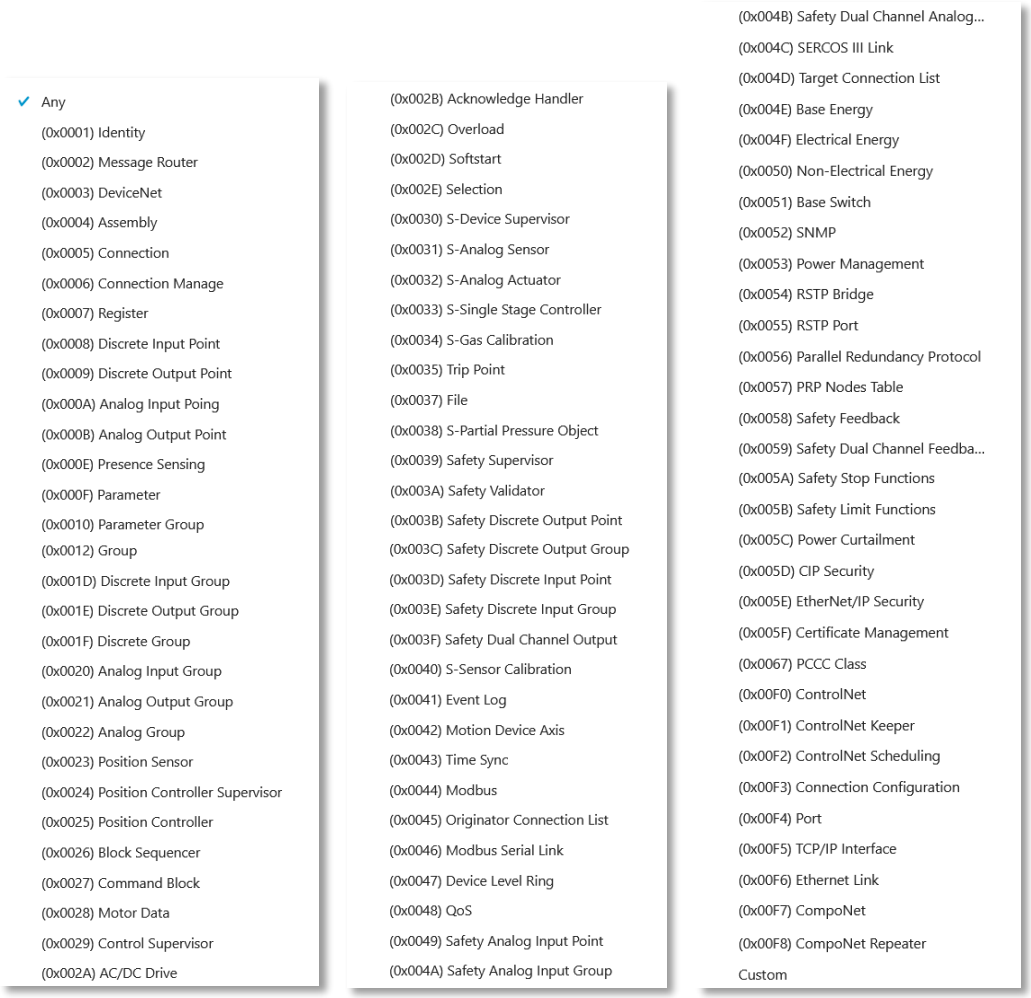
Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles].
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 for 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 commands relevant to administration configuration 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.

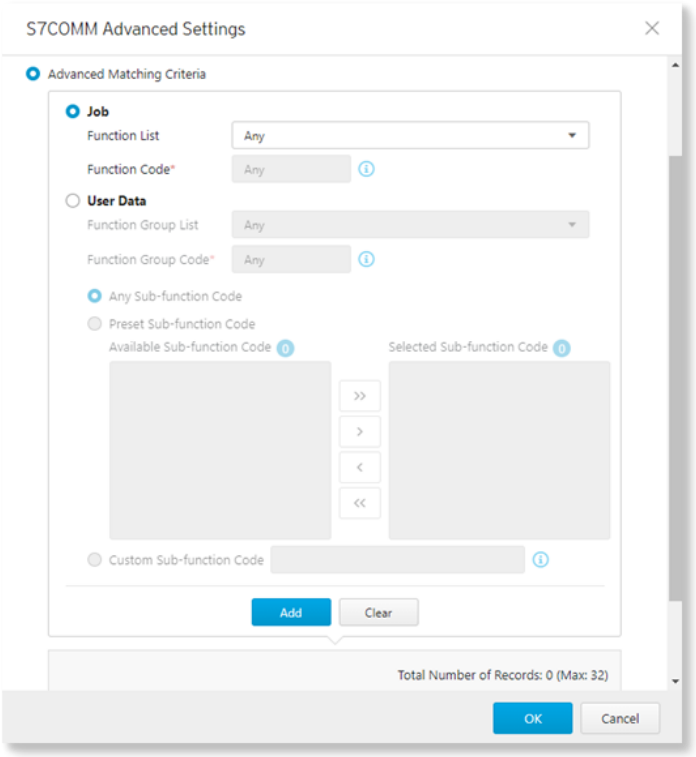


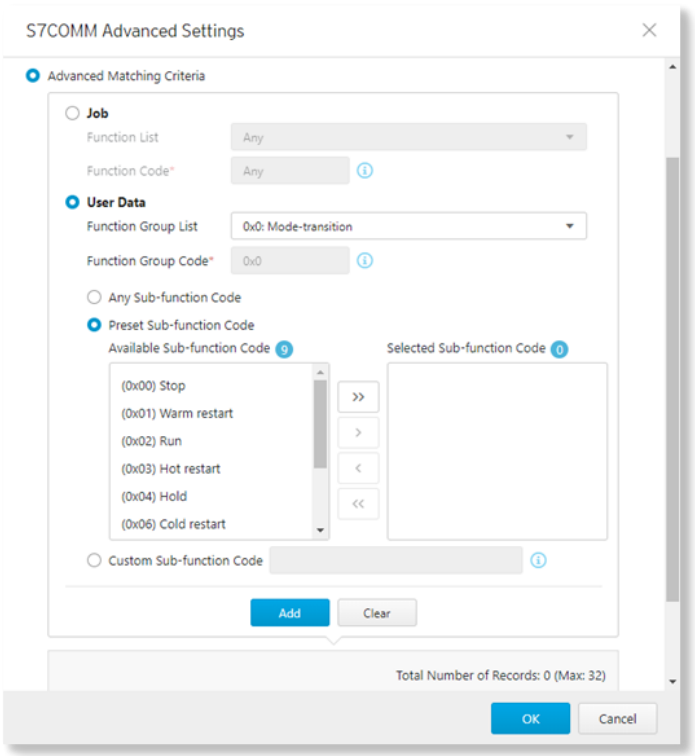
- If you want to all the service codes within the function you specified to be applied, then select [Any Service Code]
- If you want to specify one service code or multiple service codes, then select [Preset Service Code] and move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.
- If you want to specify a service code 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 [S7COMM Advanced Settings] pane, you can further specify the function code, function group code, and sub-function code against which the function will operate.

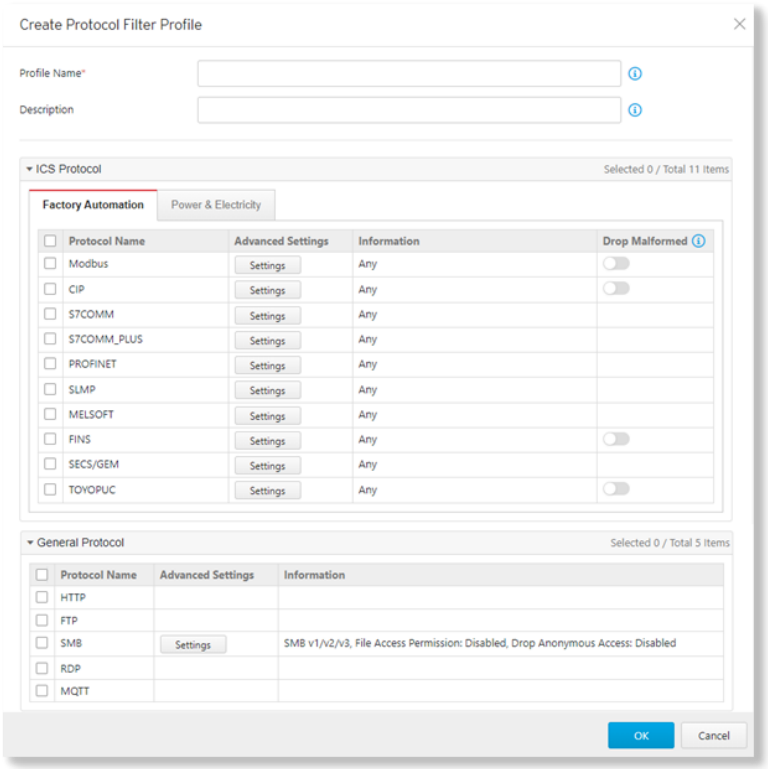




Procedure

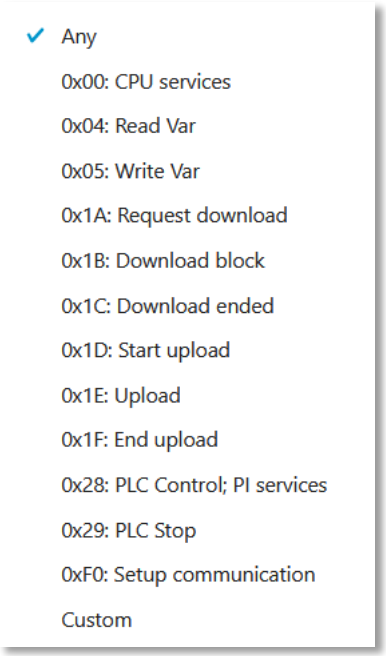
1. Go to [Object Profiles] > [Protocol Filter Profiles].

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

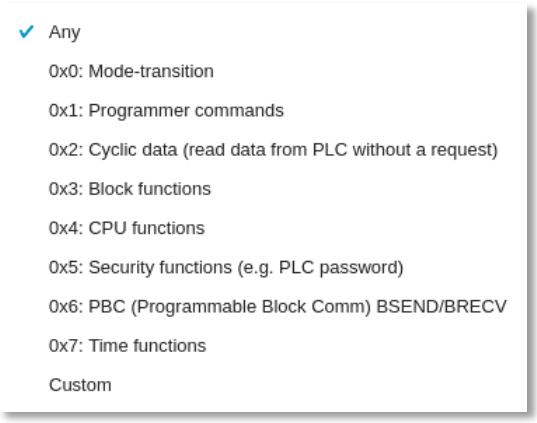


3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
   e. Click [Settings] next to a protocol, and select one of the following:
      - **Any** - Specify all available commands or function access for 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 commands relevant to administration configuration 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, then select the category [User Data] and select a function group code at the [Function Group Code] 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.

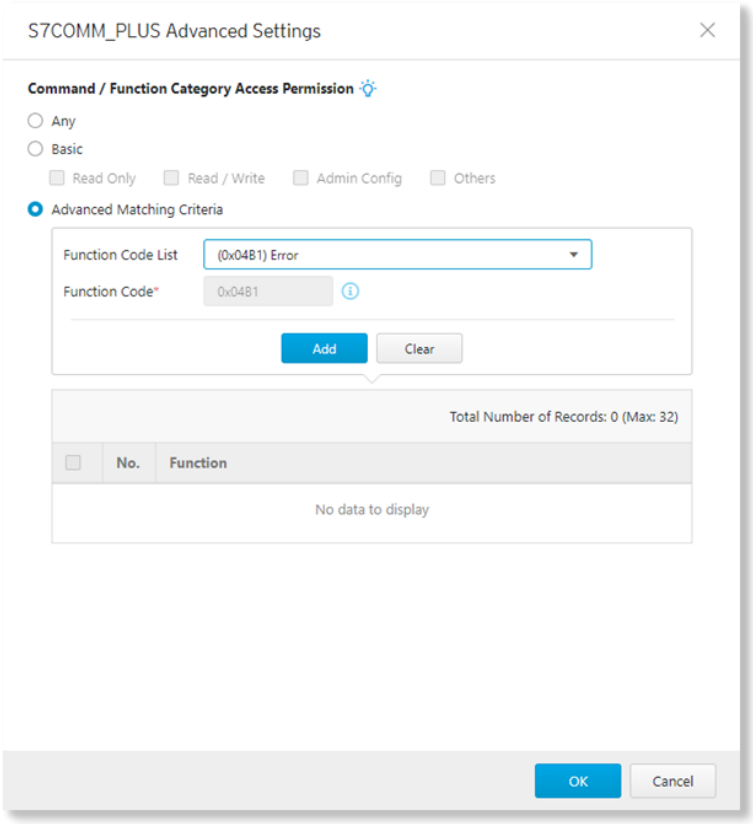
- If you want to specify a service code yourself, then select [Custom Sub-function Code] and input a sub-function code in the [Custom Sub-function Code] field.

- 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].

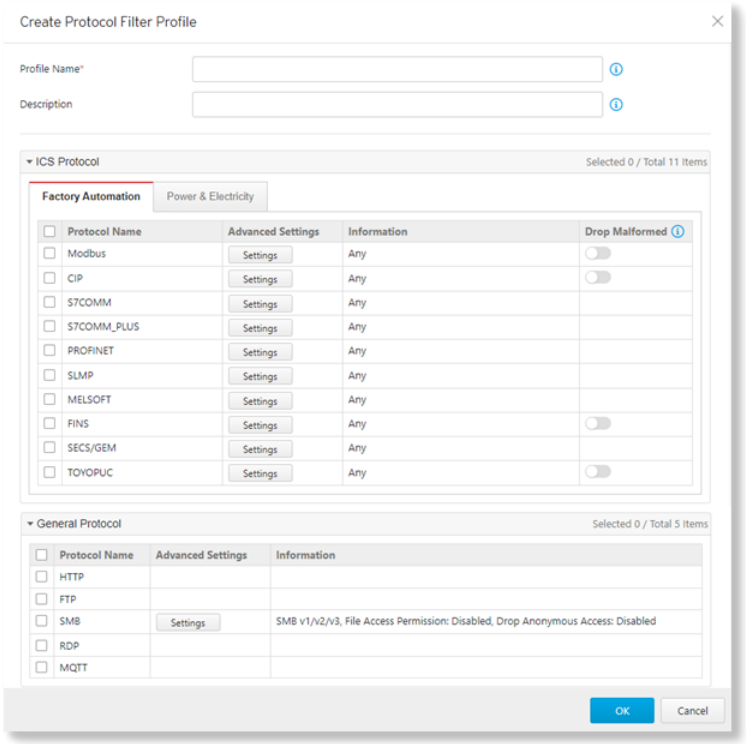
Advanced Settings for S7Comm Plus

The device features more detailed configurations for the S7Comm Plus ICS protocol. Through the [S7COMM_PLUS Advanced Settings] pane, you can further specify the function code against which the function will operate.



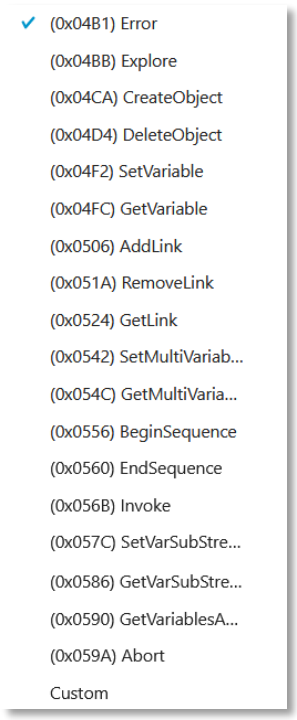
Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles].
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 for 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 commands relevant to administration configuration 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.

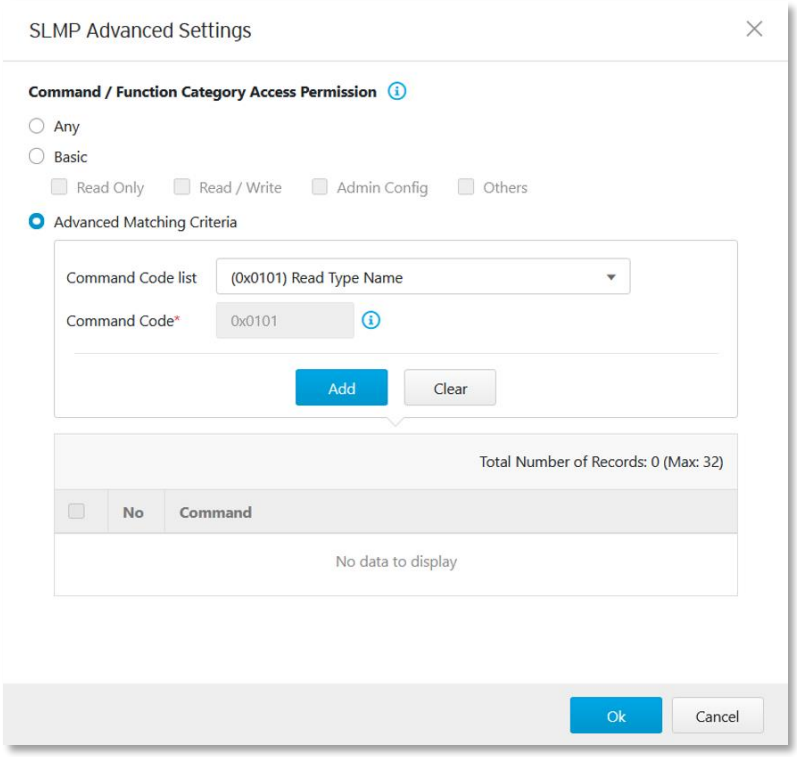


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

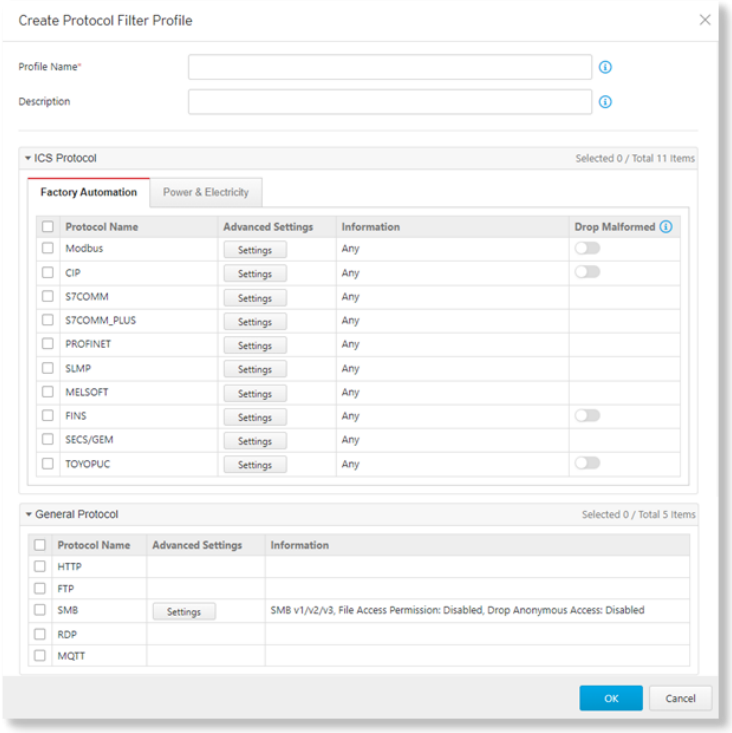
Advanced Settings for SLMP

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



Procedure

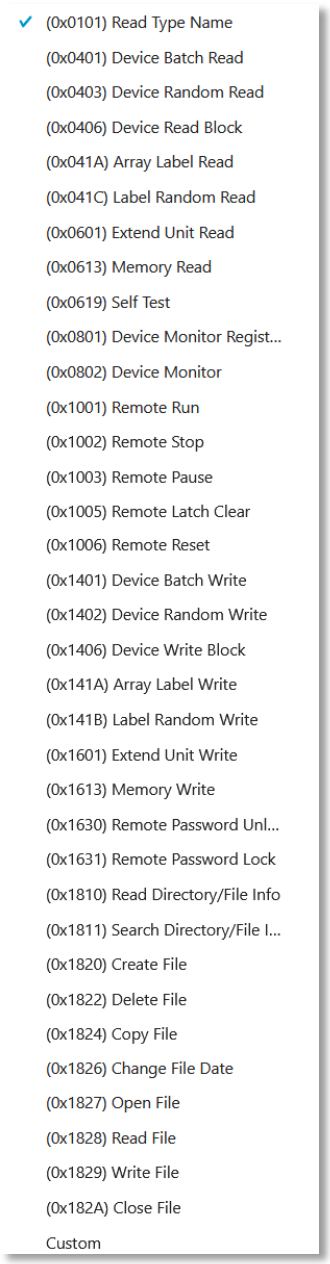
1. Go to [Object Profiles] > [Protocol Filter Profiles].
2. Click [Add] to add a protocol filter profile.
   The [Create Protocol Filter Profile] screen will appear.



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 for 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 commands relevant to administration configuration 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 function of this protocol.

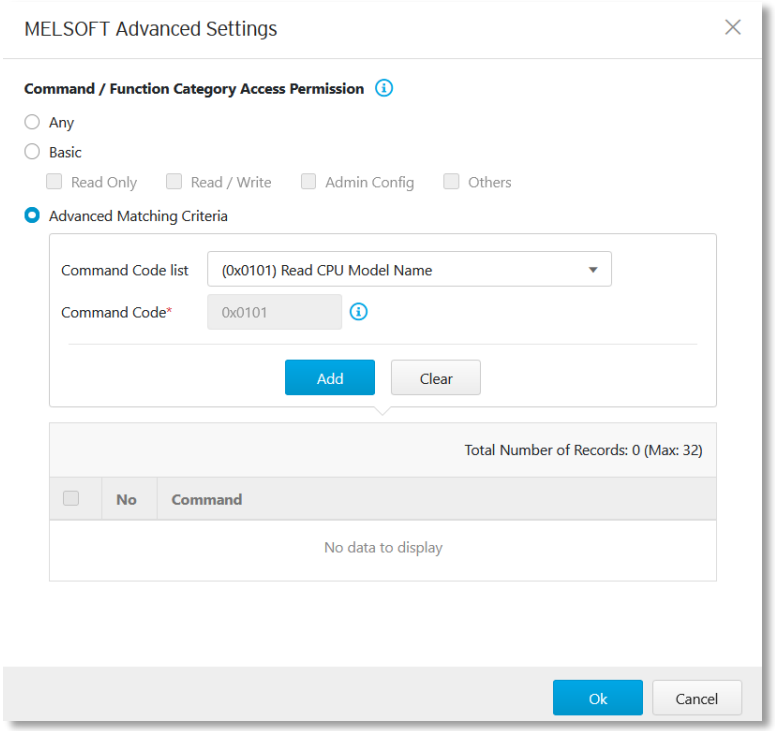


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

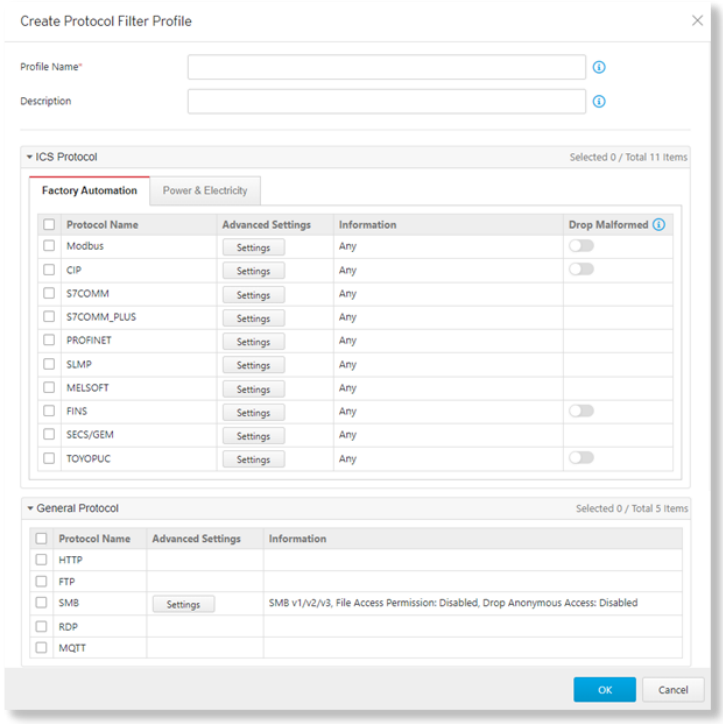
Advanced Settings for MELSOFT

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



Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles].
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 for 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:

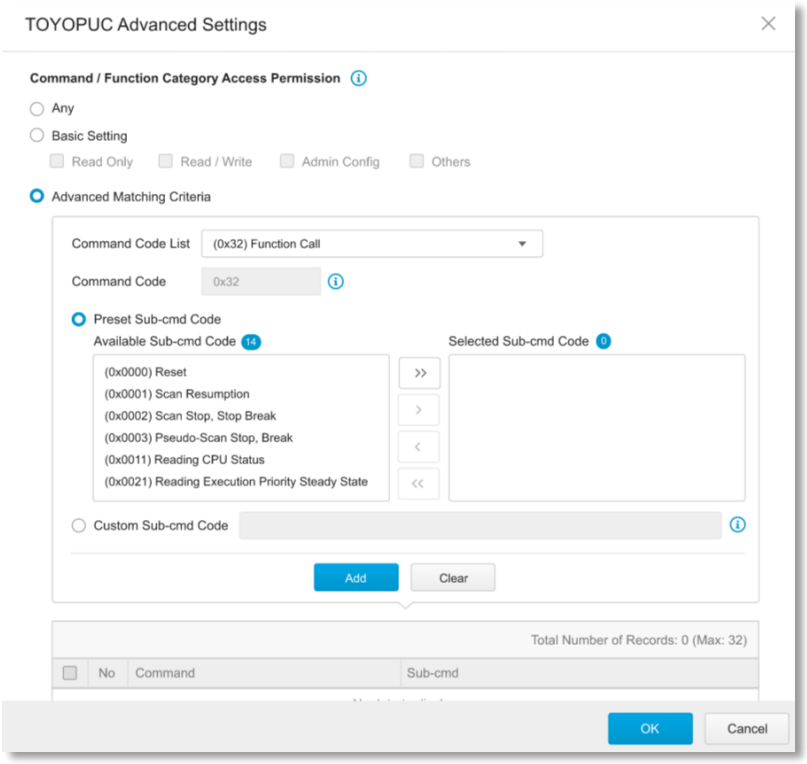
- Click [Settings] next to [MELSOFT], and select [Advanced Matching Criteria].
- At the [Command Code List] drop down menu, select a function of this protocol.

- 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].

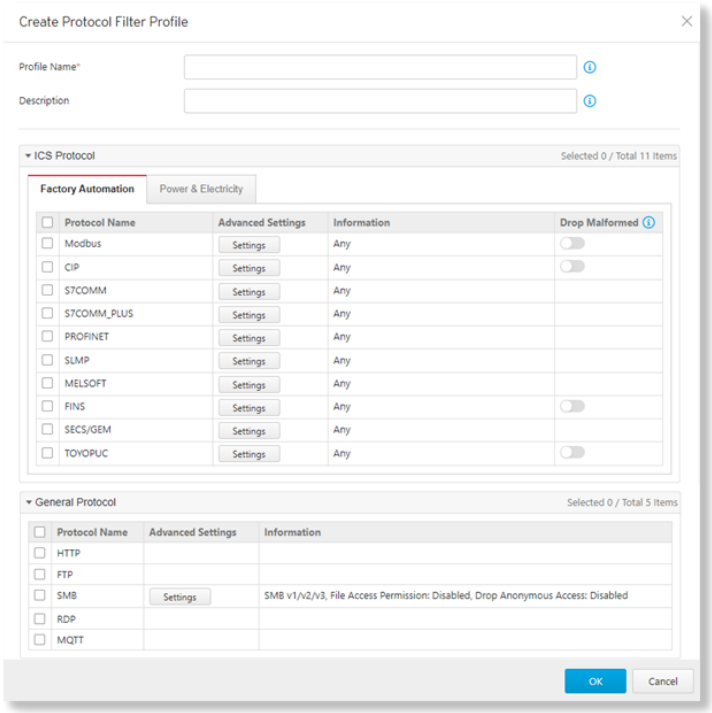
Advanced Settings for TOYOPUC

The device features more detailed configurations for the TOYOPUC ICS protocol. Through the [TOYOPUC 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.



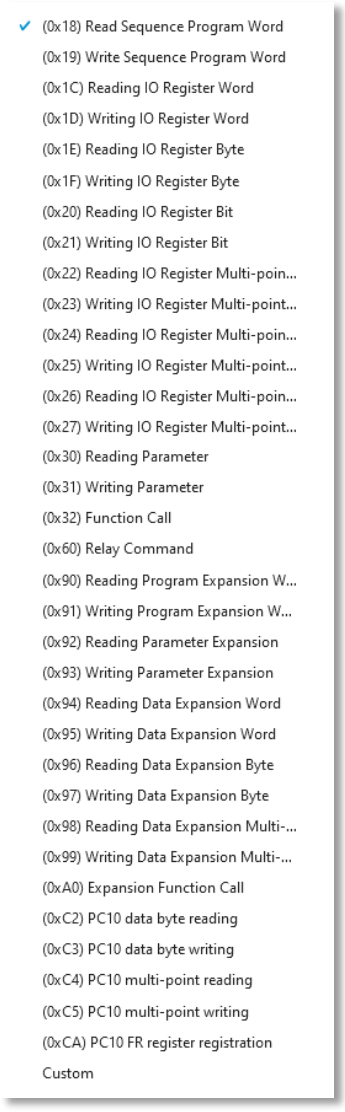
Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles]. (Restart at 1)
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.
   m. Click [Settings] next to a protocol, and select one of the following:
      - **Any** - Specify all available commands or function access for 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 commands relevant to administration configuration 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.



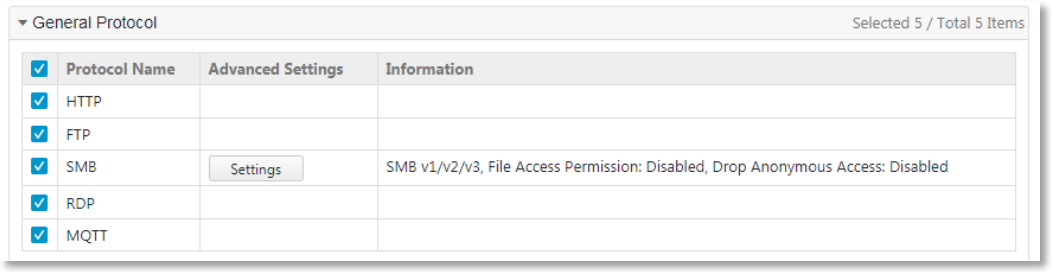
- If you want to specify one sub-command code or multiple sub-command codes, then select [Preset Sub-Cmd Code] and move the sub-function code(s) from the [Available Sub-Cmd Code] field to the [Selected Sub-Cmd Code] field.
- If you want to specify a sub-command code yourself, then select [Custom Sub-Cmd Code] and input a sub-command code in the [Custom Sub-Cmd Code] field.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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.

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

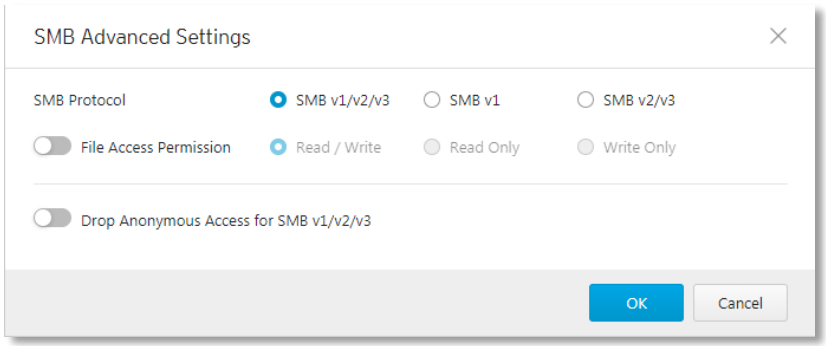
Advanced Settings for SMB

The device features more detailed configurations for the SMB protocol. Through the [SMB Advanced Settings] pane, you can specify the settings in more detail.



Procedure

1. Go to [Object Profiles] > [Protocol Filter Profiles].
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.
6. Click SMB [Settings] and select one of the following:

- **SMB Protocol** - Specify SMB the protocol version combination – options include SMBv1/v2/v3, SMBv1 and SMB v2/v3.
- **File Access** – Select access permission behavior:
  - **Read / Write**: Read and write file access
  - **Read Only**: File access for reading only
  - **Write Only**: File access for writing only

7. **Drop Anonymous Access for SMB v1/v2/v3**: Drop access over SMB v1/v2/v3 for Anonymous accounts.

Configuring IPS Profile

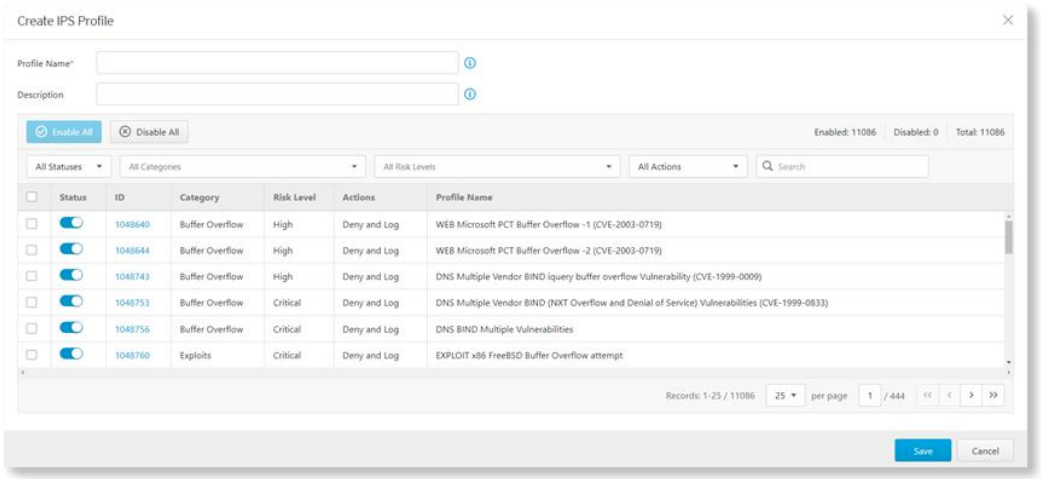
An IPS profile contains more sophisticated pattern rules that allow you to have granular control which can be applied to policy rules.

The following can be configured in an IPS profile:

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

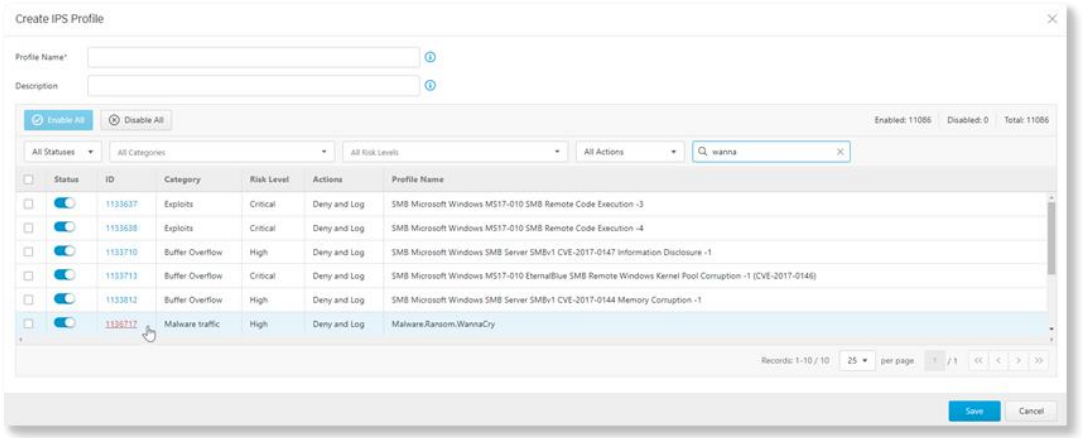
- Details of IPS protocol risk level category, including:
  - Information
  - Low
  - Medium
  - High
  - Critical

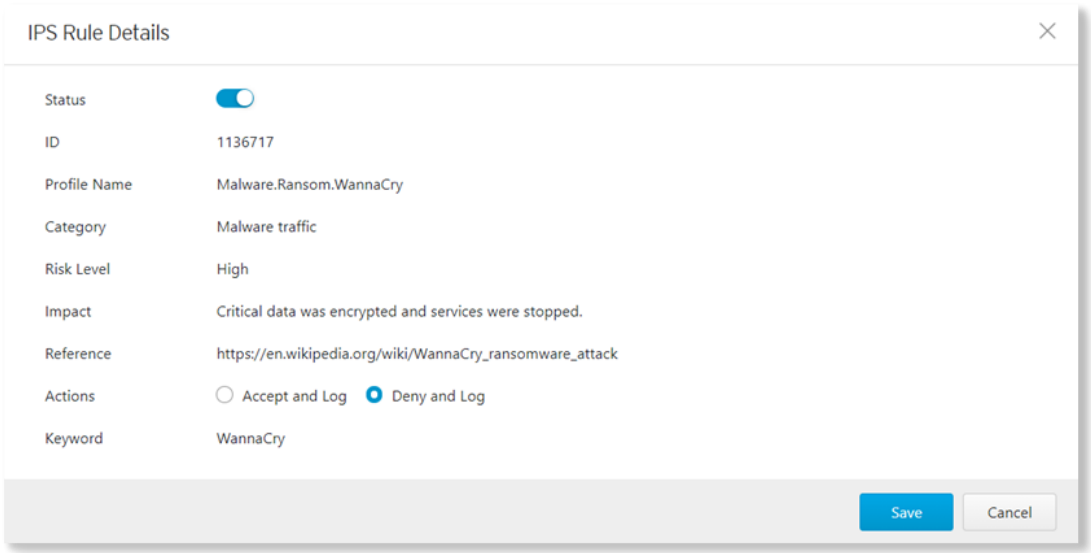
- Details of default action list for IPS patterns, including:
  - Accept and Log
  - Deny and Log



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.

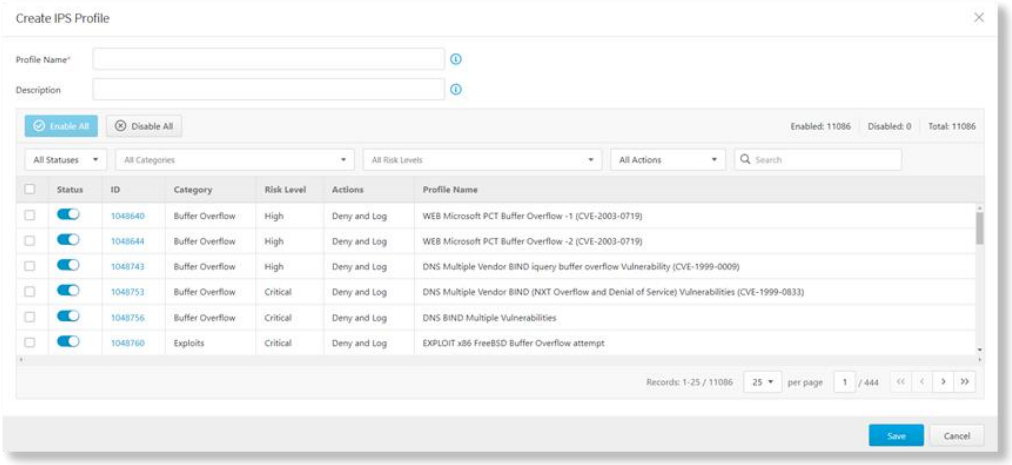




Procedure

1. Go to [Object Profiles] > [IPS Profiles].
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 Pro, the attack will be bypassed and logged for monitoring.
     - **Deny and Log**: When the attack is detected by EdgeIPS Pro, the attack will be dropped and logged for monitoring.

Field	Description
Status	The operational status of the pattern rule
ID	The pattern rule ID
Profile 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
Impact	The damage that will be caused to the target network device if the cyber attack succeeds.
Reference	The vulnerability ID of the cyber attack (e.g. CVE-2017-0147)
Actions	The preset actions for the cyber attack
keyword	The word(s) for searching the pattern rules

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

Configuring File Filter Profiles

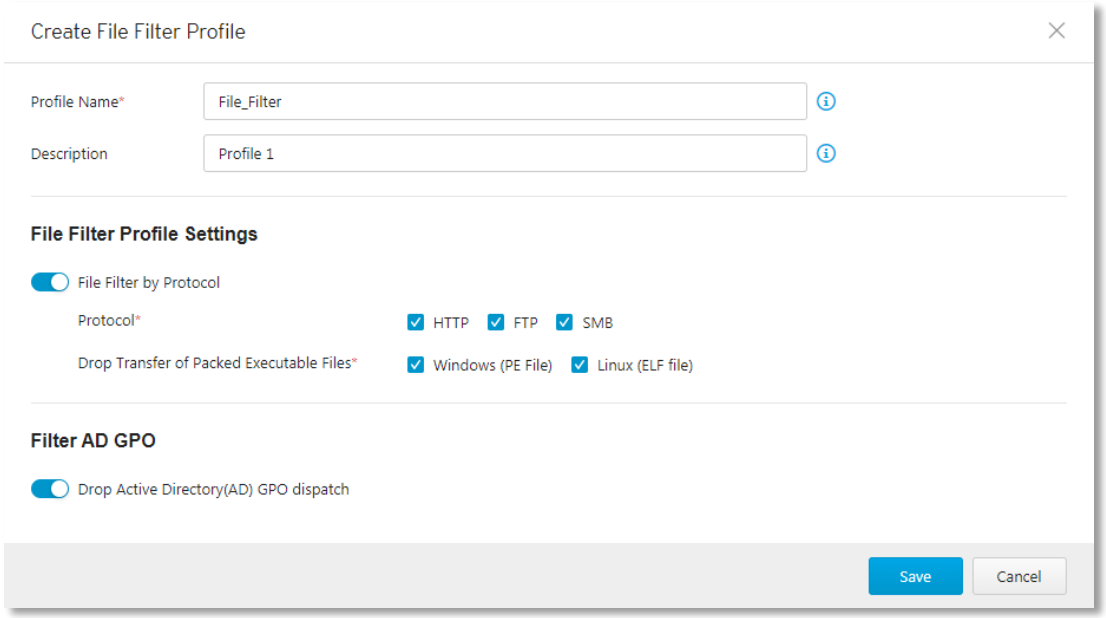
The File Filter Profile contains detailed access protocols, executable file type and Active Directory (AD) GPO dispatch settings, allowing you to create or edit profiles to apply on a policy rule.

In a profile, you can define the following:

- File Filter by Protocol
  Including: HTTP, FTP and SMB
- Drop Transfer of Packed Executable Files
  Includes: Windows (PE files) and Linux (ELF file)
- Filter AD GPO
  Enable or disable Drop Active Directory (AD) GPO

Procedure

1. Go to [File Filter Profiles] > [File Filter 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 File Filter Profile Name field.
4. Type a description.
5. Under the [File Filter Profile Settings] enable file filter by protocol
   - File Filter by Protocol, including: HTTP、FTP and SMB.
   - Drop Transfer of Packed Executable Files, including: Windows (PE files) and Linux (ELF files)
6. If you want to filter AD GPOs, you can enable "Drop Active Directory (AD) GPO dispatch"
7. Click [Save] to save profile.

The Security Tab

This chapter describes policy enforcement and port security that can be used by EdgeIPS Pro.

You can configure the following function of security for EdgeIPS Pro

- **Policy Enforcement**: Policy Enforcement allows user to define detail rule access behavior and matching rule by rule set template.
- **Port Security**: Contains the port security configuration by module slot, user can edit each pair or port configuration and apply policy enforcement rule set template, configure anomaly and bypass configuration.

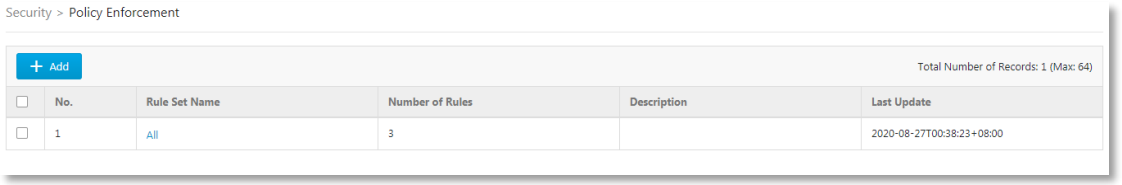
Policy Enforcement

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

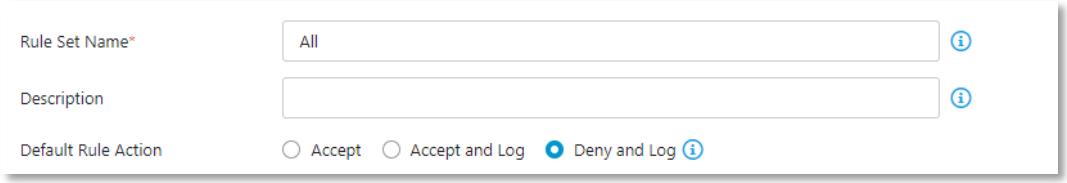
Configuring Policy Enforcement

Procedure

1. Go to [Security] > [Policy Enforcement].
2. At the [Policy Enforcement] tab you will see the [Policy Enforcement rule set] pane.



3. Click "Add" button to create Policy Enforcement Rule set.
4. Create rule set name and description if necessary.
5. At the [Policy Enforcement Default Rule Action] pane, select a default action [Accept] ,[Accept and Log] or [Deny and Log] for when no pattern is matched.



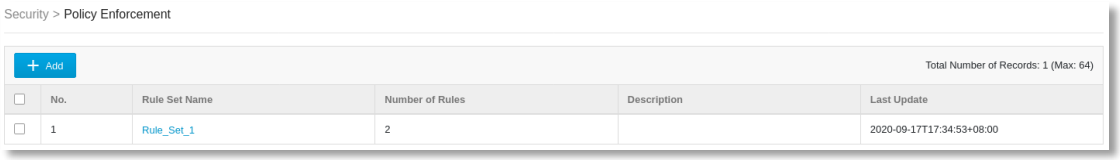
Adding Policy Enforcement Rules

Procedure

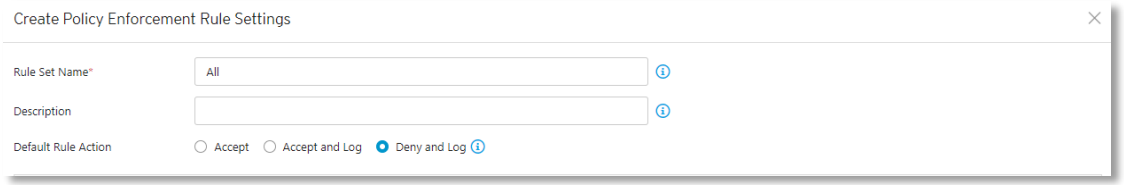
1. Configure the required object or objects.
   - IP object profiles
     For more information, see *Configuring IP Object Profile on page 22*.
   - Service object profiles
     For more information, see *Configuring Service Object Profile on page 23*.

- Protocol filter profiles
  For more information, see *Configuring Protocol Filter Profile on page 24*.

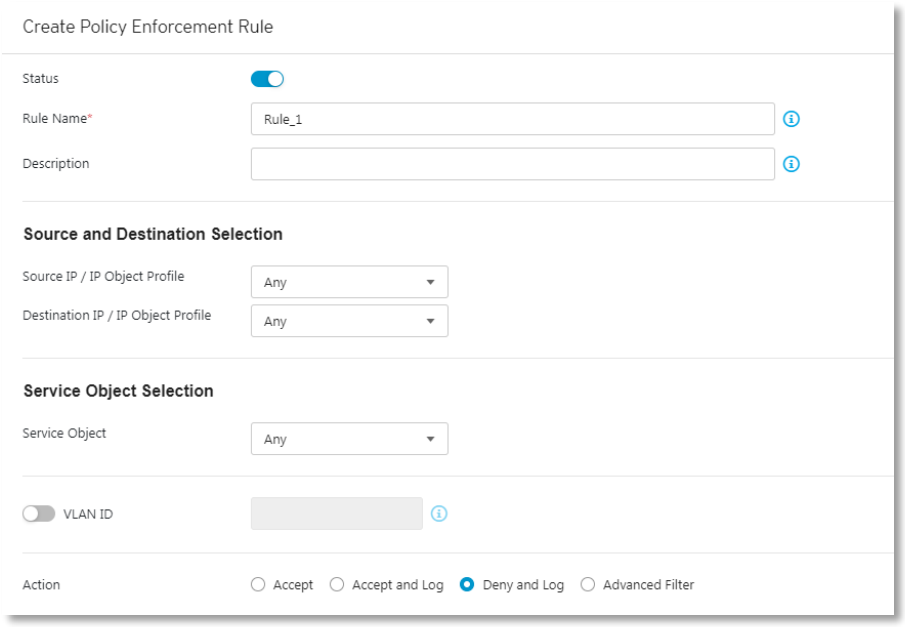
2. Go to [Security] > [Policy Enforcement]
3. Under the [Policy Enforcement] tab you will see the following panes.



4. Click the rule set name to which you want to add policy rules. For example: Rule_Set_1.



5. Click the [Add] button to add a new policy rule.
6. Use the toggle to enable or disable the policy rule.



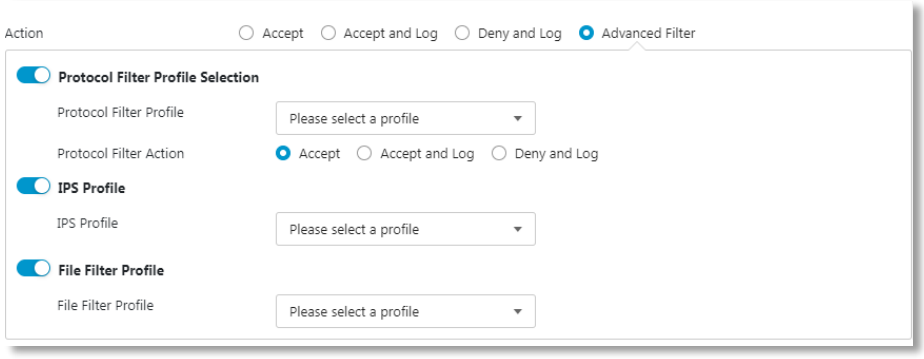
7. Input a descriptive [Rule Name].
8. Input a descriptive [Description] for the rule.
9. At the [Source IP / IP Object Profile] drop-down menu, select either one of the following for the source IP address(es):
   - Any
   - Single IP
   - IP Range
   - IP Subnet
   - IP Object

Note: If you select [Object], then you need to select the IP object from an IP object profiles that have been created beforehand.

10. 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
    - IP Object
11. 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
12. VLAN ID

You need to select the service object from service object profiles that have been created beforehand.

13. 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 with log output
    c. Deny and Log: Select this option to block network traffic that matches this rule with log output
    d. Advanced Filter: The node will take further actions based on the protocol filter, IPS or file filter profiles:
       - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
       - Under the [Protocol Filter Action], 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.
- Under the [File Filter Profile] drop-down menu, select a file filter profile you have defined beforehand.

14. Click [OK] to save the configuration.

Managing Policy Enforcement Rules

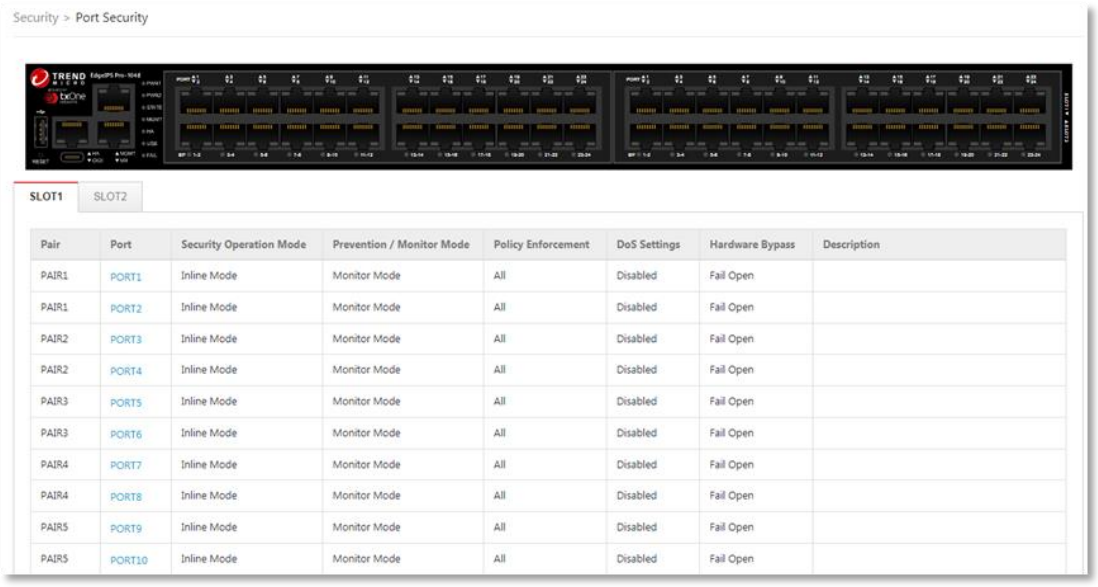
The following table lists the common tasks that are used to manage policy enforcement rules.

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 Enforcement 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.

When more than one policy enforcement rule is matched, EdgeIPS Pro 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.

Port Security Settings

This feature allows the network user to configure security settings for each port interface. When port security is configured for each interface, related actions will be performed, applying the security profile and settings.



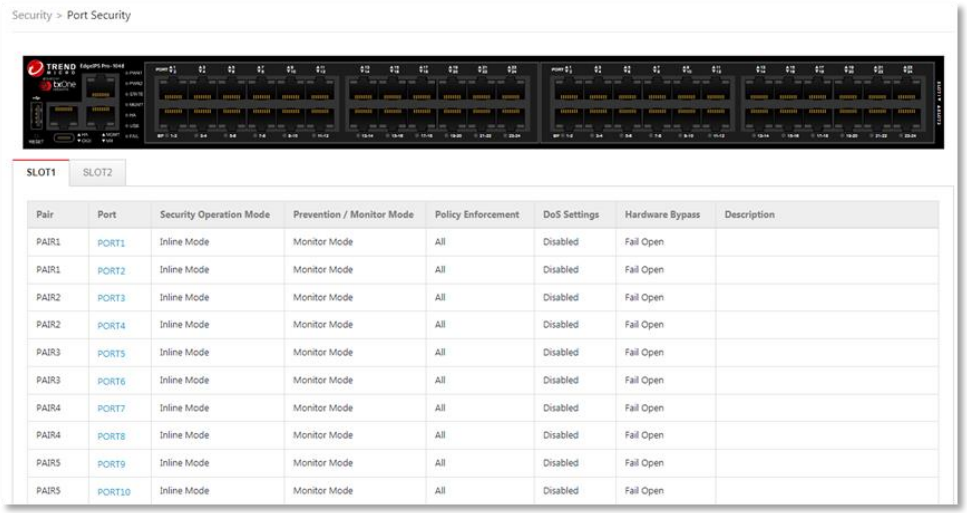
The following table describes the tasks you can perform when you configure a list of port security settings:

Settings	Description
Port name	Port name information
Description	Add a description for configuring the port
Security Operation Mode	Security operation mode includes Inline Mode and Offline mode
Prevention / Monitor Mode	Monitor mode: Detect and monitor abnormal protocol accesses to the OT assets, without blocking network attacks.
	Prevention mode: Block abnormal protocol access to OT assets and generate logs.
Hardware Bypass	Configure hardware bypass operation mode
Policy Enforcement	Apply selected policy enforcement rule set
Denial of Service Prevention Settings (DoS Settings)	Configure Denial of Service prevention settings

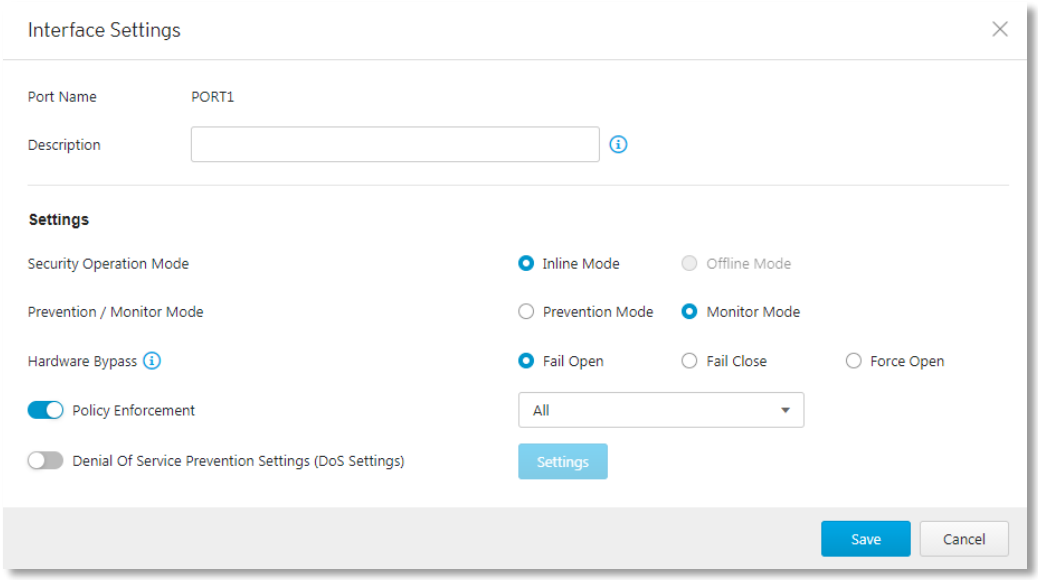
Configuring Port Security

Procedure

1. Go to [Security] > [Port Security].
2. At the [Port Security] tab you will see the following screen.
3. Port security page will be according to EdgeIPS Pro's installed I/O module card and will show the connection status on the page tab.



4. Click the specific [Port] to configure port security.



5. Input a descriptive [Description] for the port security setting.

6. Select the operation mode and configure the operation mode for the port of device

Task	Action
Inline Mode	Choose [Inline Mode] to have EdgeIPS Pro operate in Inline Mode. The pane can be connected from Port 1 or Port 2 at the same time.
Offline Mode *	Choose [Offline Mode] to have EdgeIPS Pro operate in Offline Mode.

7. At the [Prevention and Monitoring] setting you can configure prevention or monitor mode for port security.

Security Operation mode	**Prevention / Monitor**	**Action Performed**
Inline Mode	Monitor Mode	▪ Detect and monitor abnormal protocol access attempts 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	▪ Not supported.*

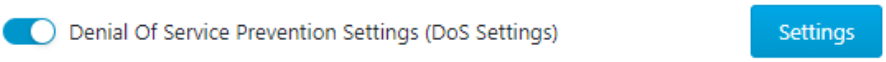
* The offline mode will be available in the future – this function will be greyed out in firmware version 1.1

8. Configure [Hardware bypass] mode as 'Fail Open', 'Fail Close', or 'Force Open'. The following table lists hardware bypass mode definitions.

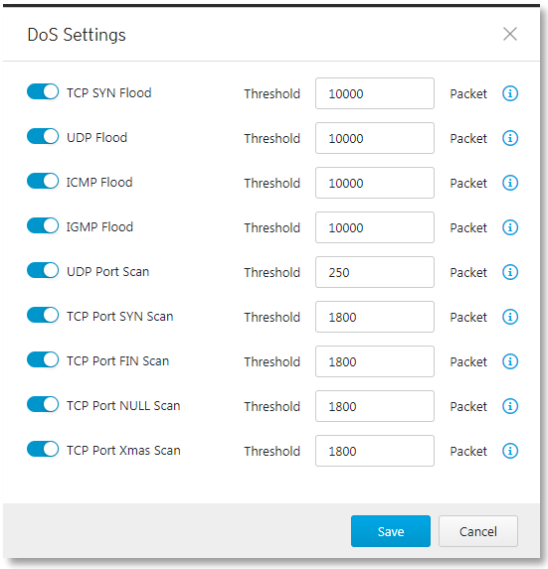
Settings	Description
Hardware Bypass	Bypass ports allow uninterrupted network traffic even if a single in-line appliance is shut down or hangs. The settings for hardware bypass mode are: ■ Fail Open: Allows all network traffic to pass through the appliance when system fail. ■ Fail Close: Closes the links for the interface pair and prevents any network traffic from passing through the appliance. ■ Force Open: Always Bypass all network traffic to pass through the appliance.

9. Use the toggle to enable policy enforcement and apply a created policy enforcement rule set

10. Use the toggle to enable [Denial of Service Prevention]



11. Click the [Settings] tab you will see the [DoS Prevention] pane.



12. You can optionally configure the thresholds of the denial of service rules.

Flood/Scan Attack Protection rules utilize a 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. 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.

13. Click [Save] to complete specific port security settings.

The Pattern Tab

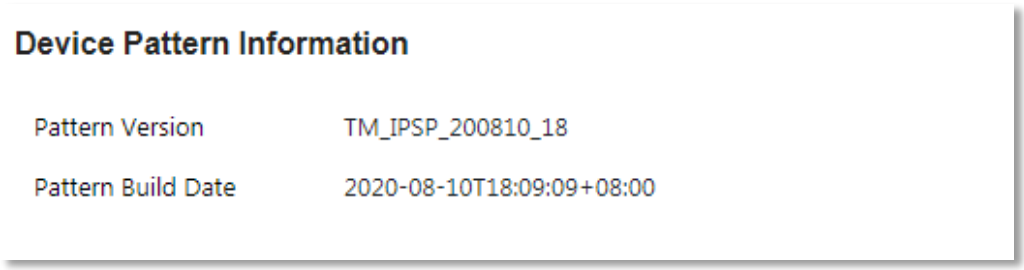
This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the EdgeIPS Pro device.

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

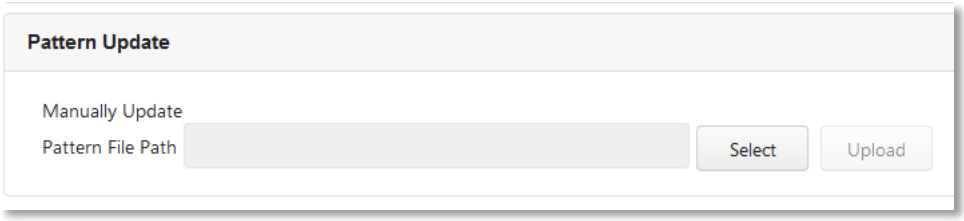
1. Go to [Pattern] > [Pattern Update].
2. At the [Pattern Update] tab you will see the following pane.
3. The [Device Pattern Information] pane shows the current [Pattern Version] and [Pattern Build Date].



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 patterns can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

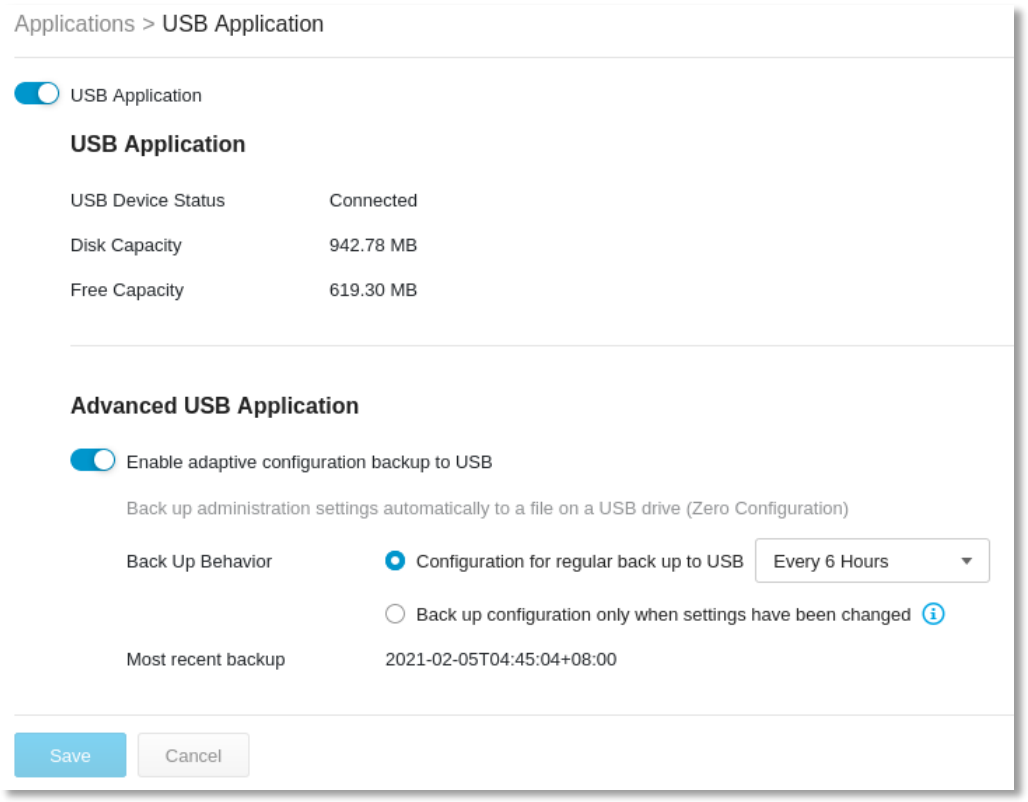
The Application Tab

This chapter describes how to use the USB application and packet capture functions.

USB Application

Procedure

1. Go to [Application] > [USB Application].
2. At the [USB Application] tab you will see the following pane.



3. Click [Enable] to enable USB Application usage. This toggle switch controls whether the USB port is enabled or not.
4. Once enabled and if a USB disk is plugged in, you can see the status and review information about the the disk capacity and remaining free space.

If USB Application is disabled, the USB port on the front panel will not connect to plugged in USB devices.

With regard to supported USB devices, please refer to "Supported USB Devices ".

Advanced USB Application

1. Click [Enable] to enable adaptive configuration backing up to a USB-based device.
2. Back up behavior can be configured as follows:

- a. Periodic backup of a configuration to USB – 6 different time periods are supported.
- b. Backup configuration to USB disk when configurations are changed.

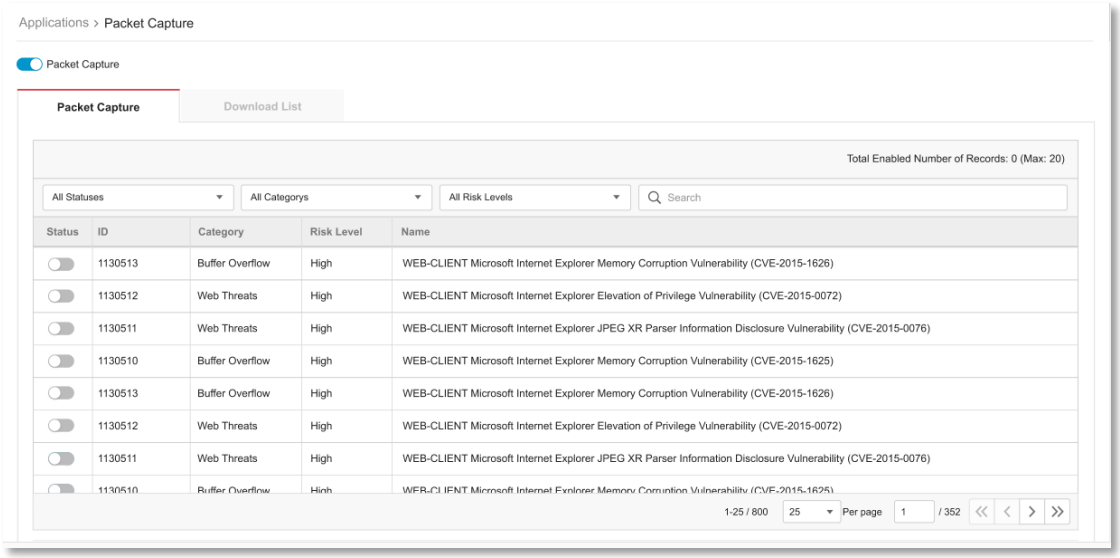
Packet Capture

The Packet capture feature allows you capture packets for further analysis. This feature allows the user to configure the capture of packets by IPS event rules. The packets that trigger the IPS events can then be further analyzed and can help support teams to quickly address false positive/false negative matching of IPS rules in the security module.

Enabling Packet Capture

Procedure

1. Go to [Application] > [Packet Capture].
2. Click [Enable] to enable IPS packet capture.



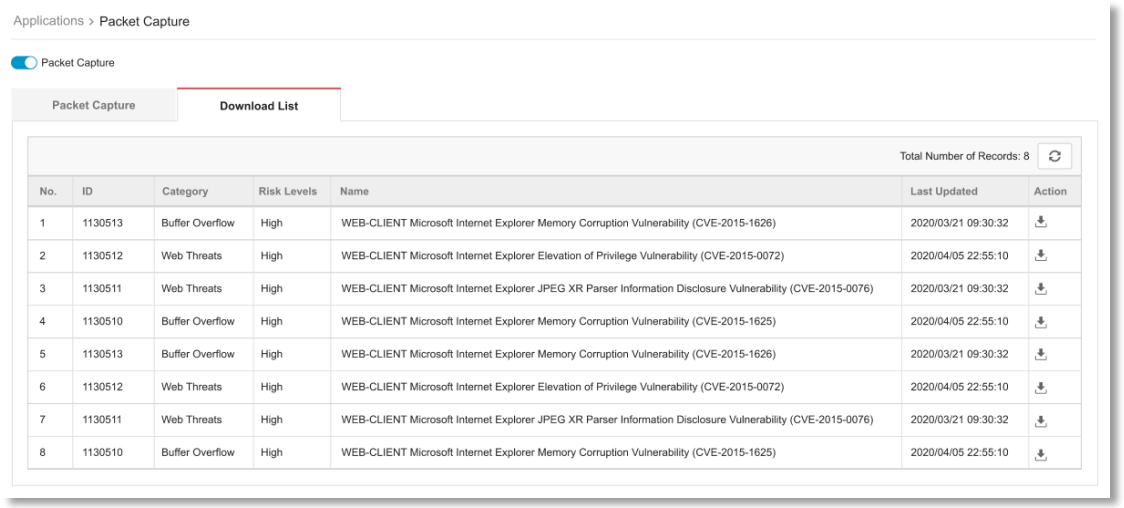
3. You can see the entire IPS rule list and select a rule to "Enable" for IPS rule capture.
4. Up to 20 rules can be selected for IPS Rule packet capture support.

Note: The packet capture feature will save selected IPS Rule event packets once the IPS rule is hit and will only save the last 10 occurrences of a particular rule. Older events will be overwritten.

Download Captured Packet

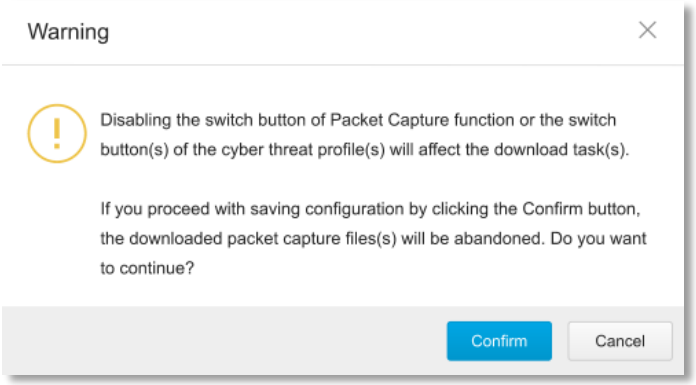
Procedure

1. Go to [Application] > [Packet Capture]
2. Click [Download List] to show a list of IPS rules where you can download a zip archive of each rule's related pcap files.



No.	ID	Category	Risk Levels	Name	Last Updated	Action
1	1130513	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)	2020/03/21 09:30:32	
2	1130512	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)	2020/04/05 22:55:10	
3	1130511	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)	2020/03/21 09:30:32	
4	1130510	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)	2020/04/05 22:55:10	
5	1130513	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)	2020/03/21 09:30:32	
6	1130512	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)	2020/04/05 22:55:10	
7	1130511	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)	2020/03/21 09:30:32	
8	1130510	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)	2020/04/05 22:55:10	

3. You can click the download icon to download the zipped archive to your disk.
4. Disabling packet capture will cause previously downloaded packet captures to be deleted. To confirm disabling of the feature, the above warning will be shown to the user.



Note. The download list will be refreshed every 10 seconds, if you want to get the latest update, please click the "manual" refresh button.

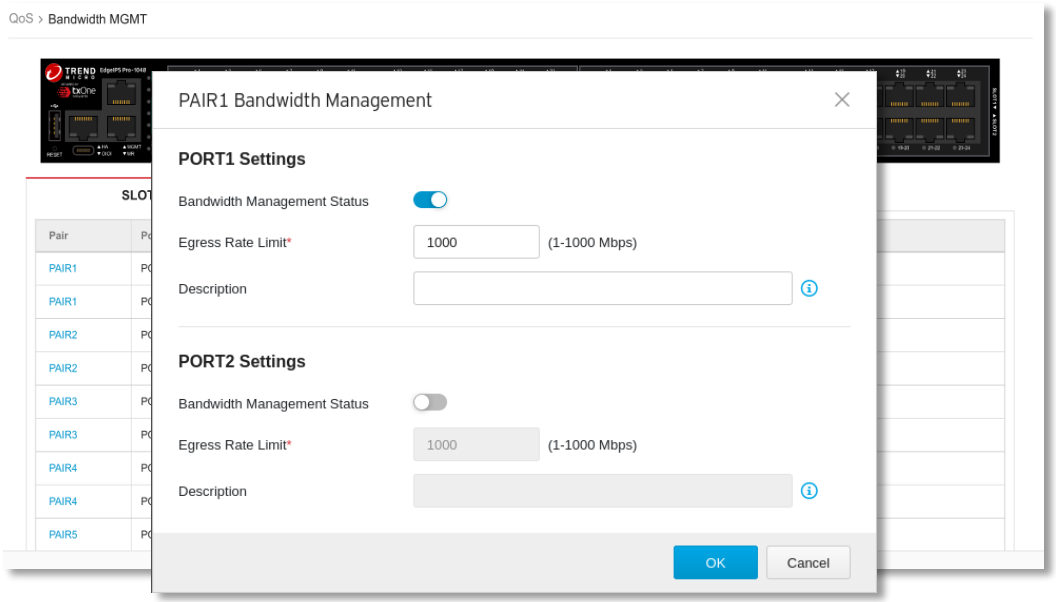
The QoS Tab

The QoS (Quality of Service) guarantee technology in Edge series products allows the network administrator to manage, monitor and allocate bandwidth for the production-critical network traffic of each pair's egress port in real-time.

Configuring Bandwidth MGMT

Procedure

1. Go to [QoS] > [Bandwidth MGMT].



2. Select a [PAIR] to manage a port's bandwidth settings.
3. Enable [Bandwidth Management Status] on the selected [Port] to configure Egress Rate Limit settings.
4. Click [OK] to complete bandwidth management.

Note: Each port's of bandwidth MGMT is configurable. The default setting will be 1000Mbps, however the user can vary this as necessary to set an upper limit on bandwidth.

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**
- **File Filter Logs**
- **Assets Detection Logs**
- **System Logs**
- **Audit Logs**

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] > [Cybersecurity 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 set and the matched policy 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 packet.
Attacker	The IP address of the host device which initiated the cyber attack.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
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 packet.
Destination IP Address	The destination IP address of the packet.
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 packet.
Ethernet Type	The ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
Action	The action performed based on the policy 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 policy rules.

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 set and the matched policy rule that was used to generate the log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
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 packet.
Destination IP Address	The destination IP address of the packet.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
IP Protocol Name	The IP protocol name of the packet.
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. The protocol filter is an advanced configuration setting 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 set and the matched policy 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 packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Port	The source port, if protocol is TCP/UDP. The ICMP type, if protocol is ICMP.

Field	Description
Destination MAC address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Ethernet Type	The Ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
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 File Filter Logs

'File Filter logs' refers to logs detected by the [File Filter] feature. The file filter is an advanced configuration setting that can be configured under [Policy Enforcement] settings.

Procedure

1. Go to [Logs] > [File 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 set and the matched policy rule that was used to generate the log.
Profile Name	The name of the file filter profile that was used to generate the log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Port	The source port, if the protocol is TCP/UDP.
Destination MAC address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Port	The destination port, if protocol is TCP/UDP.
VLAN ID	The VLAN ID of the packet.
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.
Extra Information	Extra information provided with the file filter log.
Action	The action performed based on the policy settings.

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.
Interface	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.

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

The Administration Tab

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

Account Management

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 68*.
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
Network	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
Application	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
QoS	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Logs – not including Audit Logs	View	Yes	Yes	Yes	No

Audit Logs	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

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

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 67*.

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

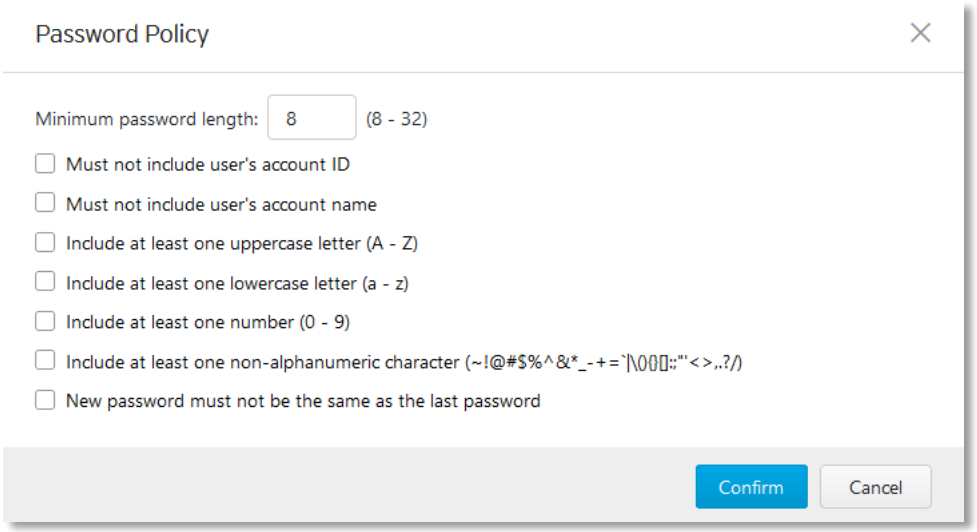
EdgeIPS Pro provides the following password policy settings to enhance web console access security:

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

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 Services

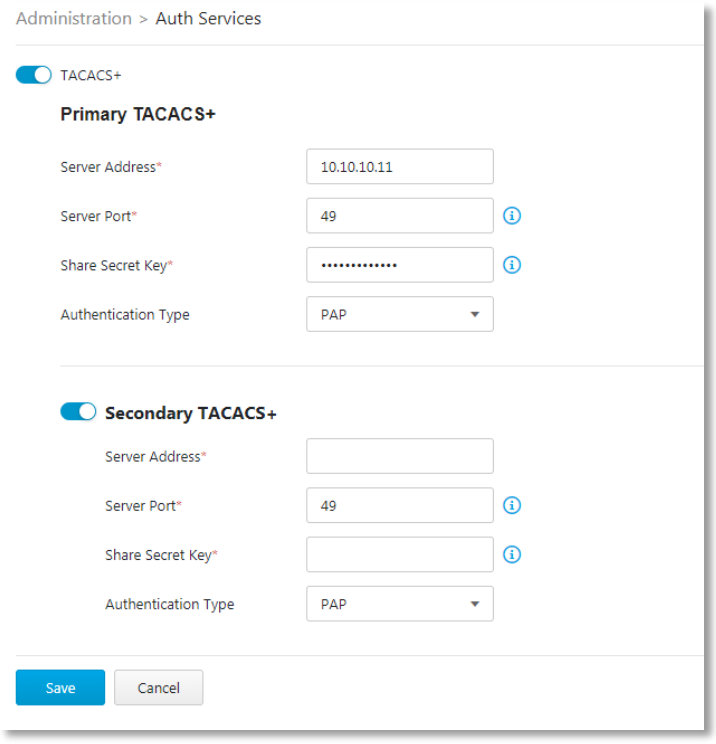
Use the [Auth Services] tab to do the following:

- Configure the TACACS+ of the device.

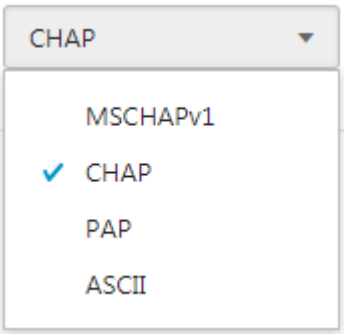
Configuring TACACS+

Procedure

1. Go to [Administration] > [Auth Services].
2. In the [TACACS] pane, provide the Primary and Secondary TACACS+ Servers for the device.



3. Enable Primary TACACS+ and configure the settings
   a. Configure Server address.
   b. Configure Server Port (Default port: 49)
   c. Configure Share Secret Key (Maximum length 64 characters)
   d. Select authentication type, options included as follows:



   e. Enable Secondary TACACS+ Server if necessary

System Management

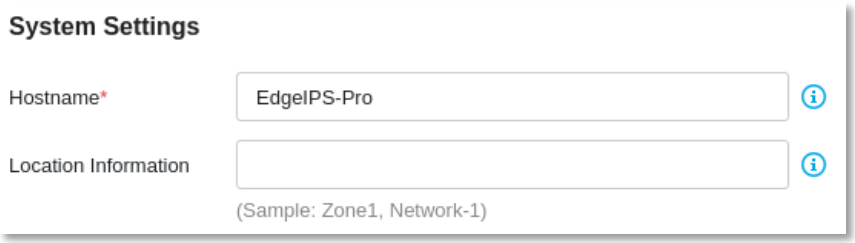
Use the [System Management] tab to do the following:

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

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 Management Method and Access Control List

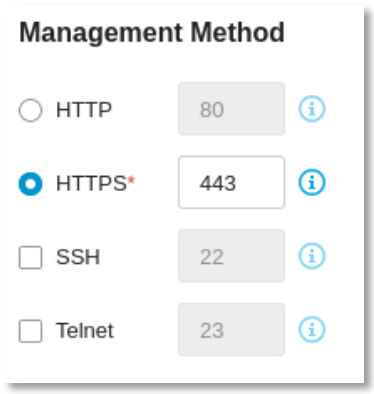
Configuring Management Protocols and Ports

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.

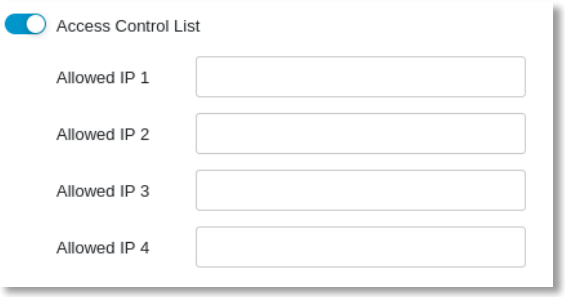


The HTTP and HTTPS protocols are used for connecting to the web management console. The SSH and Telnet protocols are used for connecting to the CLI commands.

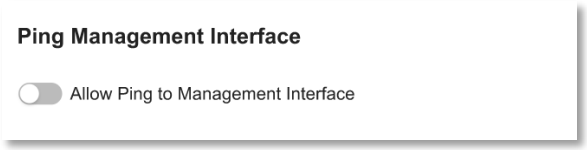
Configuring Control List Access from Management Clients

Procedure

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



4. Check if pings to the Management Interface are allowed.



The Sync Setting Tab

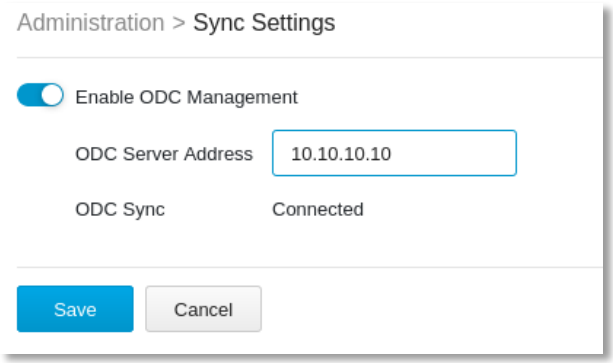
EdgeIPS Pro can be managed by a TXOne ODC (Operational Technology Defense Console). Use this tab to register the EdgeIPS Pro to a TXOne ODC.

Enabling Management by ODC

Procedure

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

2. In the pane:
   a. Use the toggle to enable management by ODC.
   b. Input the IP address of the ODC server.



The Syslog Tab

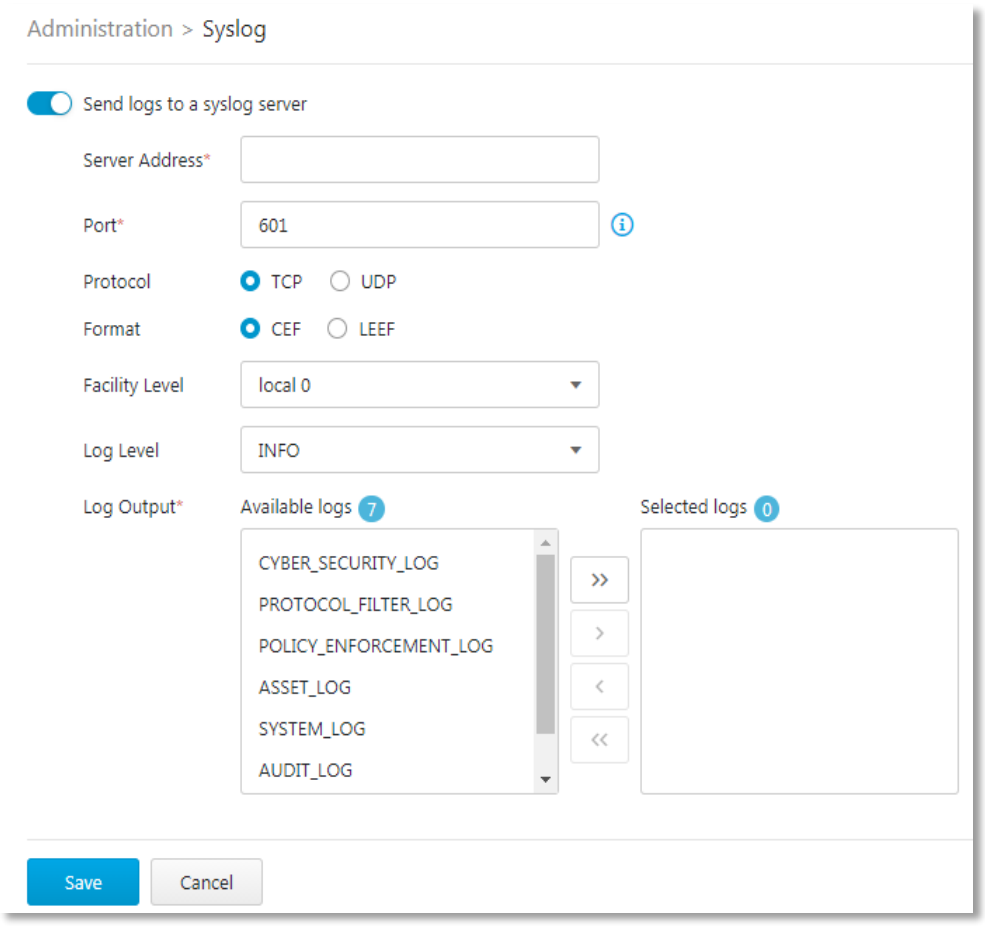
The EdgeIPS Pro system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) and Log Event Extended Format (LEEF) syslog messages are used in EdgeIPS Pro.

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. 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 75*.

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. 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/Cybersecurity and their equivalent Syslog severity levels.

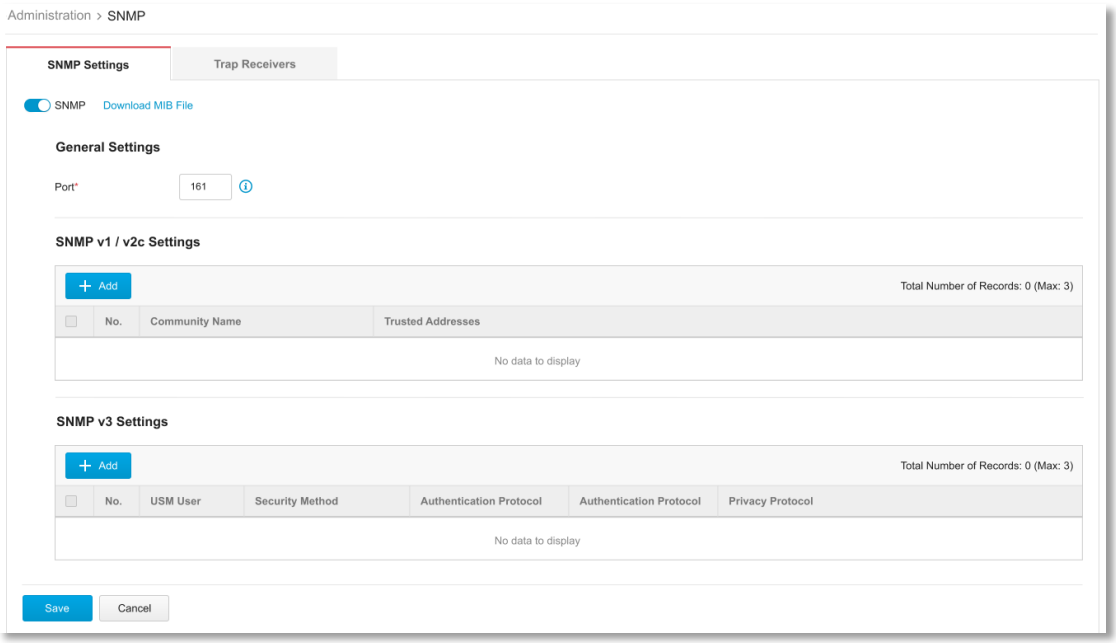
Policy Enforcement / Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
		0 - Emergency
	Critical	1 – Alert
	High	2 – Critical
		3 – Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

The SNMP Tab

The Simple Network Management Protocol is a protocol used for exchanging management information between Edge series devices. EdgeIPS Pro supports SNMP v1/v2c and more secure v3, as well as supports SNMP traps.

Procedure

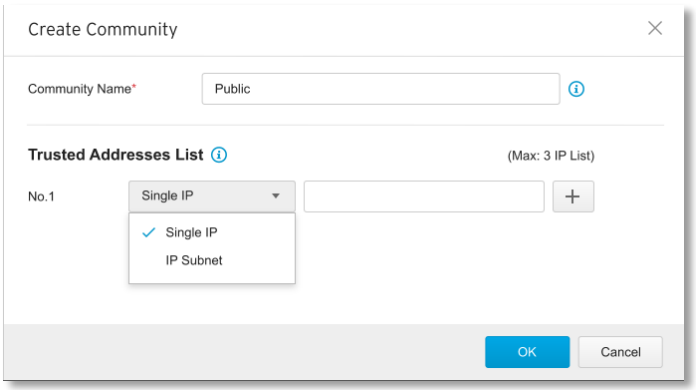
1. Go to [Administration] > [SNMP]
2. Click [Enable] to enable SNMP functionality.
3. Under General settings, you can change SNMP port. The default setting is Port 161.
4. You can click the "Download MIB file" link to download the EdgeIPS Pro's MIB file.



Configuring SNMP v1/v2c

Procedure

1. Go to [Administration] > [SNMP]
2. Click [Add] to create SNMP v1/v2c settings.

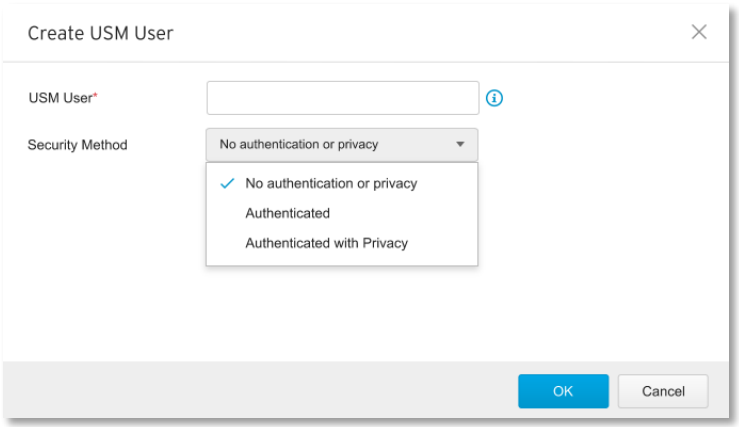


- a. Enter Community name
- b. Add a Trusted Address list. There are two supported types: Single IP and IP Subnet
- c. Click [OK] to create new SNMP v1/v2c community

Configuring SNMP v3

Procedure

1. Go to [Administration] > [SNMP]
2. Click [Add] to create SNMP v3 settings.

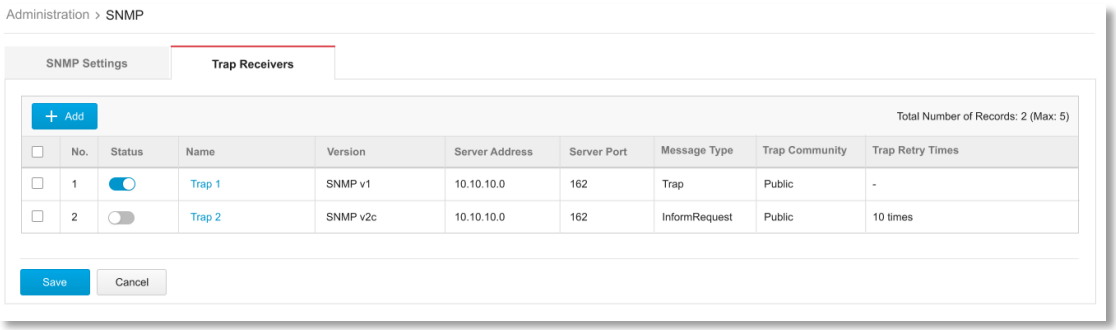


3. Enter USM user.
4. Under [Security Method], select from the following options:
   - a. No authentication or privacy.
   - b. Authenticated – this includes SHA and MD5. You can select the appropriate authentication protocol and enter an Authentication Key.
   - c. Authenticated with Privacy – this also includes SHA and MD5, and you can select appropriate authentication and privacy protocols.
5. Click [OK] to create an SNMPv3 USM User.

Configuring SNMP Trap Receivers

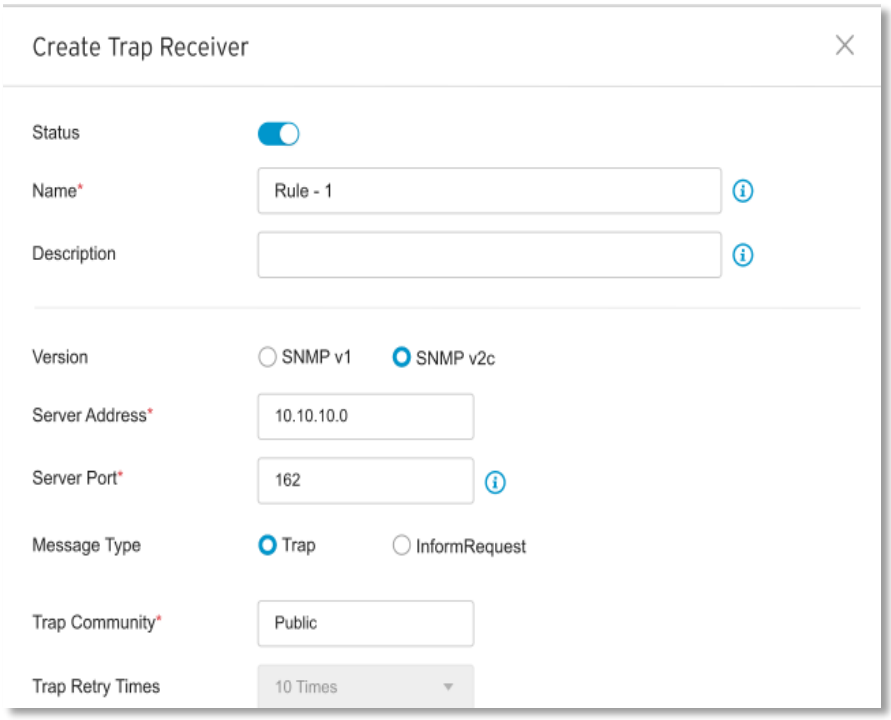
Procedure

1. Go to [Administration] > [SNMP]
2. Click the [Trap Receivers] tab.

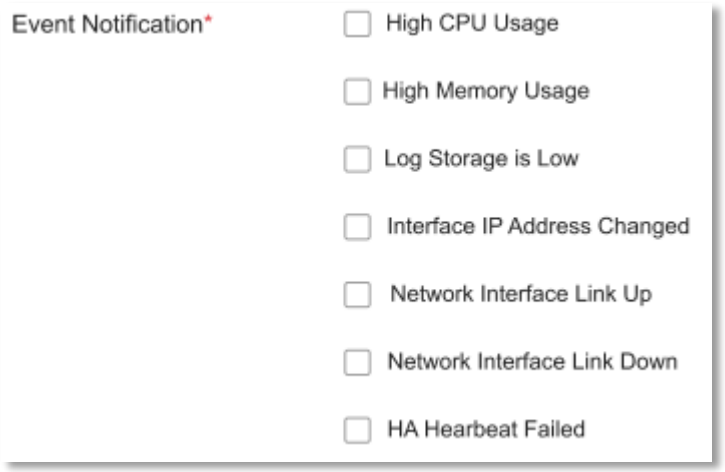


3. Click [Add] to create a new Trap Receiver.
   - a. Click the toggle under [Status] to enable a Trap Receiver.
   - b. Enter [Name] to create a Trap Receiver name.
   - c. Add [Description] if necessary.
   - d. Select SNMP version – options include SNMP v1 and SNMP v2c
   - e. Enter [Server Address]
   - f. Enter [Server Port], default setting port 162.

- g. Select message type, “Trap” and “informRequest”.
- h. Enter Trap Community, default name: PUBLIC.
- i. Trap Retry Times: The amount of retries ranges from 1-10 times



- K. Select what will trigger an Event Notification from the list as follows:



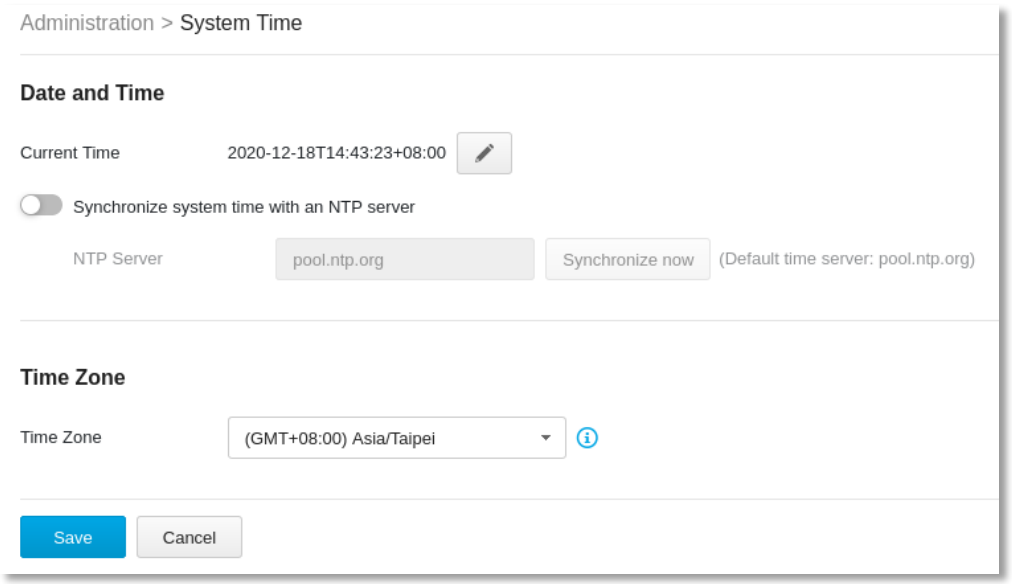
The System Time Tab

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.

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 Pro. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

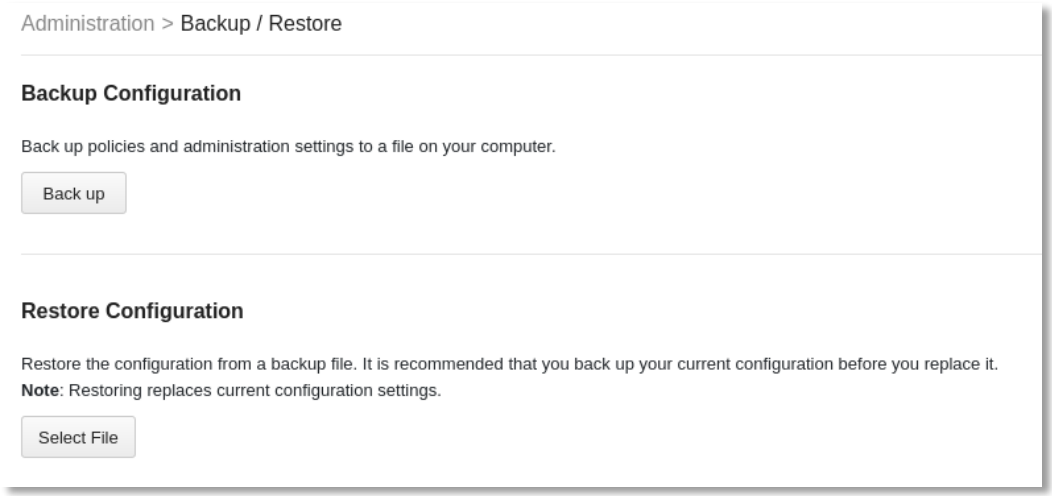
We recommend the following:

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

Backing Up a Configuration

Procedure

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



6. 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 Pro.

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:

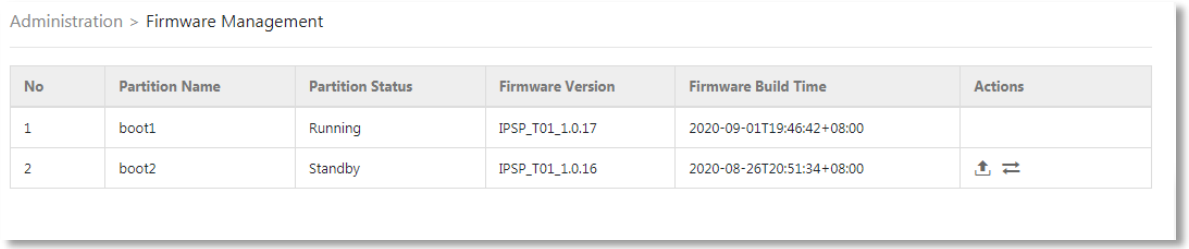
- View the firmware information for the device
- Upgrade the firmware of the device
- Boot into standby partition and firmware

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 Pro can have up to two firmware 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.

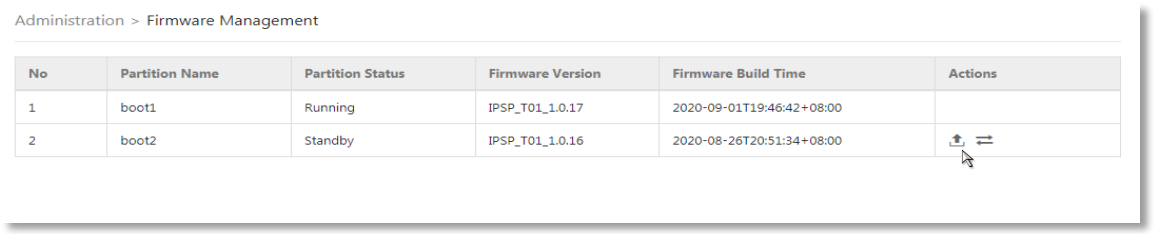


Updating Firmware

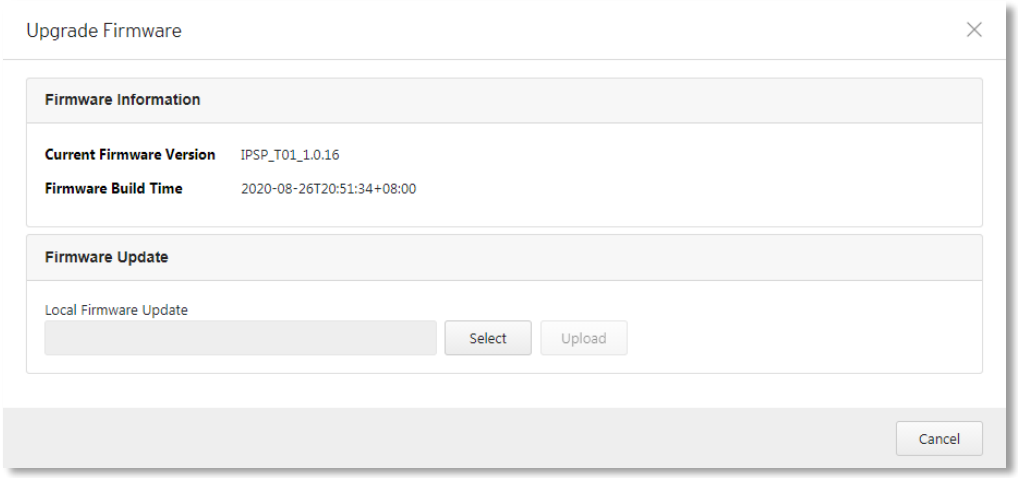
Procedure

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 partition on [Standby].



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

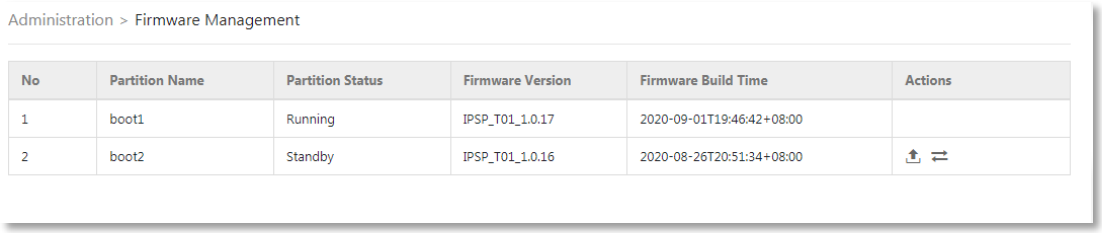
Various versions of the firmware can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

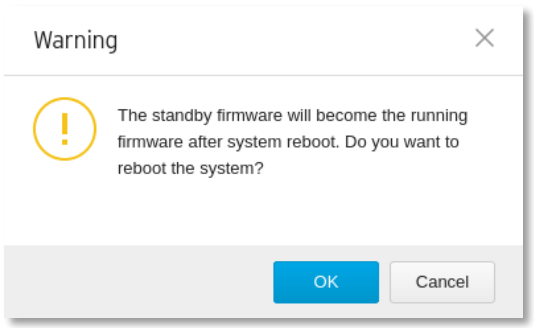
Rebooting and Applying Firmware

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 make it the [Running]

partition.

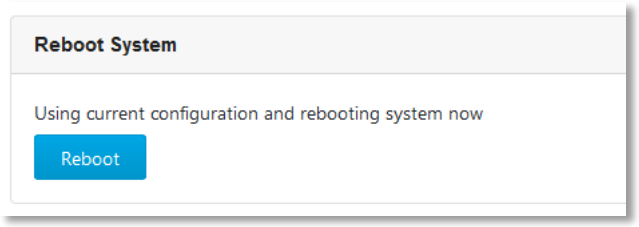
The Reboot System Tab

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 Pro™ for extended or support functionality.

To ensure optimal operation, only USB devices listed below are currently supported. This list may be updated from time to time. Please visit Trend Micro'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

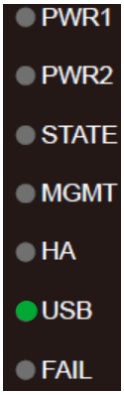
1. On-demand configuration for disk backup
2. Load pattern from disk
3. Load configuration from disk
4. Load firmware from disk

Given that this feature allows anyone with a supported USB disk device to perform various operations via the USB, the physical security of the EdgeIPS Pro 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" 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.



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

1. 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.
2. 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 LED	Green – Steady
Load/Restore Pattern	STATE	Green – Blinking (1/sec)
Load/Restore Configuration	MGMT	Green – Blinking (1/sec)
Load/Restore Firmware	STATE + MGMT	Green – Blinking (1/sec)

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

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.

5. 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 LED	Green – Blinking (Once every 0.5 sec)

6. 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
	FAIL LED	Red – Steady

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.

7. 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.
8. The USB disk device may be unplugged, after which LEDs will return to their state prior to the USB disk device being plugged in (USB LED off), and a log will be available in system logs.

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 FAIL LED will turn red.

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

Load Pattern from Disk

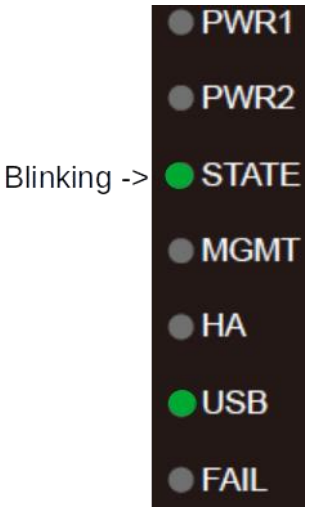
A DPI pattern file may be easily and quickly loaded from a USB disk device. This functionality allows for a floor operator to update the pattern file on the physical floor of the ICS environment without the need of a client computer to log into the device.

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".**

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 "STATE" 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 FAIL LED will turn red.
7. The system logs will also reflect whether the action was successful or not.

Load Configuration from disk

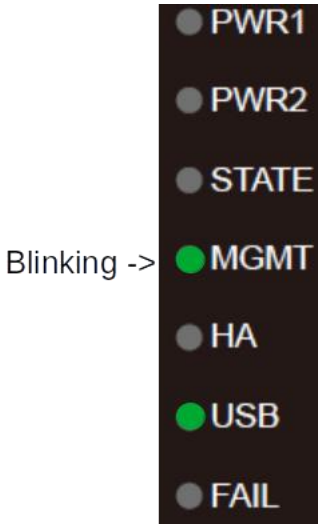
A configuration file may be easily and quickly loaded via a USB disk device. This functionality allows for a floor operator to update/restore the configuration on the physical floor of the ICS environment without the need of a client computer to log into the device.

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

Saving config files under other paths or incorrect folder names will cause the file to not be detected during the config 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 two short presses to toggle to "Load Config" action state.
4. When in the "Load Config" action state, the "MGMT" 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 FAIL LED will turn red.
7. The system logs will also reflect whether the action was successful or not.

Load Firmware from disk

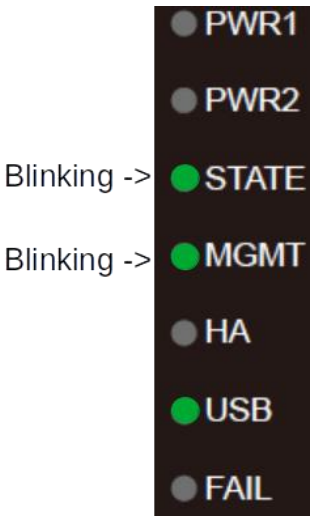
Device firmware may be easily and quickly upgraded via a USB disk device. This functionality allows for a floor operator to upgrade/change the firmware of a device on the physical floor of the ICS environment without the need of a client computer to log into the device.

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

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.

2. Plug in the USB disk. Enter the "Default Action" state.
3. In the default action state, give the reset button thre short presses to toggle to the "Load Firmware" action state.
4. When in "Load Firmware" action state, the "MGMT" and "STATE" LEDs will change to blinking green.



5. The "Load Firmware" 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 FAIL LED will turn red.
7. The system logs will also reflect whether the action was successful or not.

Various versions of the pattern/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