EdgeIPS™

Administrator's Guide

2021-09-10

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

1 About EdgeIPS™

1.1 Introduction of EdgeIPS™

EdgeIPS™ is a palm-sized platform that is equipped with dual Ethernet LAN ports. Users can access its web-based management console that provides a graphical user interface for device configuration and security policy settings. The whole management process is designed to comply with the manufacturing SOPs of the industry. The EdgeIPS™ protects your individual assets with OT visibility, cybersecurity, and OT protocol allow-listing/deny-listing.

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

TXOne 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:

- Threat detection and interception, with safeguards against the spread of worms
- Protection against Advanced Persistent Threats (APTs) and Denial of Service (DoS) attacks that target vulnerable legacy devices
- Virtual patch protection against OT device exploits

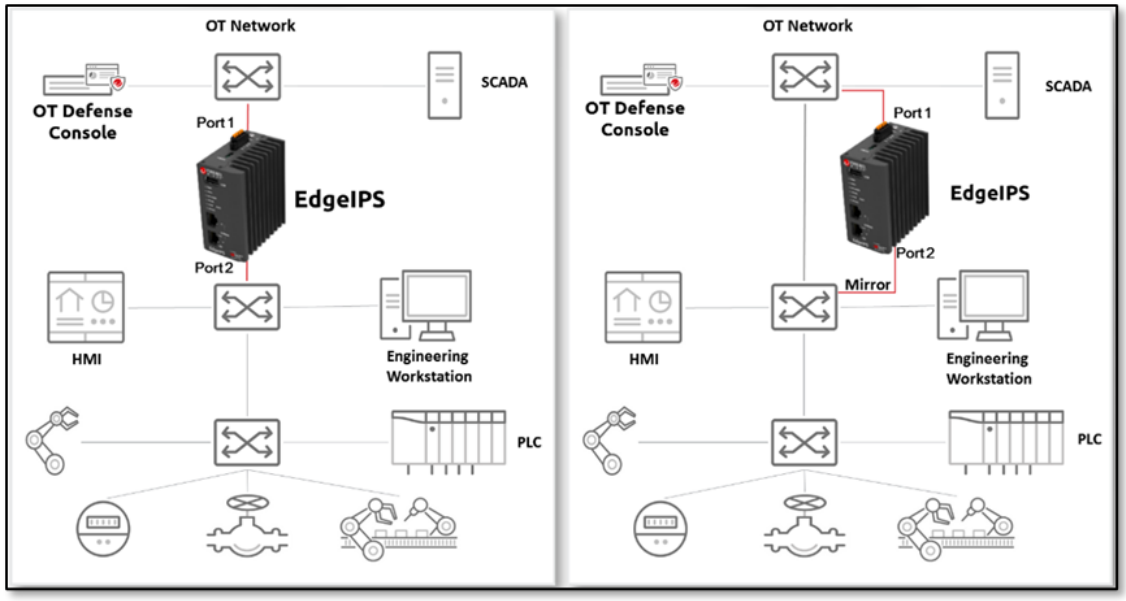


Figure 1 TXOne Security Solutions for an OT Network

1.2 Main Functions of EdgeIPS™

EdgeIPS™ is a transparent network security appliance. The main functions of this device are as follows:

Multi-Segmenting with Integrated Security

The device is designed for using 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, this Edge device fits right into your network without disrupting operations.

Policy Enforcement for Mission-Critical Machines

The device's core technology TXODI (One-pass Deep Packet Inspection for Industrial) allows administrators to maintain a Policy Enforcement database. By analyzing Layer 2 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 activities that match defined policy rules.

Intelligence Learning and Rule Generation for Daily Network Traffic

The device's machine learning technology, ICS Foresight Strike, allows administrators to generate a learning task that will analyze the network traffic of daily operations and generate baseline policy rules as a trust list. During the learning process, it creates a rule list for rapid deployment and filters potential cyber threats. This feature can help OT and IT security system administrators to silently deploy security solutions without affecting daily operations and efficiently generate policy rules with minimal manpower.

Improve Shadow OT Visibility by Integrating IT and OT Networks

The device 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

The device provides a powerful and 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'

The device can flexibly switch 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

The device 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, the device offers your systems exclusive protection from undisclosed and zero-day threats.

Easily Centralized Management with Convenient, Consolidated Overview

TXOne's EdgeOne 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

2 Getting Started

This chapter guides you on how to get started with EdgeIPS™ for 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™ - Quick Setup Guide***.

2.1 Getting Started Task List

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

Procedure

1. Open the management console.

> For more information, please refer to the section *Opening the Management Console*.

2. Change the administrator account ID and password.

> For more information, please refer to the section *Changing the Administrator Password*.

3. Configure the system time.

> For more information, please refer to the section *The System Time Tab*.

4. (Optional) Configure the Syslog settings.

> For more information, please refer to the section *Configuring Syslog Settings*.

5. Configure Object Profiles.

> For more information, please refer to the section *The Object Profiles Tab*.

6. Configure security policies.

> For more information, please refer to the section *The Security Tab*.

7. Configure the device name and device location information.

> For more information, please refer to the section *Configuring Device Name and Device Location Information*.

8. (Optional) Configure the access control list from management clients.

> For more information, please refer to the section *Configuring Control List Access from Management Clients*.

9. (Optional) Configure management protocols and ports.

> For more information, please refer to the section *Configuring Management Protocols and Ports*.

10. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device.

> For more information, please refer to the section *Manually Updating the Pattern*.

11. (Optional) Enable Management by EdgeOne.

For more information, please refer to the section *Enabling Management by ODC*.

12. Configure the network settings and network interface link modes for the device.

For more information, please refer to the section *The Device Tab*.

2.2 Opening the Management Console

We provide a built-in management console that you can use to configure and manage this Edge series device. 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; Edge version 15 or later.

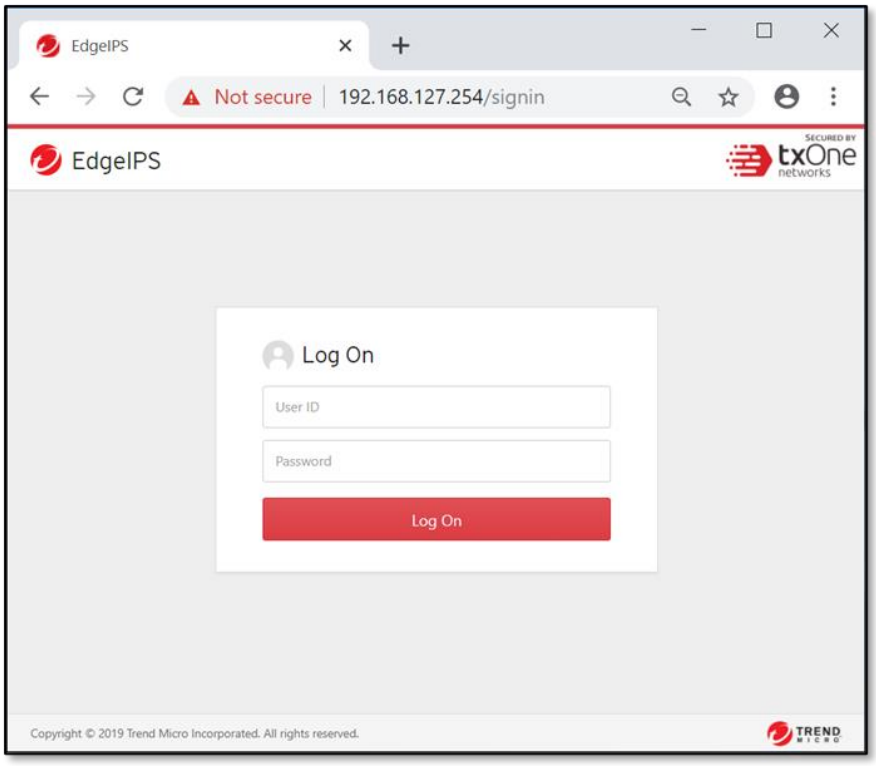
Procedure

1. In a web browser, type the address of the device management console in the following format.

https://<target server IP address or FQDN>

1. The default IP address of this Edge series device is 192.168.127.254 with subnet 255.255.255.0. Before you connect a PC/Laptop to the device, the PC's IP address should be set to an IP address that is able to access the default IP address of the device. After that, connect the PC and the device using an Ethernet cable.
2. TXOne products 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 login page will appear.

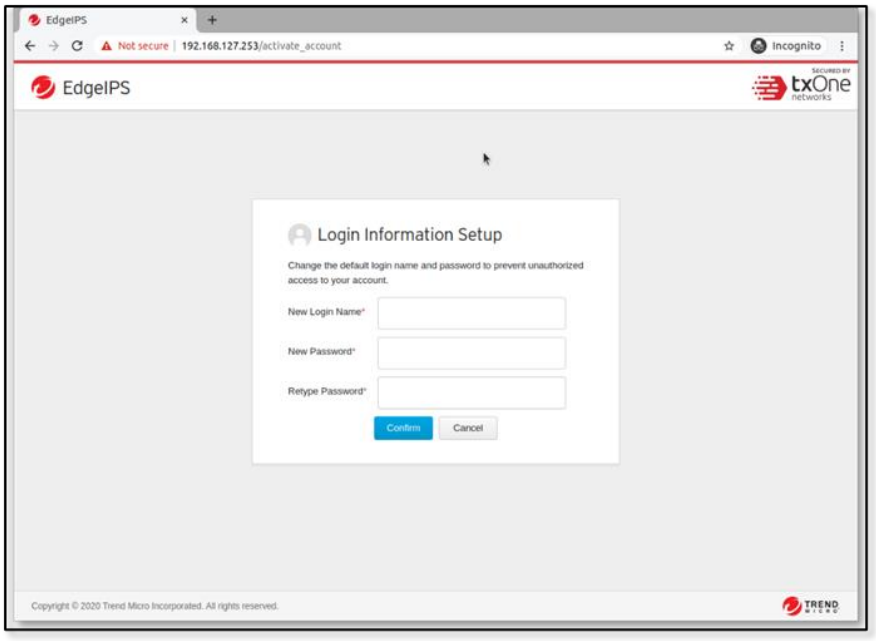


2. Input your login credentials (user ID and password). Use the default administrator credentials when logging in for the first time.

- User ID: *admin*
- Password: *txone*

3. Click [Log In].

4. When logging in for the first time or after a factory reset, you will be prompted to read and accept our End User License Agreement, and to change the default user ID and password before accessing the system.



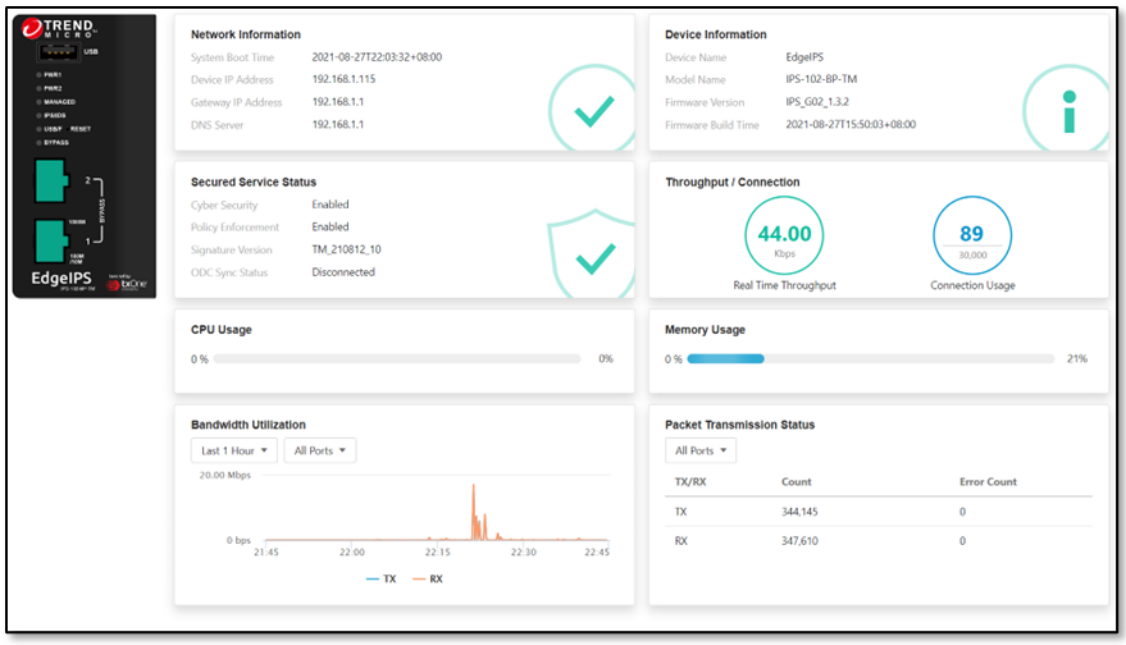
5. You will be automatically logged out of the system. The login page will appear again. Log in again using your new credentials.

2.3 Changing the Administrator Password

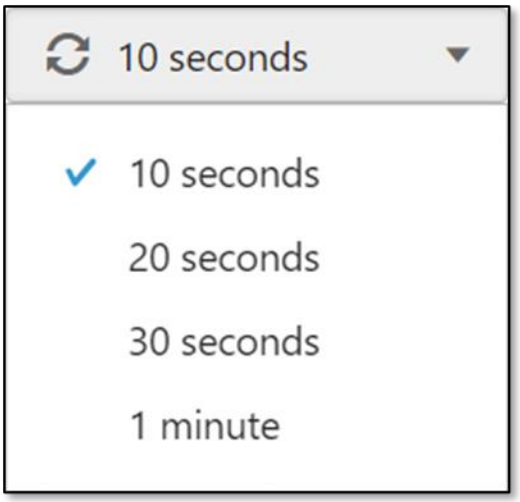
To change the admin password, please refer to the section *Changing Your Password* under *The Administration Tab > Account Management*.

3 The System Tab

Monitor the EdgeIPS Pro™ network information, device information, secured service status, throughput / connection, system resources, bandwidth utilization and packet transmission status under the [System] tab.

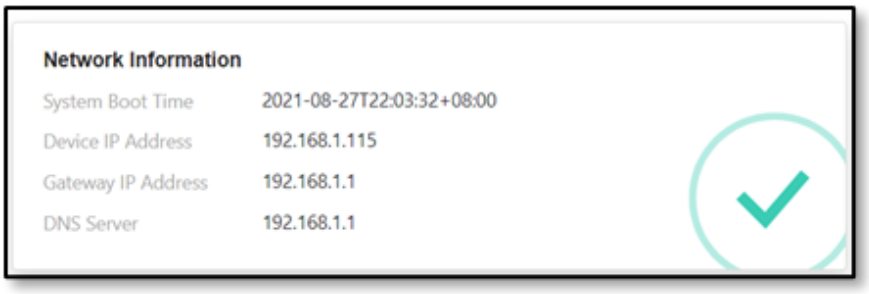


In the upper right corner, you may select **10 seconds** (default), **20 seconds**, **30 seconds** or **1 minute** for the refresh interval.



Network Information

This widget shows the system boot time and the device IP address settings.

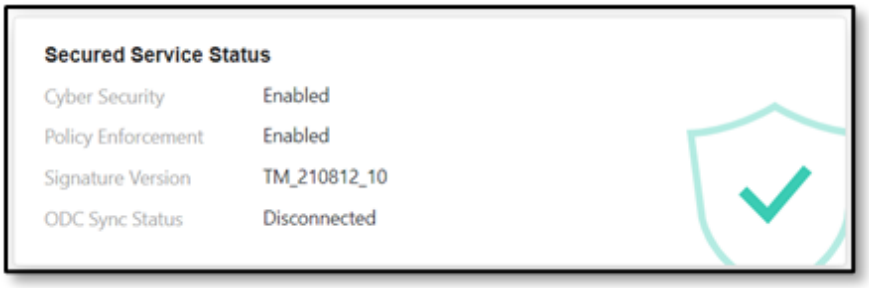


Device Information

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

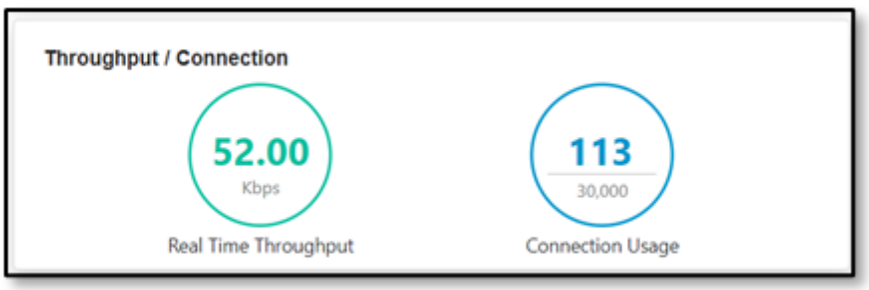
Secured Service Status

The widget shows Cyber Security status (enabled/disabled), Policy Enforcement status (enabled/disabled), the signature version on the device and ODC sync status.



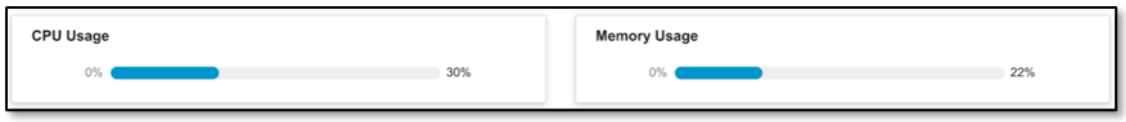
Throughput / Connection

The widget shows the current network throughput and the current network connection usage on the device (according to the refresh time settings).



System Resources

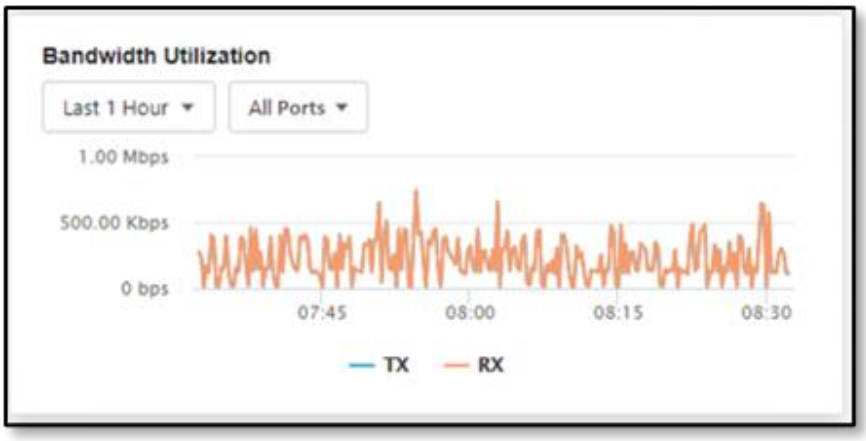
This widget shows system resources (CPU and memory) usages on the device.



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

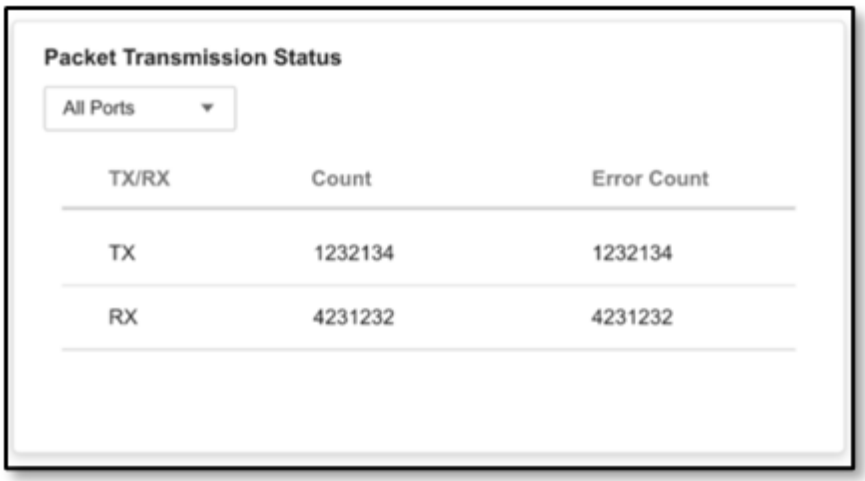
Bandwidth Utilization

This widget shows bandwidth utilization by port(s) according to different time intervals and shows TX and RX bandwidth utilization.



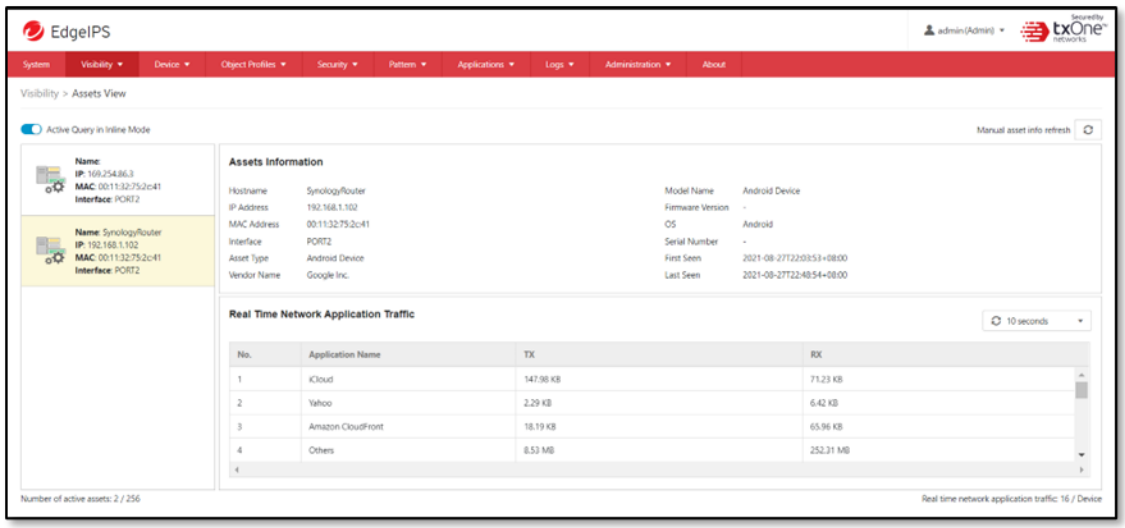
Packet Transmission Status

This widget shows the packet transmission status by port(s), including interface TX/RX, count number, and error count info.



4 The Visibility Tab

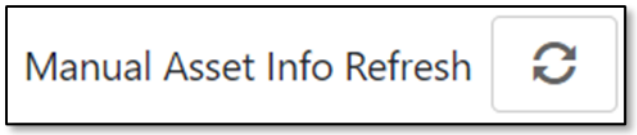
The [Asset View] page under the [Visibility] tab gives you an overview of your managed assets. The tab provides you with timely and accurate information on the assets that are managed by your Edge series device.



The assets, listed under the tab, are automatically detected by the Edge series devices.

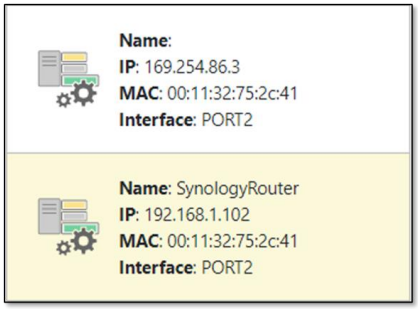
	The term **asset** in this chapter refers to a device or host that is protected by an Edge device.

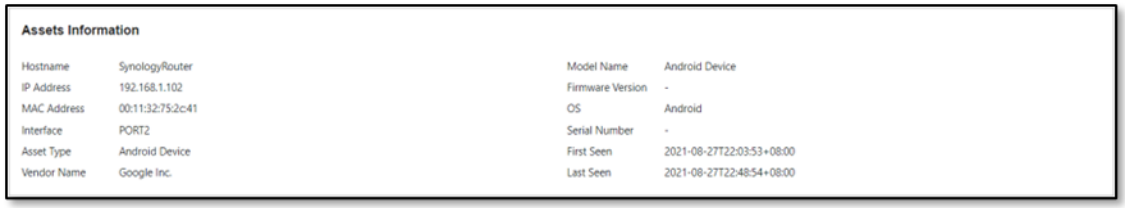
In the upper right corner, you may click the [Manually Refresh the Asset(s)] button to refresh the displayed information.



In the upper left corner, you may enable the [Active Query in Inline Mode] function to detect inactive or dormant assets or passive assets in the network.

	1. The Active Query function operates only in Inline Mode. In Offline Mode, the switch button of active query would not be configurable. 2. Starting from firmware v1.1, the Active Query function supports 4 protocols, including Modbus, CIP, OMRON FINS and SMB.


Name:
IP: 169.254.86.3
MAC: 00:11:32:75:2c:41
Interface: PORT2
Name: SynologyRouter
IP: 192.168.1.102
MAC: 00:11:32:75:2c:41
Interface: PORT2


Assets Information
Hostname SynologyRouter
IP Address 192.168.1.102
MAC Address 00:11:32:75:2c:41
Interface PORT2
Asset Type Android Device
Vendor Name Google Inc.
Model Name Android Device
Firmware Version -
OS Android
Serial Number -
First Seen 2021-08-27T22:03:53+08:00
Last Seen 2021-08-27T22:48:54+08:00


Real Time Network Application Traffic
10 seconds
No. Application Name TX RX
1 iCloud 147.98 KB 71.23 KB
2 Yahoo 2.29 KB 6.42 KB
3 Amazon CloudFront 18.19 KB 65.96 KB
4 Others 8.53 MB 252.31 MB
Real time network application traffic: 16 / Device

5 The Device Tab

This chapter describes how to configure the device settings, including network settings, port configuration and LLDP setting under the [Device] tab.

Procedure

1. Go to [Device] > [Device Settings]. The [Device Settings] page will appear.

2. Configure the following device settings.

- Network Settings

Item	Description
Device IP Address	Input an IP Address of the device.
Netmask	Input a netmask of the device.
Gateway	Input an IP address of the gateway that will send packets to a different network.
DNS	(Optional) Input a DNS address of the device.
VLAN ID	(Optional) Enable this function by clicking the toggle. If enabled, input a VLAN ID of the device to allow packets with the specified VLAN tag to access the management interface.

- Port Configuration

Item	Description
Physical Interface Link Mode (PORT1 & PORT2)	Select a speed and negotiation method, **Auto Negotiation**, **10 Mbps Full-Duplex**, **100 Mbps Full-Duplex**, **1 Gbps Full-Duplex**, **10 Mbps Half-Duplex** or **100 Mbps Half-Duplex** for the port. Select [Auto Negotiation] if you would like the interface to automatically negotiate with the highest speed that both sides can work with. Otherwise, the link speed would be set to the configured speed value based on your selection.

- LLDP Setting

Item	Description
Transmit LLDP	(Optional) Enable the LLDP function by clicking the toggle. When the transmission of LLDP (Link Layer Discovery Protocol) for discovery and configuration is enabled, it allows a network device to advertise its identity and capabilities on the network.

3. Click [Save] to save the configurations or [Cancel] to discard the changes.

6 The Object Profiles Tab

This chapter describes how to configure the following different types of object profiles to simplify policy management by storing configurations that can be used by the Edge series device under the [Object Profiles] tab.

- **IP Object Profiles**: Contains the IP addresses that you can apply to a policy rule.
- **Service Object Profiles**: 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 Profiles**: 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 Profiles**: Contains the settings of IPS (Intrusion Prevention System) pattern rules that you can create/edit profiles and apply them to a policy rule.
- **File Filter Profiles**: Contains the settings of File filter profiles that you can apply to a policy rule. Details of File filter by protocol are defined here.

Each type of object profile has the following types of sub-profile list for this device:

- **Device Profiles**: Contains the IP Object(s), Service Object(s), Protocol Filter Profile(s), IPS Profile(s) and File Filter Profile(s) created and configured by users with EdgeIPS local account privileges to be applied to a policy rule.
- **Master Profiles**: Contains the IP Object(s), Service Object(s), Protocol Filter Profile(s), IPS Profile(s), and File Filter Profile(s) synced from ODC that users with ODC local account privilege can apply them to policy rules. Users with only EdgeIPS local account privilege can only view and copy profiles(s) from Master Profiles(s) to Device Profiles.

The following are the tasks you can perform when you view a list of profiles.

- **Device 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 multiple profiles and click [Delete] to delete the profile(s).
Copy a profile	Select a profile and click [Copy] to copy the profile.

- **Master Profiles:**

Task	Description
Copy a profile	Select one or multiple profiles and click [Copy Master Profiles to Device Profiles] to copy profiles on [Master Profiles] page and paste them to [Device Profiles] page.

6.1 Configuring IP Object Profiles

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

- **Single IP address**

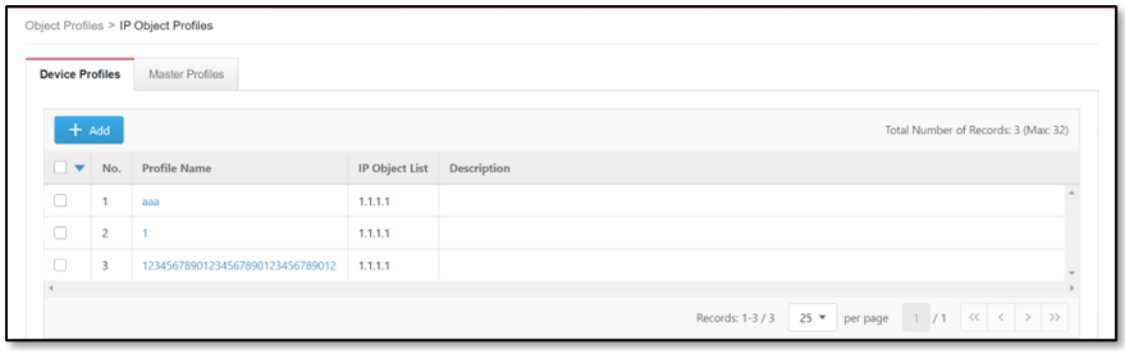
For example: 192.168.1.1

- **IP range**

For example: from 192.168.1.1 to 192.168.1.20

- **IP subnet**

For example: 192.168.1.0/24



2. Do one of the following.

- Click [Add] to create a profile. The [Create IP Object Profile] window will appear.
- Click a profile name to edit settings. The [Edit IP Object Profile] window will appear.

6.2 Configuring Service Object Profiles

You can define the following in a Service Object Profile, which can be used by other policy rules.

- **TCP protocol port range**

For example: TCP ports and service ports ranging from 100 to 120

- **UDP protocol port range**

For example: UDP ports and service ports ranging from 100 to 120

- **ICMP protocol type and code**

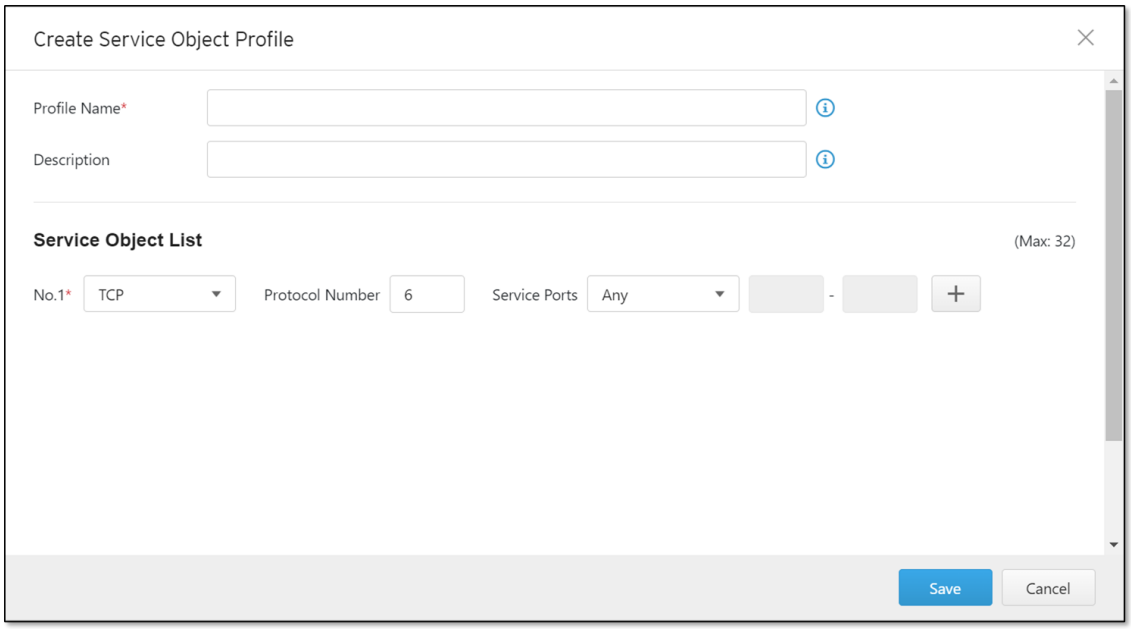
For example: ICMP type 8 code 0

- **Custom protocol with specified protocol number**

For example: protocol number 6 and service ports ranging from 100 to 120

2. Do one of the following:

- Click [Add] to create a profile. The [Create Service Object Profile] window will appear.
- Click a profile name to edit settings. The [Edit Service Object Profile] window will appear.



3. Configure the following Service Object Profile settings.

Item	Description
Profile Name	Type a profile name for this Service Object Profile.
Description	(Optional) Type a description.
Service Object List	Provide one of the following definitions. • **TCP** protocol number and its port range • **UDP** protocol number and its port range • **ICMP** protocol number and its type and code • **Custom** protocol with specified protocol number and port range Click the add button + to add another entry.

4. Click [Save] to save the configurations or [Cancel] to discard the changes.

6.3 Configuring Protocol Filter Profiles

A Protocol Filter Profile contains more sophisticated and advanced protocol settings that you can apply to a policy rule. The types of ICS protocols you can include in a Protocol Filter Profile are:

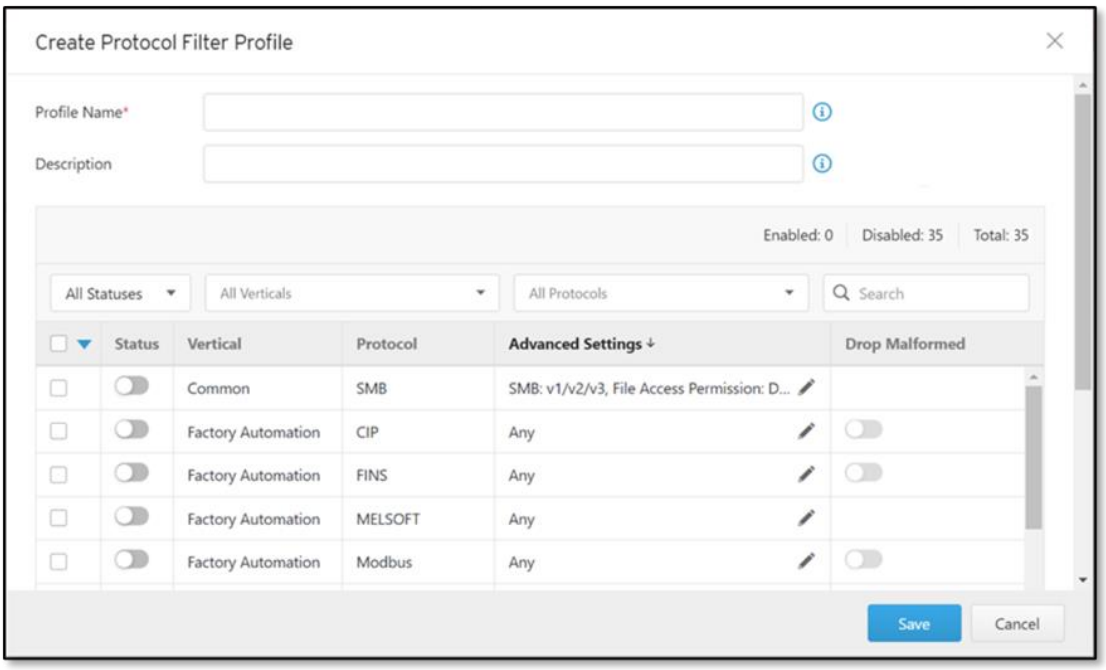
Factory Automation	• Modbus • CIP • S7COMM • S7COMM_PLUS • SLMP	• MELSOFT • TOYOPUC • FINS • PROFINET • SECS/GEM	• GE SDI • GE SRTP • HART-IP • OPC CLASSIC • OPC UA
Building Automation	• BACnet		
HealthCare	• DICOM	• HL7	
Power and Electricity	• IEC61850-MMS	• DNP3	• IEC104
Common	• SMB • FTP • HTTP • MQTT • MS RPC	• RDP • SIP • SMTP • SNMP • SSH	• TELNET • TFTP • VNC

6.3.1 Advanced Settings

The section describes the advanced settings you can configure for OT protocols supported by the Edge device.

To configure the protocol advanced settings, please first access the [Create Protocol Filter Profile] or [Edit Protocol Filter Profile] window.

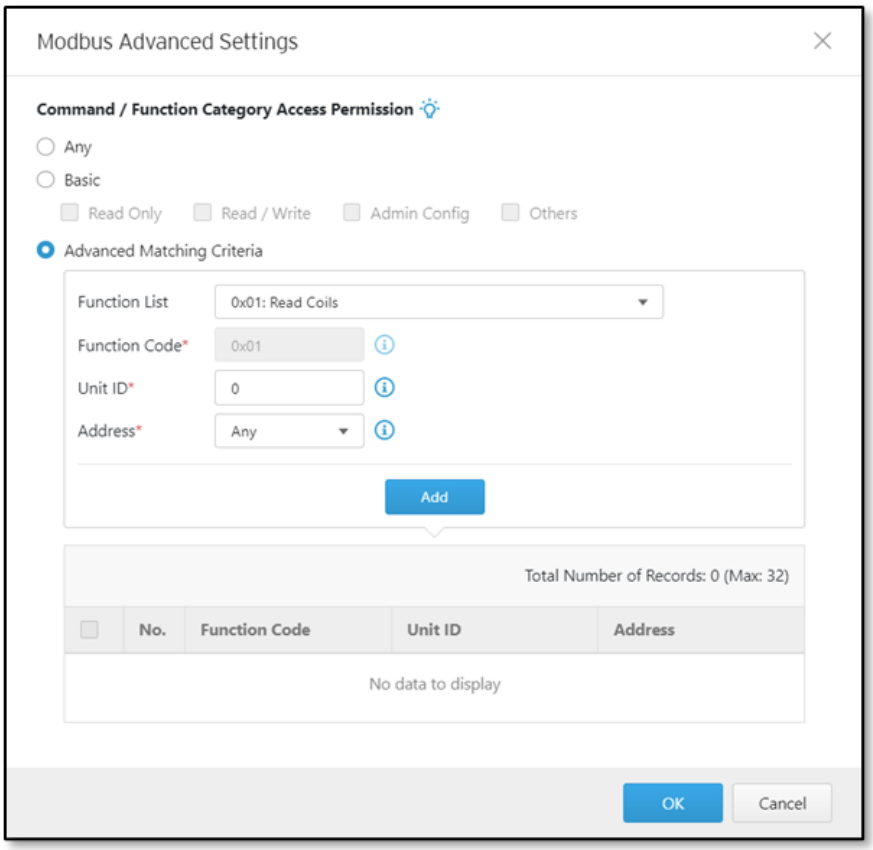
> Please refer to the procedure in the *Configuring Protocol Filter Profiles* section for accessing the [Create Protocol Filter Profile] or [Edit Protocol Filter Profile] window.



Click the edit icon of a specific protocol in the [Advance Settings] column to access the protocol advanced settings window.

6.3.1.1 Modbus Advanced Settings

Through the [Modbus Advanced Settings] window, you can further configure the command/function category access permission settings, including function codes, unit IDs and addresses based on which the function will operate.



After you have accessed the [Modbus Advanced Settings] window, follow the procedure below.

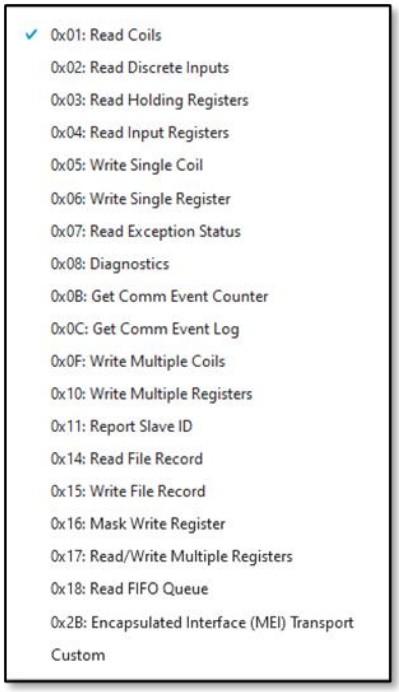
Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **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.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the function codes, unit IDs and addresses.

a. From the [Function List] drop-down menu, select a function of this protocol.



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

b. Type a unit ID in the [Unit ID] field.

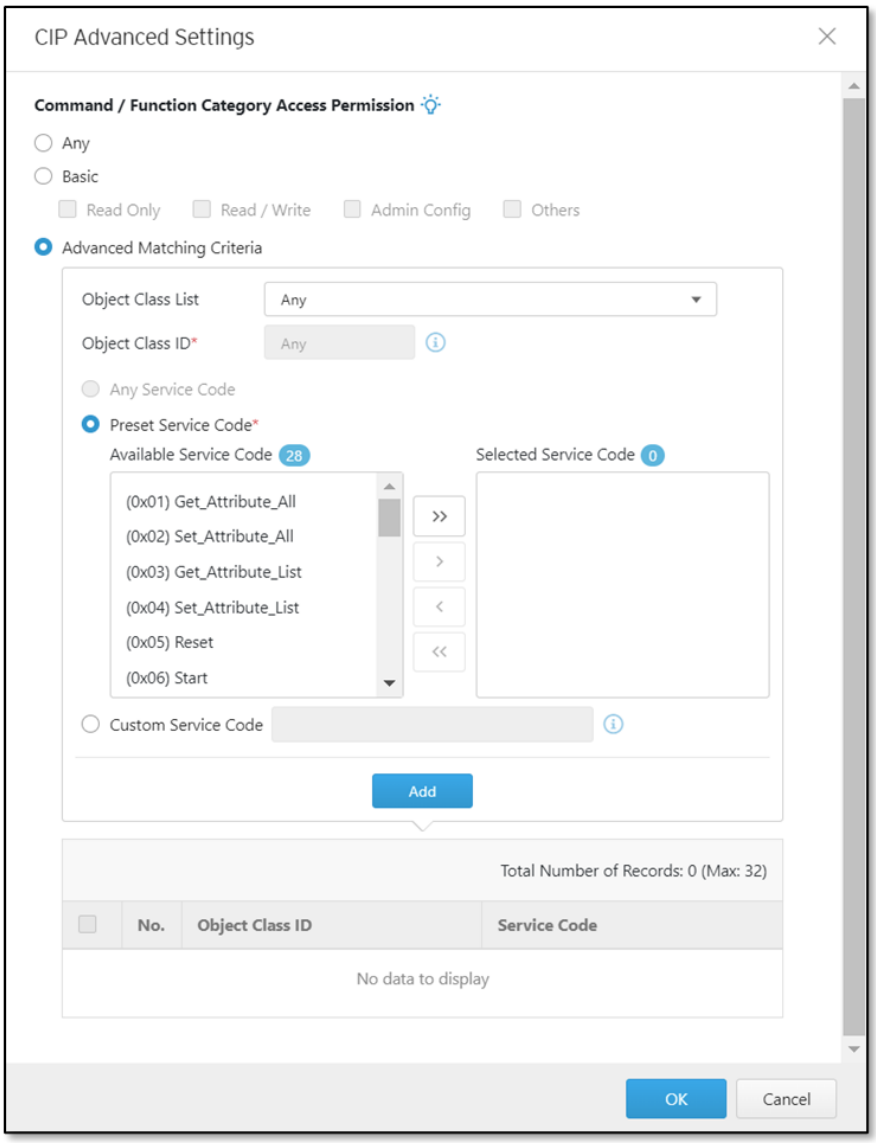
c. Type an address or range of addresses based on which the function will operate.

d. Click [Add].

e. (Optional) Repeat the above steps to add more protocol definition entries.
3. Click [OK] to save the protocol advanced settings or [Cancel] to discard the changes.

6.3.1.2 CIP Advanced Settings

Through the [CIP Advanced Settings] window, you can further configure the command/function category access permission settings, including object class IDs and service codes based on which the function will operate.



After you have accessed the [CIP Advanced Settings] window, follow the procedure below.

Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

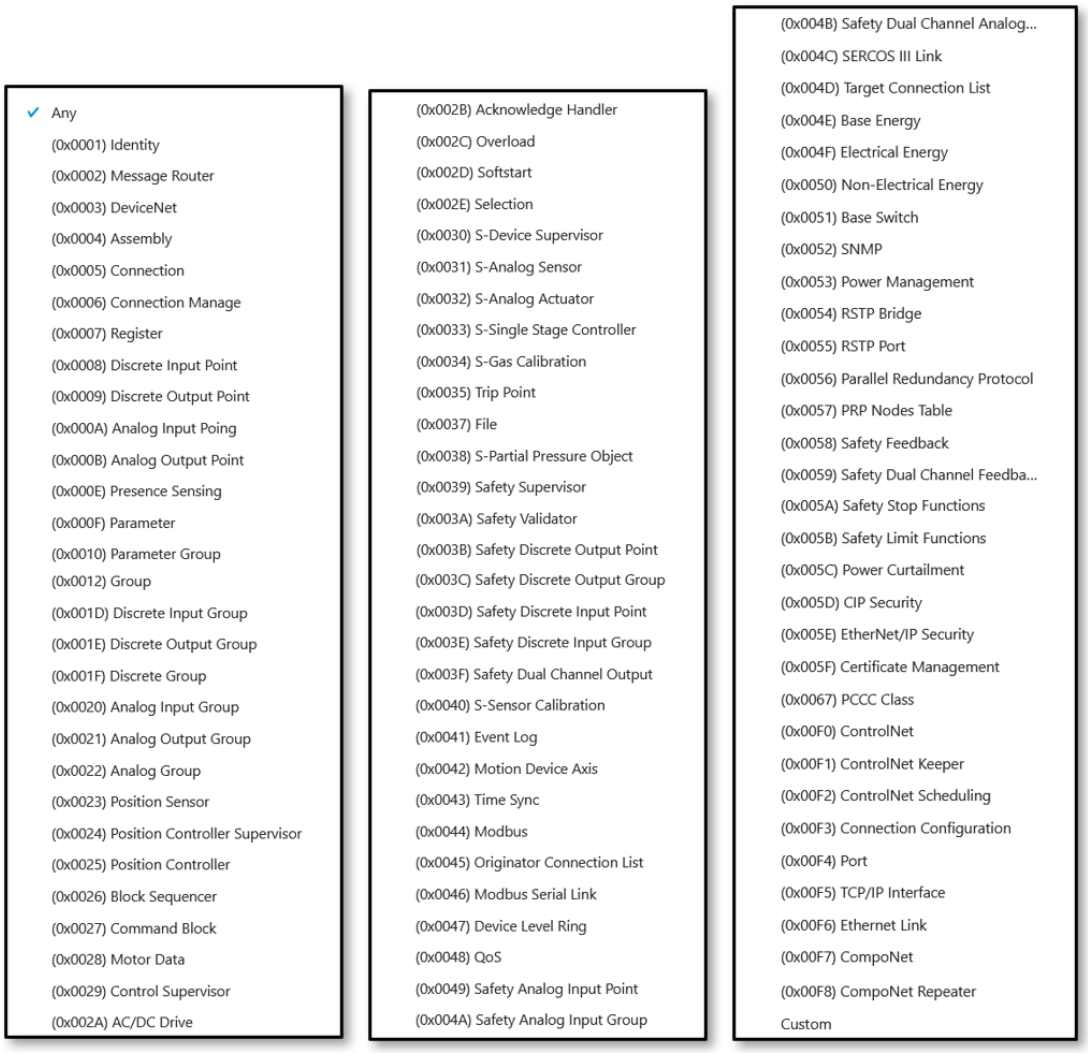
- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:

- **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.

- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the object class IDs and service codes.

a. From the [Object Class List] drop-down menu, select an object class of this protocol.



If you want to specify an object class by yourself, then select [Custom] and input an object class ID in the [Object Class ID] field.

b. Select [Any Service Code], [Preset Service Code] or [Custom Service Code] based on your needs.

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

⚠	The [Any Service Code] option is not available if the object class is [Any].

• If you want to specify one or multiple service codes, then select [Preset Service Code] and move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.

• If you want to specify a service code by yourself, then select [Custom] and input a service code in the [Custom Service Code] field.

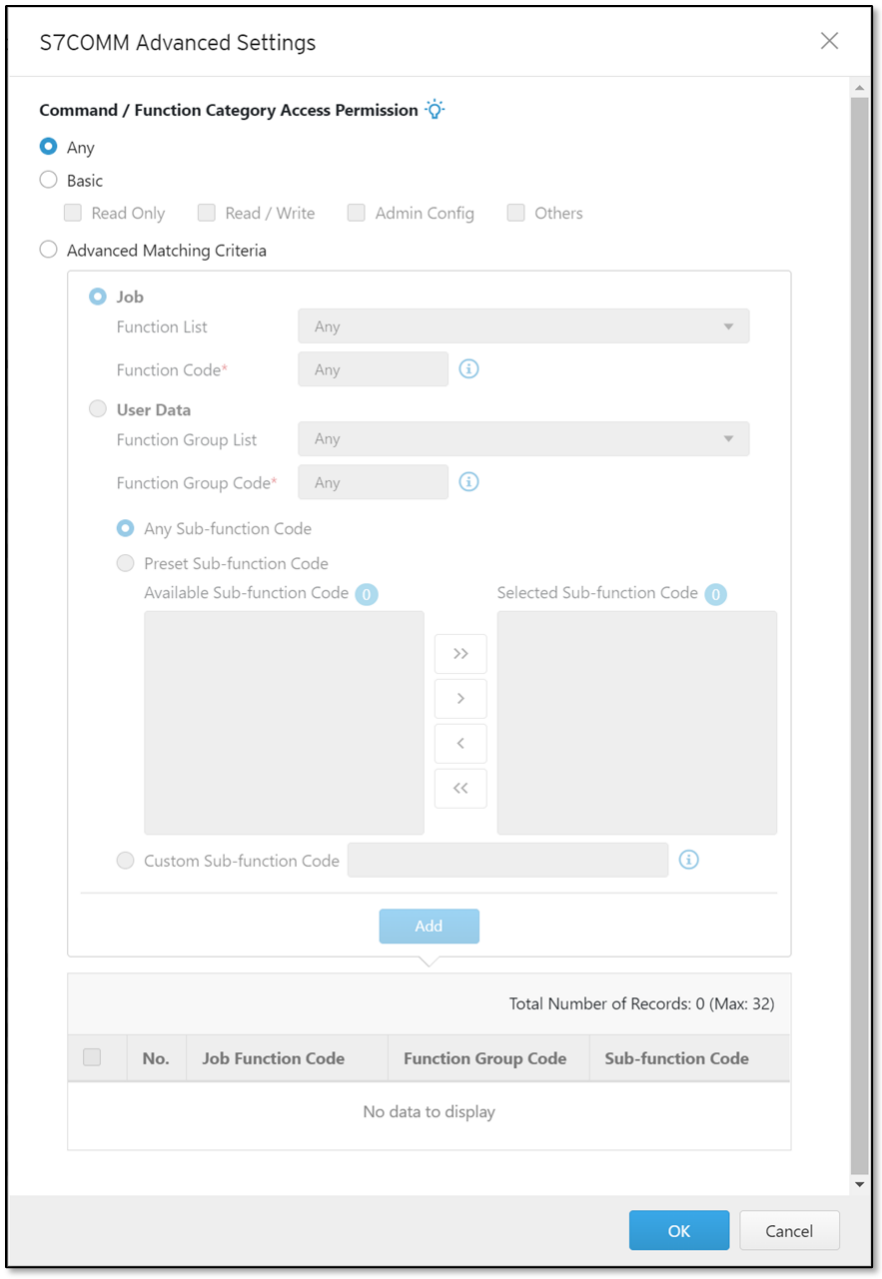
c. Click [Add].

d. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.3 S7COMM Advanced Settings

Through the [S7COMM Advanced Settings] window, you can further configure the command/function category access permission settings, including function/function group codes and sub-function codes based on which the function will operate.



After you have accessed the [S7COMM Advanced Settings] window, follow the procedure below.

Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
    - **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).

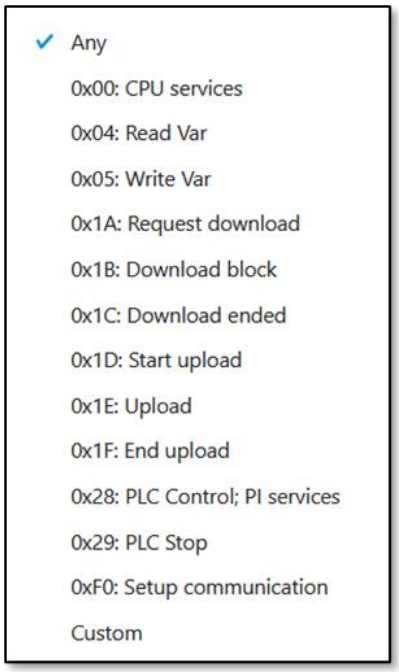
- **Read/Write**: Read and write commands sent from HMI/EWS/SCADA to PLC.
- **Admin Config**: Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands sent from EWS to PLC.
- **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the function codes / function group codes and sub-function codes.

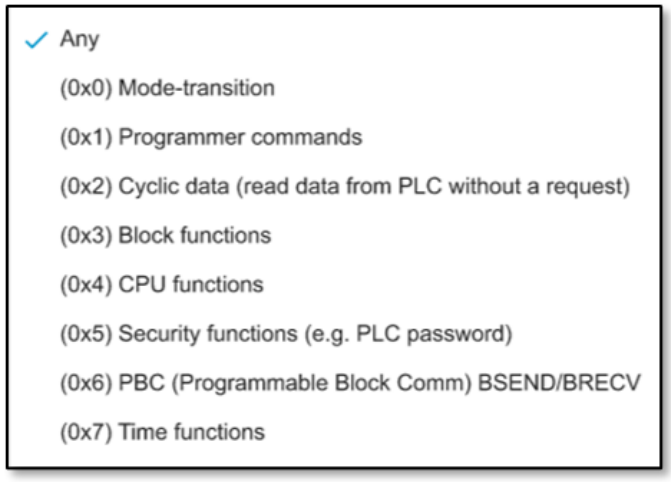
a. Select [Job] or [User Data] based on your needs.

• **Job**: Select this option to specify one function code from the [Function list] drop-down menu.



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

• **User Data**: Select this option to specify one function group code from the [Function Group List] drop-down menu.



If you want to specify a function group by yourself, then select [Custom] and input a function group code in the [Function Group Code] field.

If you select [User Data] as the advanced matching criteria, further select [Any Sub-function Code], [Preset Sub-function Code] or [Custom Sub-function Code] based on your needs.

- **Any Sub-function Code**: Select this option if you want all the sub-function codes within the function group code you specified to be applied.
- **Preset Sub-function Code**: Select this option if you want to specify one or multiple sub-function codes, and then move the sub-function code(s) from the [Available Sub-function Code] to the [Selected Sub-function Code] field.

> ⚠ The [Preset Sub-function Code] option is not available if the function group is [Any] or [Custom].

- **Custom Sub-function Code**: Select this option if you want to specify a service code by yourself, and then input a sub-function code in the [Custom Sub-function Code] field.

> ⚠ The [Custom Sub-function Code] option is not available if the function group is [Any].

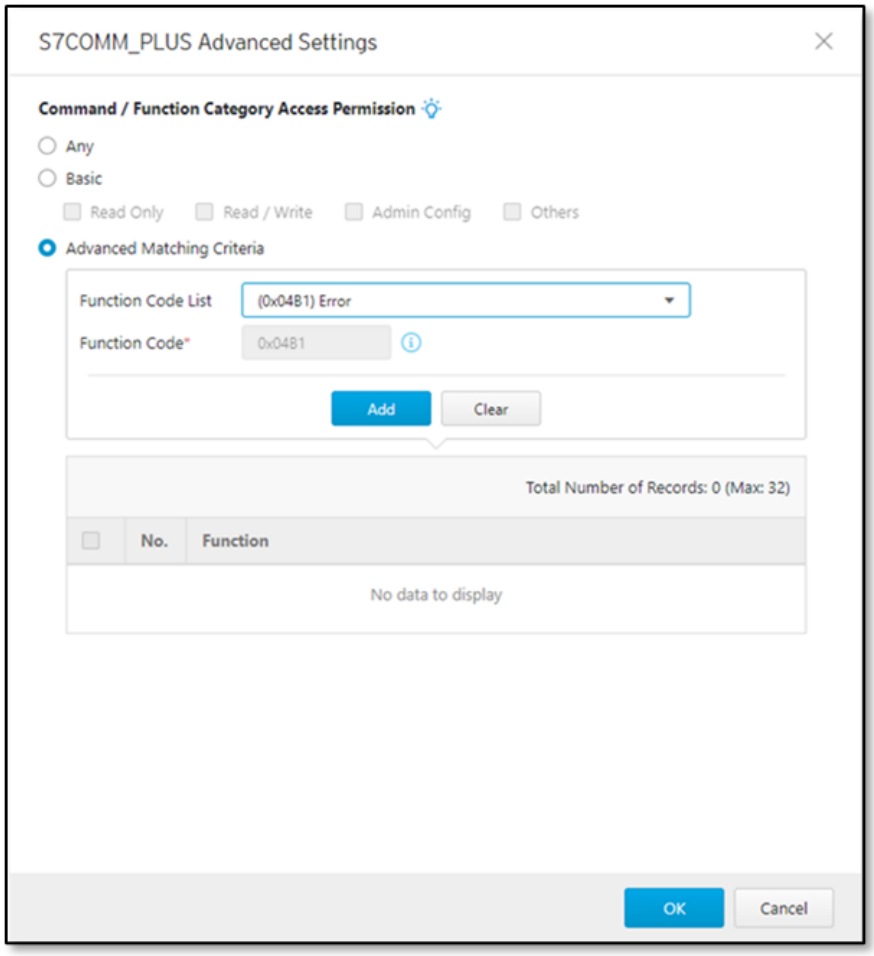
b. Click [Add].

c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.4 S7COMM_PLUS Advanced Settings

Through the [S7COMM_PLUS Advanced Settings] window, you can further configure the command/function category access permission settings, including function codes based on which the function will operate.



After you have accessed the [S7COMM_PLUS Advanced Settings] window, follow the procedure below.

Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **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.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the function codes.

a. From the [Function Code List] drop-down menu, select a function of this protocol.

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

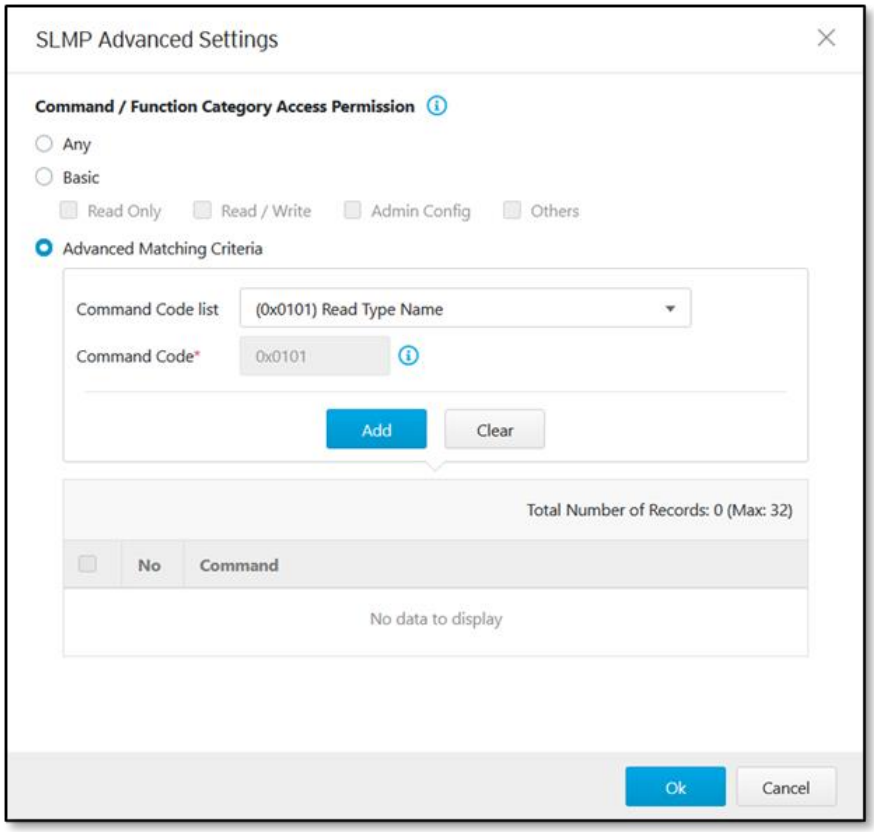
b. Click [Add].

c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.5 SLMP Advanced Settings

Through the [SLMP Advanced Settings] window, you can further configure the command/function category access permission, including command codes based on which the function will operate.



After you have accessed the [SLMP Advanced Settings] window, follow the procedure below.

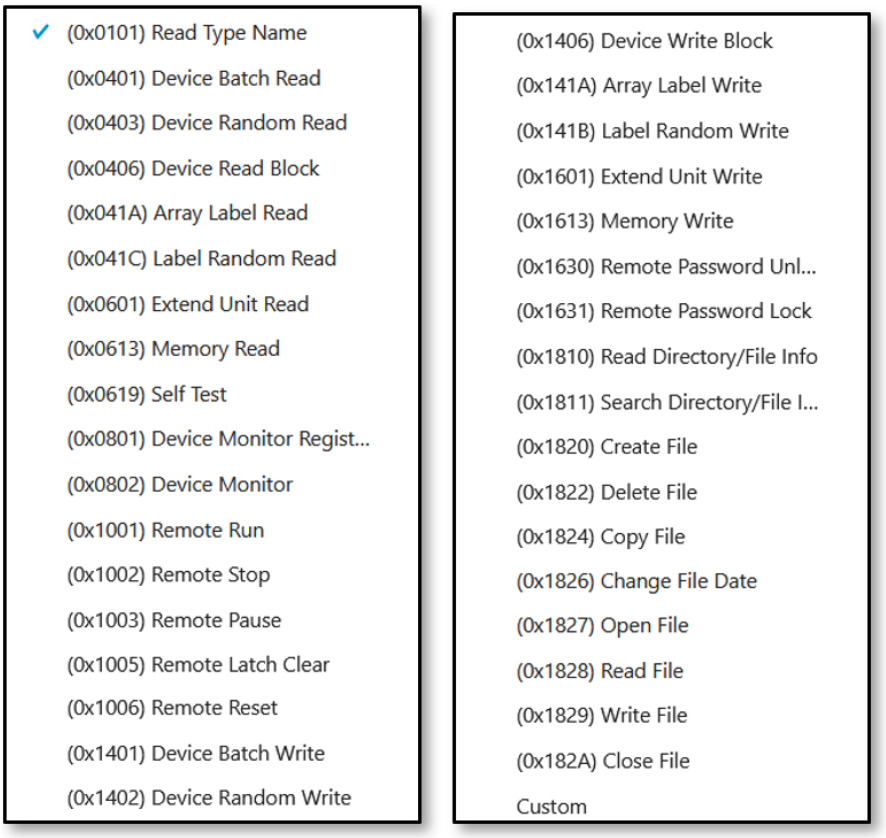
Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **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.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the command codes.

a. From the [Command Code List] drop-down menu, select a command code of this protocol.



If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

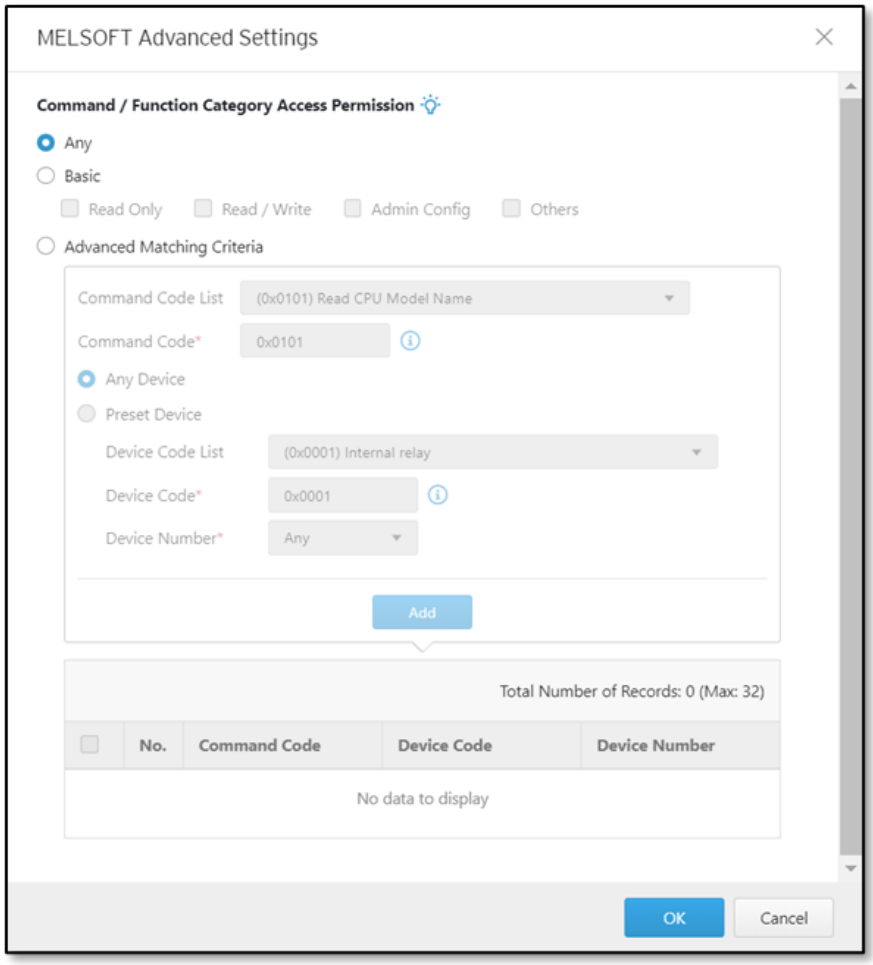
b. Click [Add].

c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.6 MELSOFT Advanced Settings

Through the [MELSOFT Advanced Settings] window, you can further configure the command/function category access permission, including command codes, device codes and device numbers based on which the function will operate.



After you have accessed the [MELSOFT Advanced Settings] window, follow the procedure below.

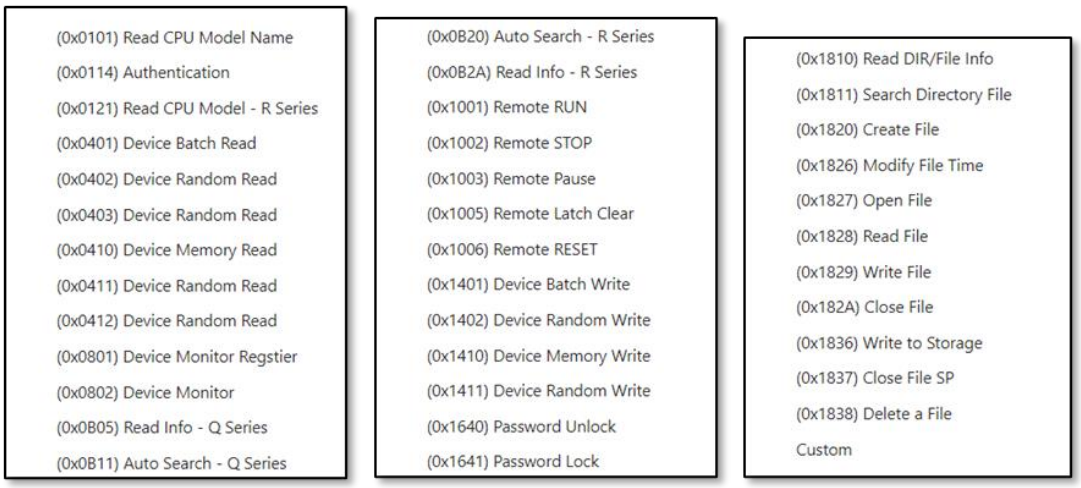
Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **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.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the command codes, device codes and device numbers.

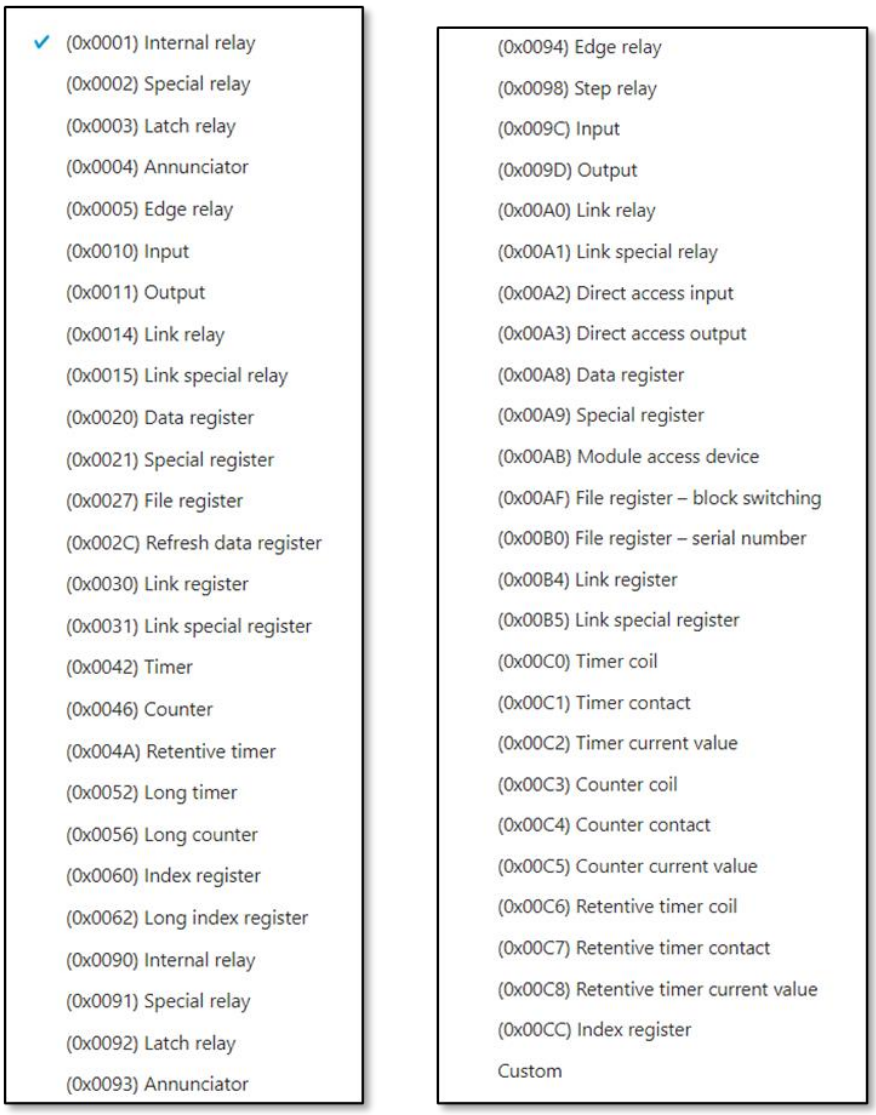
a. From the [Command Code List] drop-down menu, select a command code of this protocol.



If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

For the command codes [(0x1401) Device Batch Write], [(0x1402) Device Random Write], [(0x1410) Device Memory Write] and [(0x1411) Device Random Write], further select [Any Device] or [Preset Device] based on your needs.

- If you want all the device codes within the function you specified to be applied, then select [Any Device].
- If you want to specify one device code, then select [Preset Device] and further configure the following settings.
  - From the [Device Code List] drop-down menu, select a device code.



If you want to specify a device code by yourself, then select [Custom] and input a device code in the [Device Code] field.

• From the [Device Number] drop-down menu, select one of the following options based on your needs.

• **Any**: Select this option if you don't want to include a device number as a filter criterion.

• **Single**: Select this option if you want to specify a device number.

• **Range**: Select this option if you want to specify a range of device numbers.

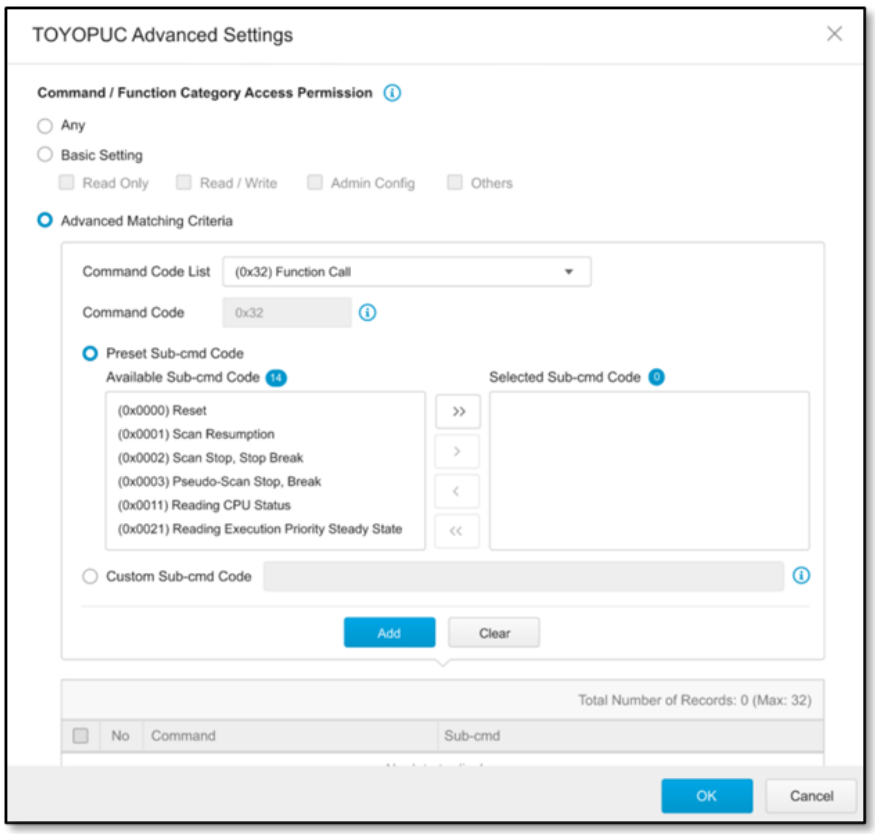
b. Click [Add].

c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.7 TOYOPUC Advanced Settings

Through the [TOYOPUC Advanced Settings] window, you can further configure the command/function category access permission settings, including command codes and sub-command codes based on which the function will operate.



After you have accessed the [TOYOPUC Advanced Settings] window, follow the procedure below.

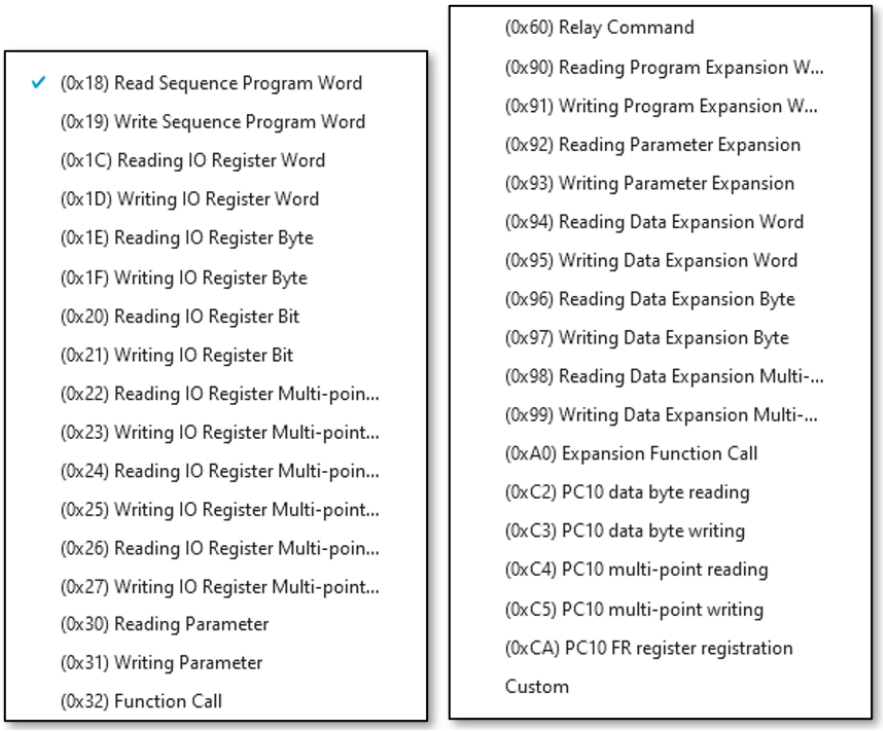
Procedure

1. Configure [Command/Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to specify all available commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
    - **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.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command/Function Category Access Permission].

2. If you have selected [Advanced Matching Criteria], follow the steps below to configure the command codes and sub-command codes.

a. From the [Command Code List] drop-down menu, select a command code of this protocol.



If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

b. For the command codes [(0x32) Function Call] and [(0xA0) Expansion Function Call], further select [Preset Sub-command Code] or [Custom Sub-command Code] based on your needs.

- **Preset Sub-command Code**: Select this option if you want to specify one or multiple sub-command codes, and then move the sub-command code(s) from the [Available Sub-command Code] field to the [Selected Sub-command Code] field.
- **Custom Sub-command Code**: Select this option if you want to specify a sub-command code by yourself, and then input a sub-command code in the [Custom Sub-command Code] field.

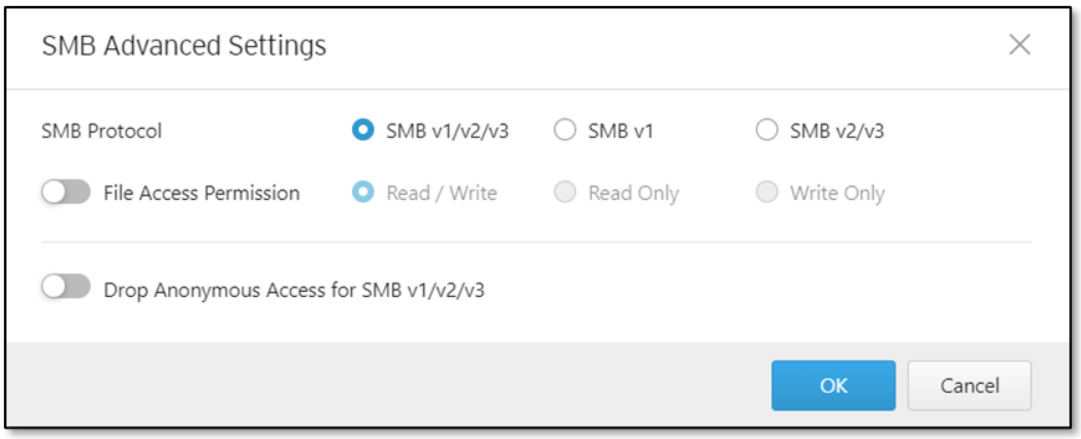
c. Click [Add].

d. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

6.3.1.8 SMB Advanced Settings

Through the [SMB Advanced Settings] window, you can further specify the SMB protocol version combination, file access permission and whether to enable the drop anonymous access function.



After you have accessed the [SMB Advanced Settings] window, follow the procedure below.

Procedure

1. Configure the following SMB advanced settings.

- **SMB Protocol**: Select an SMB protocol version combination, **SMB v1/v2/v3**, **SMB v1** or **SMB v2/v3**.
- **File Access Permission**: If needed, enable this function and select one of the following file access behaviors.
  - **Read / Write**: File access for reading and writing.
  - **Read Only**: File access for reading only.
  - **Write Only**: File access for writing only.
- **Drop Anonymous Access for SMB v1/v2/v3**: If needed, enable this function to drop access over SMB v1/v2/v3 for anonymous accounts.

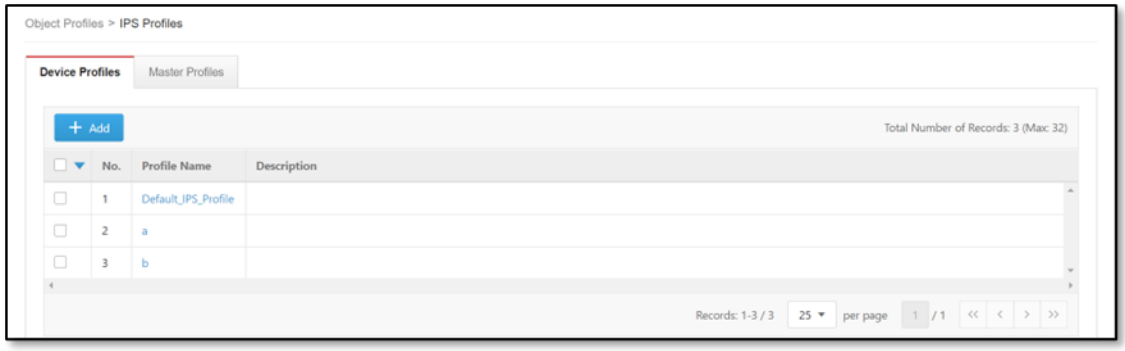
2. Click [OK] to save the protocol advanced settings or [Cancel] to discard the changes.

6.4 Configuring IPS Profiles

An IPS Profile contains more sophisticated pattern rules that allow you to have granular control on policy rules. In an IPS Profile, you may configure:

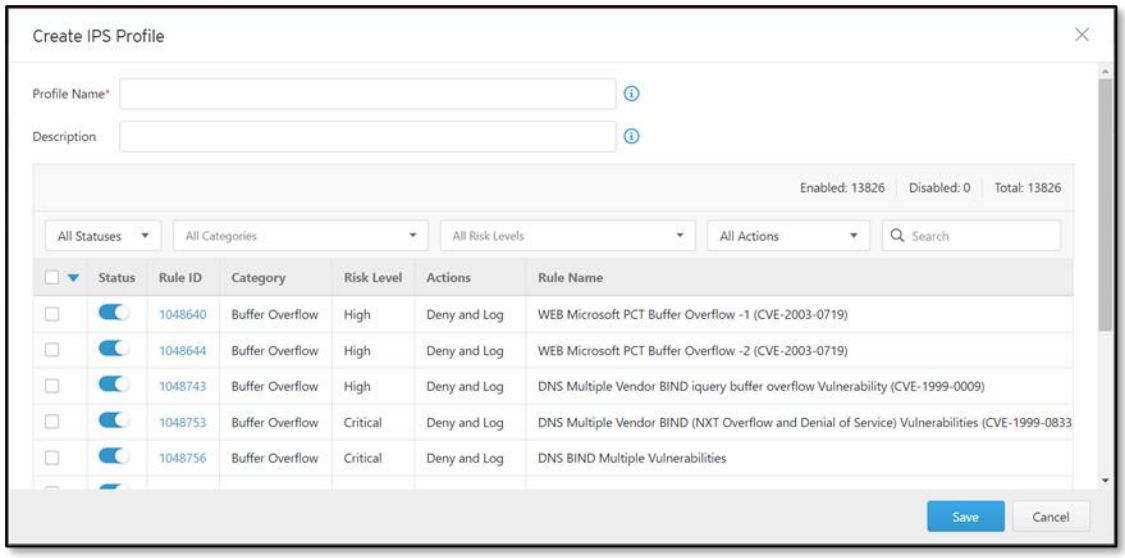
- **IPS pattern rule category**, including:
  - File Vulnerabilities
  - Buffer Overflow
  - DoS Attacks
  - Exploits
  - Malware Traffic
  - Reconnaissance
  - Web Threats
  - ICS Threats
  - Others
  - Misc

- **IPS pattern rule risk level**, including:
  - Information
  - Low
  - Medium
  - High
  - Critical
- **IPS pattern rule default actions**, including:
  - Accept and Log
  - Deny and Log



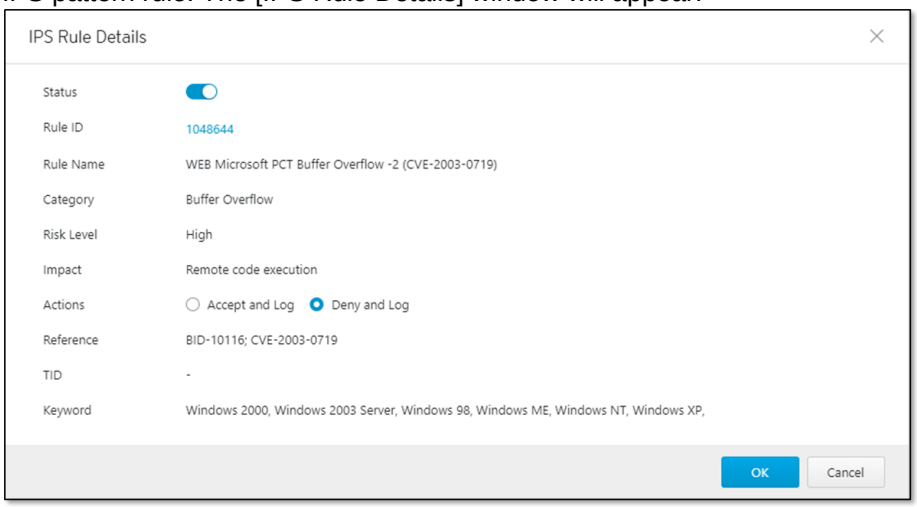
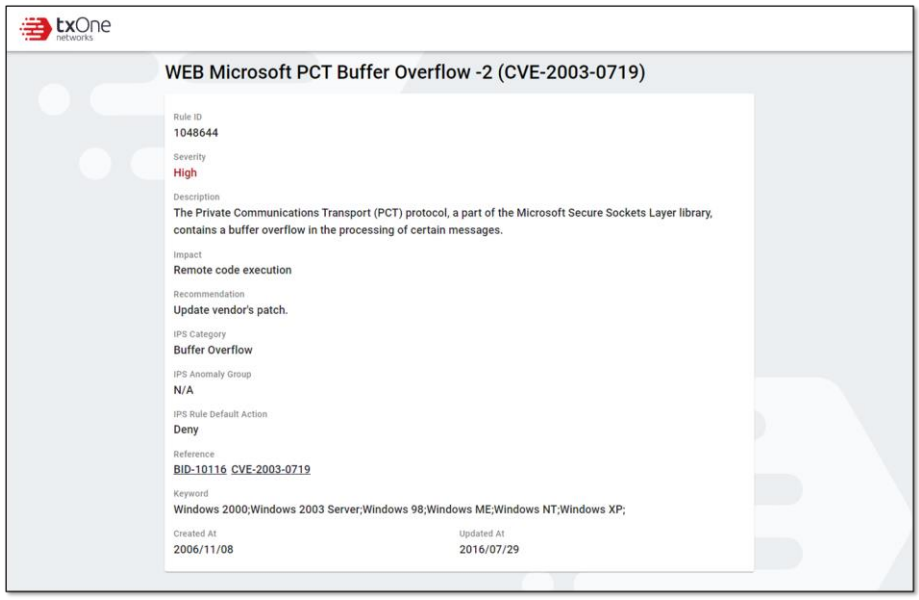
2. Do one of the following.

- Click [Add] to create a profile. The [Create IPS Profile] window will appear.
- Click a profile name to edit settings. The [Edit IPS Profile] window will appear.



3. Configure the following IPS Profile settings.

Item	Description
Profile Name	Type a profile name for this IPS Profile.
Description	(Optional) Type a description.

Item	Description
Status	Disable the operational statuses of one or multiple IPS pattern rules you want to exclude from this IPS Profile by clicking the toggles. (Default status: Enabled)
Rule ID (IPS Rule Granular Control Details)	Click the rule ID in the [Rule ID] column to configure and view details of each IPS pattern rule. The [IPS Rule Details] window will appear.  • **Status**: The operational status of this single IPS pattern rule. **Use the toggle to enable/disable this rule.** • **Rule ID**: The ID number of this IPS pattern rule. You can view the threat information regarding this IPS pattern rule in detail by clicking the rule ID number, and you will then be redirected to the TXOne Threat Encyclopedia as shown below.  • **Rule Name**: The name of this IPS pattern rule regarding the cyber attack. • **Category**: The threat category of this IPS pattern rule regarding the cyber attack, including File Vulnerabilities, Buffer Overflow, DoS Attacks, Exploits, Malware Traffic, Reconnaissance, Web Threats, ICS Threats, Others and Misc.

Item	Description

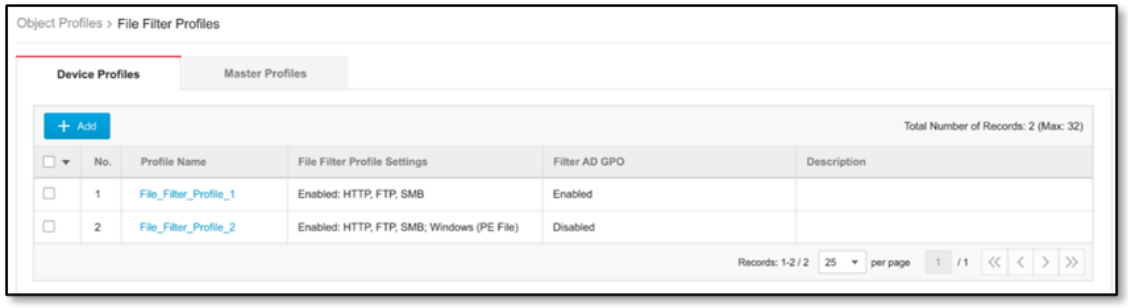
	• **Risk Level**: The suggested security level regarding the cyber attack, including Information, Low, Medium, High and Critical.
	• **Impact**: The damage that will be caused to the target network device if the cyber attack succeeds.
	• **Actions**: The preset actions for the cyber attack. **Select either Accept and Log or Deny and Log.** (Default actions: Deny and Log)
	  ○ **Accept and Log**: When the attack is detected by the Edge series device, the attack will be bypassed and logged for monitoring.
	  ○ **Deny and Log**: When the attack is detected by the Edge series device, the attack will be blocked and logged for monitoring.
	• **Reference**: The vulnerability ID of the cyber attack.
	• **TID**: MITRE ID information.
	• **Keyword**: The keywords for searching this IPS pattern rule.
	Click [OK] to save the configurations of the IPS rule details or [Cancel] to discard the changes.

4. Click [Save] to save the configurations of the IPS profile or [Cancel] to discard the changes.

6.5 Configuring File Filter Profiles

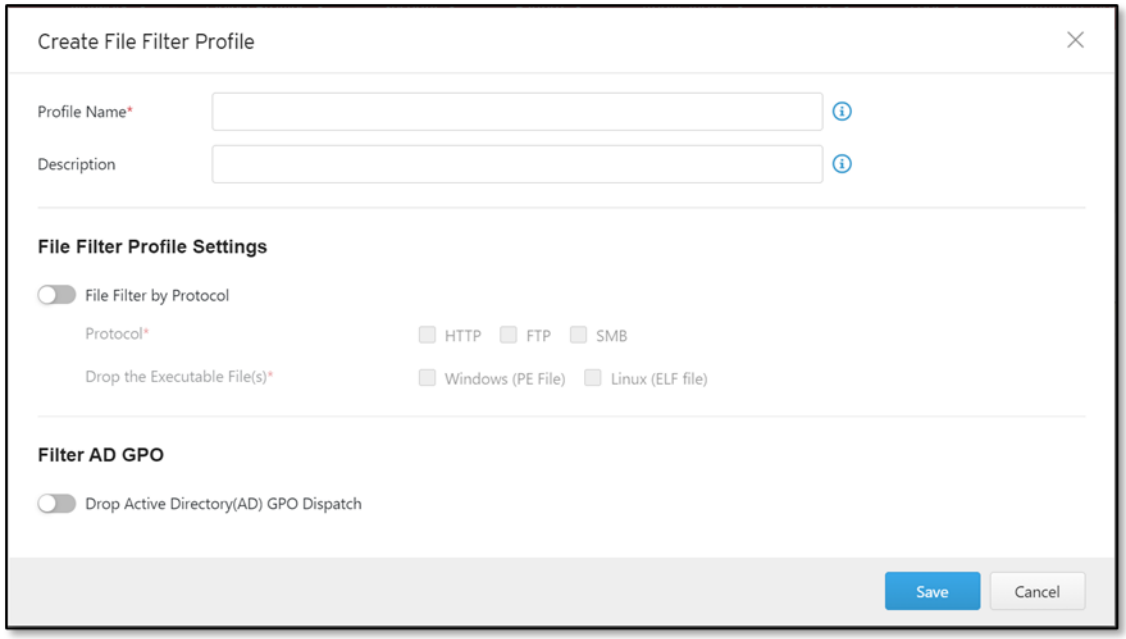
A File Filter Profile contains detailed access protocols as well as settings for executable file types and Active Directory (AD) GPO dispatch that you can apply to a policy rule. In a File Filter Profile, you may configure:

- **Protocol for File Filter function**, including:
  - HTTP
  - FTP
  - SMB
- **Executable file types to be dropped**, including:
  - Windows (PE files)
  - Linux (ELF file)
- **Filtering of Active Directory (AD) GPO**
  - Enable or disable filtering of AD GPO



2. Do one of the following:

- Click [Add] to create a profile. The [Create File Filter Profile] window will appear.
- Click a profile name to edit settings. The [Edit File Filter Profile] window will appear.



3. Configure the following File Filter Profile settings.

Item	Description
Profile Name	Type a profile name for this File Filter Profile.
Description	(Optional) Type a description.

- File Filter Profile Settings

Item	Description
File Filter by Protocol	Enable the File Filter function by clicking the toggle.
Protocol	Select one or multiple protocols for File Filter function, including **HTTP**, **FTP** and **SMB**.
Drop the Executable File(s)	Select one or multiple packed executable file types for dropping, including **Windows (PE files)** and **Linux (ELF files)**.

- Filter AD GPO

Item	Description
Drop Active Directory (AD) GPO Dispatch	(Optional) Enable this function by clicking the toggle if you want to filter AD GPOs.

4. Click [Save] to save the configurations or [Cancel] to discard the changes.

7 The Security Tab

This chapter describes security configurations for EdgeIPS. You can configure the following functions under the Security tab to protect your assets.

- **Security General Settings**: Allows you to configure Security Operation Mode of the device.
- **Cyber Security**: Allows you to configure Deny of Service Prevention (DoS) Setting.
- **Policy Enforcement**: Allows you to define the detailed access rules for ruleset templates with conditions of profiles. The selected ruleset templates are the base to match the network traffic and take action accordingly.
- **Policy Rule Auto-Learning**: Allows you to schedule an auto-leaning task for the device to collect information about legitimate network traffic and generate a trust list for policy enforcement of baseline rules in your network environment.
- **Suspicious Objects**: Allow you to sync the node-based or link-based suspicious object list with the ODC. The activities with the identical nodes or links in the list will be allowed or blocked in your network environment. Notice that when the feature is enabled, 'Suspicious Objects' is of higher priority than 'Policy Enforcement'.

7.1 Security General Settings

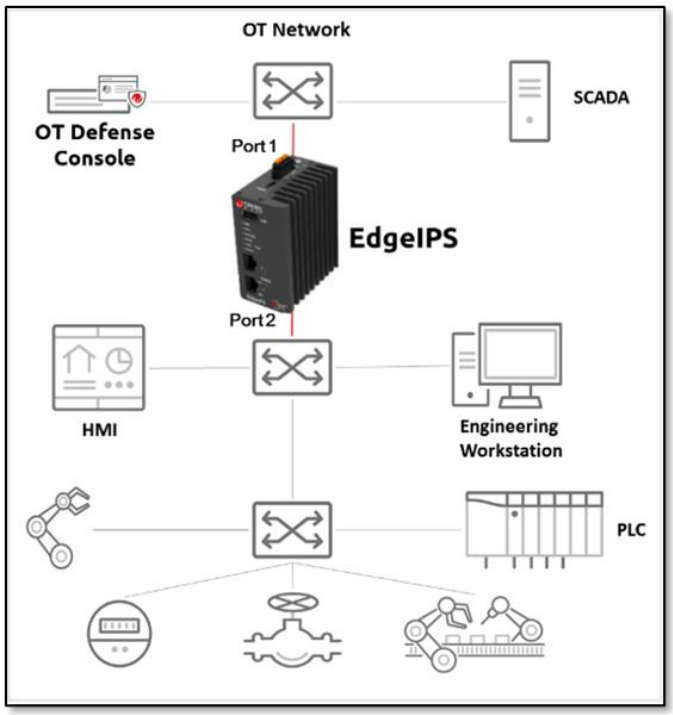
Use the [Security General Settings] tab to configure the security operation mode of the device. EdgeIPS™ offers two operation modes:

- Inline Mode
- Offline Mode

The following sections describe these two modes in detail.

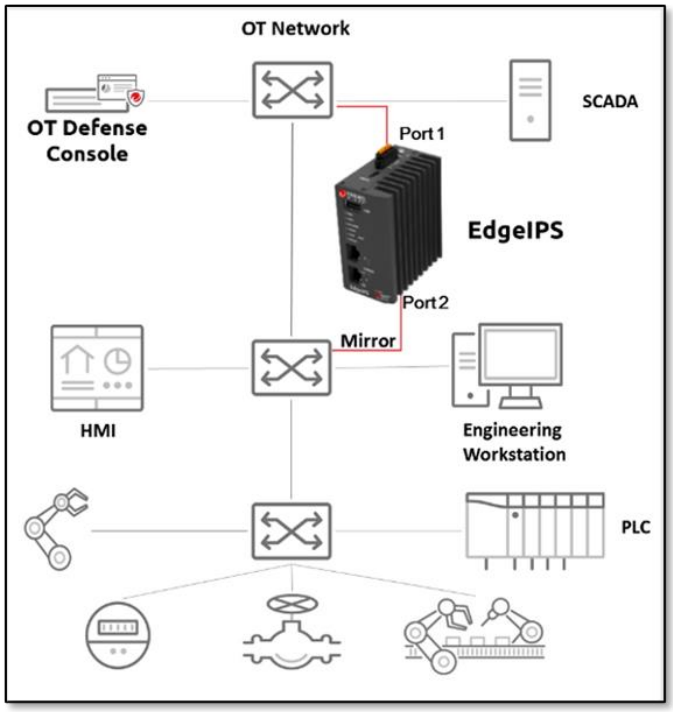
Inline Mode

EdgeIPS sits in the direct communication path between source and destination, actively analyzing, filtering, and taking actions on all traffic that passes through it.



Offline Mode

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



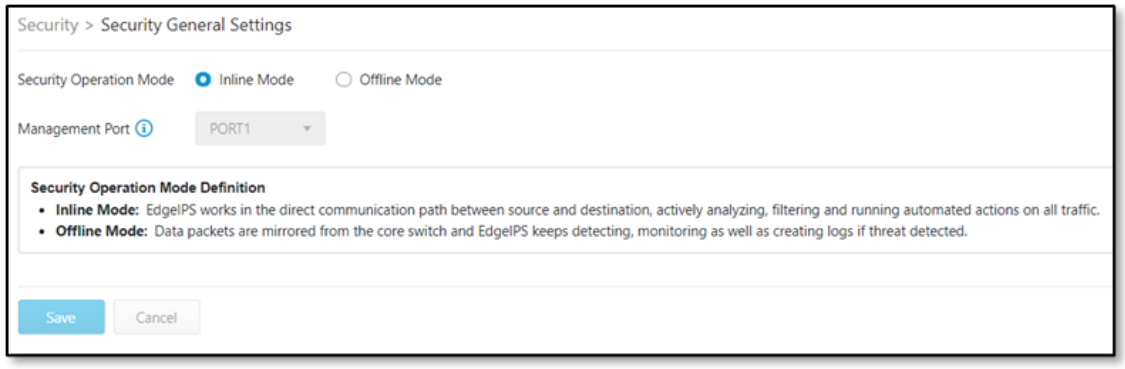
When the EdgeIPS is in Offline mode, **Port 1** of the EdgeIPS will function as a management port, which connects to another switch, allowing the EdgeIPS to be managed by ODC.

7.1.1 Configuring Security Operation Mode

Procedure

1. Go to [Security] > [Security General Settings]

2. Under the [Security General Settings] tab you will see the following screen.



3. Choose a desired operation mode for this device.

Security Operation Mode	Action
Inline Mode	The device works as an **IPS** (Intrusion Prevention System) and checks the traffic based on Policy Enforcement Rules and IPS profiles for cyber threats. Configured IP settings in the [Network Settings] pane can be connected from Port 1 or Port 2 at the same time.
Offline Mode	The device works as an **IDS** (Intrusion Detection System). Configured IP settings in the [Network Settings] pane can be connected from the selected management port (default: Port1). The management port will receive the traffic from the mirror port (default: Port 2), which is used to manage switch/firewall and detect/log cyber threats. Note that under this mode, the Prevention/Monitor Mode is not configurable. Starting from firmware 1.1, EdgeIPS can log the OT protocol activity from the mirror port of the switch if a protocol filter profile is configured and applied to the policy enforcement rule.

For more information about the [Network Settings] pane, please refer to the section *The Device Tab*.

4. If you have selected Offline mode for the device, then choose either Port 1 or Port 2 to be the management port of the device (default: Port 1).

When you switch from Inline Mode to Offline Mode for the first time, please note that you MUST connect to the physical port for device management in case you are unable to access the web console. After successfully switching to Inline Mode, you can specify Port 1 or Port 2 as the port to receive the traffic from the network device for monitoring and logging.

5. Click [Save].

⚠	Ensure that the operation mode is correctly selected. If EdgeIPS is deployed using inline network topology with the [Security Operation Mode] being set to [Offline Mode], then devices that connect to the non-management port cannot get through to outside.

7.2 Cyber Security

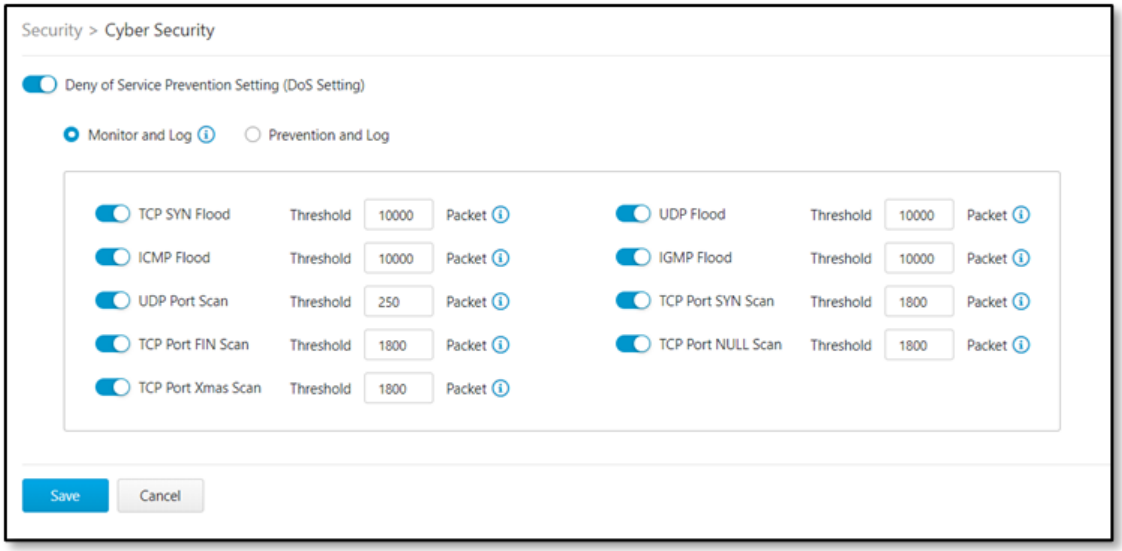
This device features Cyber Security function, which covers denial of service attack prevention. The signature rules of intrusion prevention are called the “Trend Micro DPI (Deep Packet Inspection) Pattern”. This pattern is provided by Trend Micro and can be regularly updated through ODC as well by manual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

7.2.1 Configuring Cyber Security (Denial of Service Prevention)

Procedure

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

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



3. Use the toggle to enable or disable the denial of service prevention feature.

4. Select an action ([Monitor and Log] or [Prevention and Log]) for the feature.

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

6. Click [Save].

The following table summarizes the settings:

Security Operation Mode (Security General Settings)	DoS Action Setting	Action Performed
Inline Mode	Monitor and Log	• Detect and monitor abnormal protocol access attempts to the OT assets, without blocking network attacks.

Security Operation Mode (Security General Settings)	DoS Action Setting	Action Performed
		• Generate logs.
	Prevent and Log	• Block abnormal protocol access attempts to OT assets. • Generate logs.
Offline Mode	Monitor and Log	• Passively detect and monitor abnormal protocol access attempts to the OT assets, without blocking network attacks. • Generate logs.

7.3 Policy Enforcement

Policy Enforcement allows you to define rules with various conditions, including the well-known OT protocols for your own industry. Under which conditions with specified protocols, the activity will be allowed or blocked is based on the policy you have set in the adopted rule set template.

There are two types of Policy Enforcement rule list for this device:

- **Device Rule List**: Contains the policy rule(s) created and configured by users with EdgeIPS local account privileges.
- **Master Rule List**: Contains the policy rule(s) synced from ODC that users with ODC local account privileges can apply them to the devices managed by ODC. Users with EdgeIPS local account privileges can only view these master (ODC) policy rules.

The device rules take higher priorities than the master rules when the device checks the network traffic based on both types of rules.

The following are the tasks you can perform when you view a list of profiles.

- **Device Rule List:**

Task	Description
Add a policy rule	Click [Add] to create a new policy rule.
Edit a policy rule	Click a policy rule name to edit the settings.
Delete a policy rule	Select one or multiple policy rules and click [Delete] to delete the policy rule(s).
Copy a policy rule	Select a policy rule and click [Copy] to copy the policy rule.

- **Master Rule List:**

Task	Description
N/A	The policy rules on the Master Rule List are view-only.

7.3.1 Configuring Policy Enforcement

Procedure

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

2. Under the [Policy Enforcement] tab you will see the [Policy Enforcement General Settings] pane.

3. Use the toggle to enable or disable the policy enforcement feature.

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

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

The following table summarizes the settings:

Security Operation Mode (Security General Settings)	Policy Enforcement Mode	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 attempts to OT assets. • Generate logs.
Offline Mode	Monitor and Log	• Passively detect and monitor abnormal protocol access attempts to the OT assets, without blocking network attacks. • Generate logs.

7.3.2 Adding Policy Enforcement Rules

Procedure

1. Configure the required objects.

- IP Object Profiles

For more information, see *Configuring IP Object Profiles*.

- Service Object Profiles

For more information, see *Configuring Service Object Profiles*.

- Protocol Filter Profiles

For more information, see *Configuring Protocol Filter Profiles*.

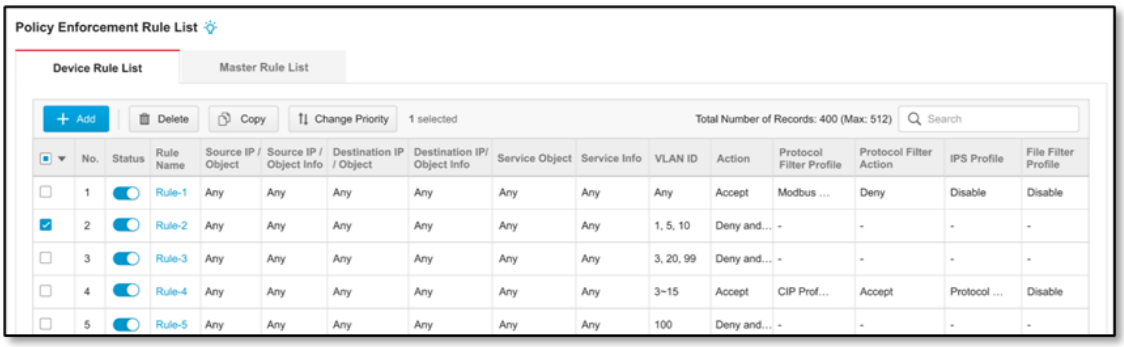
- IPS Profiles

For more information, see *Configuring IPS Profiles*.

- File Filter Profiles

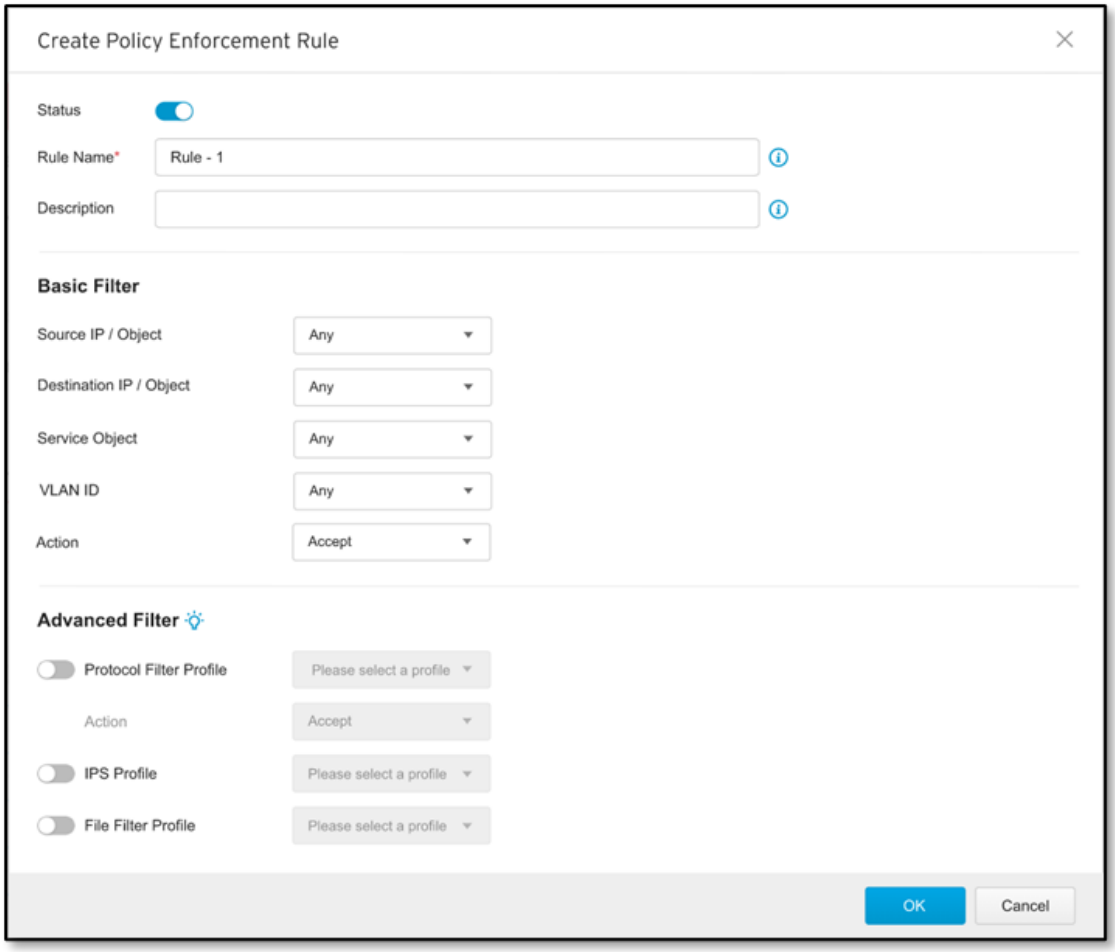
For more information, see *Configuring File Filter Profiles*.

2. Go to [Security] > [Policy Enforcement]. The [Policy Enforcement] page will appear.



4. Click the [Add] button to add a new policy rule.

5. Use the toggle under [Status] to enable or disable a policy rule.



6. Input a descriptive [Rule Name].

7. Input a [Description] for the rule.

8. From the [Source IP / Object] drop-down menu, select either one of the following for the source IP address(es):

- Any
- Single IP
- IP Range
- IP Subnet
- IP Object

If you select [IP Object], then you need to select an IP object that has been created beforehand in IP Object Profiles.

9. From the [Destination IP / Object] drop-down menu, select either one of the following for the destination IP address(es):

- Any
- Single IP
- IP Range
- IP Subnet
- IP Object

10. From the [Service Object] drop-down menu, select either one of the following for the layer 4 criteria:

- Any
- 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

If you select [Service Object], then you need to select a service object that has been created beforehand in Service Object Profiles.

11. From the [VLAN ID] drop-down menu, select either one of the following for the VLAN ID(s):

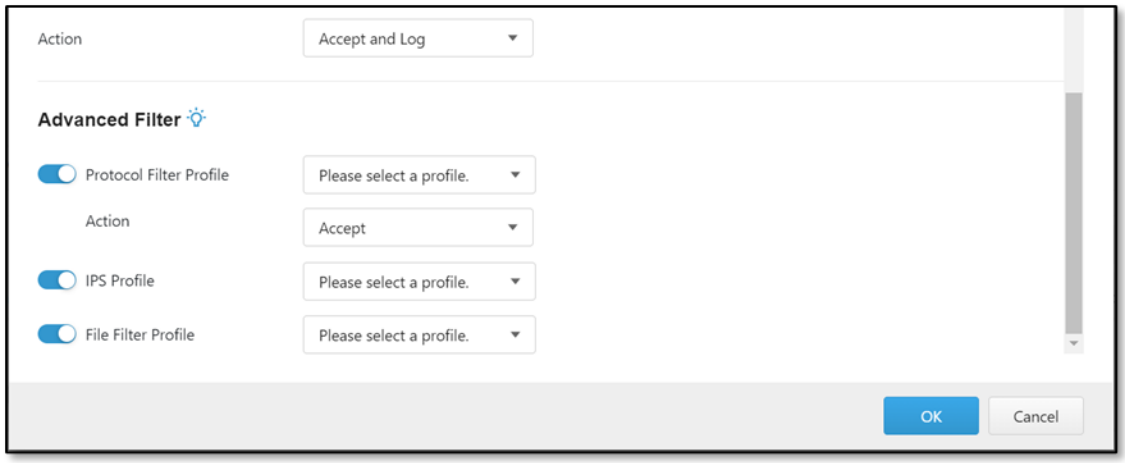
- Any
- Custom: You can specify the VLAN ID for this protocol.

A maximum of 5 VLAN IDs can be applied to one policy rule.

12. From the [Action] drop-down menu, select one of the following:

- Accept: Select this option to allow network traffic that matches this rule.
- Accept and Log: Select this option to allow network traffic that matches this rule and output a log.
- Deny and Log: Select this option to block network traffic that matches this rule and output a log.

13. If you select "Accept" or "Accept and Log" for [Action], you can enable Advanced Filter (Protocol Filter Profile, IPS Profile, File Filter Profiles and Antivirus Filter Profile) to conduct further actions.



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

- From the [File Filter Profile] drop-down menu, select a file filter profile you have defined beforehand.

14. Click [OK] to save the configuration.

7.3.3 Managing Policy Enforcement Rules

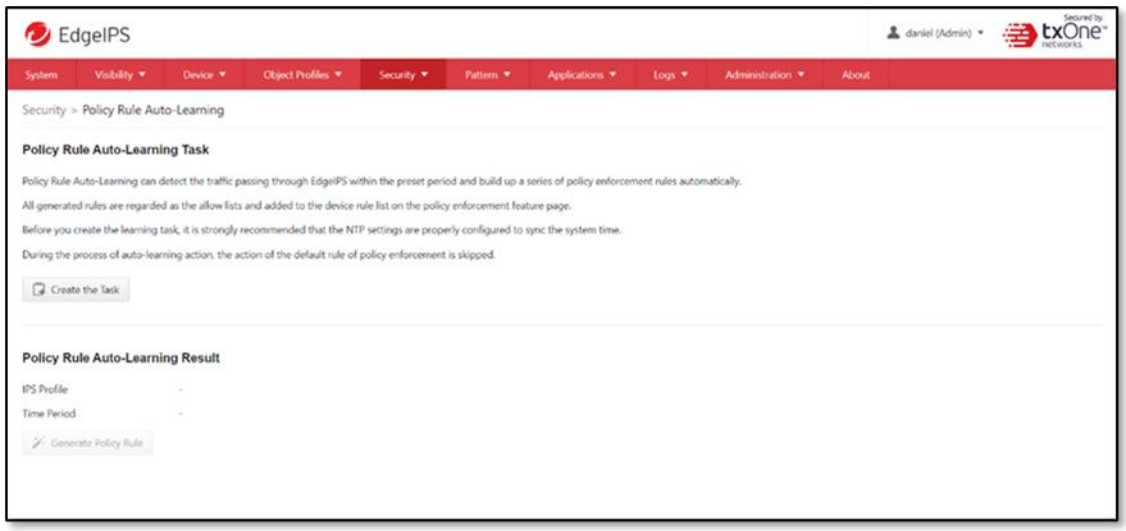
The following table lists the common tasks that are used to manage policy enforcement rules.

Tasks	Actions
To delete a policy enforcement rule	Click the check box in front of a policy enforcement rule and click the [Delete] button.
To duplicate a policy enforcement rule	Click the check box in front of a policy enforcement rule and click the [Copy] button.
To edit a policy enforcement rule	Click the name of a 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 a 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, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules are listed in the table on the UI screen ordered by priority, with the highest priority rule listed on the first row of the table.

7.4 Policy Rule Auto-Learning

Policy Rule Auto-Learning allows you to create a learning task within a scheduled period of time that collects information about legitimate network traffic then uses it to generate a trust list for policy enforcement of baseline rule(s) in your network environment.

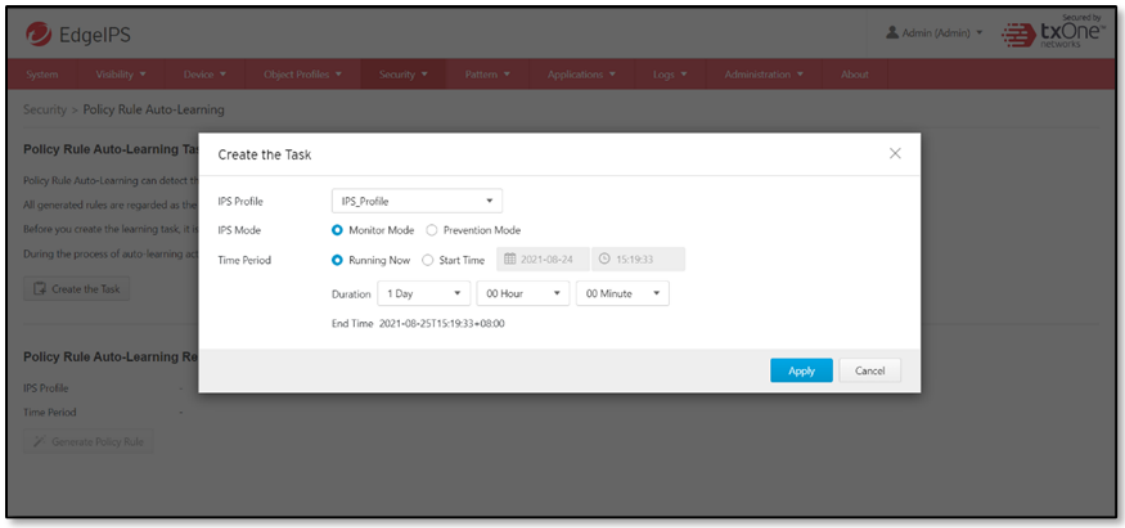


Before you create a task in Policy Rule Auto-Learning, please make sure that the IPS Profiles under the [Device Profiles] tab ([Object Profiles] > [IPS Profiles]) are properly configured.

7.4.1 Configuring Policy Rule Auto-Learning

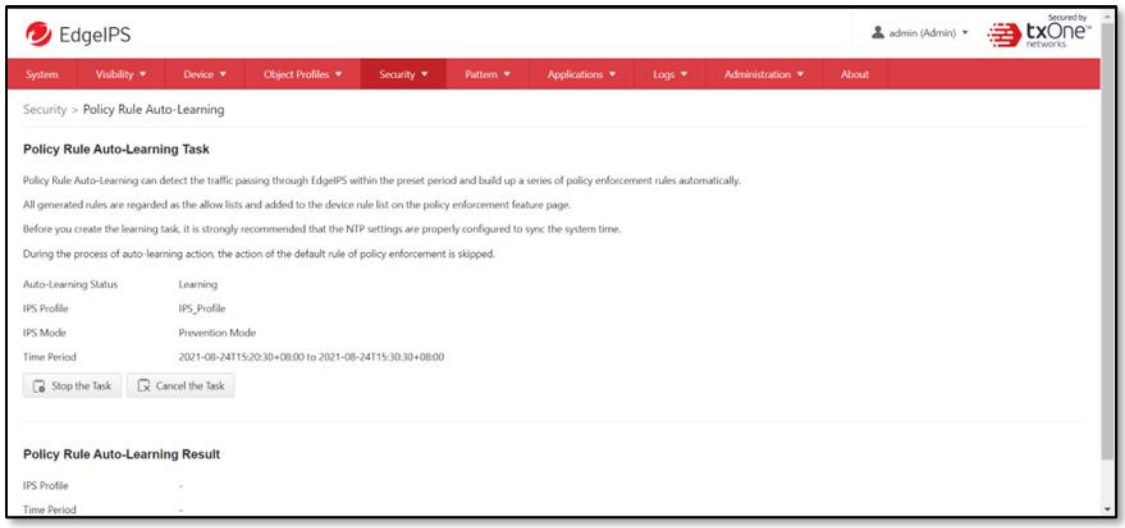
Procedure

1. Go to [Security] > [Policy Rule Auto-Learning].
2. On the [Policy Rule Auto-Learning Task] pane you will see the [Create the Task] button.
3. Click the [Create the Task] button to create an auto-learning task.
4. Select an IPS Profile to apply to the learning task.
5. Select an IPS mode ([Monitor Mode], or [Prevention Mode]) to apply to the learning task.
6. Select the time period ([Running Now], or [Start Time]) to determine when the learning task starts for the auto-learning.
7. Click [Apply] to create the task.



When a learning task is running, the configuration file cannot be uploaded to EdgeIPS to restore settings.

7.4.2 Stopping Policy Rule Auto-Learning



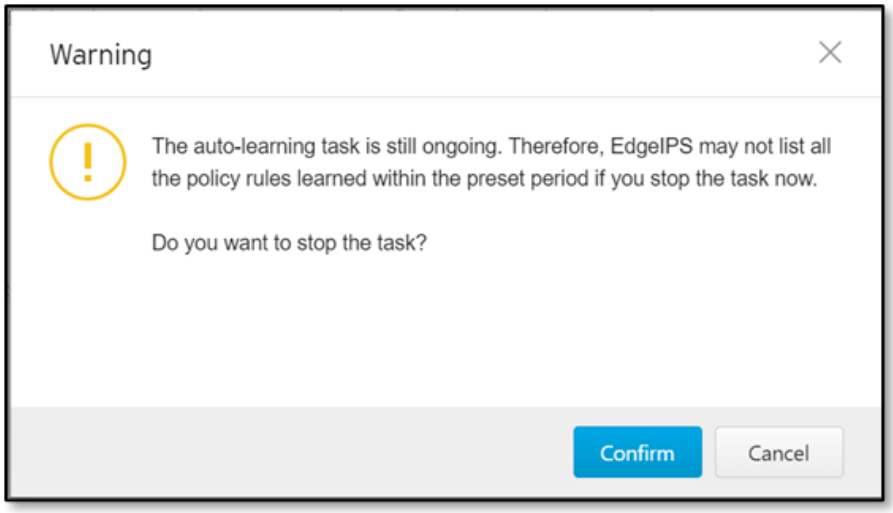
Procedure

1. When the learning task is in progress, go to [Security] > [Policy Rule Auto-Learning].

2. On the [Policy Rule Auto-Learning Task] pane you will see the [Stop the Task] and [Cancel the Task] buttons.

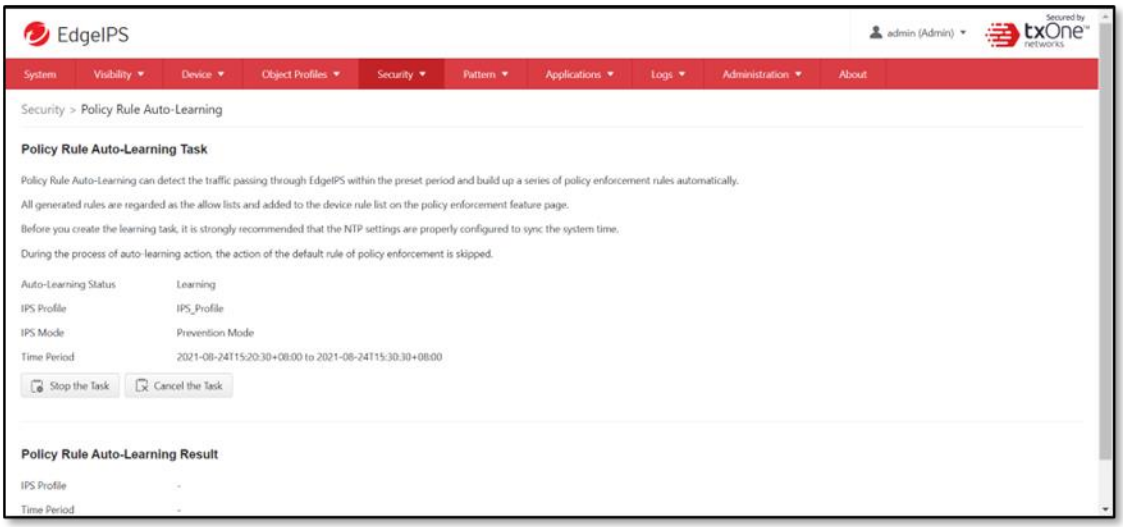
3. Click the [Stop the Task] button to stop the auto-learning task.

4. A warning message will show up for confirmation.



5. Click [Confirm] to stop the task. The learning result will still be generated for your review.

7.4.3 Canceling Policy Rule Auto-Learning



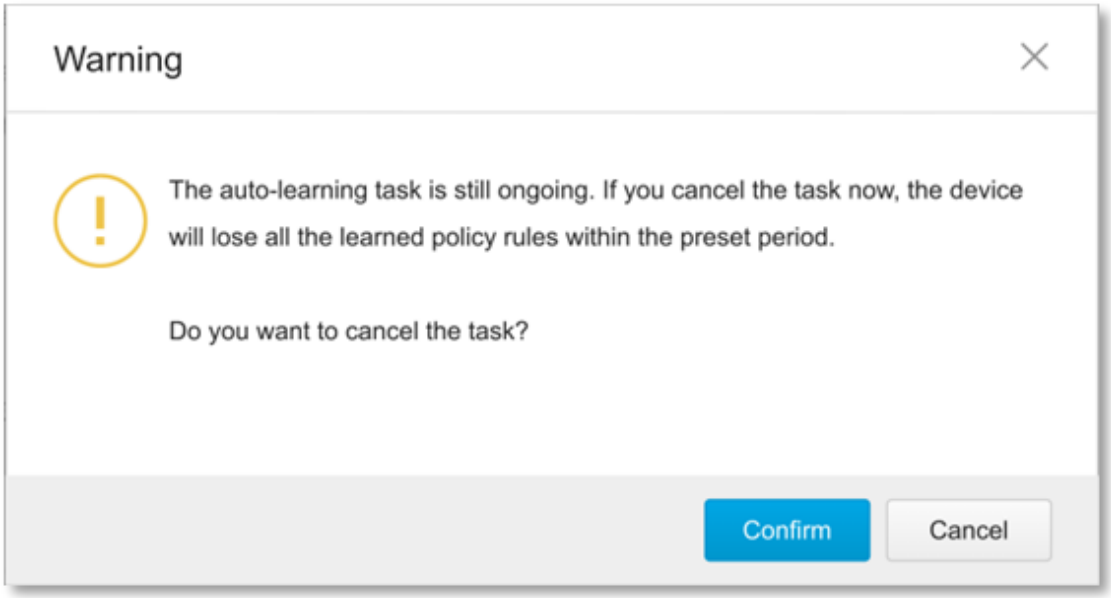
Procedure

1. When the learning task is in progress, go to [Security] > [Policy Rule Auto-Learning].

2. On the [Policy Rule Auto-Learning Task] pane you will see the [Stop the Task] and [Cancel the Task] buttons.

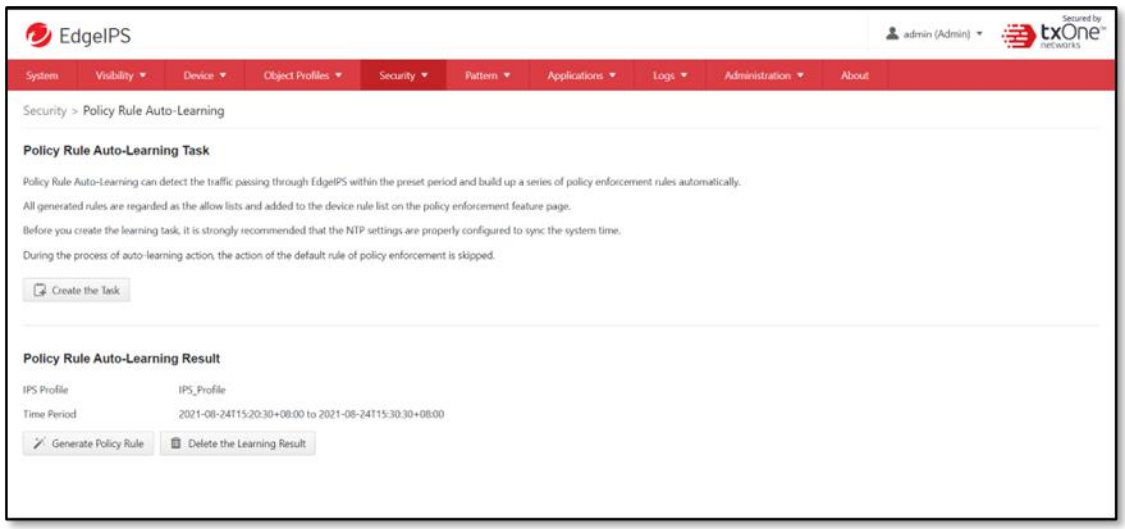
3. Click the [Cancel the Task] button to cancel the auto-learning task.

4. A warning message will show up for confirmation.



5. Click [Confirm] to cancel the task. Note that if you cancel the task, the learning result will be erased.

7.4.4 Generating the Learning Results

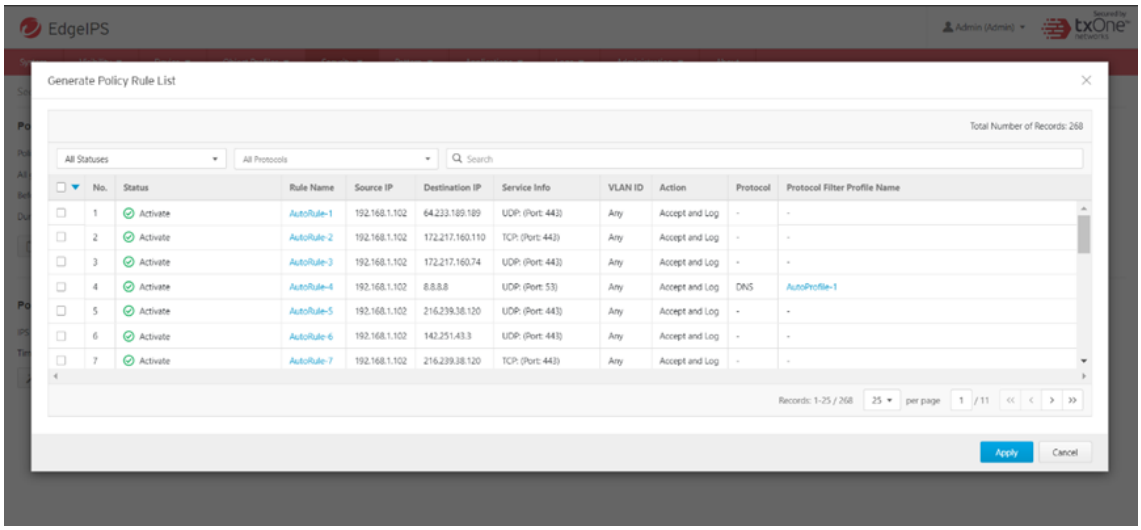


Procedure

1. During the learning task process, go to [Security] > [Policy Rule Auto-Learning].

2. In the [Policy Rule Auto-Learning Result] pane you will see the [Generate Policy Rule] and [Delete the Learning Result] buttons.

3. Click the [Generate Policy Rules] button to generate the policy rule list for review.

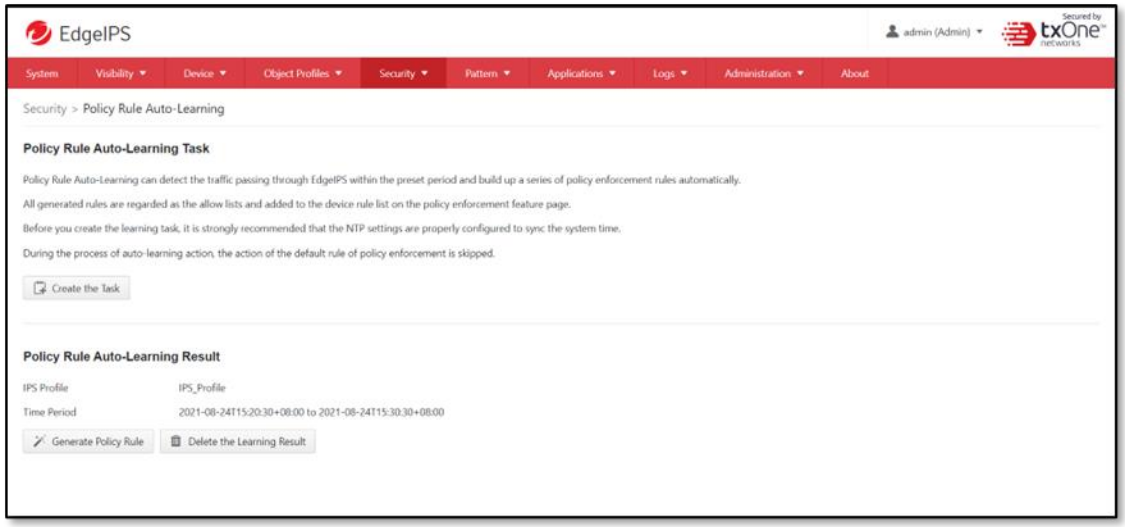


4. You can activate or deactivate policy rule(s) by clicking the checkbox on the left of the window before you apply the generated the policy rule(s) as a trust list.

5. Click [Apply] and the policy rule list will be generated and moved to the device rule list on the policy enforcement page.

On [Generate Policy Rule List], you can only review the policy rule(s) and the protocol filter profile(s) and edit rule names.

7.4.5 Deleting the Learning Results



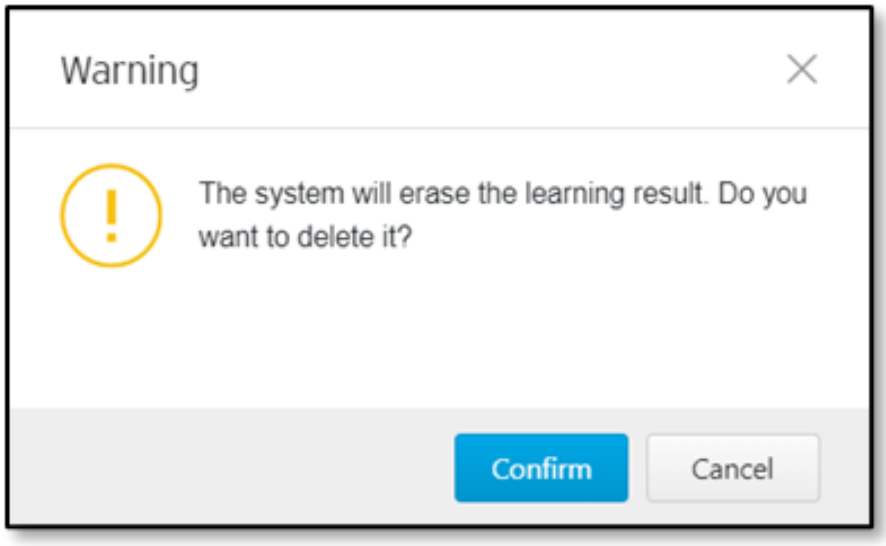
Procedure

1. After the learning task is completed, go to [Security] > [Policy Rule Auto-Learning].

2. In the [Policy Rule Auto-Learning Result] pane you will see the [Generate Policy Rule] and [Delete the Learning Result] button.

3. Click the [Delete the Learning Result] button.

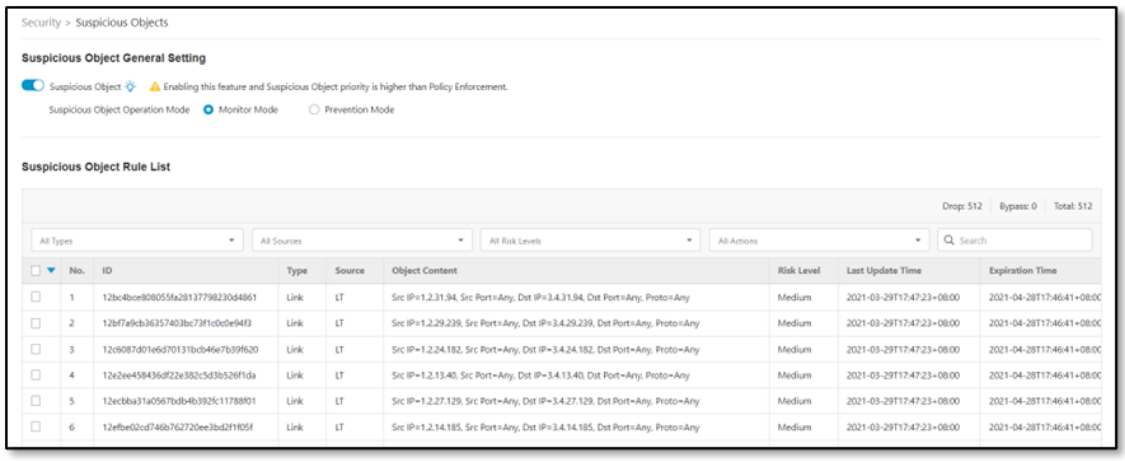
4. A warning message will show up for confirmation.



5. Click [Confirm] to delete all learned results.

7.5 Suspicious Objects

Suspicious Objects feature allows you to define a custom node-based/link-based Suspicious Object List from ODC. If any identical IP address or MAC address on the node level, or identical IP address, protocol and port numbers on the link level are detected, the activity will be allowed or blocked according to your pre-defined action for the suspicious object.



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

7.5.1 Configuring Suspicious Objects

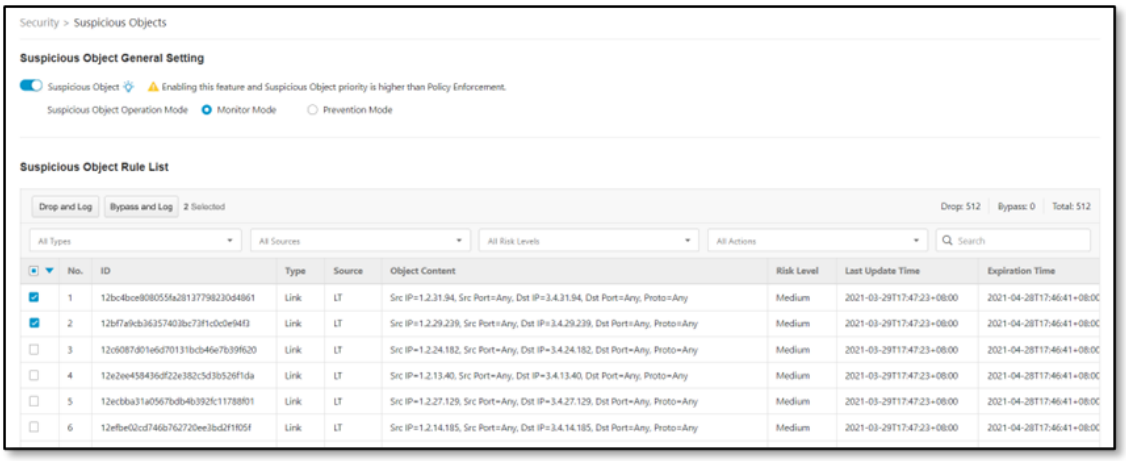
Procedure

1. Go to [Security] > [Suspicious Objects].

2. Under the [Suspicious Objects] tab, you will see the [Suspicious Object General Settings] pane.

3. Use the toggle to enable or disable the suspicious object feature.

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



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

The following table summarizes the settings.

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

The Suspicious Objects list is of higher priority than the device rule and the master rule lists for Policy Enforcement.

8 The Pattern Tab

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

8.1 Viewing Device Pattern Information

Procedure

1. Go to [Pattern] > [Pattern Update].

2. Under the [Pattern Update] tab you will see the following [IPS Pattern Update] and [Antivirus Pattern Update] panes.

3. The [IPS Pattern Update] pane shows [Pattern Version] and [Pattern Build Date] of the current IPS pattern.

8.2 Manually Updating the Pattern

Procedure

1. Go to [Pattern] > [Pattern Update].

2. Under the [Pattern Update] tab you will see the following [IPS Pattern Update] pane.

3. Click [Select].

4. Manually select the pattern to be deployed to the device.

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

8.3 Downloading Release Notes

Procedure

1. Go to [Pattern] > [Pattern Update].
2. Click the [Release Note] download button to see detailed release information.

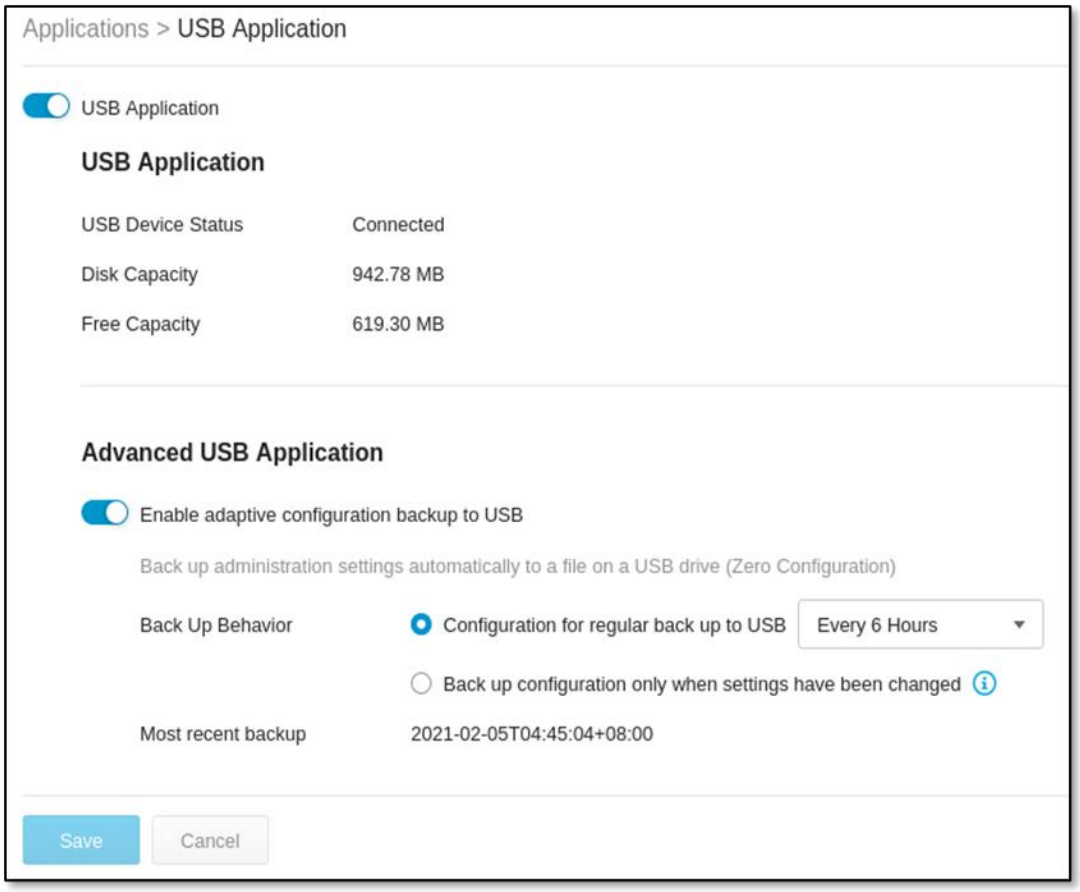
9 The Application Tab

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

9.1 USB Application

Procedure

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



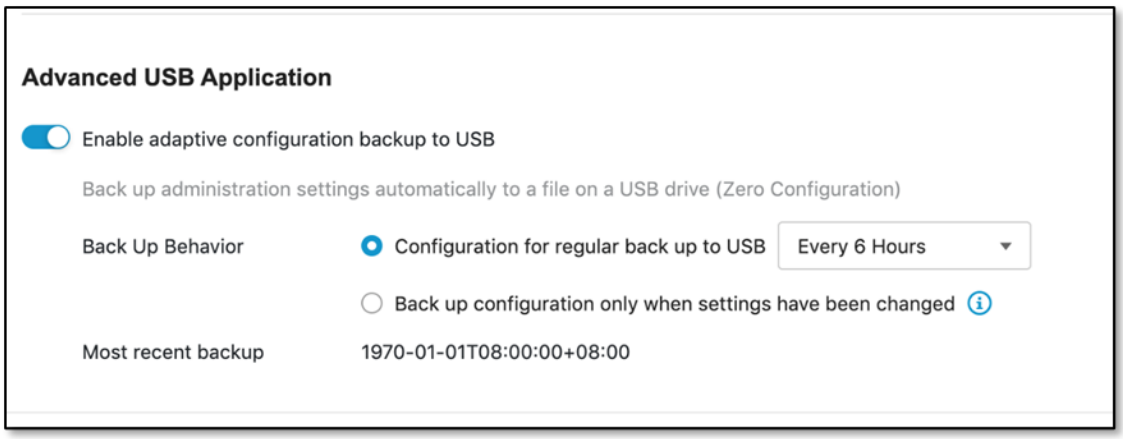
3. Click the toggle to enable USB Application usage.
4. Once the USB Application function is enabled and a USB disk is plugged in, you can see the status and view the information about the disk capacity and remaining free space.

⚠	If the USB Application function is disabled, the USB port on the front panel will not be active and cannot be used.

📖	Regarding the supported USB devices, please refer to *Supported USB Devices*.

9.1.1 Advanced USB Application

1. Click [Enable] to enable adaptive configuration backing up to a USB-based device.



2. Backup behavior can be configured as follows:

   a. Periodic backup of a configuration to USB – 6 different time periods are supported.

   b. Back up configuration to USB disk when configurations are changed.

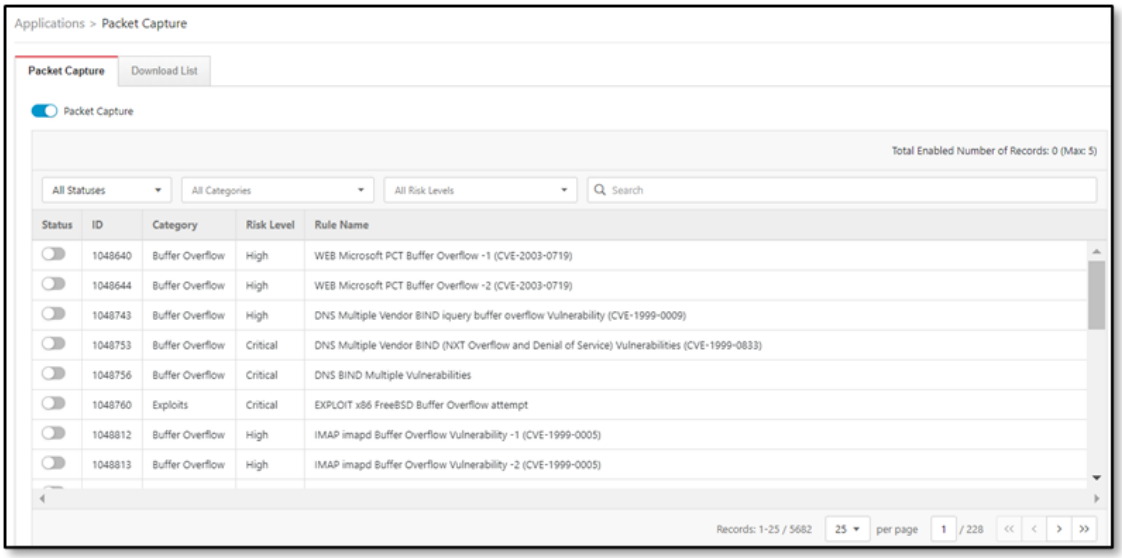
9.2 Packet Capture

The Packet Capture feature allows you capture packets for further analysis and to configure the capture of packets by IPS event rules. Packets that trigger 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.

9.2.1 Enabling Packet Capture

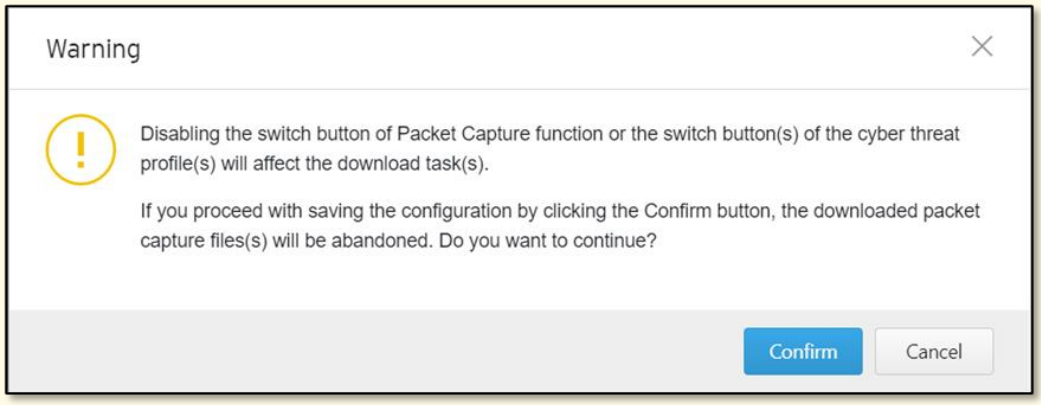
Procedure

1. Go to [Application] > [Packet Capture].



2. Enable the Packet Capture function by clicking the toggle.

Disabling the previously enabled Packet Capture function will cause previously downloaded packet captures to be deleted.



3. Once the function is enabled, you would see the entire IPS rule list. Select and enable a rule for IPS rule capture.

4. Up to 10 rules can be selected for IPS Rule packet capture support.

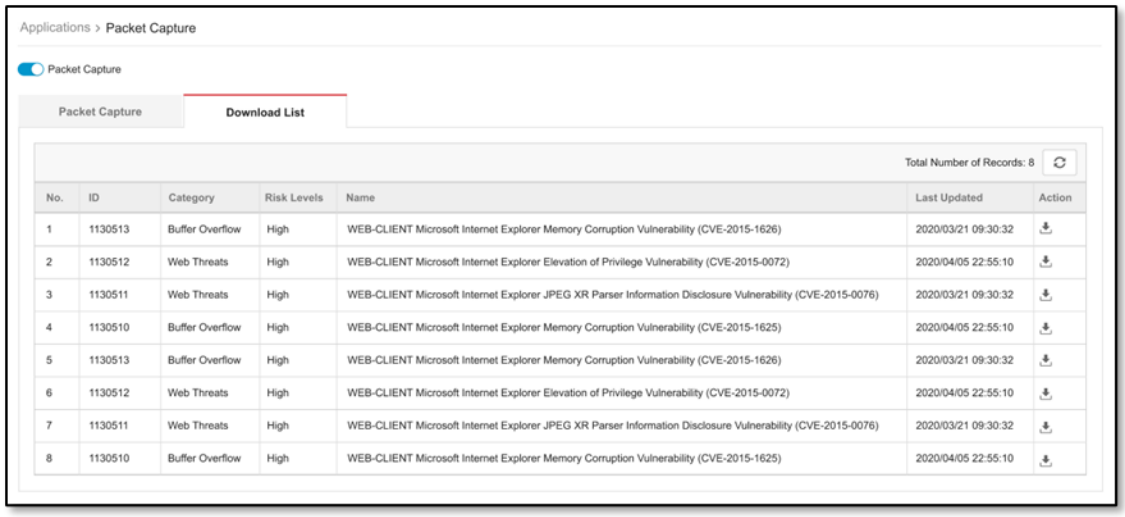
The packet capture feature will save the selected IPS Rule event packets once the IPS rule is hit and will only save the last 5 occurrences of a particular rule. Older events will be overwritten.

9.2.1.1 Downloading Captured Packet

Procedure

1. Go to [Application] > [Packet Capture]

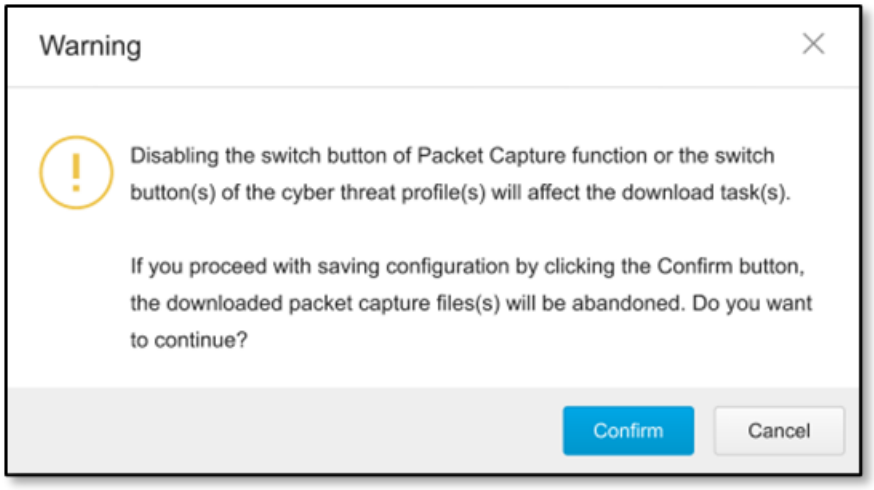
2. Click [Download List] to show a list of IPS rules where you can download a zip archive of each rule's related pcap files.



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 below warning will be shown to the user.



The download list will be refreshed every 10 seconds. If you want to get the latest update, please click the [manual] refresh button.

10 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 management console:

- Cyber Security Logs
- Policy Enforcement Logs
- Protocol Filter Logs
- File Filter Logs
- Suspicious Object Logs
- Assets Detection Logs
- System Logs
- Audit Logs

10.1 Viewing Cyber Security Logs

Cyber Security logs contain details about cyber security events detected by both Intrusion Prevention and Denial of Service Prevention features.

Procedure

Go to [Logs] > [Cybersecurity Logs].

The following table describes the Cyber Security log information.

Field	Description
Time	The time when 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.
TID	MITRE TID Information
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.

Field	Description
	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 the protocol is TCP/UDP. The ICMP code of the packet if the 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.
Count	The number of detected network packets within the detection period after the detection threshold is reached.

10.2 Viewing Policy Enforcement Logs

Policy Enforcement logs are generated 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 Policy Enforcement log information.

Field	Description
Time	The time when 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.

Field	Description
	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.

10.3 Viewing Protocol Filter Logs

Protocol Filter logs contain details about network traffic 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 protocol filter log information.

Field	Description
Time	The time when 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.
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.

Field	Description
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.

10.4 Viewing File Filter Logs

File Filter logs contain details about network traffic 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 and Antivirus Logs]

The following table describes the log table.

Field	Description
Time	The time when 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.

10.5 Viewing Suspicious Object Logs

Suspicious Object logs contain details about network traffic detected by the [Suspicious Objects] feature.

Procedure

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

The following table describes the suspicious object log information.

Field	Description
Time	The time when the log entry was created.
ID	The hash ID of the matched suspicious object.
Type	The suspicious object type, which is node type or link type.
Source	The source of suspicious object
Risk Level	The threat level of suspicious object
Expiration Time	The expiration time of the suspicious object. When the expiration time reaches, the suspicious object will be deleted.
Interface	The physical port interface which receives the suspicious object
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the suspicious object settings.
Count	The number of detected suspicious object within the detection threshold.

10.6 Viewing Assets Detection Logs

Asset detection logs contain details about the system status changes of the managed assets.

Procedure

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

The following table describes the asset detection log information.

Field	Description
Time	The time when 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 IP address of the asset.

10.7 Viewing System Logs

System logs contain details about system events on the device.

Procedure

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

The following table describes the system log information.

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

10.8 Viewing Audit Logs

Audit logs contain details about user access, configuration changes, and other events that occurred when the device is operating.

Procedure

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

The following table describes the audit log information.

Field	Description
Time	The time when 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 audit logs, please log in with the default “audit” account.

11 The Administration Tab

This chapter describes the available administrative settings for the Edge Series device.

11.1 Account Management

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 by using custom user accounts.

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

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

11.1.1 User Roles

The following table describes the permissions matrix for user roles.

		User Role			
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

		User Role			
QoS	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Logs - excluding 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

11.1.2 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

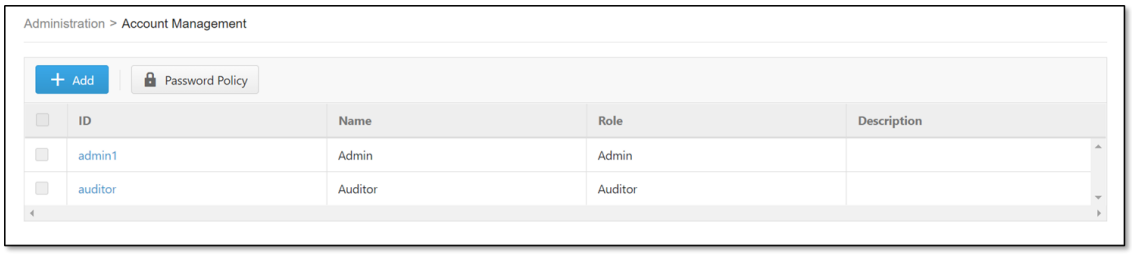
The built-in user accounts cannot be deleted from the device. Ensure that the passwords of the built-in accounts are changed when you first set up the device.

11.1.3 Adding a User Account

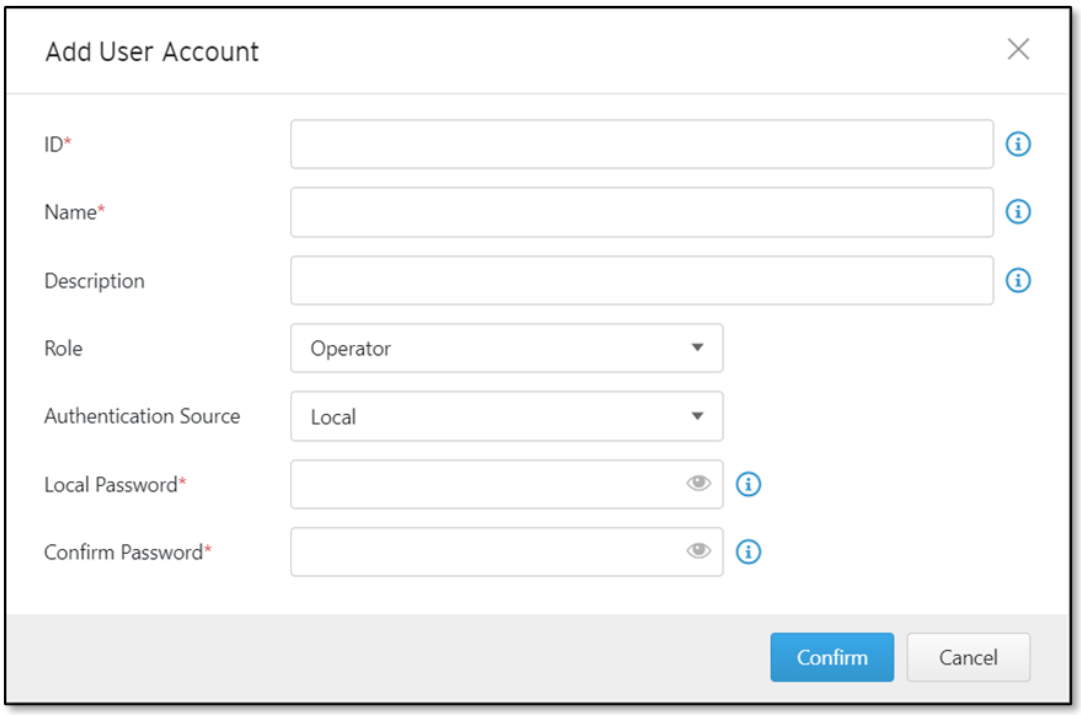
When you log in using the administrator account (admin), you can create new user accounts to access the system.

Procedure

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



2. Click [Add]. The [Add User Account] window 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*.

4. Click [Save].

11.1.4 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. Modify the password settings.
   - Current password
   - New password
   - Confirm password
4. Click [OK].

11.1.5 Configuring Password Policy Settings

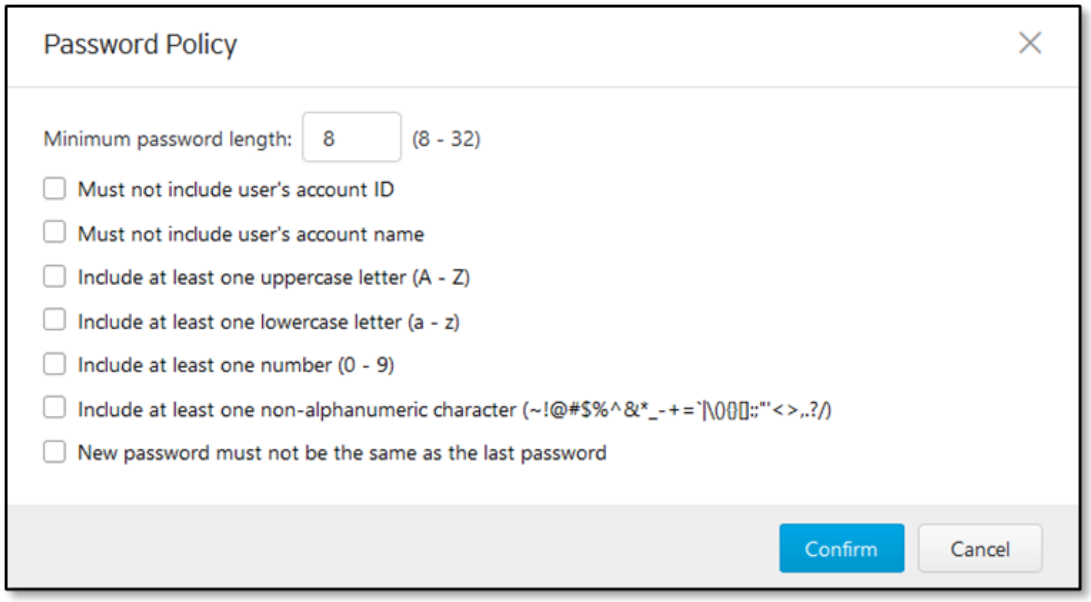
By configuring password policy settings, users may enhance web console access security.

Configure 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 a user submits a new password, the password policy determines whether the password meets your company's established requirements. If strong passwords are required, 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 that would increase their vulnerability to threats. When establishing a password policy, balance the necessity of highly secured password with the utility of easily-recalling password 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 multiple options that meet your required password policy.
4. Click [Confirm].

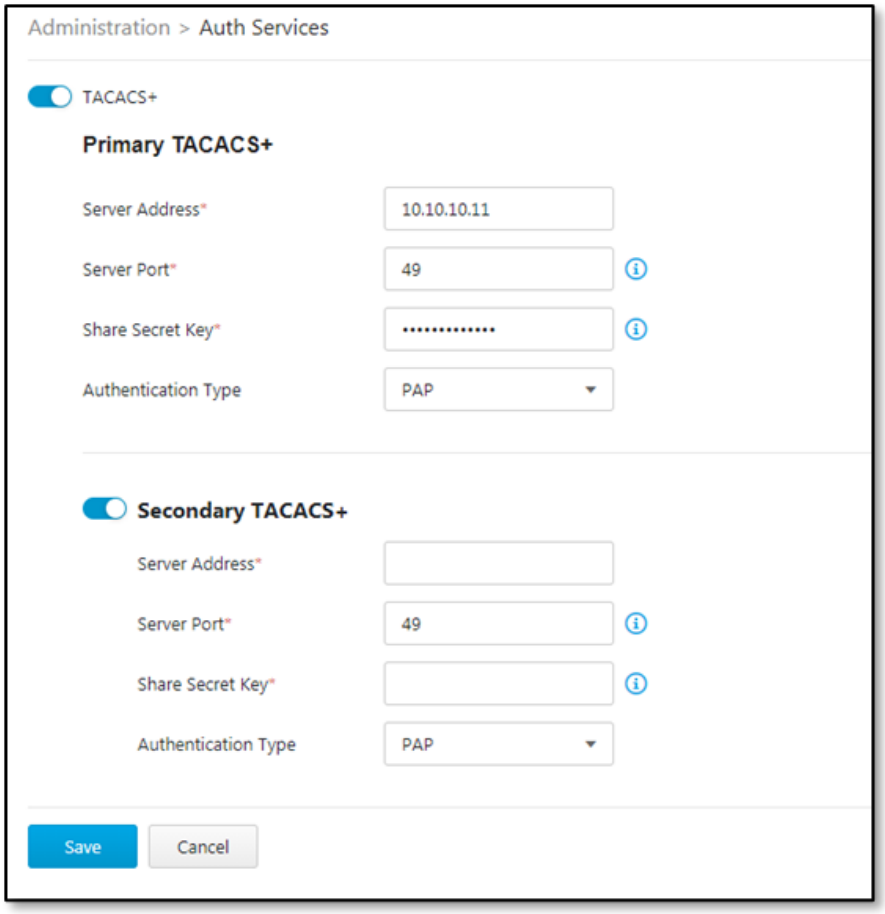
11.2 Auth Service

Use the [Auth Services] tab to configure the TACACS+ of the device.

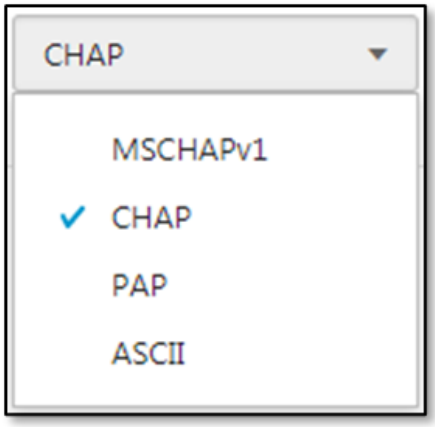
11.2.1 Configuring TACACS+

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 following settings:
   - Configure Server address.
   - Configure Server Port (Default port: 49).
   - Configure Share Secret Key (Maximum length 64 characters).
   - Select an authentication type from the following list:



   - Enable Secondary TACACS+ Server if necessary.
4. Click [Save].

11.3 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

11.3.1 Configuring Device Name and Device Location Information

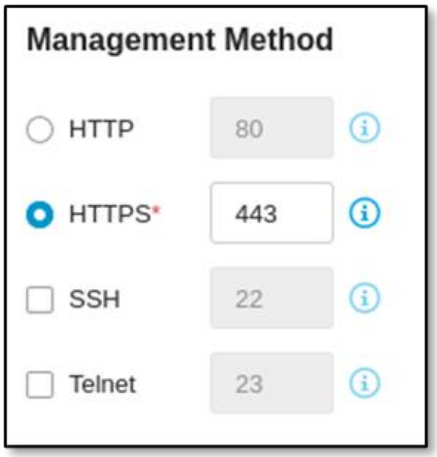
Procedure

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

11.3.2 Configuring Management Protocols and Ports

Procedure

1. Go to [Administration] > [System Management].
2. In the [Management Method] pane:
    - Select the protocols that are allowed to be used.
    - 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.

11.3.3 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. If the connection between the Edge Series device and your network is not stable or is disconnected, enable the toggle to ping to the Management Interface.

11.4 Sync Settings

This Edge Series device can be managed by a TXOne ODC (Operational Technology Defense Console). Use this tab to register your device to a TXOne ODC.

11.4.1 Enabling Management by ODC

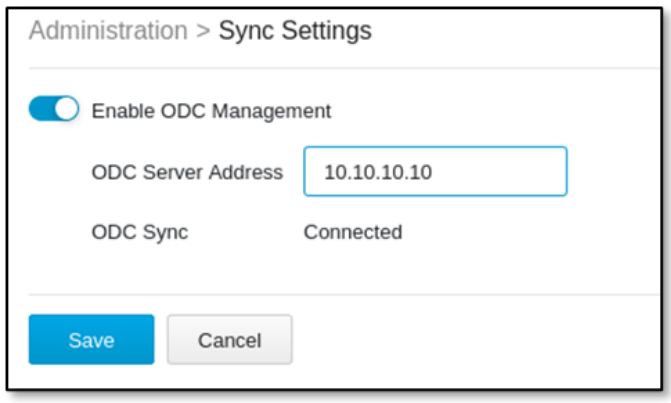
Procedure

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

2. In the pane:

Use the toggle to enable management by ODC.

Input the IP address of the ODC server.

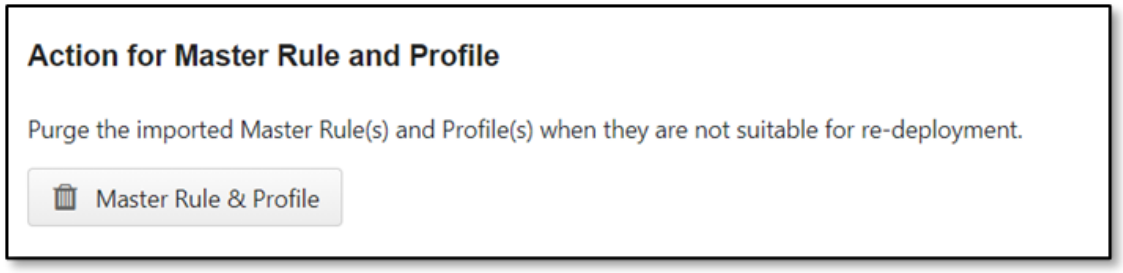


11.4.2 Action for Master Rule and Profile

Procedure

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

2. Click the [Master Rule & Profile] button to delete Object Profiles and Policy Enforcement rules synced from ODC.



11.5 Syslog

The system of this Edge Series device 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 the device.

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

11.5.1 Configuring Syslog Settings

Procedure

1. Go to [Administration] > [Syslog].

Field	Description
Server address	Type the IP address of the Syslog server.
Port	Type the port number.
Protocol	Select a protocol for the communication.
Format	Select a syslog format: CEF or LEEF
Facility Level	Select a facility level to determine the source and priority of the logs.

Field	Description
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*.

4. Click [Save].

11.5.2 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 lead to a large amount of Syslog traffic in a busy network. Use with caution.

11.5.3 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

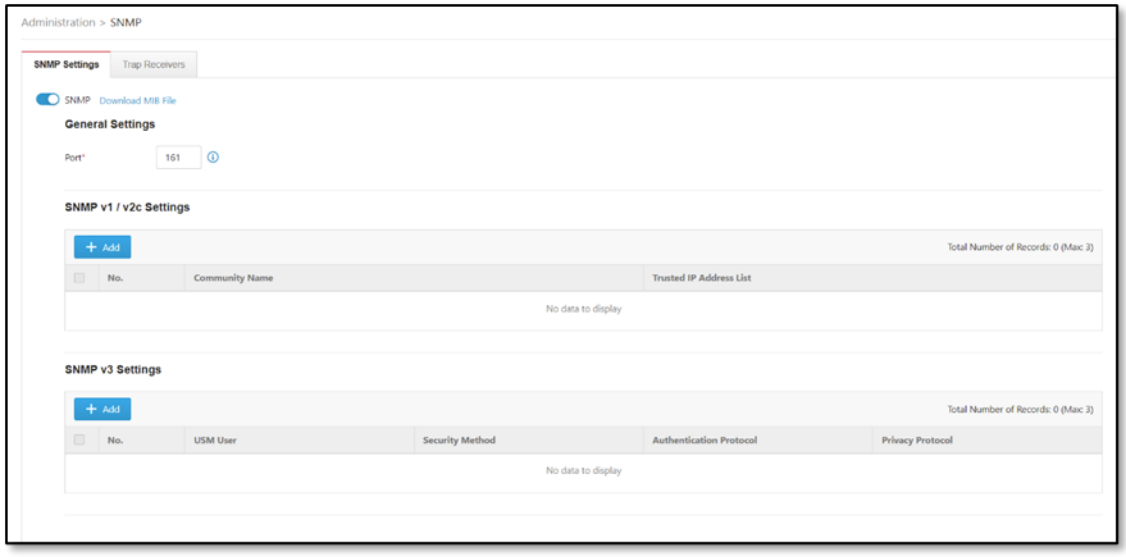
Policy Enforcement/Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
	High	2 – Critical
		3 – Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

11.6 SNMP

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

Procedure

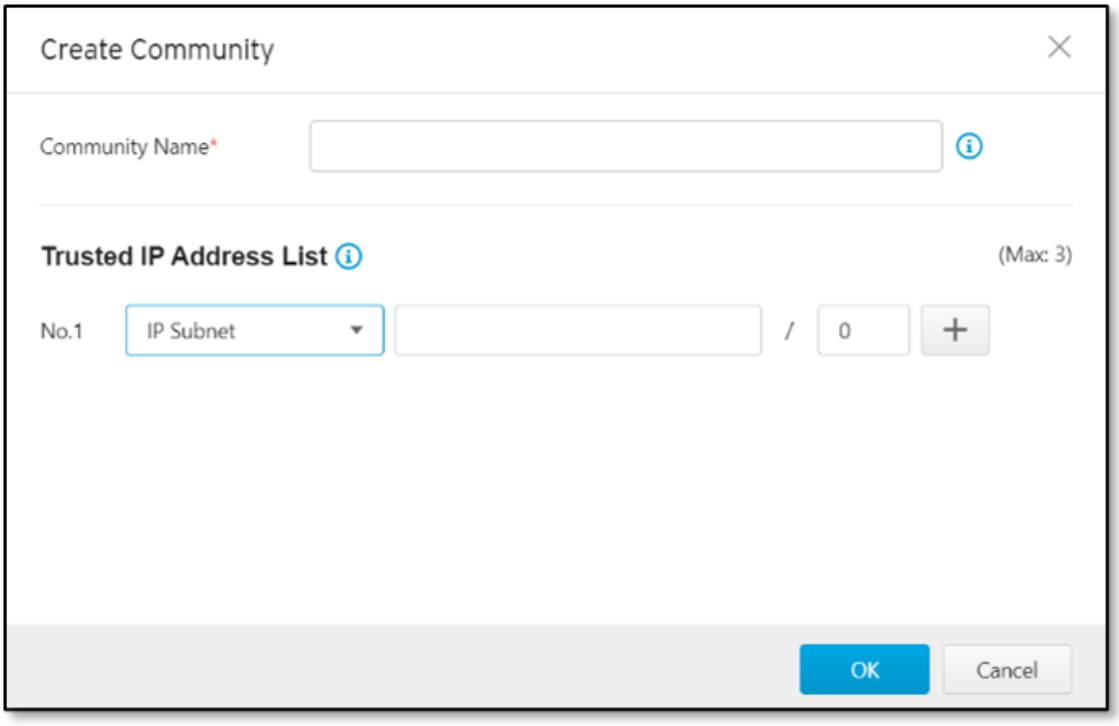
1. Go to [Administration] > [SNMP].
2. Click the toggle to enable the SNMP function.
3. Under [General Settings], you can change SNMP port. The default setting is Port 161.
4. You can click the [Download MIB file] link to download the EdgeIPS Pro MIB file.



11.6.1 Configuring SNMPv1/v2c

Procedure

1. Go to [Administration] > [SNMP].
2. Click [Add] to create a SNMP v1/v2c community and configure the settings.



a. Enter Community name.

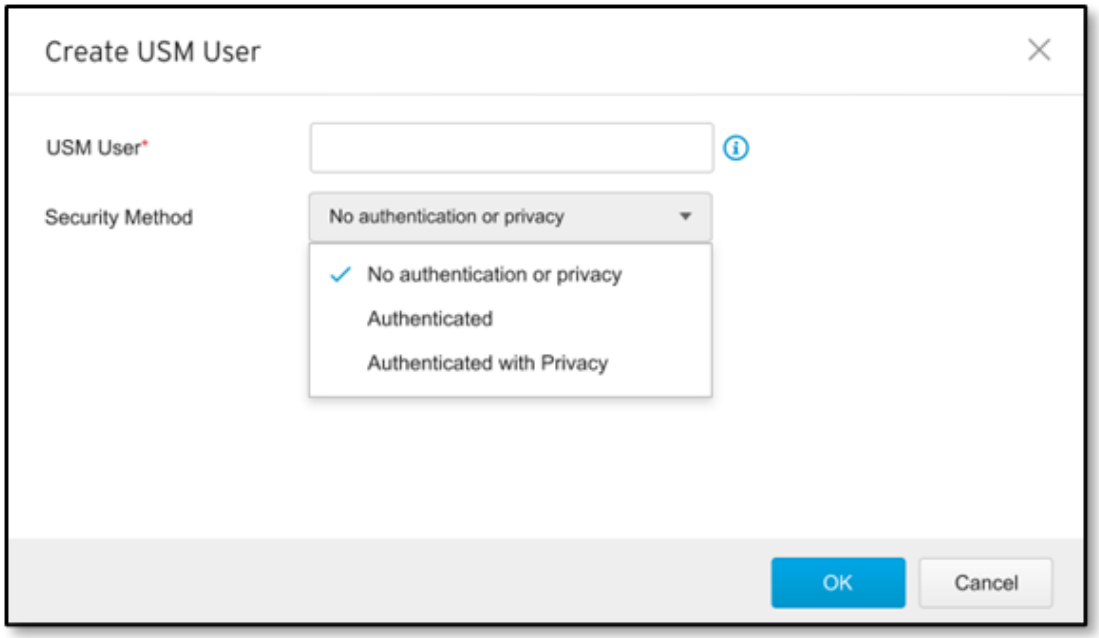
b. Add a Trusted Address list. There are two supported types: Single IP and IP Subnet.

c. Click [OK] to create a new SNMP v1/v2c community.

11.6.2 Configuring SNMPv3

Procedure

1. Go to [Administration] > [SNMP].
2. Click [Add] to create an SNMP v3 USM User and configure the settings.



3. Enter USM user.

4. Under [Security Method], select one of the following options:

   a. No authentication or privacy.

   b. Authenticated – including SHA and MD5. You can select an appropriate authentication protocol and enter an Authentication Key.

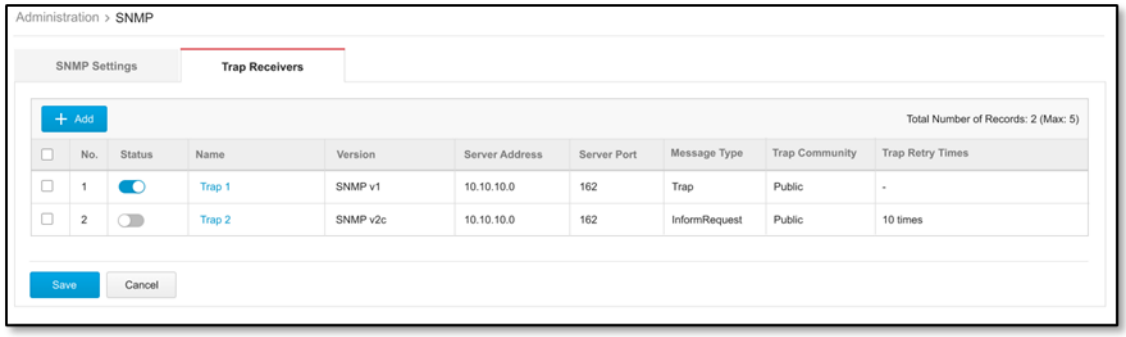
   c. Authenticated with Privacy – also including SHA and MD5. You can select appropriate authentication and privacy protocols.

5. Click [OK] to create an SNMPv3 USM User.

11.6.3 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 an SNMP version, **SNMP v1** or **SNMP v2c**.

   e. Enter [Server Address].

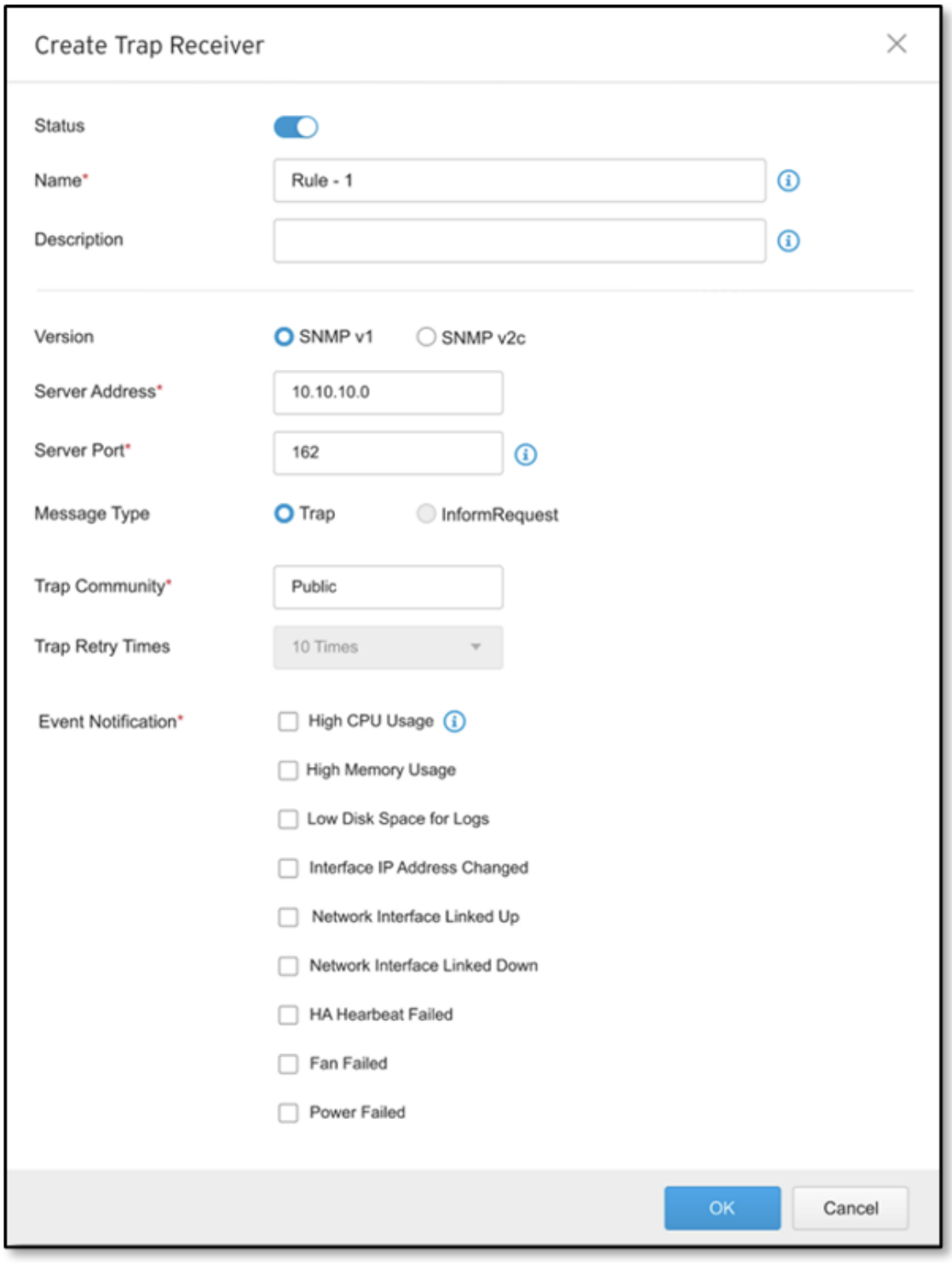
   f. Enter [Server Port]. The default setting is port 162.

   g. Select a message type, **Trap** or **informRequest**.

   h. Enter Trap Community. The default name is PUBLIC.

   i. Trap Retry Times: The amount of retries ranges from 1 to 10 times.

   k. Select what will trigger an Event Notification.



1. When the CPU usage reaches 70%, 80% or 95%, the system will send an event notification.
2. When the memory usage reaches 80%, the system will send an event notification.
3. When the log storage reaches 95%, the system will keep sending event notifications until the log storage is below 95%.

4. When the fan fails, the system will keep sending event notifications until the fan status is recovered.
5. When the power fails, the system will keep sending event notifications until the power status is recovered.

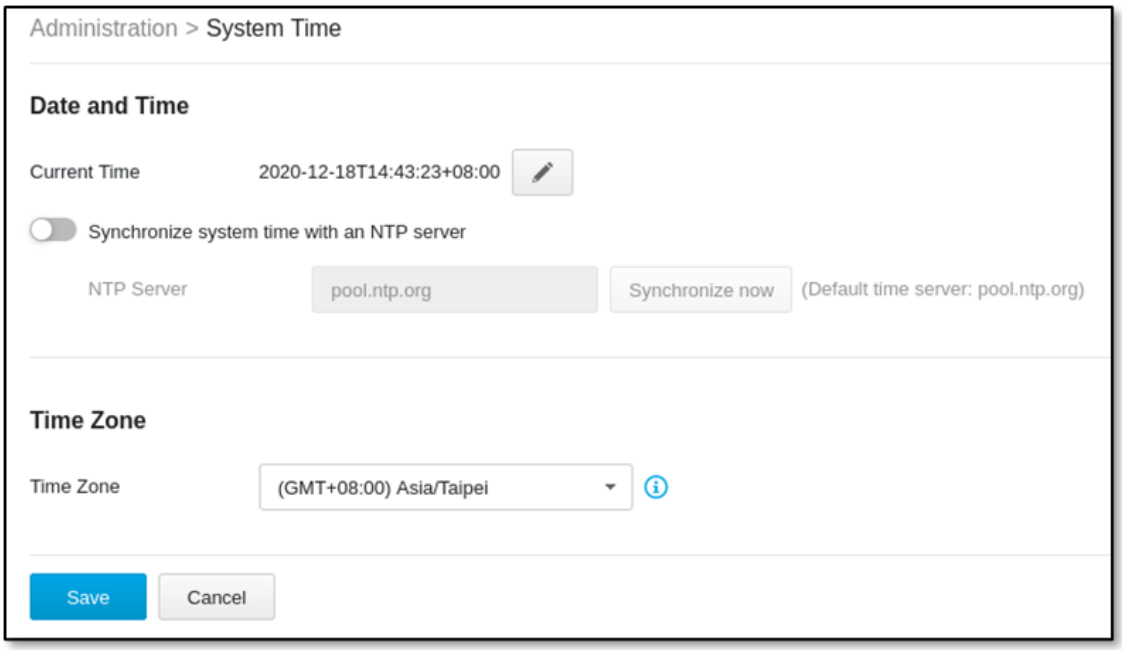
11.7 System Time

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.

11.7.1 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 select the date and time.

   b. Set the hour, minute, and second.

   c. Click [Apply].
3. From the [Time Zone] drop-down list, select a time zone.
4. Click [Save].

ODC system synchronizes the system time with its managed instances.

11.8 Backup/Restore

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

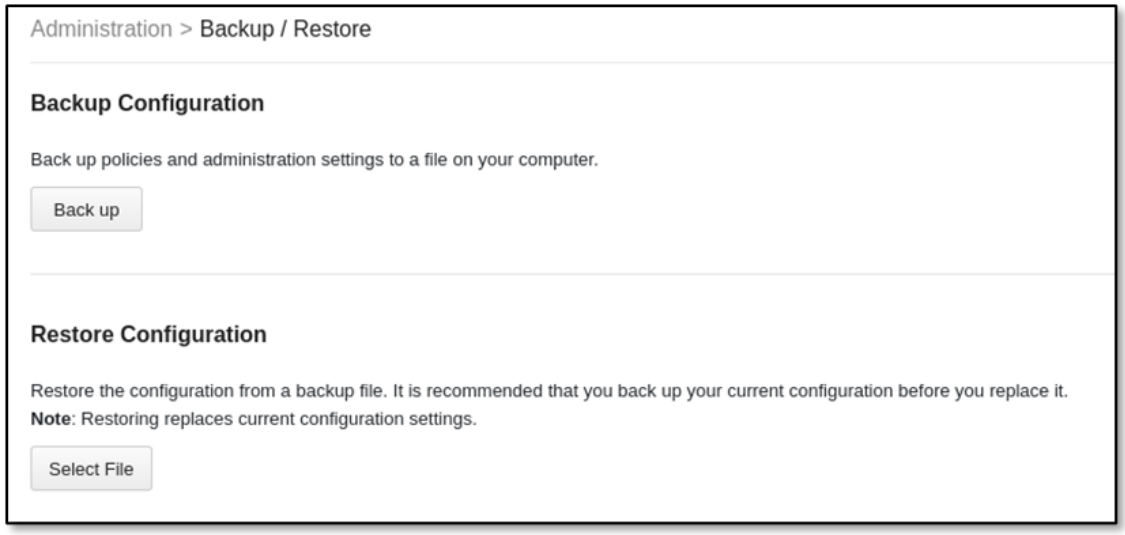
We recommend the following:

- Backing up the current configuration before each import operation.
- Performing the backup operation when the device is idle. Importing and exporting configuration settings affect the performance of your device.

11.8.1 Backing Up Device Configuration

Procedure

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



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

11.8.2 Restoring Device Configuration

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.

11.9 Firmware Management

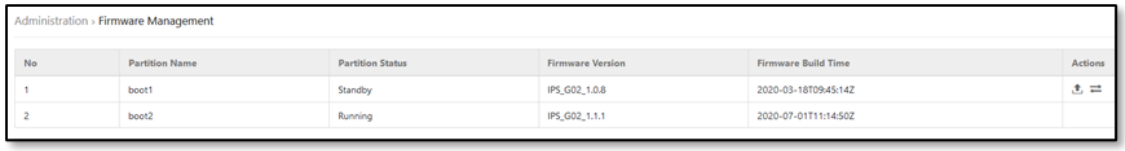
Use the [Firmware Management] tab to:

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

11.9.1 Viewing Device Firmware Information

Procedure

1. Go to [Administration] > [Firmware Management]. The [Firmware Management] page will appear.



The device can have up to two firmwares to be 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.

11.9.2 Updating Firmware

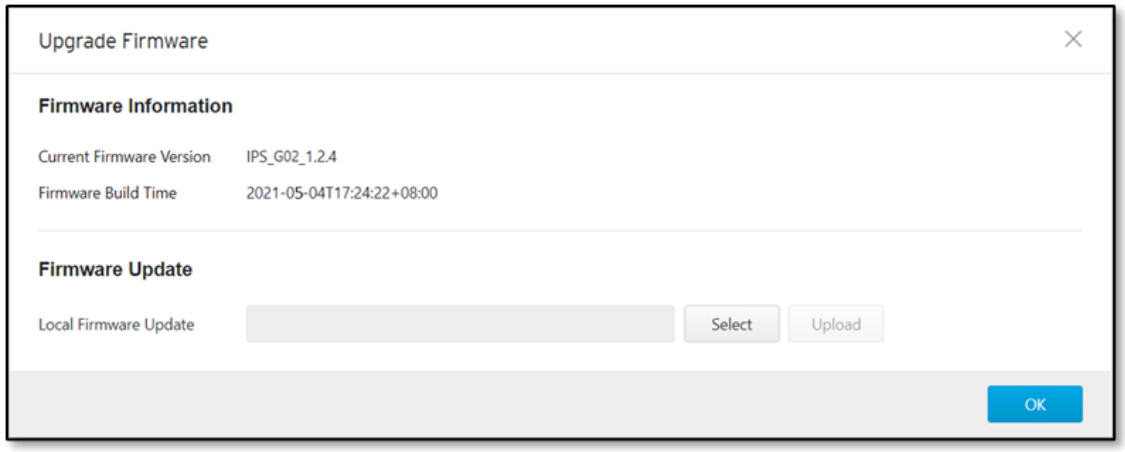
Procedure

1. Go to [Administration] > [Firmware Management]. The [Firmware Management] page will appear.

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.

3. In the [Firmware Update] pane, click [Select] to import a firmware file from your local device, and then click [Upload] to install the firmware to the partition on [Standby].

4. Click [OK].

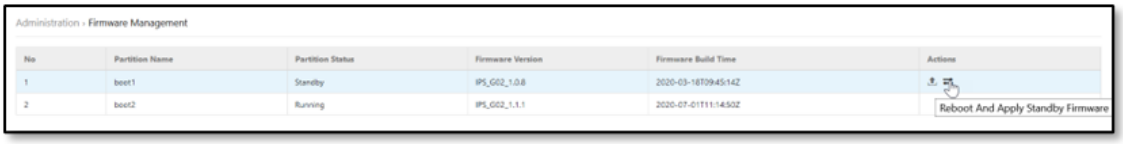


11.9.3 Rebooting and Applying Firmware

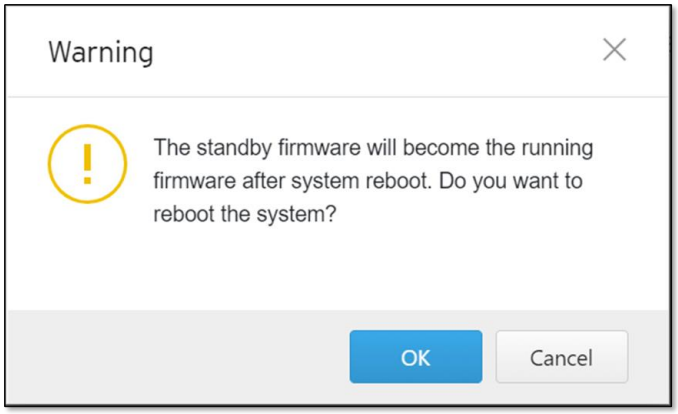
To boot into an upgraded firmware or to revert to a previous firmware, you would need to boot into the [Standby] partition and load the firmware from it.

Procedure

1. Go to [Administration] > [Firmware Management]. The [Firmware Management] page will appear.



3. The below warning will be shown to the user. Click [OK] to proceed with rebooting into the [Standby] partition and making it the [Running] partition.



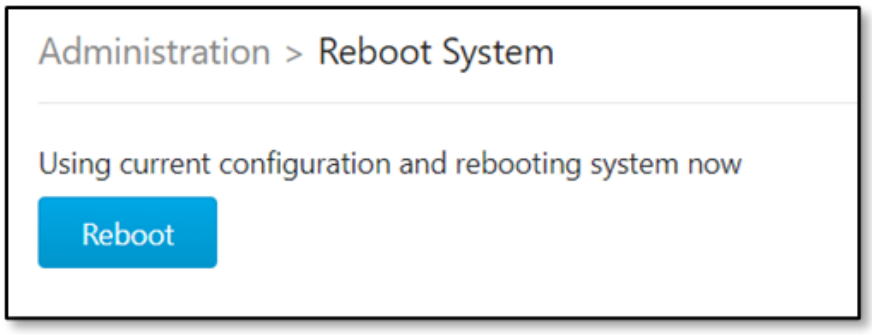
11.10 Reboot System

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

11.10.1 Rebooting the System

Procedure

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



12 Supported USB Devices

This chapter describes the use of supported USB devices with the Edge Series device for extended or supported functions.
To ensure optimal operation, only the USB devices listed below are currently supported. This list may be updated from time to time. Please visit Trend Micro's support page for an up-to-date list.

#	Model		Device Type
1	MOXA Backup Configurator (ABC-02 Series) Model: ABC-02-USB-T		USB Disk Drive
2	Innodisk Industrial USB 2.0 16GB (USB Drive 2SE)		USB Disk Drive
3	Apacer industrial USB disk 16GB (AH355)		USB Disk Drive

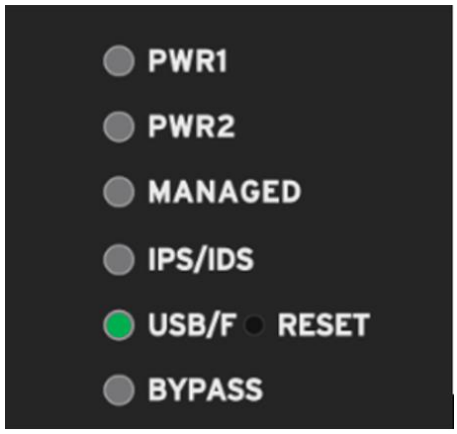
12.1 Supported Actions via USB Disk

> ⚠ Given that this feature allows anyone with a supported USB disk device to perform various operations via the USB, the physical security of your Edge series device must be considered carefully. Only supported USB disk devices may be used for this feature.

Procedure

1. Plug the supported USB disk device into the Edge series device's USB port.

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



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

3. The function of the reset button will also change until the USB device is unplugged. When a USB device is plugged in, the reset button will 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 during this time.

4. Users 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	Color/State
Default State – USB Plugged in Backup Configuration	USB/F	Green – Steady
Load/Restore Pattern	IPS/IDS	Green – Blinking (1/sec)
Load/Restore Configuration	MANAGED	Green – Blinking (1/sec)
Load/Restore Firmware	IPS/IDS & MANAGED	Green – Blinking (1/sec)

5. After selecting an action, you must confirm the action by pressing the Reset button for more than 3 seconds (a long and steady press).

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

6. If an action is being attempted and there is a USB disk data transfer, the following LEDs will indicate it as shown below and then return to previous states after data transfer is complete.

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

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

Error Indication (on any error while action was being processed)	LED	Color/State
	USB/F	Red – Steady

An error can only be cleared if:

1. the reset button is pressed once more (LEDs return to default states 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 not. If an action is successful, LEDs will be restored to their default states 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 states prior to the USB disk device being plugged in (“USB/F” LED off), and a log will be available in system logs.

12.1.1 On-Demand Configuration Backup

Procedure

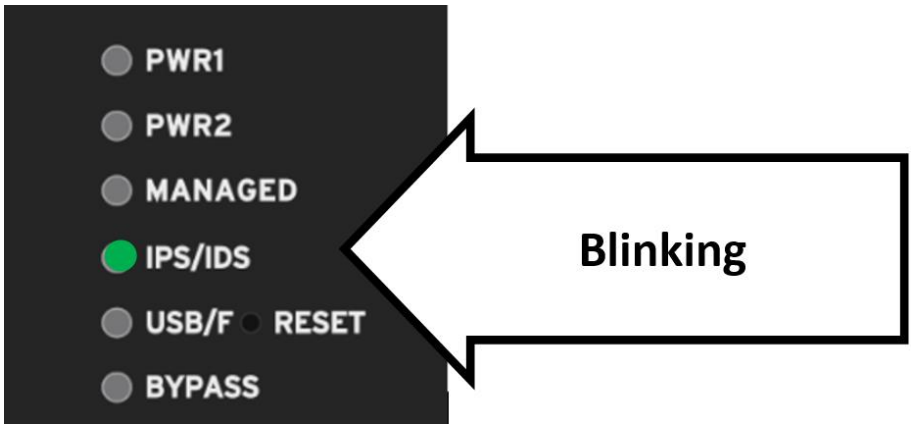
1. In the “Default Action” state, on-demand configuration backup to disk can be performed by holding down the reset button for more than 10 seconds. During file transfer, the USB/F LED may blink. However, since configuration files are usually not very large, this process may finish quickly.

2. Save the current running configuration 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**”.

3. After you have saved the config, if successful, the USB app will return to the “Default Action” state. If any error occurs, the USB/F LED will turn red. The system logs will also reflect whether the action was successful or not.

12.1.2 Loading Pattern from Disk

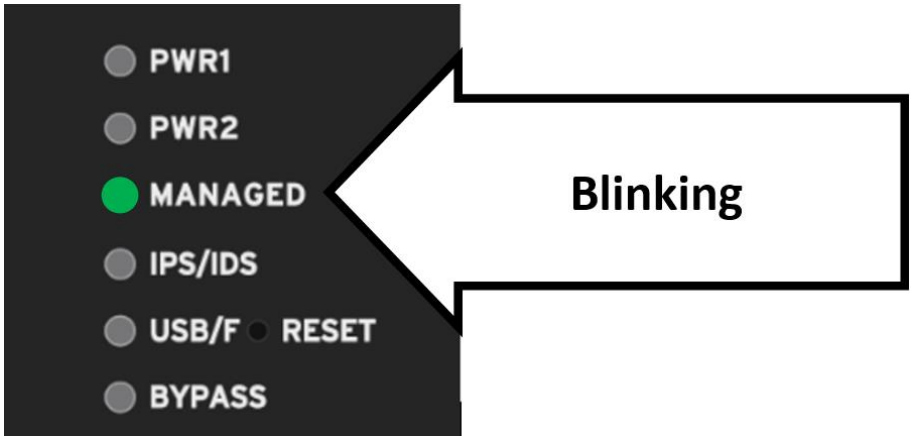
4. When the device is in the “Load Pattern” action state, the “IPS/IDS” LED will change to blinking green.



6. After the confirmation, the action will be attempted. If successful, the USB app will return to the “Default Action” state. If any error occurs, the USB/F LED will turn red. The system logs will also reflect whether the action was successful or not.

12.1.3 Loading Configuration from Disk

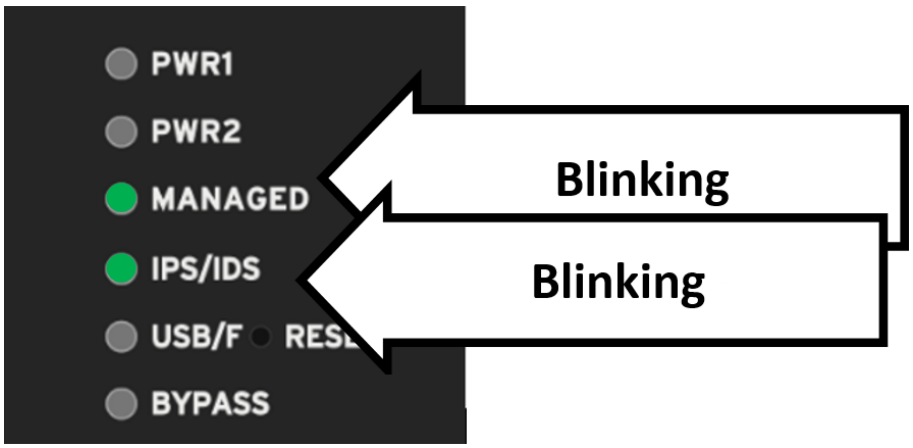
4. When the device is in the “Load Config” action state, the “MANAGED” LED will change to blinking green.



6. After the confirmation, the action will be attempted. If successful, the USB app will return to the “Default Action” state. If any error occurs, the USB/F LED will turn red. The system logs will also reflect whether the action was successful or not.

12.1.4 Loading Firmware from Disk

4. When the device is in the “Load Firmware” action state, the “MANAGED” and “IPS/IDS“ LEDs will change to blinking green.



6. After the confirmation, the action will be attempted. If successful, the USB app will return to the “Default Action” state. If any error occurs, the USB/F LED will turn red. The system logs will also reflect whether the action was successful or not.

13 Appendix A: 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