



EdgeIPS™ Pro 216

Administrator's Guide

Ver 1.3
2022-08-05

Copyright © 2022 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.



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

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

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

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

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

Table of Contents

Chapter 1	6
About EdgeIPS [™] Pro 216.....	6
Introduction	6
Main Functions.....	7
Multi-segmenting with Integrated Security	7
High Port Density and Flexible Deployment.....	7
Extensive Support for Industrial Protocols.....	7
Policy Enforcement for Mission-Critical Machines	7
Improve Shadow OT Visibility by Integrating IT and OT Networks	7
Intrusion Prevention and Intrusion Detection.....	7
Antivirus Protection.....	7
Switch Between Two Flexible Modes, ‘Monitor’ & ‘Prevention’	7
Top Threat Intelligence and Analytics	8
Easily Centralized Management with Convenient, Consolidated Overview	8
Chapter 2	9
Getting Started.....	9
Getting Started: Task List	9
Opening the Management Console.....	9
Changing the Administrator’s Password.....	11
Chapter 3	12
The System Tab	12
Device Information.....	12
Secured Service Status	13
Throughput / Connection.....	13
Bandwidth Utilization	13
Real Time Session Status.....	13
Packet Transmission Status	14
System Resources.....	14
Chapter 4	15
The Visibility Tab	15
Viewing Asset Information.....	15
Viewing Real Time Network Application Traffic.....	16
Chapter 5	17
The Network Tab.....	17
Configuring Device Settings	17
Configuring Port Settings	18
Configuring HA Settings	19
Configuring Port Mirror Settings	21
Chapter 6	22
The Object Profiles Tab	22
Configuring IP Object Profiles	22
Configuring Service Object Profiles.....	23
Configuring Protocol Filter Profiles	24
Specifying Commands Allowed in an ICS Protocol.....	25
Applying the Drop Malformed Option to an ICS Protocol.....	25
Advanced Settings	26
Advanced Settings for Modbus Protocol.....	26
Advanced Settings for CIP Protocol.....	29
Advanced Settings for S7Comm	32
Advanced Settings for S7Comm Plus.....	35
Advanced Settings for SLMP	37
Advanced Settings for MELSOFT	40
Advanced Settings for TOYOPUC.....	43
Advanced Settings for SMB	45
Configuring IPS Profiles	46
Configuring a Pattern Rule for Granular Control	47

Configuring File Filter Profiles	49
Configuring File Exclusions	50
Configuring Antivirus Profiles	53
Configuring File Exceptions	54
Chapter 7	56
The Security Tab	56
Policy Enforcement	56
Configuring Policy Enforcement	56
Adding Policy Enforcement Rules	57
Managing Policy Enforcement Rules	60
Port Security	60
Configuring Port Security	61
Suspicious Objects	65
Configuring Suspicious Objects	65
Chapter 8	67
The Pattern Tab	67
Viewing Device Pattern Information	67
Manually Updating the Pattern	67
Downloading Release Notes	68
Chapter 9	69
The Application Tab	69
USB Application	69
Advanced USB Application	70
Packet Capture	70
Enabling Packet Capture	70
Download Captured Packet	71
Chapter 10	72
The QoS Tab	72
Configuring Bandwidth MGMT	72
Chapter 11	73
The Logs Tab	73
Viewing Cyber Security Logs	73
Viewing Policy Enforcement Logs	74
Viewing Protocol Filter Logs	74
Viewing File Filter and Antivirus Logs	75
Viewing Suspicious Object Logs	76
Viewing Asset Detection Logs	76
Viewing System Logs	76
Viewing Audit Logs	77
Chapter 12	78
The Administration Tab	78
Account Management	78
User Roles	78
Built-in User Accounts	79
Adding a User Account	79
Changing Your Password	79
Configuring Password Policy Settings	80
Auth Services	80
Configuring TACACS+	80
System Management	81
Configuring Device Name and Device Location Information	82
Configuring Management Method and Access Control List	82
Configuring Management Protocols and Ports	82
Configuring Control List Access from Management Clients	82
The Sync Setting Tab	83
Enabling Management by ODC	83
The Syslog Tab	83
Configuring Syslog Settings	84
Syslog Severity Levels	85

Syslog Severity Level Mapping Table.....	85
The SNMP Tab	86
Configuring SNMP v1/v2c	86
Configuring SNMP v3.....	87
Configuring SNMP Trap Receivers.....	87
The System Time Tab.....	88
Configuring System Time.....	89
The Back Up / Restore Tab.....	89
Backing Up a Configuration.....	89
Restoring a Configuration	90
The Firmware Management Tab.....	90
Viewing Device Firmware Information.....	90
Updating Firmware.....	91
Rebooting and Applying Firmware	92
The Reboot System Tab.....	92
Rebooting the System.....	92
Chapter 13	93
Supported USB Devices.....	93
Supported actions via USB Disk	93
On-demand Configuration backup	95
Load Pattern from Disk	95
Load Configuration from disk	96
Load Firmware from disk	96
Appendix A.....	98
Terms and Acronyms.....	98

About EdgeIPS™ Pro 216

Introduction

EdgeIPS Pro 216 is a purpose-built appliance, set up for friendly, rack-mounted deployment and equipped with in-depth OT protocol filtering to enable administrators to easily manage micro-segmentation for a complex environment. Created using the solid ICS security building block EdgeIPS, it is built from the ground up to isolate and protect multi-segment networks. This security solution is designed specifically to fit transparently into the IT/OT convergence network environment.

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

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

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

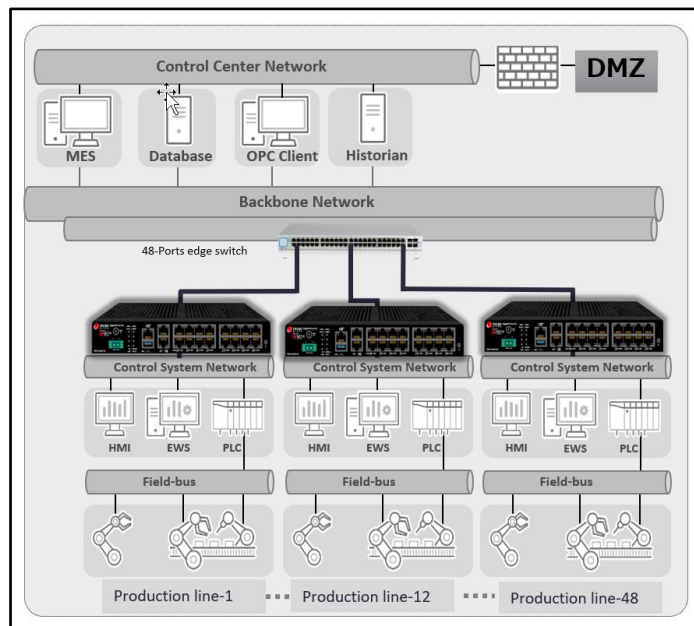


Figure 1. TXOne Security Solutions for an OT Network

Main Functions

EdgeIPS Pro 216 is a transparent network security appliance. The main functions of the product are as follows:

Multi-segmenting with Integrated Security

EdgeIPS Pro 216 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, EdgeIPS Pro 216 fits right into your network without disrupting operations.

High Port Density and Flexible Deployment

EdgeIPS Pro 216 comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant visibility of your shadow OT environment.

Extensive Support for Industrial Protocols

EdgeIPS Pro 216 supports the identification of a wide range of industrial control protocols, including Modbus and other protocols used by well-known international companies such as Siemens, Mitsubishi, Schneider Electric, ABB, Rockwell, Omron, and Emerson. In addition to allowing OT and IT security system administrators to work together, this feature also allows the flexibility to deploy defense measures in appropriate network segments and seamlessly connects them to existing factory networks.

Policy Enforcement for Mission-Critical Machines

EdgeIPS Pro's core technology TXODI (One-pass Deep Packet Inspection for Industrial) allows administrators to maintain a policy enforcement database. By analyzing Layer 3 to Layer 7 network traffic between mission-critical production machines, policy enforcement executes filtering of control commands within the protocols and blocks traffic that is not defined in the policy rules. This feature can help prevent unexpected operational traffic, block unknown network attacks, and block other activities that match defined policy rules.

Improve Shadow OT Visibility by Integrating IT and OT Networks

EdgeIPS Pro 216 comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant visibility of your shadow OT environment.

Intrusion Prevention and Intrusion Detection

EdgeIPS Pro 216 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.

Antivirus Protection

EdgeIPS Pro 216 Antivirus protects against the latest malware variants, spyware, and other content-level threats. Highly effective antivirus protection reduces the risk of data breach or damage caused by malware infection.

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

EdgeIPS Pro 216 flexibly switches between 'Monitor' and 'Prevention' modes. 'Monitor' mode will log traffic without interfering, while 'Prevention' mode will filter traffic based on policies you create. These modes work together to preserve your productivity while maximizing security.



Top Threat Intelligence and Analytics

EdgeIPS Pro 216 provides advanced protection against unknown threats with its up-to-date threat information. With the help of the Zero Day Initiative (ZDI) vulnerability reward program, EdgeIPS Pro 216 offers your systems exclusive protection from undisclosed and zero-day threats.

Easily Centralized Management with Convenient, Consolidated Overview

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

All protections are deployed throughout the entire information technology (IT) and operational technology (OT) infrastructure. These include:

- A centralized policy deployment and reporting system
- Full visibility into assets, operations, and security threats
- IPS and policy enforcement configuration can be assigned per device group, allowing all devices in the same device group to share the same policy configuration
- Management permissions for device groups can be assigned per user account

Getting Started

This chapter describes the EdgeIPS Pro 216 and how to get started with configuring the initial settings.

Note: For an overview of the physical hardware and characteristics, or a more condensed manual to help with initial setup of the device, please refer to the document "EdgeIPS Pro 216 - Quick Setup Guide."

Getting Started: Task List

This task list provides a high-level overview of all procedures required to get EdgeIPS Pro 216 up and running as quickly as possible. Each step links to more detailed instructions found later in the document.

Procedure

1. Open the management console. For more information, see [Opening the Management Console on page 9](#).
2. Change the administrator password. For more information, see [Changing the Administrator's Password on page 11](#).
3. Configure the system time. For more information, see
4. [The System Time Tab](#)
5. [on page 88](#).
6. (Optional) Configure the Syslog settings. For more information, see [Configuring Syslog Settings on page 84](#).
7. Configure object profiles. For more information, see [The Object Profiles Tab on page 22](#).
8. Configure security policies. For more information, see [The Security Tab on page 56](#).
9. Configure the device name and device location information. For more information, see [Configuring Device Name and Device Location Information on page 82](#).
10. (Optional) Configure the access control list from management clients. For more information, see [Configuring Control List Access from Management Clients on page 82](#).
11. Configure management protocols and ports. For more information, see [Configuring Management Method and Access Control List](#)
12. [Configuring Management Protocols and Ports on page 82](#).
13. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device. For more information, see [Manually Updating the Pattern on page 67](#).
14. (Optional) Enable Management by ODC. For more information, see [Enabling Management by ODC on page 83](#).
15. Configure the network settings and network interface link modes for the device. For more information, see [The Network on page 17](#).

Opening the Management Console

EdgeIPS Pro 216 provides a built-in management web console that you can use to configure and manage the product. View the management console using a web browser.

Note: View the management console using Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; Edge version 15 or later.

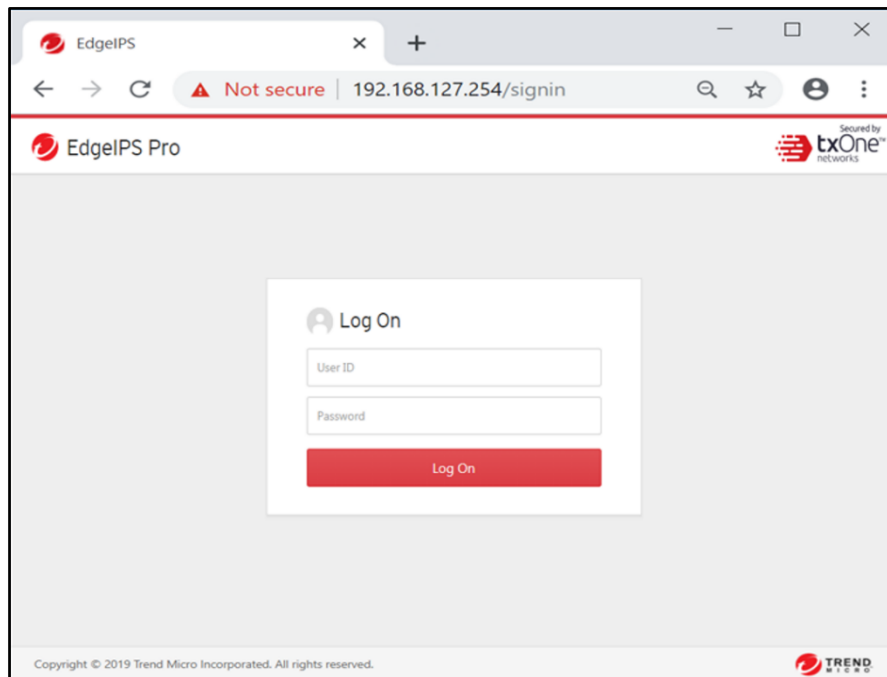
Procedure

1. In a web browser, type the address of the EdgeIPS Pro 216 in the following format:
<https://192.168.127.254>

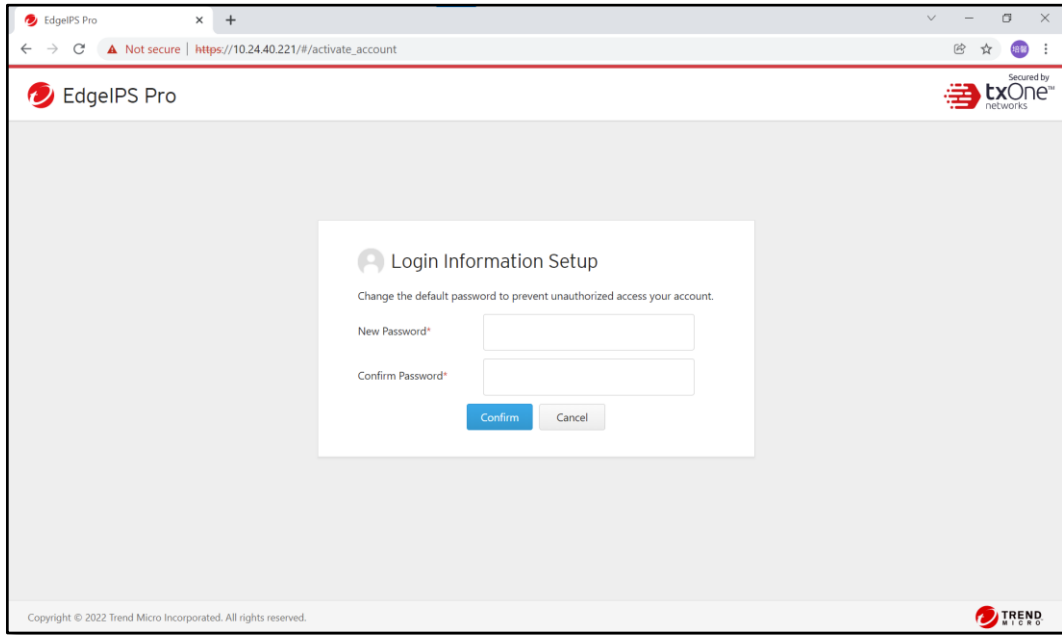
Note: TXOne devices use an automatically generated self-signed SSL certificate to encrypt communications to and from the client accessing the device. Given that the certificate is self-signed, most browsers will not trust the certificate and will give a warning that the certificate being used is not signed by a known authority.

The logon screen will appear.

Note: The default IP address of EdgeIPS Pro 216 is 192.168.127.254 with subnet 255.255.255.0. Before you connect a PC/Laptop to EdgeIPS Pro, the PC's IP address should be set to an IP address that is able to access the default IP address of EdgeIPS Pro. After that, connect the PC and EdgeIPS Pro 216 using an Ethernet cable.



2. Input the logon credentials (user ID and password).
Use the default administrator logon credentials when logging on for the first time:
 - User ID: `admin`
 - Password: `txone`
3. Click Log On.
4. When logging in for the first time or after a factory reset, you will be prompted to change the default user ID and password. The default user ID and password cannot be used.



5. Log in with newly changed user ID/password credentials.

Changing the Administrator's Password

Refer to section [Changing Your Password](#) under Chapter 11 *The Administration Tab > Account Management*.

The System Tab

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

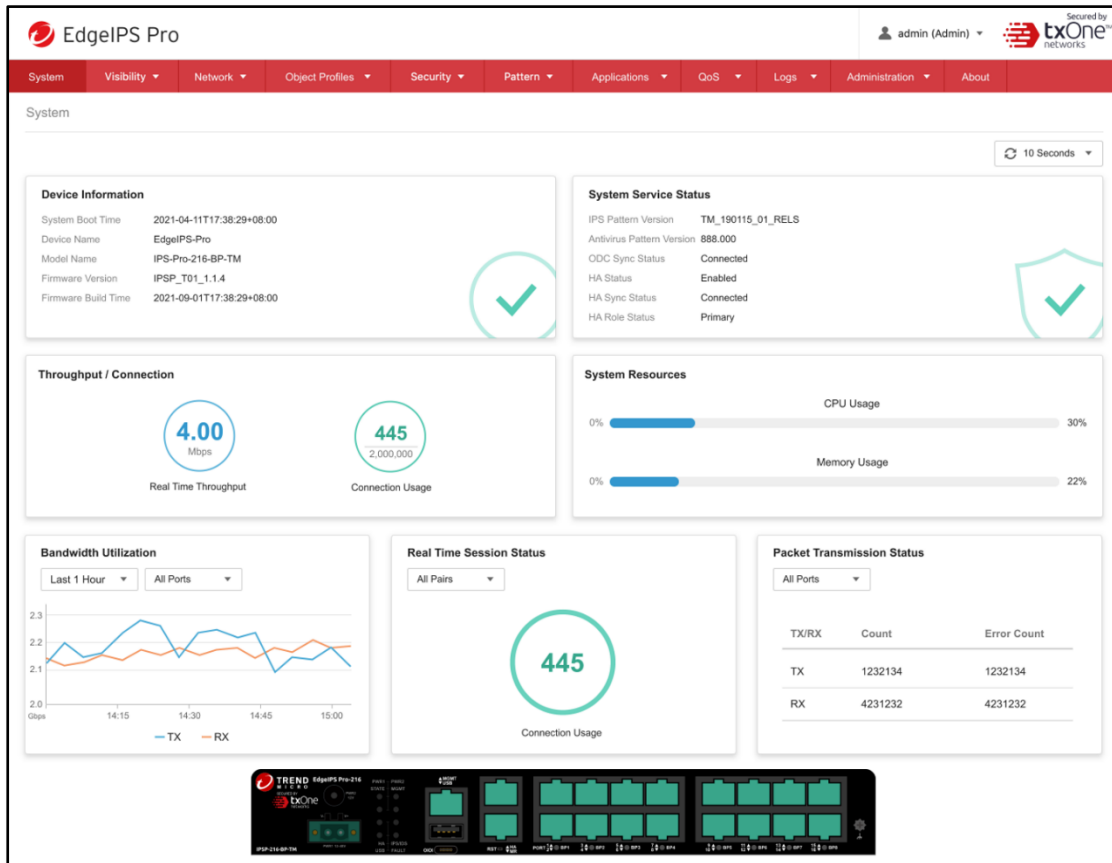
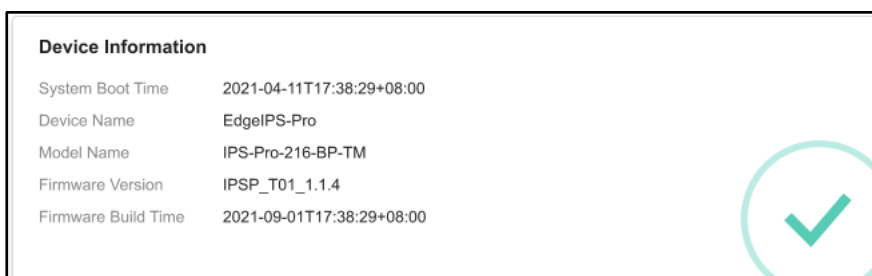


Figure 2. EdgeIPS™ Pro 216

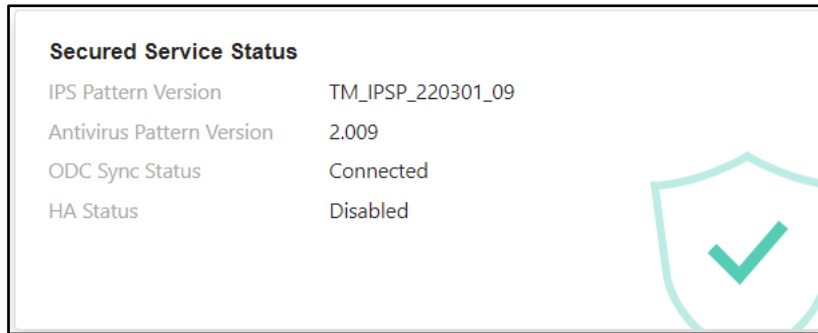
Device Information

This widget shows the system boot time, device name, model name, firmware version, and firmware build date / time.



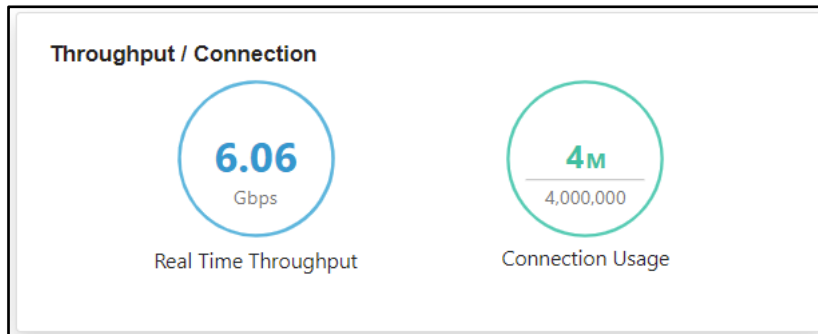
Secured Service Status

The widget shows the signature version on the device, ODC sync status, and HA status.



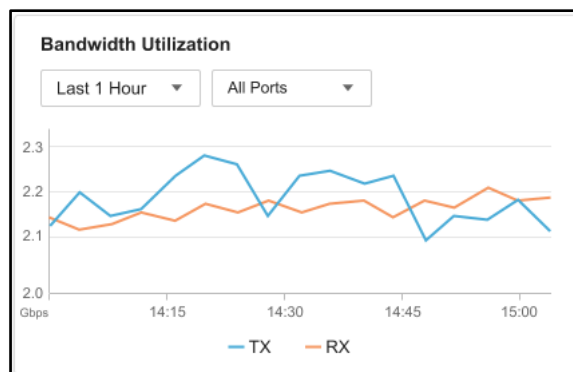
Throughput / Connection

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



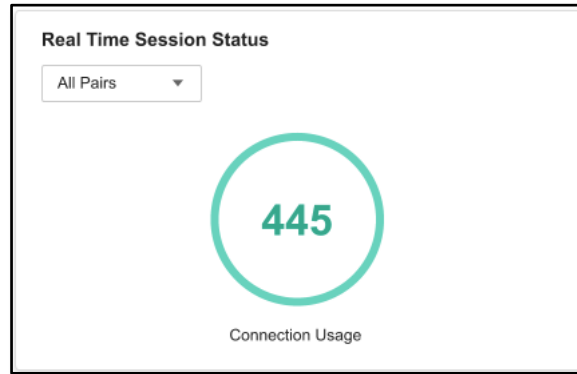
Bandwidth Utilization

This widget shows bandwidth utilization by module cards according to different time intervals and shows TX and RX bandwidth utilization.



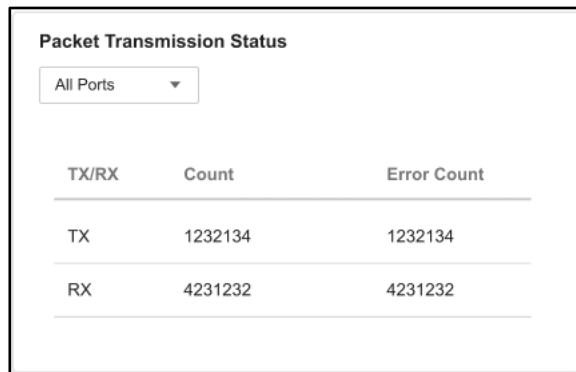
Real Time Session Status

This widget shows how many sessions are currently in use and can check each interface session status according to module slot and port.



Packet Transmission Status

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



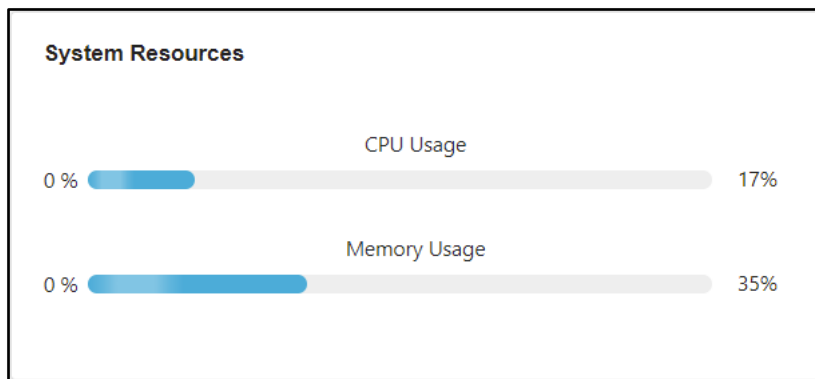
Packet Transmission Status

All Ports ▼

TX/RX	Count	Error Count
TX	1232134	1232134
RX	4231232	4231232

System Resources

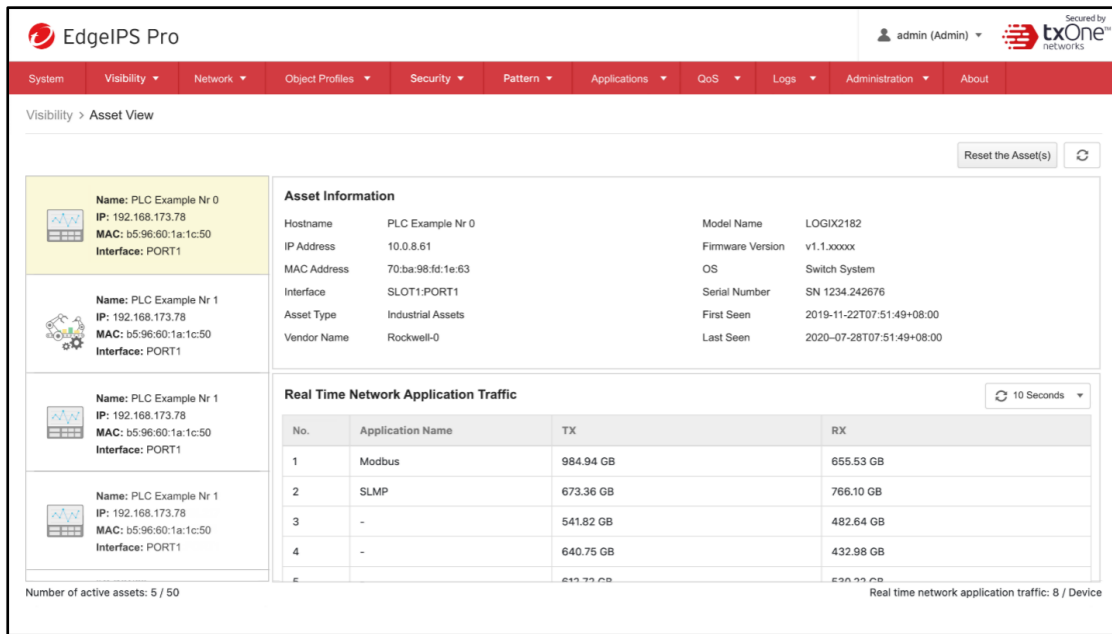
This widget shows system resource usage on the device.



Items	Descriptions
CPU Usage	Real time CPU utilization % (according to the refresh time settings)
Memory Usage	Real time memory utilization % (according to the refresh time settings)

The Visibility Tab

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



The screenshot shows the 'Asset View' page in the EdgeIPS Pro interface. It features a navigation menu at the top with options like System, Visibility, Network, Object Profiles, Security, Pattern, Applications, QoS, Logs, Administration, and About. The main content area is divided into several sections:

- Asset Information:** A table listing details for 'PLC Example Nr 0' and 'PLC Example Nr 1', including Hostname, IP Address, MAC Address, Interface, Model Name, Firmware Version, OS, Serial Number, Asset Type, Vendor Name, First Seen, and Last Seen.
- Real Time Network Application Traffic:** A table showing traffic data for various applications like Modbus and SLMP, with columns for No., Application Name, TX, and RX.

At the bottom of the interface, it indicates 'Number of active assets: 5 / 50' and 'Real time network application traffic: 8 / Device'.

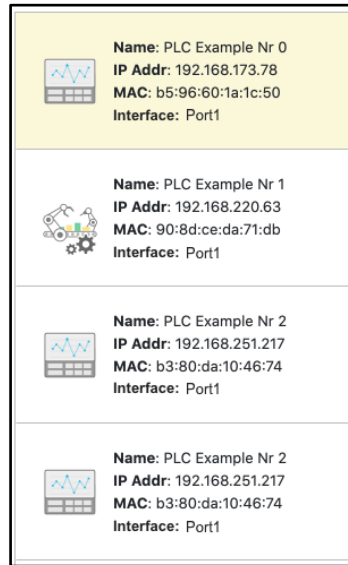
The assets, listed under the tab, are automatically detected by EdgeIPS Pro™ devices.

Note: The term asset in this chapter refers to a device or host that is protected by the EdgeIPS Pro™ 216.

Viewing Asset Information

Procedure

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



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

Fields	Descriptions
Host Name	The name of the asset.
IP Address	The IP address of the asset.
MAC Address	The MAC address of the asset.
Interface	The interface of the asset.
Asset Type	The asset type of the asset.
Vendor Name	The vendor name of the asset.
Model Name	The model name of the asset.
Firmware Version	The firmware version of the asset.
OS	The operating system of the asset.
Serial Number	The serial number of the asset.
First Seen	The date and time when the asset was first seen.
Last Seen	The date and time when the asset was last seen.

Viewing Real Time Network Application Traffic

Procedure

3. Go to [Visibility] > [Asset View].
4. Click an asset icon and view its detailed information.
5. The [Real Time Network Application Traffic] pane shows a list of the network traffic statics for the asset.

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

Note: Click the [Reset the Asset(s)] on the top-right of the window to set back to the initial state. This is only available for Admin role.

Note: Click the [Manually Refresh the Asset(s)] to refresh the displayed information.

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

The Network Tab

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

Configuring Device Settings

Procedure

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

Network > Device Settings

Management Port Settings

Device IP Address*

Netmask*

Gateway*

DNS

VLAN ID i

LLDP Setting

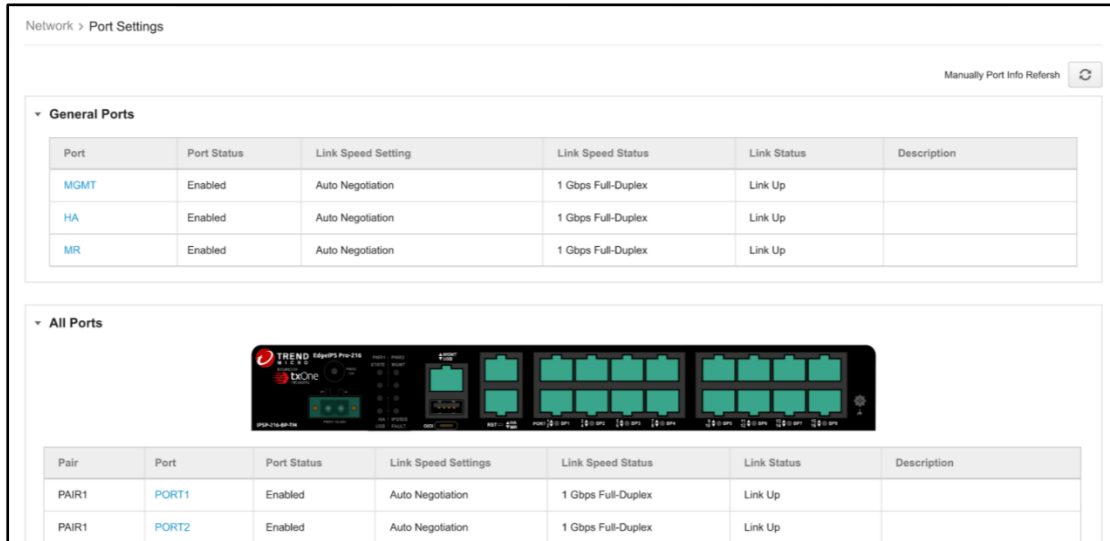
Transmit LLDP

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

Configuring Port Settings

Procedure

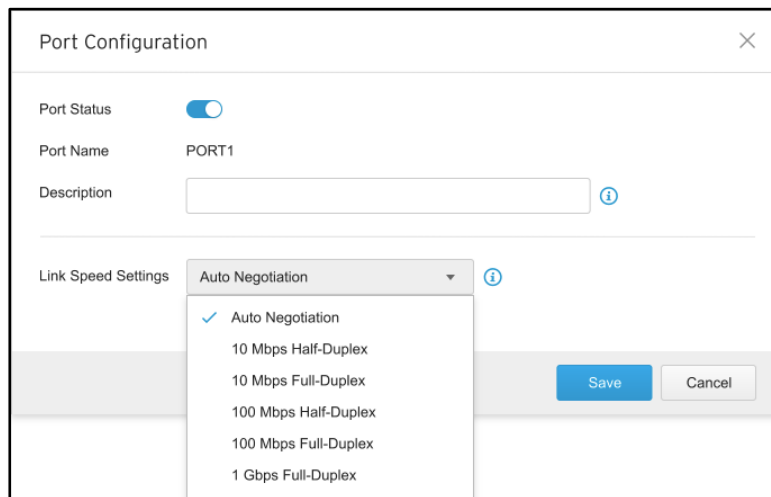
1. Go to [Network] > [Port Settings]
2. Click a port in the [Port Name] column to configure the port:



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

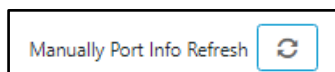
Note: The MGMT port cannot be disabled.

- b. Under the [Link Speed] dropdown menu, select a speed and negotiation method for the port.



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

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



Configuring HA Settings

Using a single device for network security and traffic flow can create a single point of failure. EdgeIPS Pro 216 provides a High Availability (HA) feature that enables redundancy by way of the ability to add and synchronize configurations with a secondary backup device. This eliminates the single point of failure and allows for a seamless switchover from primary device to secondary backup device in case of primary device failure. Thus, it allows for the planning and building of a fault-tolerant, resilient, and secure network to minimize any OT operational downtime.

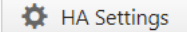
The HA feature allows for the grouping of two devices to form an HA group where configurations of the devices in the group are synchronized to support full fail-over redundancy. This section describes how to configure HA.

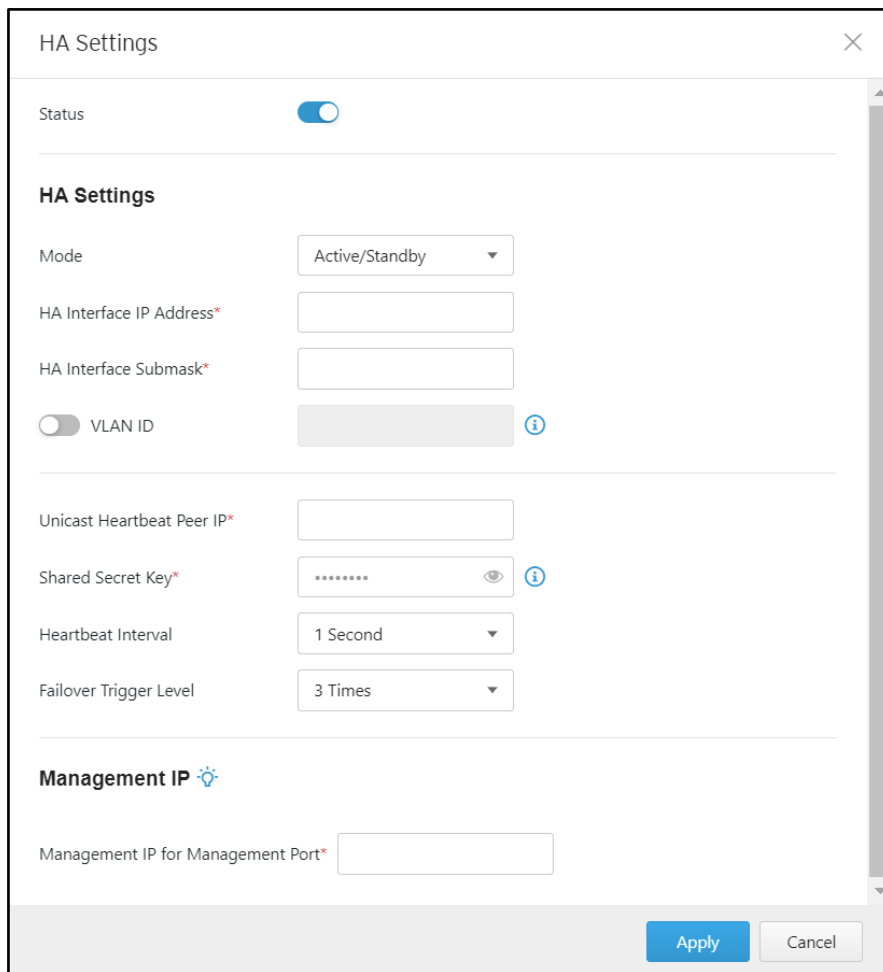
Procedure

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

HA status will be shown as below, including:

- **High Availability:** the status of HA, **Enabled** or **Disabled**.
If High Availability is enabled, the following status information will be shown:
- **Connection Status:** the status of connection, **Connected** or **Disconnected**.
- **Peer Sync Status:** the status of peer synchronization, **Synced** or **Un-Synced**.
- **Device Role Status:** the status of device role, **Primary** or **Secondary**.

2. Click  and the HA Settings window will appear.



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

Fields	Descriptions
Status	Shows HA sync status between two EdgeIPS Pros in the same HA group. This also displays the sync progress.
Modes	<p>There are 2 different HA modes, 'Active-Active' and 'Active-Standby'.</p> <p>Active-Active: Both devices in the HA group are fully active and online. Traffic may flow via either device. If a single connection's traffic is split across the two devices, it may cause the packet classifier to not be able to classify the traffic and thus not be able to apply any filtering/security policies. A single connection's complete session must pass through a single device.</p> <p>In this mode, the switching/flow of traffic between devices is handled by an external/upper layer that is outside the devices.</p> <p>Active-Standby: Only one device in the HA group is active and online. The secondary/standby device is only brought online in case of primary device failure and traffic only flows via the active device. In this mode, the switching of traffic between devices is handled internally on the devices via HA protocol logic set up between the devices.</p>
HA Interface Address	IP Address of the HA interface that will send/receive HA heartbeats and data messages to/from its peer
HA Interface Submask	Subnet mask of the HA interface
Enable VLAN-ID	VLAN ID of the HA Interface
Unicast Heartbeat Peer IP	The IP address of the HA peer
Shared Secret key	Shared secret key to allow for two HA peers to authenticate and communicate with each other
Heartbeat Interval	Interval between sent heartbeats - supports range of 1-10 seconds
Failover Trigger Level	Failover retry time supports range of 1-10 heartbeats: Maximum number of consecutive missed heartbeats before secondary to primary switch is triggered

- In the [Management IP] pane, input the Management IP address for the Management Port.

Note: When HA is enabled and the configuration is synced up, the IP settings for all the interfaces will be synced to the active device. To access the management interface of the active device or the stand-by device, you need to create at least a management IP to bridge to a designated management interface.

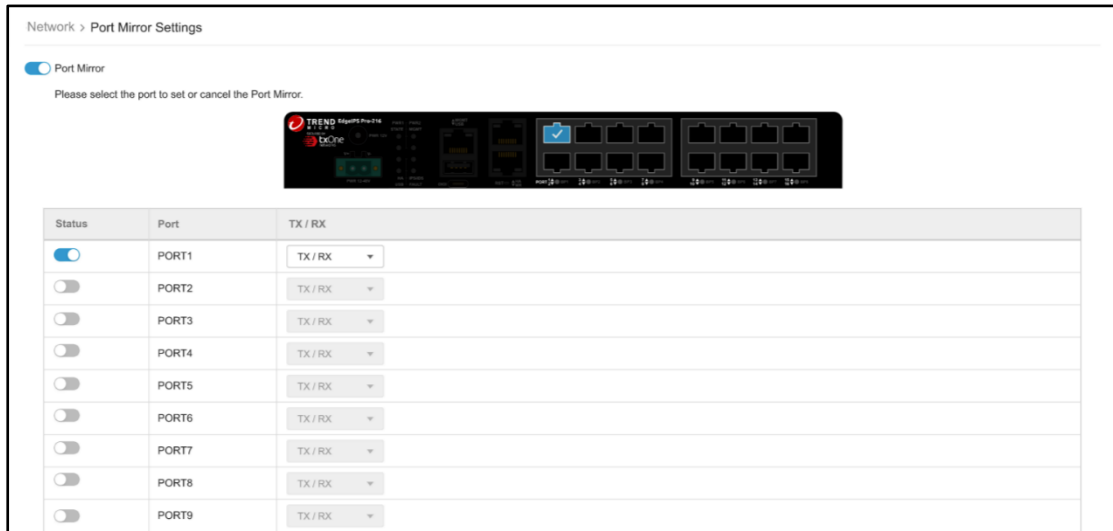
Configuring Port Mirror Settings

To monitor the network, all the traffic from any of the protected segments will be mirrored to the reserved port, i.e., the Mirror Port.

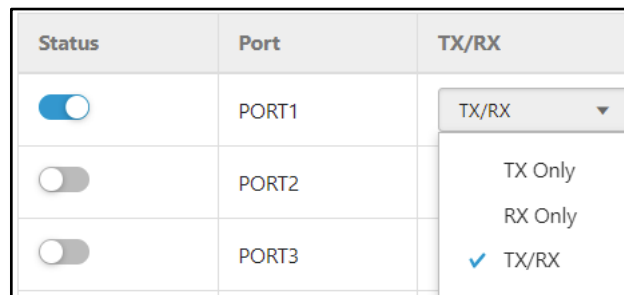
Note: Instead of pair-based, Port Mirror feature is port-based.

Procedure

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



2. Click on a front panel port to configure it:
 - a. Use the toggle to enable or disable the port.
 - b. Under the [TX/RX] dropdown menu, select the mirror traffic direction for the port.



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

The Object Profiles Tab

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

You can configure the following types of object profiles for this device:

- **IP Object 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.
- **Antivirus Profiles:** Streaming-based antivirus profiles provide an extra layer of protection under EdgeIPS Pro 216 for scanning, optimizing memory utilization for large archive files by decompressing the files on the fly and scanning the PE and ELF format malware files.

The following table describes the tasks you can perform when you view a list of the profiles:

Tasks	Descriptions
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].
Copy a profile	Select a profile and click [Copy].

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 address 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

Procedure

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

Create IP Object Profile ✕

Profile Name* i

Description i

IP Object List (Max: 8)

No.1*

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

Configuring Service Object Profiles

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

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

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

Procedure

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


Create Service Object Profile ✕

Profile Name* i

Description i

Service Object List (Max: 8)

No.1* ~

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

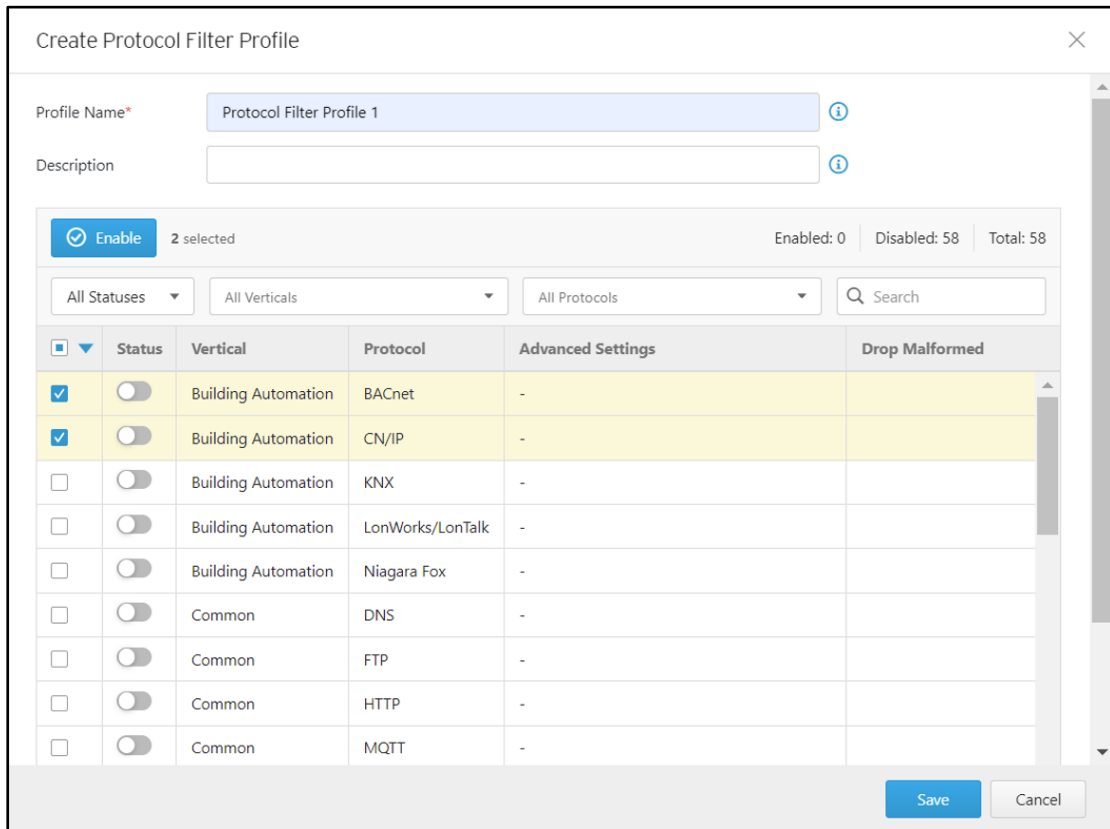
Configuring Protocol Filter Profiles

A protocol filter profile contains more sophisticated and advanced protocol settings that you can apply to a policy rule.

The following can be configured in a protocol filter profile:

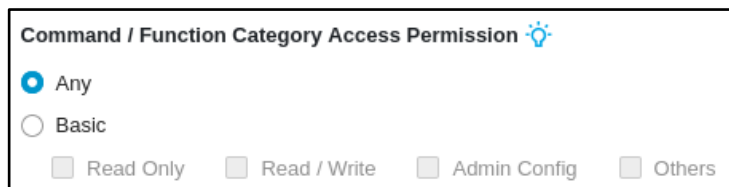
Details of ICS protocols, including:

- Factory Automation
 - Modbus
 - CIP
 - S7COMM
 - S7COMM PLUS
 - PROFINET
 - SLMP
 - MELSOFT
 - FINS
 - SECS/GEM
 - TOYOPUC
 - OPC UA
 - OPC CLASSIC
 - GE SDI
 - GE-SRTP
 - HART-IP
- Building Automation
- HealthCare
- Power and Electricity
- General Protocol, including:
 - BACnet
 - DICOM
 - HL7
 - DNP3
 - IEC104
 - IEC61850-MMS
 - HTTP
 - FTP
 - SMB
 - RDP
 - MQTT
 - MSRPC
 - SIP
 - SMTP
 - SNMP
 - SSH
 - TELNET
 - TFTP
 - VNC



Specifying Commands Allowed in an ICS Protocol

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



Applying the Drop Malformed Option to an ICS Protocol

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

When the toggle [Drop Malformed] is enabled, EdgeIPS Pro 216 will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, EdgeIPS Pro 216 will drop the packets of the ICS protocol.

Create Protocol Filter Profile
✕

Profile Name* ⓘ

Description ⓘ

Enabled: 4 | Disabled: 54 | Total: 58

All Statuses

Factory Automation
↑
↓
✕

All Protocols
Q Search

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CIP	Any ✎	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Factory Automation	CODESYS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson DeltaV	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson ROC	-	
<input type="checkbox"/>	<input type="checkbox"/>	Factory Automation	FANUC FOCAS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FINS ✎	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Factory Automation	GE EGD	-	
<input type="checkbox"/>	<input type="checkbox"/>	Factory Automation	GE SDI	-	

Save
Cancel

Note: Since firmware version v1.0, Drop Malformed feature supports 4 protocols, including Modbus, CIP, FINS and TOYOPUC.

Advanced Settings

Below is a list of advanced settings for OT protocols supported by EdgeIPS Pro.

Advanced Settings for Modbus Protocol

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

Modbus Advanced Settings ✕

Command / Function Category Access Permission 💡

Any
 Basic

Read Only
 Read / Write
 Admin Config
 Others

Advanced Matching Criteria

Function List: 0x01: Read Coils ▼

Function Code*: 0x01 ⓘ

Unit ID*: 0 ⓘ

Address*: Any ⓘ

Add

Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No.	Function Code	Unit ID	Address
No data to display				

OK
 Cancel

Procedure

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

Create Protocol Filter Profile ✕

Profile Name*: Protocol Filter Profile 1 ⓘ

Description: ⓘ

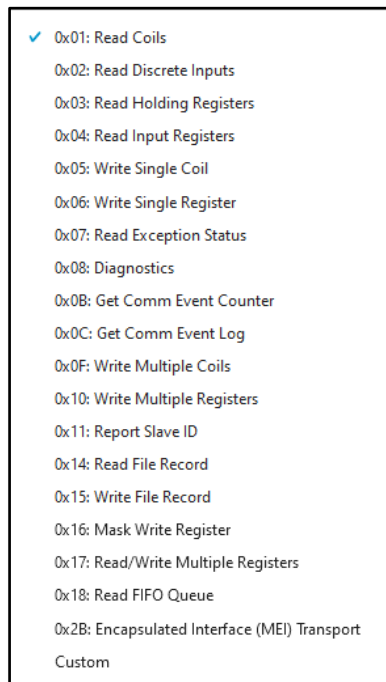
Enabled: 23 | Disabled: 35 | Total: 58

All Statuses ▼
 Factory Automation ×
 All Protocols ▼
 Search

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CIP	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CODESYS	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson DeltaV	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson ROC	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FANUC FOCAS	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FINS	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE EGD	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE SDI	-	<input type="checkbox"/>

Save
 Cancel

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [↗] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
 - If you have selected [Modbus], you can optionally configure advanced settings for this protocol:
 - Click the [↗] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
 - Under the [Function list] dropdown menu, select a function of this protocol.



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

6. Click [OK].

Advanced Settings for CIP Protocol

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

CIP Advanced Settings
✕

Command / Function Category Access Permission ⚙️

Any
 Basic

Read Only
 Read / Write
 Admin Config
 Others

Advanced Matching Criteria

Object Class List: Any ▼

Object Class ID*: Any ⓘ

Any Service Code
 Preset Service Code*

Available Service Code 28

- (0x01) Get_Attribute_All
- (0x02) Set_Attribute_All
- (0x03) Get_Attribute_List
- (0x04) Set_Attribute_List
- (0x05) Reset
- (0x06) Start

>>

>

<

<<

Selected Service Code 0

Custom Service Code ⓘ

Add

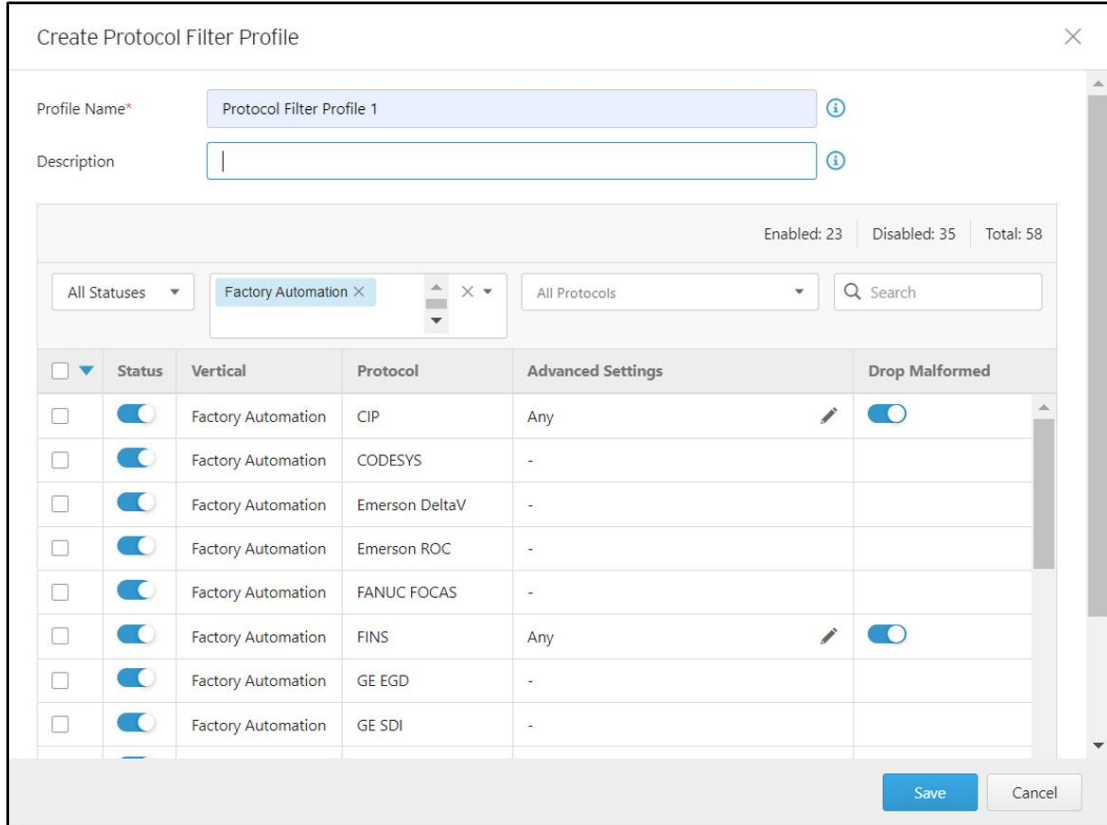
Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No.	Object Class ID	Service Code
No data to display			

OK
Cancel

Procedure

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



Create Protocol Filter Profile

Profile Name* ⓘ

Description ⓘ

Enabled: 23 | Disabled: 35 | Total: 58

All Statuses × Search

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CIP	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CODESYS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson DeltaV	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson ROC	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FANUC FOCAS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FINS	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE EGD	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE SDI	-	

Save Cancel

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [/] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
- If you have selected [CIP], you can optionally configure advanced settings for this protocol:

- Click the [↗] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
- Under the [Object Class List] dropdown menu, select a function of this protocol.

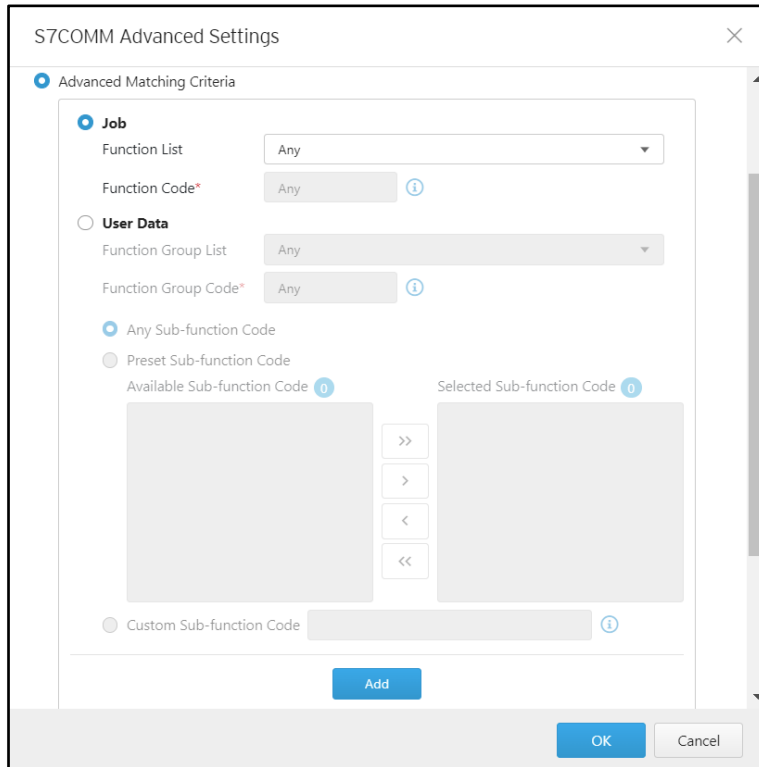
<ul style="list-style-type: none"> ✓ Any (0x0001) Identity (0x0002) Message Router (0x0003) DeviceNet (0x0004) Assembly (0x0005) Connection (0x0006) Connection Manage (0x0007) Register (0x0008) Discrete Input Point (0x0009) Discrete Output Point (0x000A) Analog Input Poing (0x000B) Analog Output Point (0x000E) Presence Sensing (0x000F) Parameter (0x0010) Parameter Group (0x0012) Group (0x001D) Discrete Input Group (0x001E) Discrete Output Group (0x001F) Discrete Group (0x0020) Analog Input Group (0x0021) Analog Output Group (0x0022) Analog Group (0x0023) Position Sensor (0x0024) Position Controller Supervisor (0x0025) Position Controller (0x0026) Block Sequencer (0x0027) Command Block (0x0028) Motor Data (0x0029) Control Supervisor (0x002A) AC/DC Drive 	<ul style="list-style-type: none"> (0x002B) Acknowledge Handler (0x002C) Overload (0x002D) Softstart (0x002E) Selection (0x0030) S-Device Supervisor (0x0031) S-Analog Sensor (0x0032) S-Analog Actuator (0x0033) S-Single Stage Controller (0x0034) S-Gas Calibration (0x0035) Trip Point (0x0037) File (0x0038) S-Partial Pressure Object (0x0039) Safety Supervisor (0x003A) Safety Validator (0x003B) Safety Discrete Output Point (0x003C) Safety Discrete Output Group (0x003D) Safety Discrete Input Point (0x003E) Safety Discrete Input Group (0x003F) Safety Dual Channel Output (0x0040) S-Sensor Calibration (0x0041) Event Log (0x0042) Motion Device Axis (0x0043) Time Sync (0x0044) Modbus (0x0045) Originator Connection List (0x0046) Modbus Serial Link (0x0047) Device Level Ring (0x0048) QoS (0x0049) Safety Analog Input Point (0x004A) Safety Analog Input Group 	<ul style="list-style-type: none"> (0x004B) Safety Dual Channel Analog... (0x004C) SERCOS III Link (0x004D) Target Connection List (0x004E) Base Energy (0x004F) Electrical Energy (0x0050) Non-Electrical Energy (0x0051) Base Switch (0x0052) SNMP (0x0053) Power Management (0x0054) RSTP Bridge (0x0055) RSTP Port (0x0056) Parallel Redundancy Protocol (0x0057) PRP Nodes Table (0x0058) Safety Feedback (0x0059) Safety Dual Channel Feedba... (0x005A) Safety Stop Functions (0x005B) Safety Limit Functions (0x005C) Power Curtailment (0x005D) CIP Security (0x005E) EtherNet/IP Security (0x005F) Certificate Management (0x0067) PCCC Class (0x00F0) ControlNet (0x00F1) ControlNet Keeper (0x00F2) ControlNet Scheduling (0x00F3) Connection Configuration (0x00F4) Port (0x00F5) TCP/IP Interface (0x00F6) Ethernet Link (0x00F7) CompoNet (0x00F8) CompoNet Repeater Custom
--	--	--

- If you want all the service codes within the function you specified to be applied, then select [Any Service Code]
- If you want to specify one or multiple service code(s), then select [Preset Service Code] and move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.
- If you want to specify a service code by yourself, then select [Custom Service Code] and input a service code in the [Custom Service Code] field.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

Advanced Settings for S7Comm

The device features more detailed configurations for the S7Comm ICS protocol. Through the [S7COMM Advanced Settings] pane, you can further specify the function code, function group code, and sub-function code based on which the function will operate.



S7COMM Advanced Settings

Advanced Matching Criteria

Job

Function List: Any

Function Code*: Any

User Data

Function Group List: Any

Function Group Code*: Any

Any Sub-function Code

Preset Sub-function Code

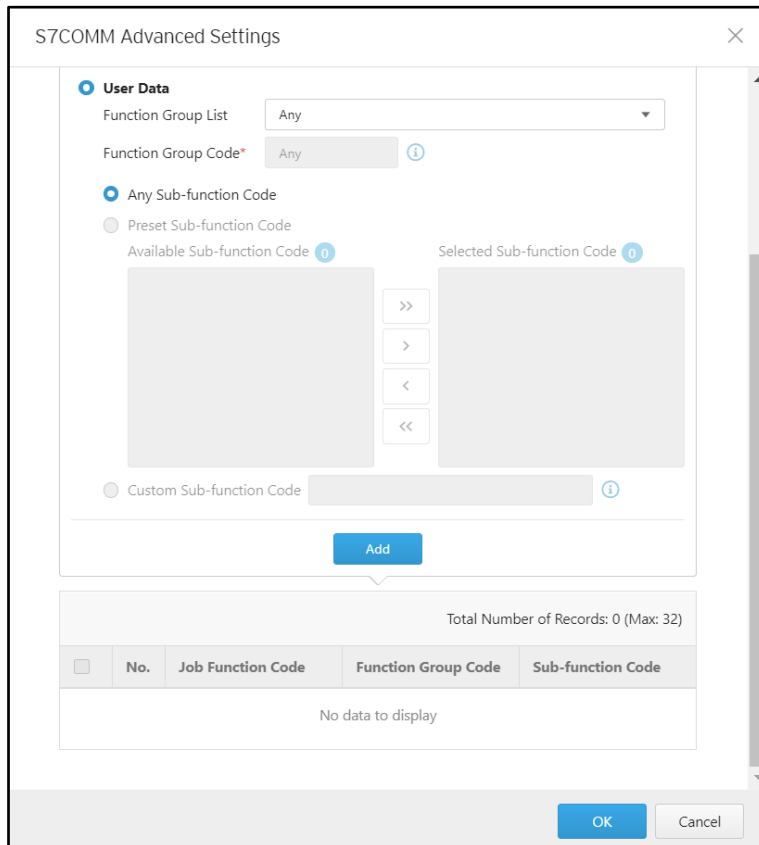
Available Sub-function Code: 0

Selected Sub-function Code: 0

Custom Sub-function Code: []

Add

OK Cancel



S7COMM Advanced Settings

User Data

Function Group List: Any

Function Group Code*: Any

Any Sub-function Code

Preset Sub-function Code

Available Sub-function Code: 0

Selected Sub-function Code: 0

Custom Sub-function Code: []

Add

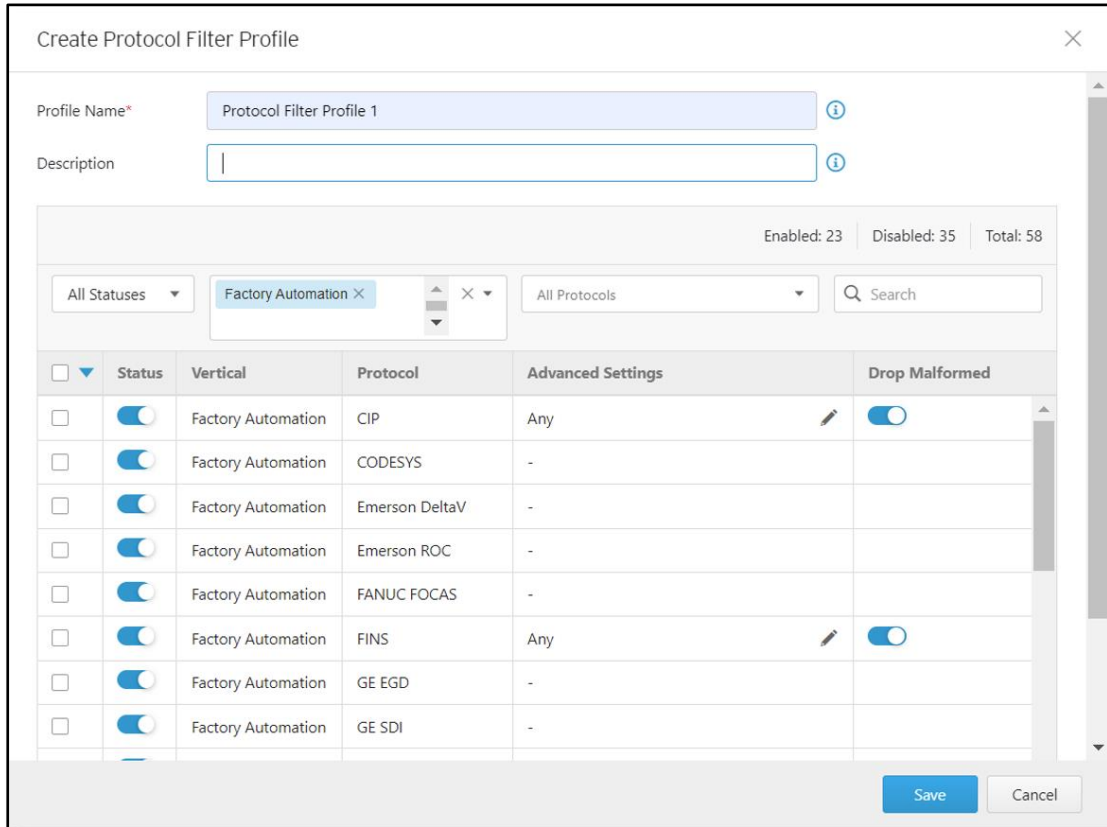
Total Number of Records: 0 (Max: 32)

No.	Job Function Code	Function Group Code	Sub-function Code
No data to display			

OK Cancel

Procedure

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



Enabled: 23 | Disabled: 35 | Total: 58

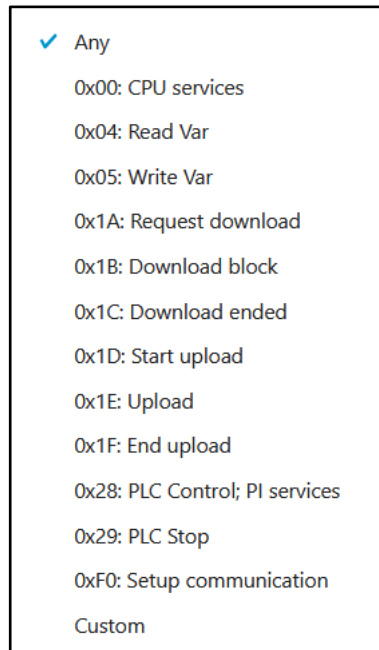
All Statuses | Factory Automation × | All Protocols | Search

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CIP	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CODESYS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson DeltaV	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson ROC	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FANUC FOCAS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FINS	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE EGD	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE SDI	-	

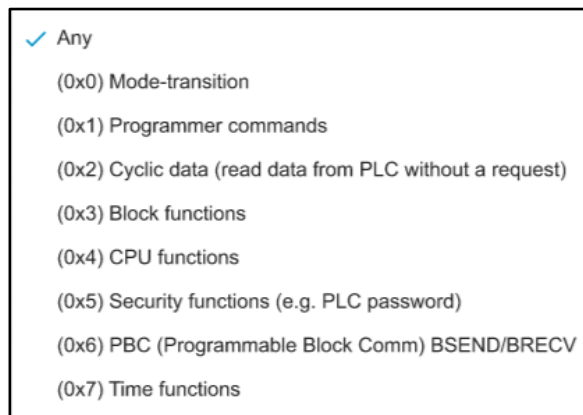
Save Cancel

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [/] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
 - If you have selected [S7COMM], you can optionally configure advanced settings for this protocol:
 - Click the [/] icon in the [Advanced Settings] column and select [Advanced Matching Criteria].

- If you want to specify one function code from the category [Job], then select the category [Job] and select a function from the [Function list] dropdown menu.



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

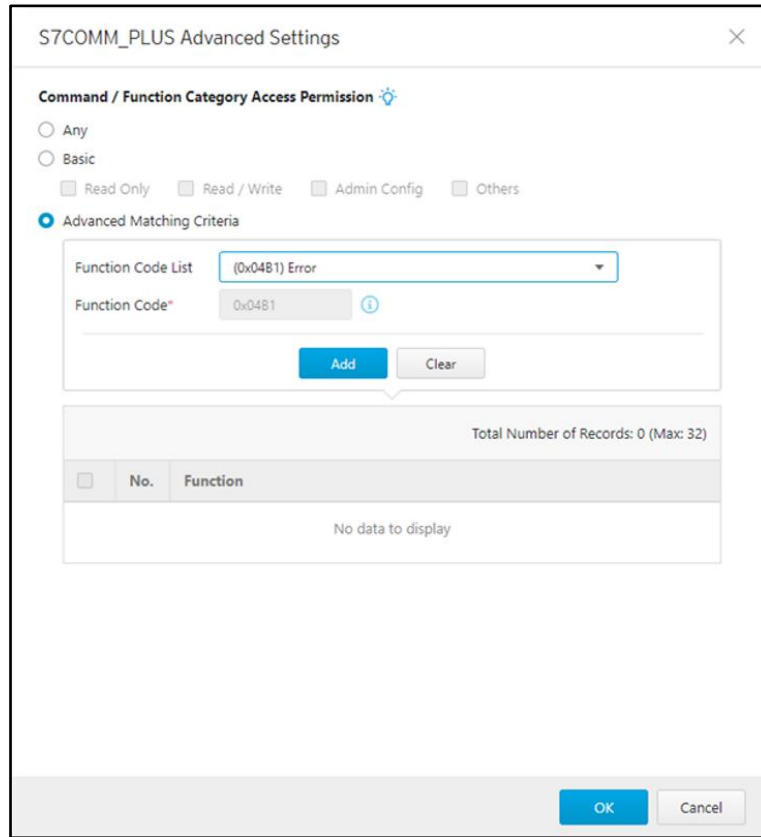


- If you want all the sub-function codes within the function group code you specified to be applied, then select [Any Sub-function Code]
- If you want to specify one or multiple sub-function code(s), then select [Preset Sub-function Code] and move the sub-function code(s) from the [Available Sub-function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

6. Click [OK].

Advanced Settings for S7Comm Plus

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



S7COMM_PLUS Advanced Settings

Command / Function Category Access Permission

Any

Basic

Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Function Code List: (0x04B1) Error

Function Code*: 0x04B1

Add Clear

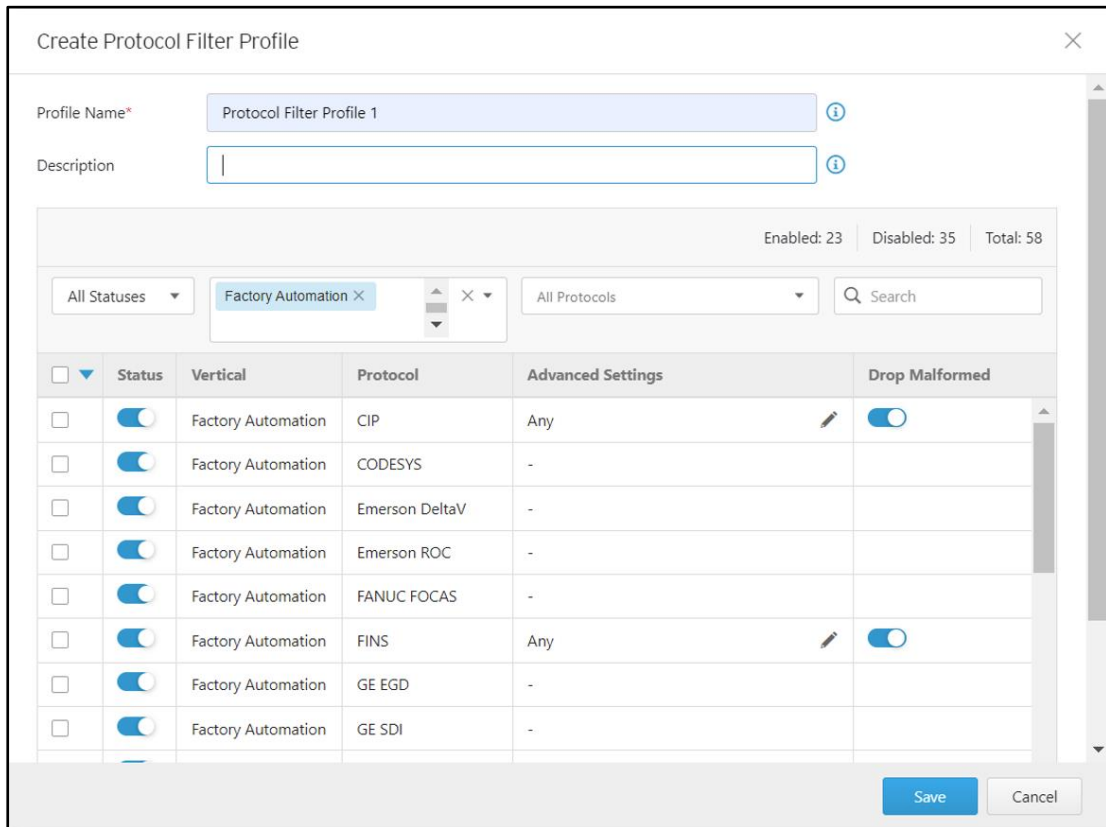
Total Number of Records: 0 (Max: 32)

No.	Function
No data to display	

OK Cancel

Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [/] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
 - If you have selected [S7COMM_PLUS], you can optionally configure advanced settings for this protocol:
 - Click the [/] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
 - Under the [Function Code List] dropdown menu, select a function of this protocol.

- (0x04B1) Error
- (0x04BB) Explore
- (0x04CA) CreateObject
- (0x04D4) DeleteObject
- (0x04F2) SetVariable
- (0x04FC) GetVariable
- (0x0506) AddLink
- (0x051A) RemoveLink
- (0x0524) GetLink
- (0x0542) SetMultiVariab...
- (0x054C) GetMultiVaria...
- (0x0556) BeginSequence
- (0x0560) EndSequence
- (0x056B) Invoke
- (0x057C) SetVarSubStre...
- (0x0586) GetVarSubStre...
- (0x0590) GetVariablesA...
- (0x059A) Abort
- Custom

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

6. Click [OK].

Advanced Settings for SLMP

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

SLMP Advanced Settings
✕

Command / Function Category Access Permission ⓘ

Any
 Basic
 Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Command Code list: (0x0101) Read Type Name ▾

Command Code*: 0x0101 ⓘ

Total Number of Records: 0 (Max: 32)

<input type="checkbox"/>	No	Command
No data to display		

Procedure

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

Create Protocol Filter Profile
✕

Profile Name* ⓘ

Description ⓘ

Enabled: 23
Disabled: 35
Total: 58

All Statuses ▾

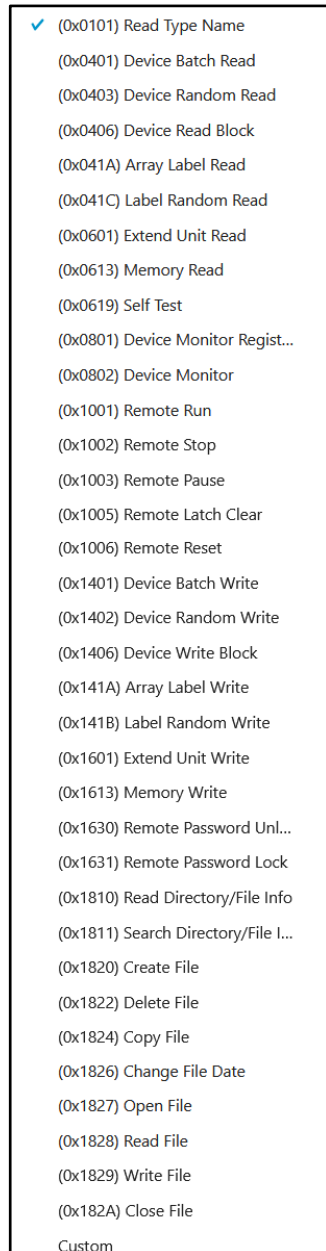
Factory Automation ×

All Protocols ▾

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CIP	Any ✎	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	CODESYS	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson DeltaV	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	Emerson ROC	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FANUC FOCAS	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	FINS	Any ✎	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE EGD	-	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Factory Automation	GE SDI	-	<input type="checkbox"/>

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [✎] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.

- If you have selected [SLMP], you can optionally configure advanced settings for this protocol:
 - Click the [↗] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
 - Under the [Command Code List] dropdown menu, select a command code of this protocol.



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

Advanced Settings for MELSOFT

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

Procedure

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

Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	Factory Automation	CIP	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Factory Automation	CODESYS	-	<input type="checkbox"/>
<input type="checkbox"/>	Factory Automation	Emerson DeltaV	-	<input type="checkbox"/>
<input type="checkbox"/>	Factory Automation	Emerson ROC	-	<input type="checkbox"/>
<input type="checkbox"/>	Factory Automation	FANUC FOCAS	-	<input type="checkbox"/>
<input type="checkbox"/>	Factory Automation	FINS	Any	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Factory Automation	GE EGD	-	<input type="checkbox"/>
<input type="checkbox"/>	Factory Automation	GE SDI	-	<input type="checkbox"/>

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [↗] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
- If you have selected [MELSOFT], you can optionally configure advanced settings for this protocol:
 - Click the [↗] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
 - Under the [Command Code List] dropdown menu, select a function of this protocol.

(0x0101) Read CPU Model Name
 (0x0114) Authentication
 (0x0121) Read CPU Model - R Series
 (0x0401) Device Batch Read
 (0x0402) Device Random Read
 (0x0403) Device Random Read
 (0x0410) Device Memory Read
 (0x0411) Device Random Read
 (0x0412) Device Random Read
 (0x0801) Device Monitor Register
 (0x0802) Device Monitor
 (0x0B05) Read Info - Q Series
 (0x0B11) Auto Search - Q Series
 (0x0B20) Auto Search - R Series
 (0x0B2A) Read Info - R Series
 (0x1001) Remote RUN
 (0x1002) Remote STOP
 (0x1003) Remote Pause
 (0x1005) Remote Latch Clear
 (0x1006) Remote RESET
 (0x1401) Device Batch Write
 (0x1402) Device Random Write
 (0x1410) Device Memory Write
 (0x1411) Device Random Write
 (0x1640) Password Unlock
 (0x1641) Password Lock

(0x1810) Read DIR/File Info
 (0x1811) Search Directory File
 (0x1820) Create File
 (0x1826) Modify File Time
 (0x1827) Open File
 (0x1828) Read File
 (0x1829) Write File
 (0x182A) Close File
 (0x1836) Write to Storage
 (0x1837) Close File SP
 (0x1838) Delete a File
 Custom

- If you want to specify one device code, then select [Preset Device] and select one of the device codes from the dropdown list.

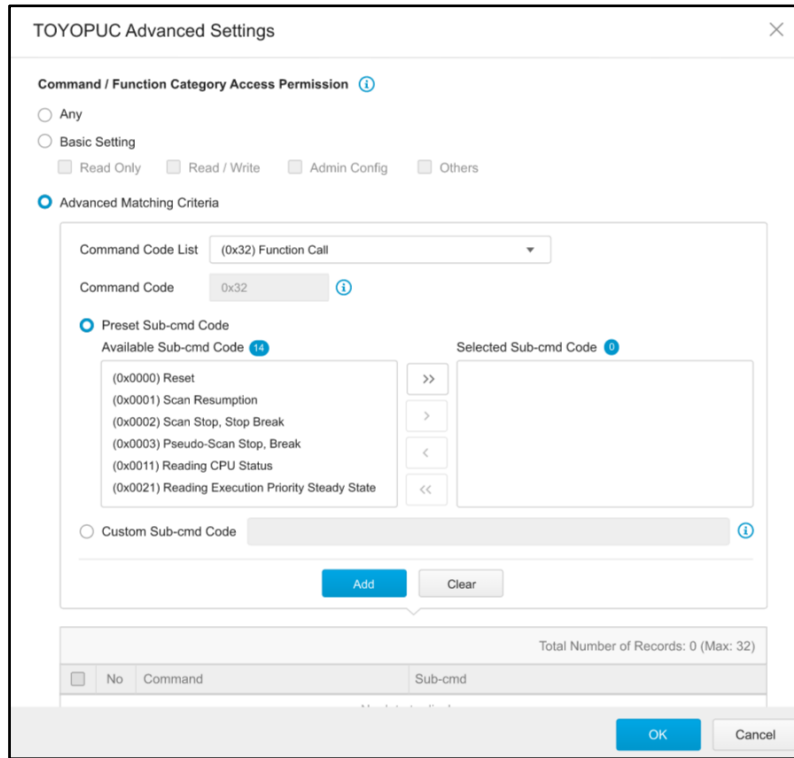
<ul style="list-style-type: none"> ✓ (0x0001) Internal relay (0x0002) Special relay (0x0003) Latch relay (0x0004) Annunciator (0x0005) Edge relay (0x0010) Input (0x0011) Output (0x0014) Link relay (0x0015) Link special relay (0x0020) Data register (0x0021) Special register (0x0027) File register (0x002C) Refresh data register (0x0030) Link register (0x0031) Link special register (0x0042) Timer (0x0046) Counter (0x004A) Retentive timer (0x0052) Long timer (0x0056) Long counter (0x0060) Index register (0x0062) Long index register (0x0090) Internal relay (0x0091) Special relay (0x0092) Latch relay (0x0093) Annunciator 	<ul style="list-style-type: none"> (0x0094) Edge relay (0x0098) Step relay (0x009C) Input (0x009D) Output (0x00A0) Link relay (0x00A1) Link special relay (0x00A2) Direct access input (0x00A3) Direct access output (0x00A8) Data register (0x00A9) Special register (0x00AB) Module access device (0x00AF) File register – block switching (0x00B0) File register – serial number (0x00B4) Link register (0x00B5) Link special register (0x00C0) Timer coil (0x00C1) Timer contact (0x00C2) Timer current value (0x00C3) Counter coil (0x00C4) Counter contact (0x00C5) Counter current value (0x00C6) Retentive timer coil (0x00C7) Retentive timer contact (0x00C8) Retentive timer current value (0x00CC) Index register Custom
--	--

- If you don't want to include a device number as a filter criterion, then select [Any] from the dropdown list.
- If you want to specify a device number, then select [Single] from the dropdown list.
- If you want to specify a range of device numbers, then select [Range] from the dropdown list.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

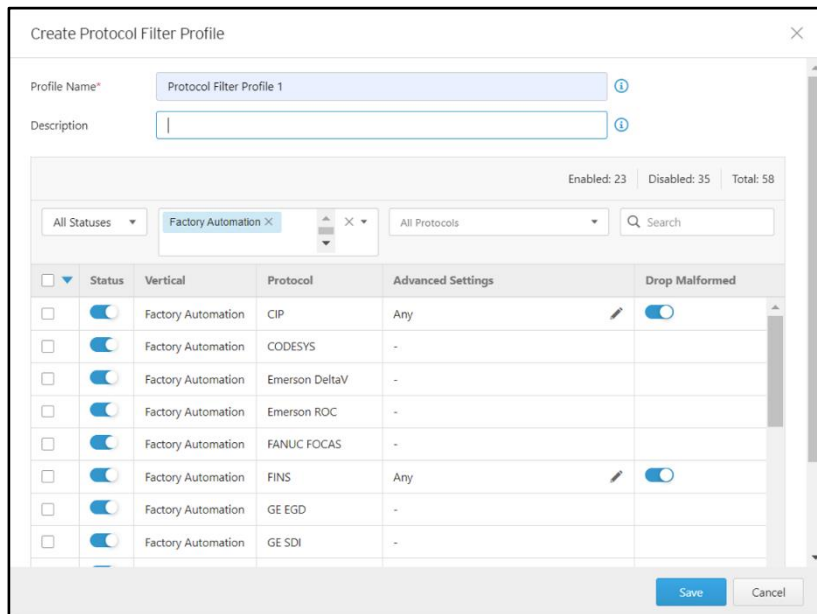
Advanced Settings for TOYOPUC

The device features more detailed configurations for the TOYOPUC ICS protocol. Through the [TOYOPUC Advanced Settings] pane, you can further specify the command code, preset sub-command code and custom sub-command code based on which the function will operate.



Procedure

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



3. Type a profile name for the protocol filter.

4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [status] column.
 - Click the [↗] icon in the [Advance Settings] column, then select one of the following:
 - **Any** - 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.
- If you have selected [TOYOPUC], you can optionally configure advanced settings for this protocol:
 - Click the [↗] icon in the [Advance Settings] column, and select [Advanced Matching Criteria].
 - Under the [Command Code List] dropdown menu, select a function of this protocol.

- ✓ (0x18) Read Sequence Program Word
- (0x19) Write Sequence Program Word
- (0x1C) Reading IO Register Word
- (0x1D) Writing IO Register Word
- (0x1E) Reading IO Register Byte
- (0x1F) Writing IO Register Byte
- (0x20) Reading IO Register Bit
- (0x21) Writing IO Register Bit
- (0x22) Reading IO Register Multi-poin...
- (0x23) Writing IO Register Multi-point...
- (0x24) Reading IO Register Multi-poin...
- (0x25) Writing IO Register Multi-point...
- (0x26) Reading IO Register Multi-poin...
- (0x27) Writing IO Register Multi-point...
- (0x30) Reading Parameter
- (0x31) Writing Parameter
- (0x32) Function Call

- (0x60) Relay Command
- (0x90) Reading Program Expansion W...
- (0x91) Writing Program Expansion W...
- (0x92) Reading Parameter Expansion
- (0x93) Writing Parameter Expansion
- (0x94) Reading Data Expansion Word
- (0x95) Writing Data Expansion Word
- (0x96) Reading Data Expansion Byte
- (0x97) Writing Data Expansion Byte
- (0x98) Reading Data Expansion Multi-...
- (0x99) Writing Data Expansion Multi-...
- (0xA0) Expansion Function Call
- (0xC2) PC10 data byte reading
- (0xC3) PC10 data byte writing
- (0xC4) PC10 multi-point reading
- (0xC5) PC10 multi-point writing
- (0xCA) PC10 FR register registration
- Custom

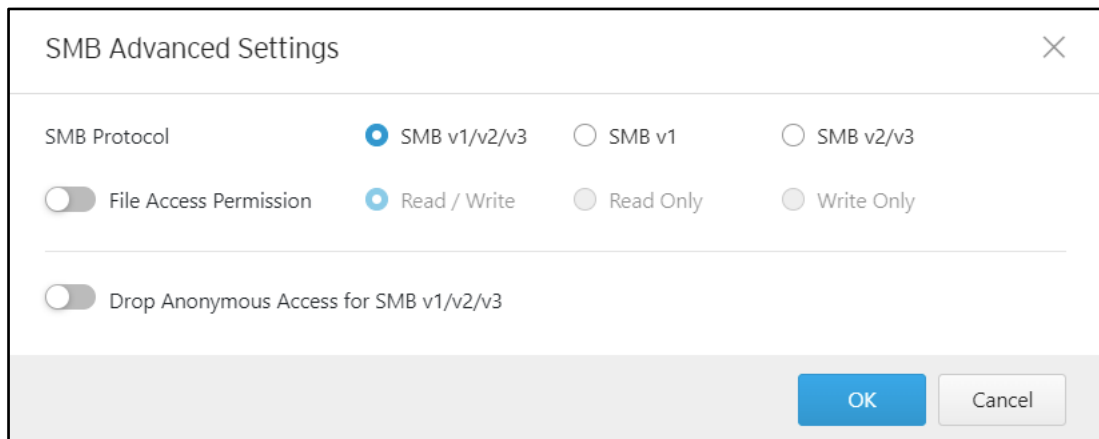
- If you want to specify one sub-command code or multiple sub-command codes, then select [Preset Sub-command Code] and move the sub-function code(s) from the [Available Sub-command Code] field to the [Selected Sub-command Code] field.
- If you want to specify a sub-command code by yourself, then select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

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

6. Click [OK].

Advanced Settings for SMB

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



Procedure

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

Create Protocol Filter Profile
✕

Profile Name* ⓘ

Description ⓘ

Enabled: 37 | Disabled: 21 | Total: 58

All Statuses ▾

Common ×

▲
 ▼

✕ ▾

All Protocols ▾

<input type="checkbox"/>	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	DNS	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	FTP	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	HTTP	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	MQTT	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	MS RPC	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	RDP	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	SIP	-	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Common	SMB	SMB: v1/v2/v3, File Access Permission: D... ✎	

3. Type a profile name for the protocol filter.
4. Type a description.
5. Select the protocols you want to include in the protocol filter.
 - Click the enable switch in the [Status] column.
 - Click the [↗] icon in the [Advanced Settings] column, then select one of the following:
 - **SMB Protocol** - Specify the SMB protocol version combination – options include SMBv1/v2/v3, SMBv1 and SMB v2/v3.
 - **File Access** – Select access permission behavior:
 - **Read / Write:** Read and write file access
 - **Read Only:** File access for reading only
 - **Write Only:** File access for writing only
 - **Drop Anonymous Access for SMB v1/v2/v3:** Drop access over SMB v1/v2/v3 for Anonymous accounts.

Configuring IPS Profiles

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

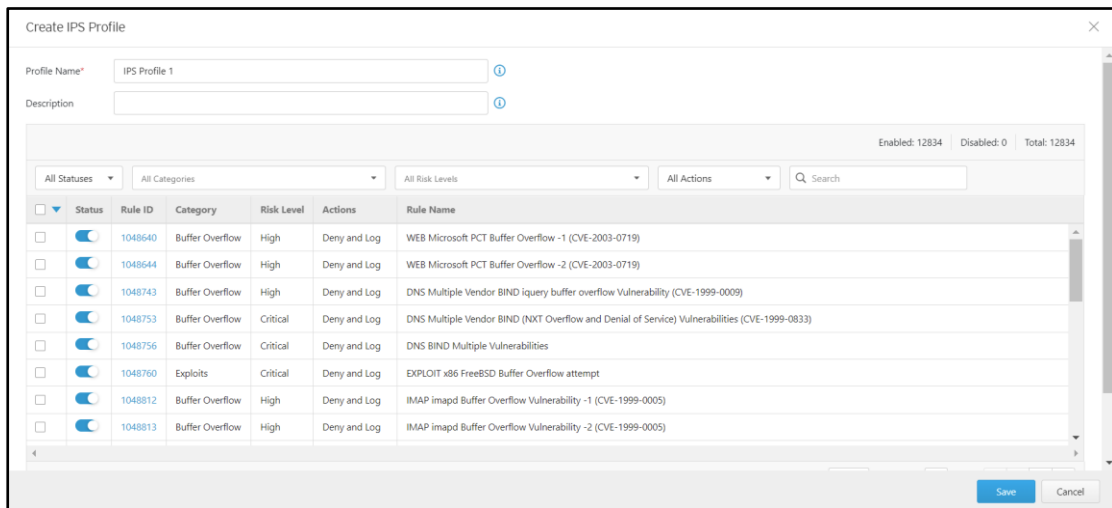
The following can be configured in an IPS profile:

- Details of IPS protocol category, including:
 - File Vulnerabilities
 - Buffer Overflow
 - DoS Attacks
 - Exploits
 - Malware Traffic

- Reconnaissance
 - Web Threats
 - ICS Threats
 - Others
 - Misc
- Details of IPS protocol risk level categories, including:
 - Information
 - Low
 - Medium
 - High
 - Critical
 - Details of default action list for IPS patterns, including:
 - All Actions
 - Accept and log
 - Deny and Log

Configuring a Pattern Rule for Granular Control

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



IPS Rule Details ✕

Status

Rule ID 1048640

Rule Name WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719)

Category Buffer Overflow

Risk Level High

Impact Remote code execution

Actions Accept and Log Deny and Log

Reference BID-10116; CVE-2003-0719

TID -

Keyword Windows 2000, Windows 2003 Server, Windows 98, Windows ME, Windows NT, Windows XP,

Procedure

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

Create IPS Profile ✕

Profile Name*

Description

Enabled: 11086 Disabled: 0 Total: 11086

All Statuses All Categories All Risk Levels All Actions

<input type="checkbox"/>	Status	ID	Category	Risk Level	Actions	Profile Name
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048640	Buffer Overflow	High	Deny and Log	WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048644	Buffer Overflow	High	Deny and Log	WEB Microsoft PCT Buffer Overflow -2 (CVE-2003-0719)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048743	Buffer Overflow	High	Deny and Log	DNS Multiple Vendor BIND query buffer overflow Vulnerability (CVE-1999-0009)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048753	Buffer Overflow	Critical	Deny and Log	DNS Multiple Vendor BIND (NXT Overflow and Denial of Service) Vulnerabilities (CVE-1999-0833)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048756	Buffer Overflow	Critical	Deny and Log	DNS BIND Multiple Vulnerabilities
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1048760	Exploits	Critical	Deny and Log	EXPLOIT x86 FreeBSD Buffer Overflow attempt

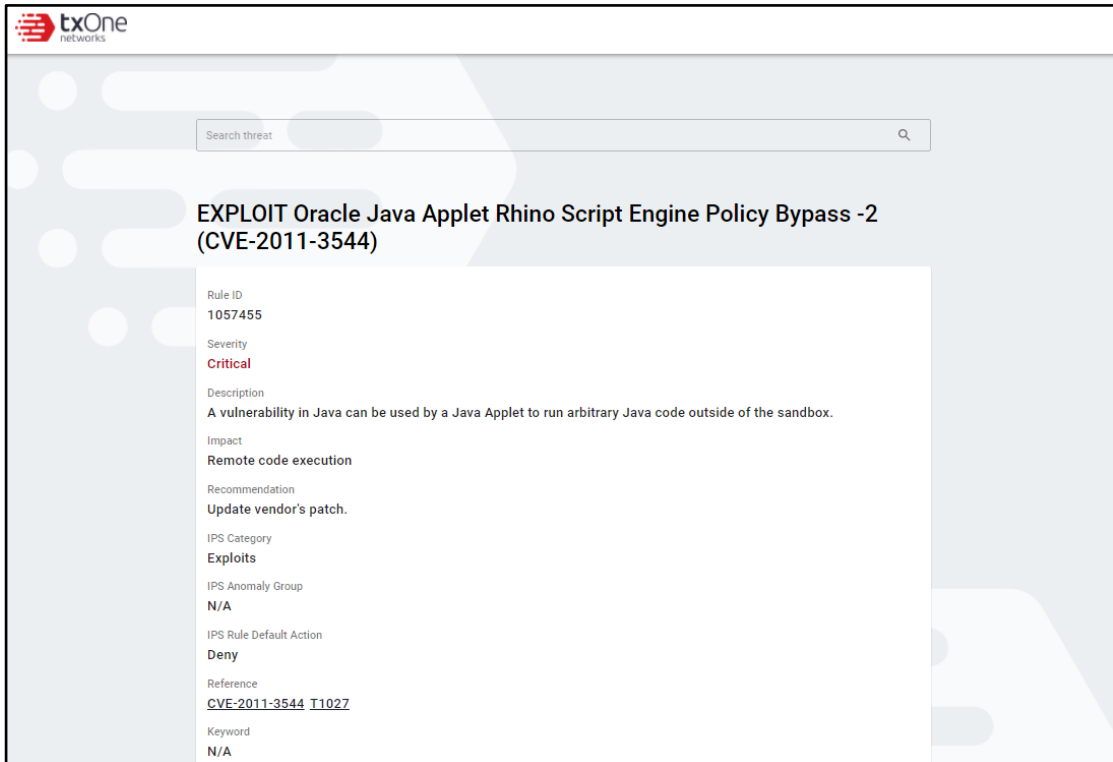
Records: 1-25 / 11086 25 per page 1 / 444

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

- **Deny and Log:** When the attack is detected by EdgeIPS Pro, the attack will be blocked and logged for monitoring.

Fields	Descriptions
Status	The operational status of the pattern rule
ID	The pattern rule ID
Rule Name	The pattern name for the cyber attack
Category	The threat category for the cyber attack
Risk Level	The suggested security level for the cyber attack
Impact	The damage that will be caused to the target network device if the cyber attack succeeds
Reference	The vulnerability ID of the cyber attack (e.g. CVE-2017-0147)
TID	MITRE ID information
Actions	The preset actions for the cyber attack
Keyword	The word(s) for searching the pattern rules

7. For more detailed threat information, click 'Rule ID Info' to be redirected to the TXOne Threat Encyclopedia.



txOne networks

Search threat

EXPLOIT Oracle Java Applet Rhino Script Engine Policy Bypass -2 (CVE-2011-3544)

Rule ID
1057455

Severity
Critical

Description
A vulnerability in Java can be used by a Java Applet to run arbitrary Java code outside of the sandbox.

Impact
Remote code execution

Recommendation
Update vendor's patch.

IPS Category
Exploits

IPS Anomaly Group
N/A

IPS Rule Default Action
Deny

Reference
[CVE-2011-3544](#) [T1027](#)

Keyword
N/A

8. When you are satisfied with your configurations for the pattern rule, click [Save].

Configuring File Filter Profiles

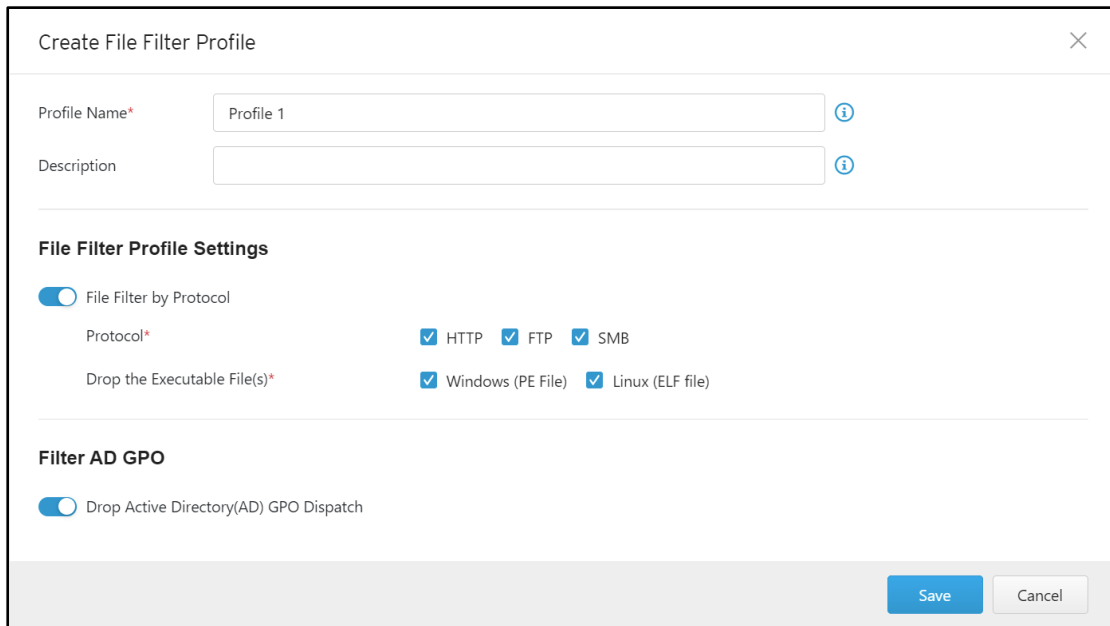
The File Filter Profile contains detailed access protocols as well as settings for executable file type and Active Directory (AD) GPO dispatch, allowing you to create or edit profiles to apply to a policy rule. In a profile, you can define the following:

- File Filter by Protocol
Including: HTTP, FTP and SMB

- Drop Transfer of Packed Executable Files
Including: Windows (PE files) and Linux (ELF file)
- Filter AD GPO
Enable or disable filtering of Active Directory (AD) GPO

Procedure

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



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

Configuring File Exclusions

File Exclusions are advanced configurations to exclude certain files from the file filter profile(s) you're enabling. The system skips the file type scanning based on your list in [File Exclusion Settings]. This can increase the flexibility of configuration and obtain the real control for your OT network.

Object Profiles > File Filter Profiles

File Exclusions

The system skips the file type scanning based on the list in File Exclusion Settings.
To import the list into File Exclusion Settings, please download the CSV template and fill in the full filename(s) and the description(s).

Total Number of File Exclusion(s): 3

File Filter Profiles

Total Number of Records: 2 (Max: 256)

<input type="checkbox"/>	No.	Profile Name	Protocol Settings	Filter AD GPO	Description
<input type="checkbox"/>	1	Default_AV_Profile	Enabled HTTP Protocol (Deny and Log), Enabled FTP Protocol (Deny and Log)	Enabled Maximum File Size for Scanning, Enabled Scan Compressed File	
<input type="checkbox"/>	2	AV_Profile1	Disabled HTTP Protocol, Enabled FTP Protocol (Accept and Log)	Enabled Maximum File Size for Scanning, Disabled Scan Compressed File	

Records: 1-2 / 2 25 Per page 1 / 1 << < > >>

Two styles of operation scenarios are provided, either adding file items one by one or importing an edited CSV file with multiple **filename** items. Click to download a CSV template file for you to edit.

Procedure

1. Access the web user interface of the EdgeIPS™ Pro 216 device.
2. Go to [Object Profiles] > [File Filter Profiles].

Scenario 1: Add File Items One by One (Steps 3 & 4)

3. Click [File Exclusion Settings].
4. Click [Add] to add file exclusion settings item by item.

File Exclusion Settings ✕

The file system is not case sensitive. Filenames in upper-case or lower-case are recognized as the same file.

Total Number of Records: 3 (Max: 2000)

Q Search

<input type="checkbox"/>	No.	Full Filename	Description
<input type="checkbox"/>	1	abc.exe	
<input type="checkbox"/>	2	xyz	
<input type="checkbox"/>	3	defghijk	

Records: 1-3 / 3 25 Per page 1 / 1 << < > >>

Scenario 2: Import an Edited CSV File with Multiple File Items (Steps 5 & 6)

5. Click the [Download CSV Template] button to download the CSV template, and fill in complete filenames and descriptions.
6. Click the [Import] button to import the edited CSV file to the file system.

File Exclusion Settings ✕

The file system is not case sensitive. Filenames in upper-case or lower-case are recognized as the same file.

+ Add
↶ Import

Total Number of Records: 3 (Max: 2000)

<input type="checkbox"/>	No.	Full Filename	Description
<input type="checkbox"/>	1	abc.exe	
<input type="checkbox"/>	2	xyz	
<input type="checkbox"/>	3	defghijk	

Records: 1-3 / 3
25
Per page
1 / 1
⏪ ⏩

Save
Cancel

Note: You do not need to unzip zip/gz file(s) for scanning each compressed file, as the system can identify zip/gz file(s) and determine whether the filename list contains the file items for exclusions. Notice that zip/gz files larger than 100MB will be ignored.

Note: The full filename format can be **Filename.File Extension** (e.g. abc.exe), or just **Filename** (e.g. abc).

Note: Notice that the file system is not case sensitive. Filenames in uppercase or lowercase are identified as the same file. In addition, Whitespace character(s) cannot be included in the beginning and the end of a filename. Special characters (<, >, :, ", /, \, |, ? and *) are not allowed.

Note: The maximum full filename length is 128 bytes with UTF-8. When the UTF-8 user input is based on English characters, the maximum full filename length is 128 characters. When the UTF-8 user input is based on non-English characters, the maximum full filename length may be reduced to 32 characters.

- After you have completed the file exclusion settings by either of the methods, click [Save]. A Confirm window will appear. Notice that if there is any file item and click [Confirm].

Confirm ✕

The file will be appended to the File Exclusion List. If there is any file item with the identical full filename while importing, the file item will be replaced with the new one from the imported file.

Confirm
Cancel

- Use the search bar to search for the information you need.

Configuring Antivirus Profiles

EdgeIPS Pro 216 antivirus is a streaming-based design. The Antivirus Profile can be configured to check HTTP or FTP protocols, and has advanced settings which include file size limitations, compressed file scanning, and the creation or editing of profiles to apply to a policy rule.

In a profile, you can define the following:

- File exceptions (able to import an SHA1-based exception list)
 - Protocol settings for HTTP and FTP
- Advanced settings include:
1. Maximum file size
 2. Scan compressed file

Procedure

1. Go to [Object Profiles] > [Antivirus Profile].
2. Click [Add] to create an Antivirus profile.

The [Create Antivirus Profile] screen will appear.

Create Antivirus Profile
✕

Profile Name* ⓘ

Description ⓘ

Protocol Settings ⚙️

<input checked="" type="checkbox"/> HTTP Protocol Check	Actions when matched	<input type="radio"/> Accept and Log	<input checked="" type="radio"/> Deny and Log
<input checked="" type="checkbox"/> FTP Protocol Check	Actions when matched	<input type="radio"/> Accept and Log	<input checked="" type="radio"/> Deny and Log
<input checked="" type="checkbox"/> SMB Protocol Check	Actions when matched	<input type="radio"/> Accept and Log	<input checked="" type="radio"/> Deny and Log

Advanced Settings

Maximum File Size for Scanning* (1-10 MB)

Deny Oversize File(s)

Scan Compressed File(s) (ZIP & GZIP) ⓘ

Deny Password Protected File(s)

Destroy File(s) Failed to be Decompressed

Save
Cancel

3. Type a descriptive name for the Antivirus profile
4. Type a description.
5. Under [Antivirus Profile Settings] enable:
 - File Filter by Protocol, including: HTTP, FTP and SMB.
 - Actions when matched, including 'Accept and Log' or 'Deny and Log'
6. In advanced settings you can enable:
 - Maximum file size for scanning: maximum file size ranges from 1 to 10MB.
 - Which action to take for oversized files.
7. If you want to scan a compressed file
 - ZIP and GZIP file formats are supported

- Two options are available: "Deny password protected file" and "Destroy files that cannot be decompressed".

8. Click [Save] to save profile.

Configuring File Exceptions

File Exceptions are advanced configurations to except certain files from the antivirus profile(s) you're enabling. The system skips the file scanning based on your list in [File Exception Settings]. This can increase the flexibility of configuration and obtain the real control for your OT network.

The screenshot shows the 'File Exceptions' configuration page. A red box highlights the 'File Exceptions' section, which includes instructions and a 'Download CSV Template' button. Below this is a table of 'Antivirus Profiles' with two entries.

No.	Profile Name	Protocol Settings	Advanced Settings	Description
1	Default_AV_Profile	Enabled HTTP Protocol (Deny and Log), Enabled FTP Protocol (Deny and Log)	Enabled Maximum File Size for Scanning, Enabled Scan Compressed File	
2	AV_Profile1	Disabled HTTP Protocol, Enabled FTP Protocol (Accept and Log)	Enabled Maximum File Size for Scanning, Disabled Scan Compressed File	

Two styles of operation scenarios are provided, either adding file items one by one or importing an edited CSV file with multiple **SHA-1** items. [Download CSV Template](#) Click to download a CSV template file for you to edit.

Procedure

1. Access the web user interface of the EdgeIPS™ Pro 216 device.
2. Go to [Object Profiles] > [Antivirus Profiles].

Scenario 1: Add Each File One at a Time (Steps 3 & 4)

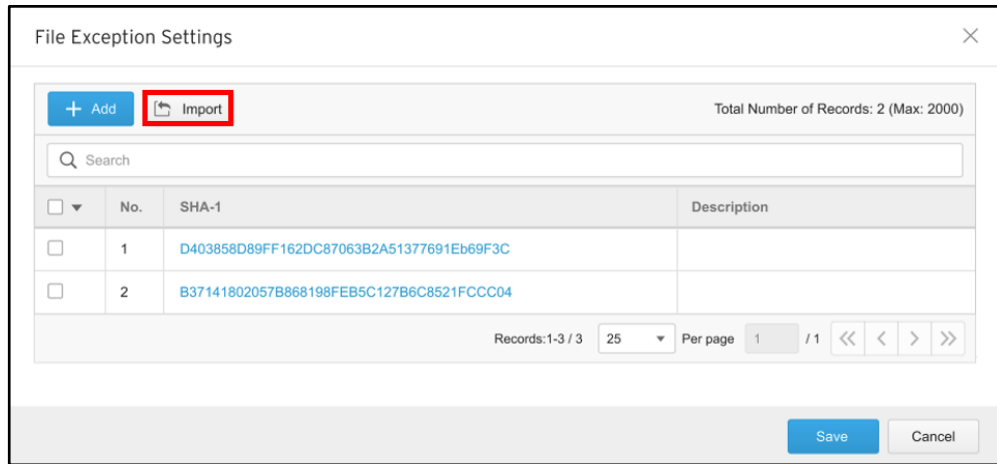
3. Click [File Exception Settings].
4. Click [Add] to add file exception settings item by item.

The screenshot shows the 'File Exception Settings' dialog box. A red box highlights the '+ Add' button. The dialog contains a table with two entries, each with a SHA-1 hash and a description.

No.	SHA-1	Description
1	D403858D89FF162DC87063B2A51377691Eb69F3C	
2	B37141802057B868198FEB5C127B6C8521FCCC04	

Scenario 2: Import an Edited CSV File with Multiple File Items (Steps 5 & 6)

- Click the [Download CSV Template] button to download the CSV template, and fill in complete SHA-1 values and descriptions.
- Click the [Import] button to import the edited CSV file to the file system.



File Exception Settings

+ Add **Import** Total Number of Records: 2 (Max: 2000)

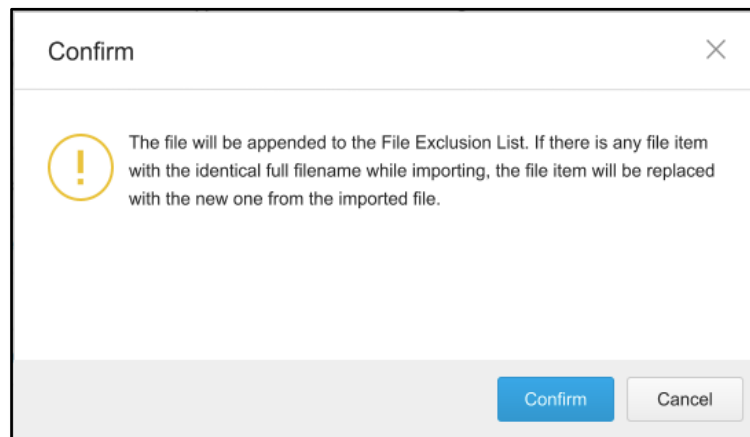
Q Search

<input type="checkbox"/>	No.	SHA-1	Description
<input type="checkbox"/>	1	D403858D89FF162DC87063B2A51377691Eb69F3C	
<input type="checkbox"/>	2	B37141802057B868198FEB5C127B6C8521FCCC04	


Records: 1-3 / 3 25 Per page 1 / 1 << < > >>

Save Cancel

- After you have completed the file exclusion settings by either of the methods, click [Save]. The Confirm window will appear. Notice that if there is any file item and click [Confirm].



Confirm

 The file will be appended to the File Exclusion List. If there is any file item with the identical full filename while importing, the file item will be replaced with the new one from the imported file.

Confirm Cancel

- Use the search bar to search for the information you need.

The Security Tab

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

- **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.
- **Port Security** allows you to set types of security configurations for pair or port, including applying the previous-defined Policy Enforcement ruleset templates.
- **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'.

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.

Configuring Policy Enforcement

Procedure

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



Security > Policy Enforcement

[+ Add](#) Total Number of Records: 1 (Max: 64)

<input type="checkbox"/>	No.	Rule Set Name	Number of Rules	Description	Last Update
<input type="checkbox"/>	1	All	3		2020-08-27T00:38:23+08:00

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

Create Policy Enforcement Rule Settings

Rule Set Name* ⓘ

Description ⓘ

Default Rule Action ⓘ

No.	Status	Rule Name	Source IP / Object Info	Destination IP / Object	D
<input type="checkbox"/>					

Adding Policy Enforcement Rules

Procedure

1. Configure the required object(s).
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 22](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 23](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 24](#).
 - File filter profiles
For more information, see [Configuring File Filter Profiles on page 49](#).
 - Antivirus profiles
For more information, see [Configuring Antivirus Profiles on page 52](#).
2. Go to [Security] > [Policy Enforcement]
3. Under the [Policy Enforcement] tab you will see the following panes:

Security > Policy Enforcement

Total Number of Records: 1 (Max: 64)

No.	Rule Set Name	Number of Rules	Description	Last Update
<input type="checkbox"/> 1	Rule_Set_1	2		2020-09-17T17:34:53+08:00

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

Edit Policy Enforcement Rule Settings

Rule Set Name* ⓘ

Description ⓘ

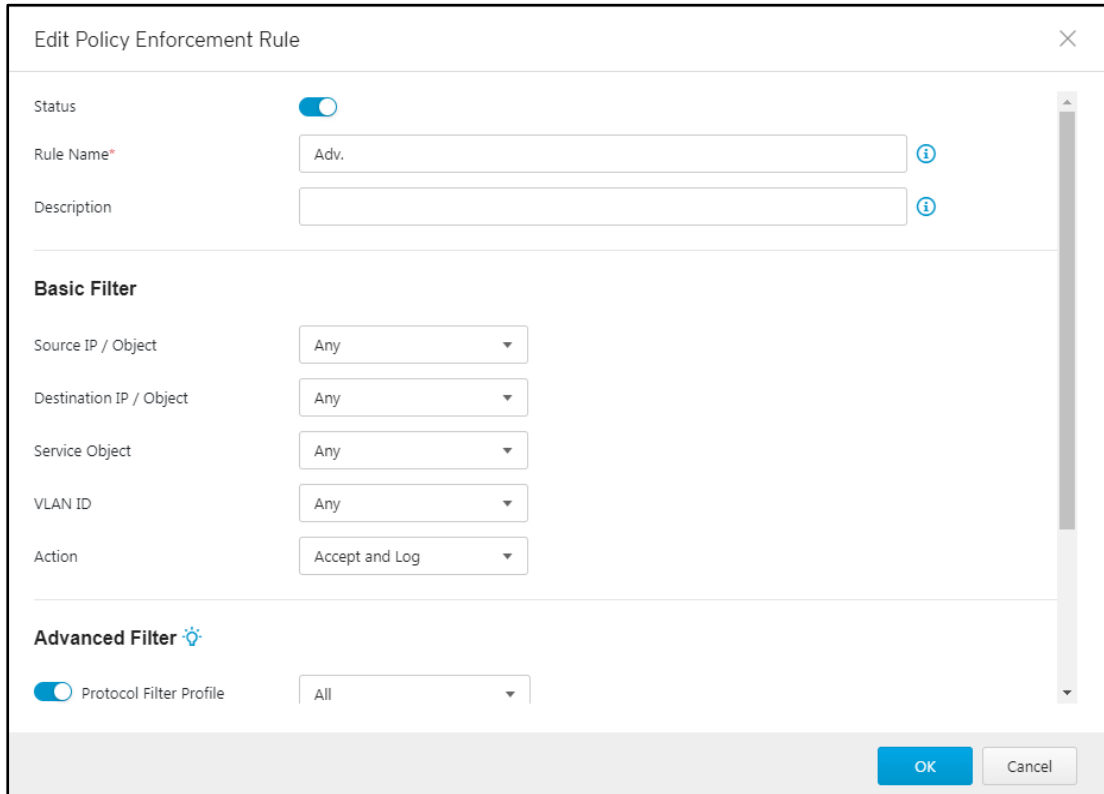
Default Rule Action ⓘ

Total Number of Records: 3 (Max: 2048)

No.	Status	Rule Name	Source IP / Object	Source IP / Object Info	Destination IP / Object	Destination IP / Object Info	Service Object	Service Info	VLAN ID	Action	Protocol Filter Profile	Protocol F
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	ftp	Any	Any	Any	Any	Object (FTP)	TCP (20 - 21)	Any	Deny and Log	-	-
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	smb	Any	Any	Any	Any	Object (SMB)	TCP (139),TCP (445)	Any	Deny and Log	-	-
<input type="checkbox"/> 3	<input checked="" type="checkbox"/>	Adv.	Any	Any	Any	Any	Any	Any	Any	Accept and Log	All	Deny and L

Records: 1-3 / 3 25 per page 1 / 1 << < > >>

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



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

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

10. Under the [Destination IP / IP Object Profile] drop-down menu, select either one of the following for the destination IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object
11. Under the [Service Object] drop-down menu, select either one of the following for the layer 4 criteria:
 - TCP
 - You can further specify the port range for this protocol.

- UDP
You can further specify the port range for this protocol.
- ICMP
You can further specify the Type and Code for this protocol.
- Custom
You can further specify the protocol number for this protocol. The term 'protocol number' refers to the one defined in the internet protocol suite.
- Service Object

Note: You need to select a [service object] from service object profiles that have been created beforehand.

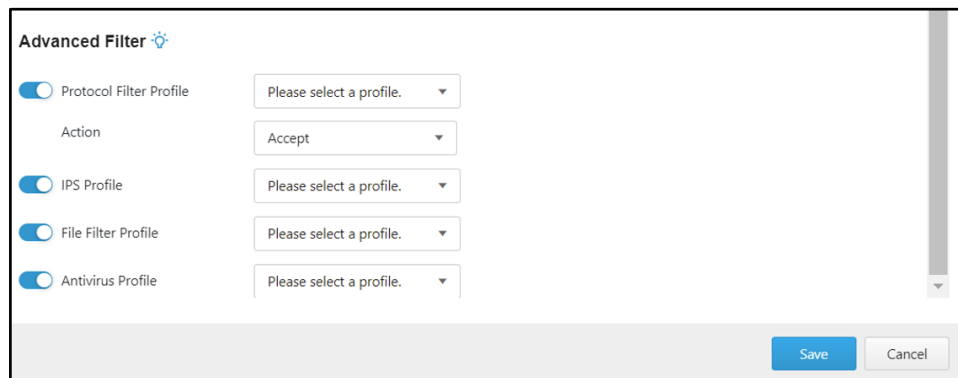
12. Under the [VLAN ID] drop-down menu, select either one of the following for the layer 4 criteria:

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

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

13. Under 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.
- Advanced Filter Enable: When you select "Accept" or "Accept and Log" you will be able to conduct further actions based on the protocol filter, IPS, file filter profiles and Antivirus Filter profile.
 - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
 - Under the [Protocol Filter Action], select whether to allow or deny network traffic that matches the protocol filter.



Advanced Filter ⚙️

<input checked="" type="checkbox"/> Protocol Filter Profile	Please select a profile. ▾
Action	Accept ▾
<input checked="" type="checkbox"/> IPS Profile	Please select a profile. ▾
<input checked="" type="checkbox"/> File Filter Profile	Please select a profile. ▾
<input checked="" type="checkbox"/> Antivirus Profile	Please select a profile. ▾

Save Cancel

- Under the [IPS Profile] drop-down menu, select an IPS profile you have defined beforehand.
 - Under the [File Filter Profile] drop-down menu, select a file filter profile you have defined beforehand.
 - Under the [Antivirus Filter Profile] drop-down menu, select a file filter profile you have defined beforehand.
14. Click [OK] to save the configuration.

Managing Policy Enforcement Rules

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

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.

Note: When more than one policy enforcement rule is matched, EdgeIPS Pro 216 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.

Port Security

Port Security settings allows you to set security configurations per pair or per port.

Security Operation Mode ('Inline/Offline Mode'), as a system operation mode, is designed to detect the traffic and see if any cyber threats intrude into your network. If an intrusion occurs, you can decide to act immediately or only record the data via the port mirroring.

Prevention/Monitor Mode, as a security deployment mode, is functioned to decide to prevent or monitor cyber threats.

Hardware Bypass Mode, is the feature to provide different scenarios to overcome the failover situations on your OT network. **'Fail Open'** allows all network traffic to pass through the appliance 'even' when the system failed. With the higher priority on access than security, the system will remain open to operate under failure conditions. **'Fail Close'** shuts down links for interface pairs and prevents any network traffic from passing through the appliance when failure is detected. Since the security concern overrides the need for access, the further system operation will be prevented. **'Force Open'** bypasses all network traffic to pass through the appliance to troubleshoot problems.

DoS Settings are aimed at preventing the Denial of the Service attack to flood/crash the service with the traffic or the trigger, making it inaccessible for the intended users.

LFPT, Link Fault Pass Through, is configured to constantly monitor the physical links to prevent data loss, lest, when one side of the link fails, the other side still continues to transmit packets

and waits for a response that will never arrive. When an incident of link failure occurred on one node, the link failure signal will pass to the other node so system administrators are able to troubleshoot the problem within a short period of time, minimalizing the potentially severe impact on the service.

Note: Before you configure Port Security, Port Settings should be configured first.

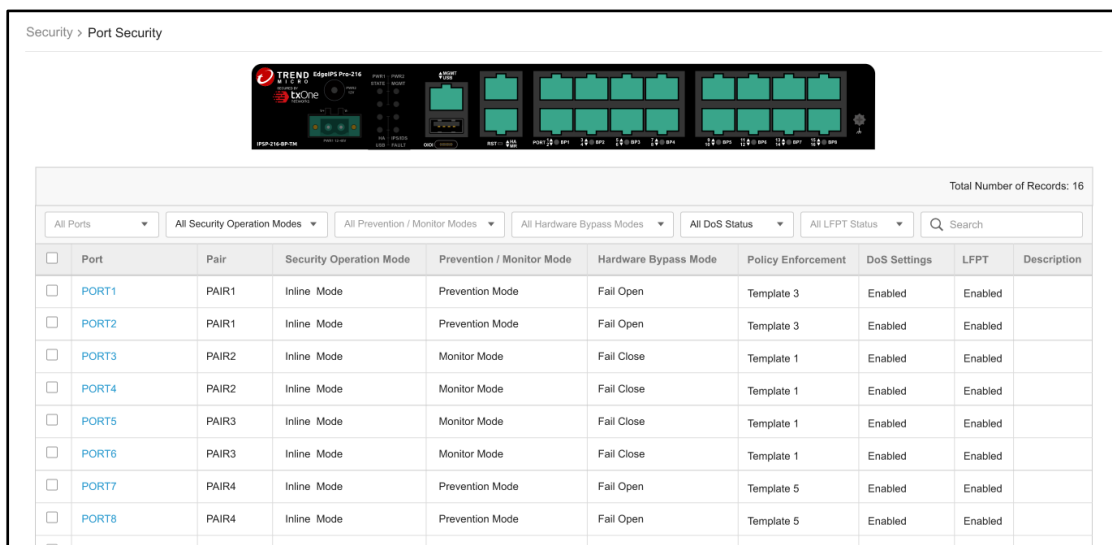
The following table describes the tasks you can perform when you configure a list of port security settings:

Settings	Descriptions
Interface	Port name information
Pair Info	Port pair information
Description	Add a description for configuring the port
Security Operation Mode	Security operation mode includes Inline Mode and Offline mode
Prevention / Monitor Mode	Monitor mode: Detect and monitor abnormal protocol accesses to the OT assets, without blocking network attacks.
	Prevention mode: Block abnormal protocol access to OT assets and generate logs.
Hardware Bypass	Configure hardware bypass operation mode
Policy Enforcement	Apply selected policy enforcement rule set
Denial of Service Prevention Settings (DoS Settings)	Configure Denial of Service prevention settings
LFPT	The Link Fault Pass Through (LFPT) provides constant monitoring of the links connected to EdgeIPS Pro. If one side of the physical port link is lost, EdgeIPS Pro 216 disconnects the other side of the physical port link as well.

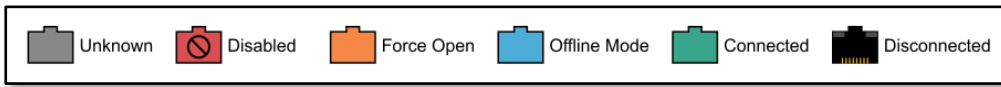
Configuring Port Security

Procedure

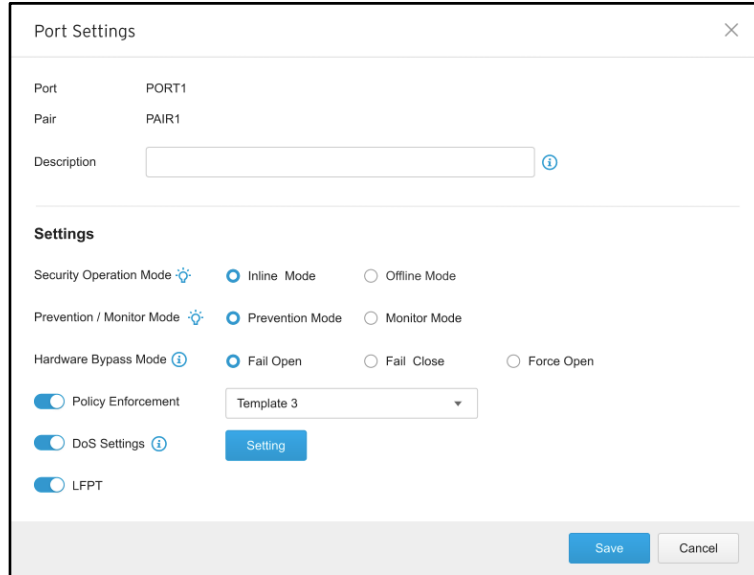
1. Access the web user interface of the EdgeIPS™ Pro 216 device.
2. Go to [Security] > [Port Security].
3. On the [Port Security] page, the following screen will appear.



The illustration below shows each type of status.



4. Click a specific [Port] to configure port security. The following window will pop up.



Note: Before you configure [Port Security], [Port Settings] should be configured first.

- Input a remark for [Description] to facilitate the management.
- Select a mode (either 'Inline Mode' or 'Offline Mode') for [Security Operation Mode]. The following table lists security operation mode definitions.

Security Operation Modes	Descriptions
Inline Mode	EdgeIPS™ Pro 216 works as an IPS (Intrusion Prevention System) and checks the traffic in each pair with Policy Enforcement Rule(s) and IPS profiles(s) for cyber threats.
Offline Mode	EdgeIPS™ Pro 216 works as an IDS (Intrusion Detection System). The odd number of port(s) will be disabled and the even number of port(s) will be enabled to receive the traffic from the mirror port which is used to manage switch/firewall and detect/log cyber threats. Besides, Prevention Mode/Monitor Mode, Hardware Bypass Mode and LFPT are not configurable.

- Select a mode (either 'Prevention Mode' or 'Monitor Mode') for [Prevention/Monitor Mode]. The following table lists the according actions.

Security Operation Modes	Prevention/Monitor Modes	Actions
'Inline Mode'	'Monitor Mode'	<ul style="list-style-type: none"> Monitor and detect abnormal protocol access attempts to the OT assets, without blocking network attacks. Generate logs.
	'Prevention Mode'	<ul style="list-style-type: none"> Block abnormal protocol access to OT assets. Generate logs.
'Offline Mode'	Monitor and Log	<ul style="list-style-type: none"> Monitor and detect abnormal protocol access attempts to the OT assets, without blocking network attacks. Generate logs.

8. Select a mode ('Fail Open', 'Fail Close', or 'Force Open') for [Hardware Bypass Mode]. The following table lists hardware bypass mode definitions.

Settings	Descriptions
Hardware Bypass Mode	Bypass ports allow uninterrupted network traffic even if a single in-line appliance is shut down or hangs. The settings for hardware bypass mode are listed as below: <ul style="list-style-type: none"> 'Fail Open': Allows all network traffic to pass through the appliance when system fail. 'Fail Close': Closes the links for the interface pair and prevents any network traffic from passing through the appliance. 'Force Open': Always Bypasses all network traffic to pass through the appliance.

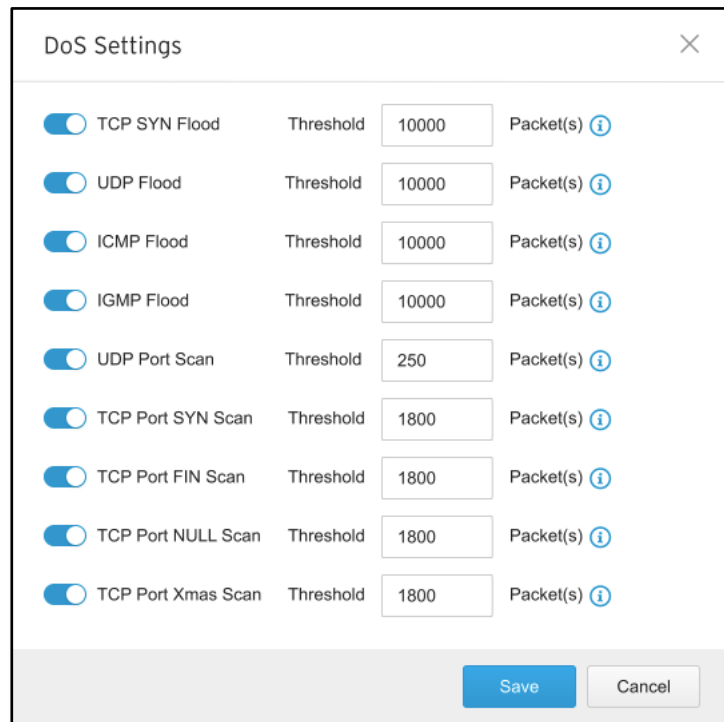
9. Use the toggle to enable [Policy Enforcement], then apply a created policy enforcement rule set from the dropdown list.



10. Use the toggle to enable [DoS Settings].



11. Click the [Setting] button. Then the following window will pop up.



The image shows a 'DoS Settings' dialog box with a close button (X) in the top right corner. It contains a list of nine DoS attack types, each with a toggle switch, a 'Threshold' label, a text input field, and a 'Packet(s)' label with an information icon (i). The settings are as follows:

Attack Type	Threshold	Packet(s)
TCP SYN Flood	10000	Packet(s) i
UDP Flood	10000	Packet(s) i
ICMP Flood	10000	Packet(s) i
IGMP Flood	10000	Packet(s) i
UDP Port Scan	250	Packet(s) i
TCP Port SYN Scan	1800	Packet(s) i
TCP Port FIN Scan	1800	Packet(s) i
TCP Port NULL Scan	1800	Packet(s) i
TCP Port Xmas Scan	1800	Packet(s) i

At the bottom right of the dialog box are two buttons: 'Save' and 'Cancel'.

12. You can optionally configure the threshold of packets for each types of DoS rules.

Note: Flood/Scan Attack Protection rules utilize a detection period and threshold mechanisms to detect an attack. During a detection period (typically every 5 seconds), if the number of anomalous packets reaches the specified threshold, an attack detection occurs. The security node blocks subsequent anomalous packets until the end of the detection period. After the detection period, the security node will again allow anomalous packets until the threshold is reached.

13. Use the toggle to enable [LFPT].



14. Click [Save] to complete the specific port security settings.

Suspicious Objects

Suspicious objects are objects with the potential to expose systems to danger or loss. This 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.

The screenshot shows the EdgIPS web interface. At the top, there's a navigation bar with tabs like System, Viability, Device, Object Profiles, Security, Pattern, Logs, Administration, and About. The main content area is titled 'Security > Suspicious Objects'. Under 'Suspicious Object General Setting', there's a toggle for 'Suspicious Object' which is turned on, and a note: 'Enabling this feature and Suspicious Object priority is higher than Policy Enforcement.' Below that, there are radio buttons for 'Suspicious Object Operation Mode' with 'Monitor Mode' selected and 'Prevention Mode' unselected. The 'Suspicious Object Rule List' section contains a table with columns: No., ID, Type, Source, Object Content, Risk Level, Last Update Time, and Expiration Time. The table lists six rules, all of type 'Link' and source 'LT', with various IP addresses and protocols in the 'Object Content' column. All rules have a 'Medium' risk level and update times from 2021-03-29T17:47:23+08:00.

The suspicious objects are imported to ODC from the external SO sources, such as third-party products, via the Suspicious Object API keys. Two third-party source support options for importing malicious nodes and links are TrendMicro DDI (Version 5.8) and Nozomi Guardian.



The Suspicious Objects feature can bring benefits for you to:

- Extend the protection from IT network to OT network
- Align the security policy with the central management
- Block malicious files for download and malicious links for unauthorized access
- Customize actions for specific suspicious objects with the local device management

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

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.

Security > Suspicious Objects

Suspicious Object General Settings

Suspicious Objects Enabling this feature and Suspicious Object is of higher priority than Policy Enforcement.

Suspicious Object Operation Mode Monitor Mode Prevention Mode

Suspicious Object Rule List

Drop and Log | Bypass and Log | 2 selected Drop: 412 | Bypass: 100 | Total: 512

All Types | All Sources | All Risk Levels | All Actions |

<input type="checkbox"/>	ID	Type	Source	Object Content	Risk Level	Last Update Time	Expiration Time	Action Status
<input checked="" type="checkbox"/>	12123412	Node	DDI-1	10.10.10.1	High	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Drop and Log
<input checked="" type="checkbox"/>	22123412	Link	DDI-2	Src IP=10.100.100.9, Dst IP=192.168.1.1, Proto=6*	Critical	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Bypass and Log
<input type="checkbox"/>	32123412	Node	Nozomi-1	10.10.10.1	High	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Drop and Log
<input type="checkbox"/>	42123412	Link	Nozomi-2	Src IP=10.100.100.9, Dst IP=192.168.1.1, Proto=6*	High	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Bypass and Log
<input type="checkbox"/>	52123412	Link	DDI-2	Src IP=10.100.100.9, Dst IP=192.168.1.1, Proto=6*	Critical	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Drop and Log
<input type="checkbox"/>	62123412	Node	Nozomi-1	10.10.10.1	Critical	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Drop and Log
<input type="checkbox"/>	72123412	Link	Nozomi-1	Src IP=10.100.100.9, Dst IP=192.168.1.1, Proto=6*	Critical	2020-11-22T07:51:49+08:00	2020-11-22T07:51:49+08:00	Drop and Log

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:

Modes	Suspicious Object Operation Modes	Action Settings	Actions Performed
Inline Mode	Prevention Mode	Prevent and Log	<ul style="list-style-type: none"> Blocks network node or network link. Generates logs.
	Monitor Mode	Monitor and Log	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Detects network node or network link Generates logs.

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

The Pattern Tab

This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the EdgeIPS Pro 216 device.

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

Viewing Device Pattern Information

Procedure

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

Pattern > Pattern Update

IPS Pattern Update

Pattern Version: TM_IPSP_220211_09

Pattern Build Date: 2022-02-11T01:10:23Z

Pattern Update File Path:

Pattern Information:

Antivirus Pattern Update

Pattern Version: 2.007

Pattern Build Date: 2021-12-29T03:27:02Z

Pattern Update File Path:

Pattern Information:

3. The [IPS Pattern information] pane shows the current [IPS Pattern Version] and [IPS Pattern Build Date].
4. The [Antivirus Pattern information] pane shows the current [Antivirus Pattern Version] and [Antivirus Pattern Build Date].

Manually Updating the Pattern

Procedure

1. Go to [Pattern] > [Pattern Update].
2. Under the [Pattern Update] tab you will see the following pane by IPS pattern or Antivirus pattern.

3. Click [Select] by IPS Pattern or Antivirus pattern.
4. Manually select the pattern to be deployed to the device.

IPS Pattern Update	
Pattern Version	TM_IPSP_210719_21
Pattern Build Date	2021-07-19T13:07:10Z
Pattern Update File Path	<input type="text"/> <input type="button" value="Select"/> <input type="button" value="Upload"/>

Antivirus Pattern Update	
Pattern Version	2.004
Pattern Build Date	2021-08-05T00:57:37Z
Pattern Update File Path	<input type="text"/> <input type="button" value="Select"/> <input type="button" value="Upload"/>

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

Downloading Release Notes

Procedure

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

Pattern Information	<input type="button" value="↓ Release Note"/>
-------------------------------------	---

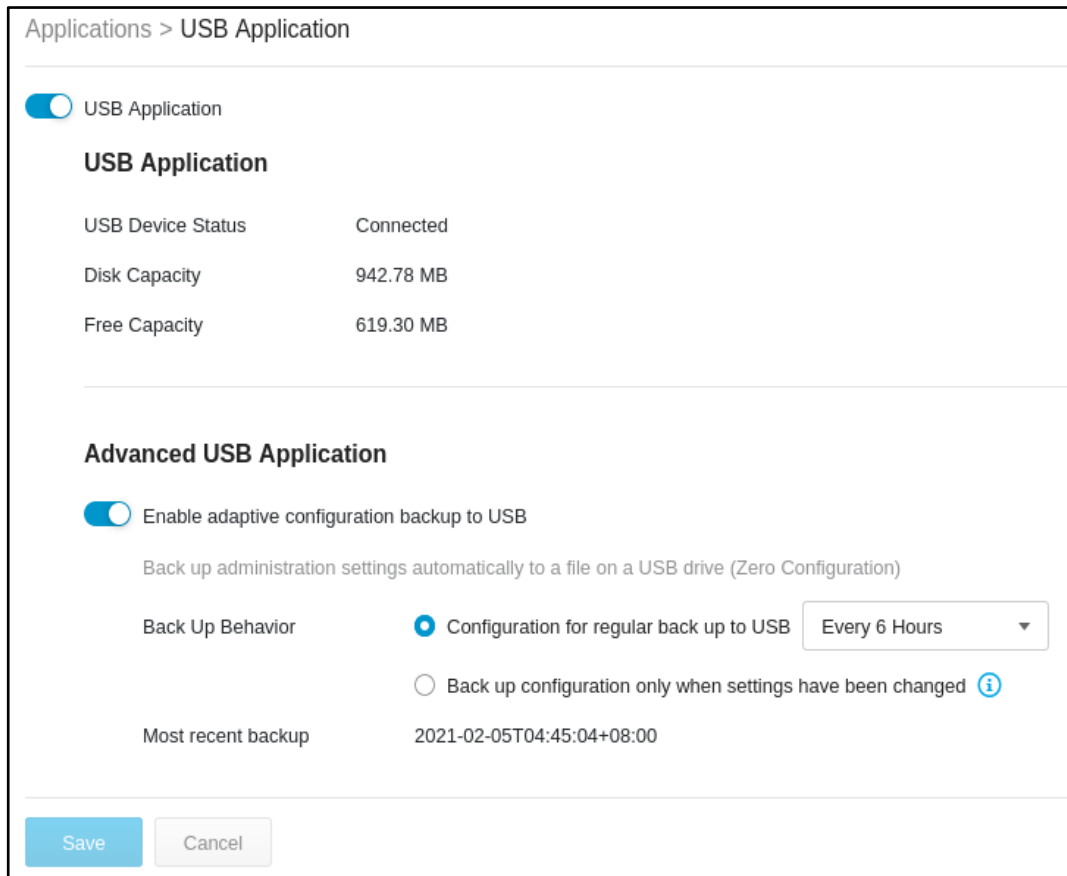
The Application Tab

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

USB Application

Procedure

1. Go to [Application] > [USB Application].
2. Under the [USB Application] tab you will see the following pane.
3. Click [Enable] to enable USB Application usage. This toggle switch controls whether the USB port is enabled or not.



4. Once enabled and if a USB disk is plugged in, you can see the status and view the information about the disk capacity and remaining free space.

Note: If USB Application 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 on page 93](#).

Advanced USB Application

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

Advanced USB Application

Enable adaptive configuration backup to USB

Back up administration settings automatically to a file on a USB drive (Zero Configuration)

Back Up Behavior Configuration for regular back up to USB Every 6 Hours ▼

Back up configuration only when settings have been changed ⓘ

Most recent backup 1970-01-01T08:00:00+08:00

2. Back up 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.

Packet Capture

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

Enabling Packet Capture

Procedure

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

Applications > Packet Capture

Packet Capture

Packet Capture Download List

Total Enabled Number of Records: 0 (Max: 20)

All Statuses ▼ All Categorys ▼ All Risk Levels ▼

Status	ID	Category	Risk Level	Name
<input type="checkbox"/>	1130513	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)
<input type="checkbox"/>	1130512	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)
<input type="checkbox"/>	1130511	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)
<input type="checkbox"/>	1130510	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)
<input type="checkbox"/>	1130513	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)
<input type="checkbox"/>	1130512	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)
<input type="checkbox"/>	1130511	Web Threats	High	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)
<input type="checkbox"/>	1130510	Buffer Overflow	High	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)

1-25 / 800 25 Per page 1 / 352 << < > >>

2. Click [Enable] to enable IPS packet capture.
3. You can see the entire IPS rule list and select a rule to "Enable" for IPS rule capture.

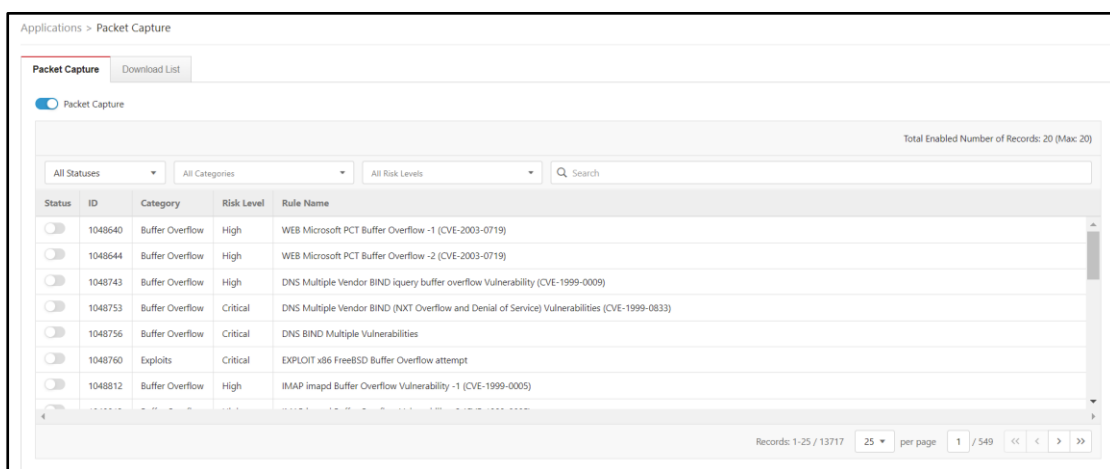
- Up to 20 rules can be selected for IPS Rule packet capture support.

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

Download Captured Packet

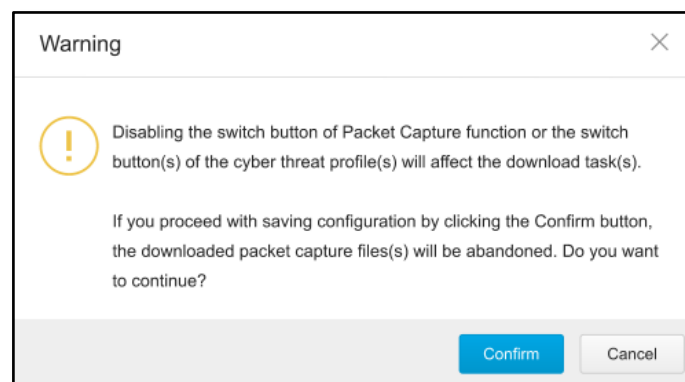
Procedure

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



The screenshot shows the 'Packet Capture' interface. At the top, there are tabs for 'Packet Capture' and 'Download List'. A toggle switch for 'Packet Capture' is turned on. Below this, there are filters for 'All Statuses', 'All Categories', and 'All Risk Levels', along with a search bar. A table lists several rules with columns for Status, ID, Category, Risk Level, and Rule Name. The rules listed include: WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719), WEB Microsoft PCT Buffer Overflow -2 (CVE-2003-0719), DNS Multiple Vendor BIND query buffer overflow Vulnerability (CVE-1999-0009), DNS Multiple Vendor BIND (NXT Overflow and Denial of Service) Vulnerabilities (CVE-1999-0833), DNS BIND Multiple Vulnerabilities, EXPLOIT x86 FreeBSD Buffer Overflow attempt, and IMAP imapd Buffer Overflow Vulnerability -1 (CVE-1999-0005). At the bottom right, it shows 'Records: 1-25 / 13717' and '25 per page'.

- You can click the download icon to download the zipped archive to your disk.
- 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.



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

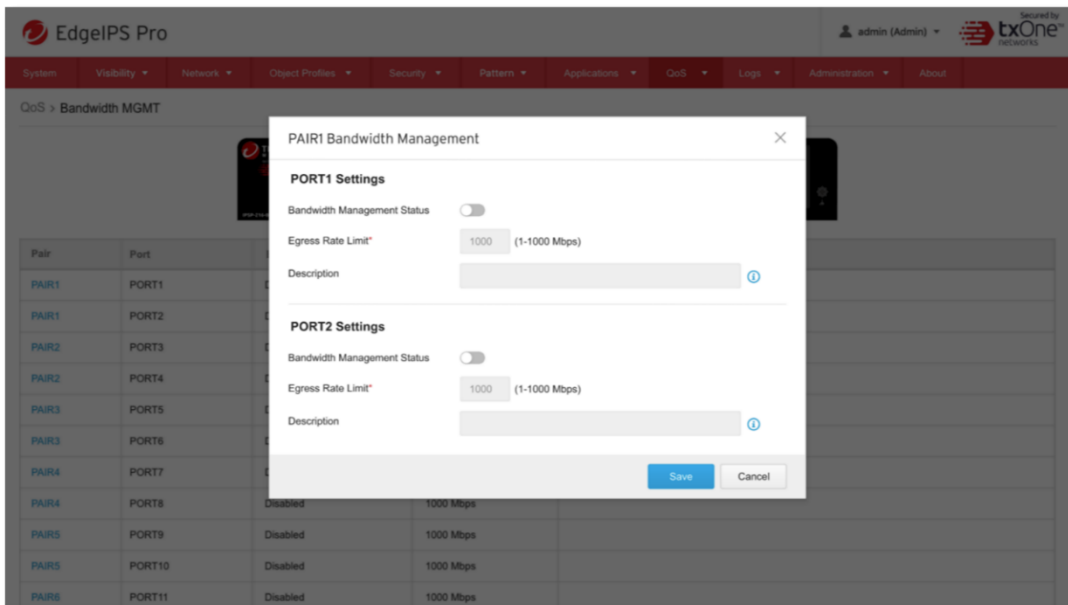
The QoS Tab

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

Configuring Bandwidth MGMT

Procedure

1. Go to [QoS] > [Bandwidth MGMT].
2. Select a [PAIR] to manage a port's bandwidth settings.



3. Enable [Bandwidth Management Status] on the selected [Port] to configure Egress Rate Limit settings.
4. Click [OK] to complete bandwidth management.

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

The Logs Tab

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

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

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

Viewing Cyber Security Logs

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

Procedure

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

The following table describes the cyber security log information.

Fields	Descriptions
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. 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.

Fields	Descriptions
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.

Viewing Policy Enforcement Logs

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

Procedure

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

The following table describes the policy enforcement log information.

Fields	Descriptions
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. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
IP Protocol Name	The IP protocol name of the packet.
Action	The action performed based on the policy settings.

Viewing Protocol Filter Logs

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

Procedure

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

The following table describes the protocol filter log information.

Fields	Descriptions
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule set and the matched policy rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.

Fields	Descriptions
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.
Cmd / Fun No.	The command or function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing File Filter and Antivirus Logs

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

Procedure

1. Go to [Logs] > [File Filter and Antivirus Logs]

The following table describes the log table.

Fields	Descriptions
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 Type	The type of log, either "File Filter" or "Antivirus"
Profile Name	The name of the file filter profile or AntiVirus 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.
Virus Name	The name of the virus
Extra Information	Extra information provided with the file filter log.
Action	The action performed based on the policy settings.

Viewing Suspicious Object Logs

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

Procedure

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

The following table describes the suspicious object log information.

Fields	Descriptions
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.

Viewing Asset Detection Logs

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

Procedure

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

The following table describes the asset detection log information.

Fields	Descriptions
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.

Viewing System Logs

You can view details about system events on the device.

Procedure

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

The following table describes the system log information.

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

Viewing Audit Logs

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

Procedure

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

The following table describes the audit log information.

Fields	Descriptions
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.

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

The Administration Tab

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

Account Management

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.

Tasks	Descriptions
Add account	Click Add to create a new user account. For more information, see Adding a User Account on page 79 .
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.

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

User Roles

The following table describes the permissions matrix for user roles.

Sub-Tabs	Actions	User Roles			
		Admin	Operator	Viewer	Auditor
System	View	Yes	Yes	Yes	Yes
	All operations	Yes	Yes	Yes	Yes
Visibility	View	Yes	Yes	Yes	No
	All operations	Yes	Yes	Yes	No
Network	View	Yes	Yes	No	No
	All operations	Yes	No	No	No
Object Profiles	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Security	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Pattern	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Application	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
QoS	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Logs -	View	Yes	Yes	Yes	No

excluding Audit Logs					
Audit Logs	View	No	No	No	Yes
Administration	View	Yes	No	No	No
	All operations	Yes	No	No	No

Built-in User Accounts

The following table lists the built-in user accounts in the device.

Built-in default Account IDs	User Roles	Default Passwords
admin	Admin	txone
auditor	Auditor	txone

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

Adding a User Account

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

Procedure

1. Go to [Administration] > [Account Management].
2. Click [Add].
The Add User Account screen will appear.
3. Configure the account settings.

Fields	Descriptions
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 <i>Note: Log on to the management console with an administrator account to access the Accounts tab. User Roles on page 78.</i>

4. Click [Save].

Changing Your Password

Procedure

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

4. Click [Save].

Configuring Password Policy Settings

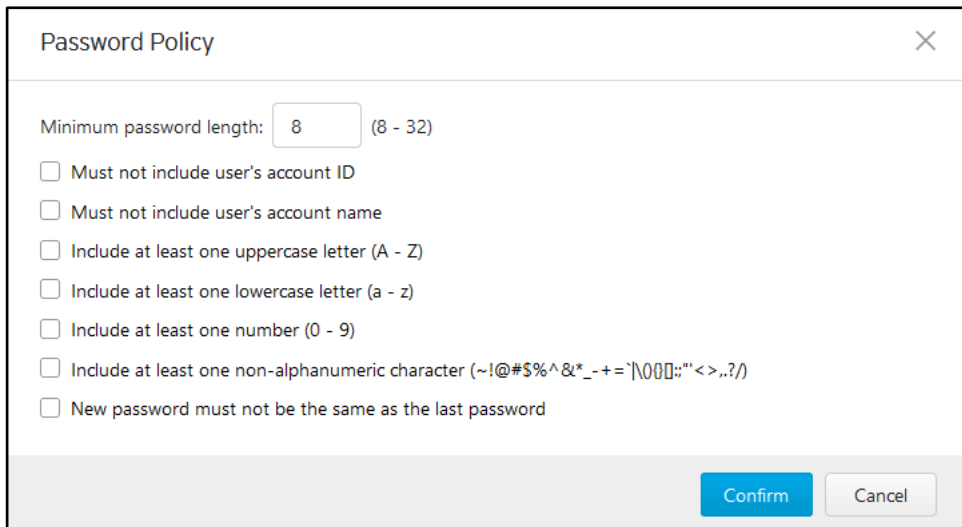
EdgeIPS Pro 216 provides password policy settings to enhance web console access security.

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.

Note: If strong passwords are required, when a user submits a new password, the password policy determines whether the password meets your company's established requirements. Strict password policies may sometimes increase costs to an organization when users select passwords that are too difficult to remember. Users call the help desk when they forget their passwords, or keep passwords in easily accessible locations 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 option(s) that meet(s) your required password policy.
4. Click Save.

Auth Services

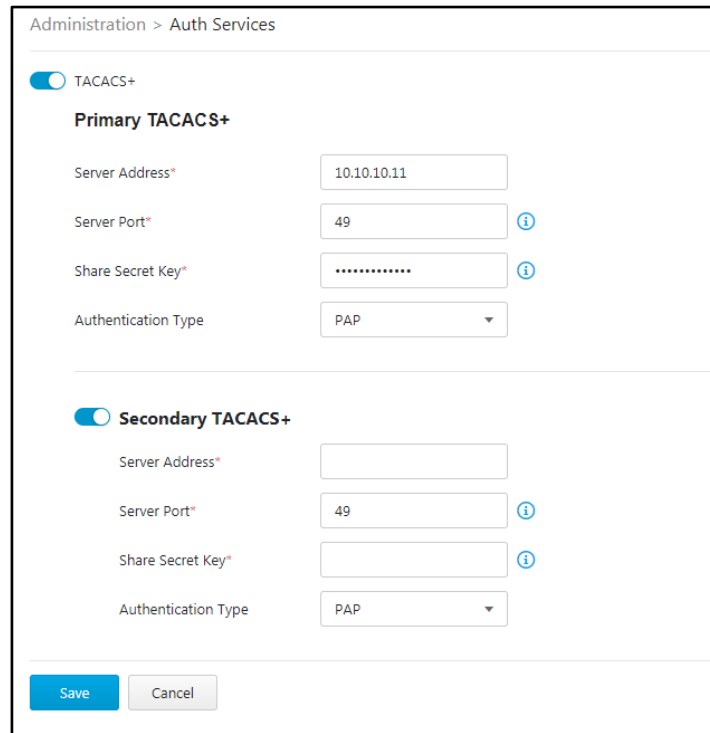
Use the [Auth Services] tab to configure the TACACS+ of the device.

Configuring TACACS+

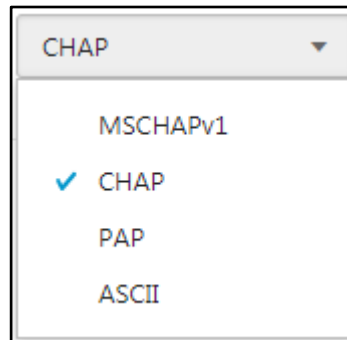
Procedure

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

- In the [TACACS] pane, provide the Primary and Secondary TACACS+ Servers for the device.



- 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.

System Management

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

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

Configuring Device Name and Device Location Information

Procedure

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

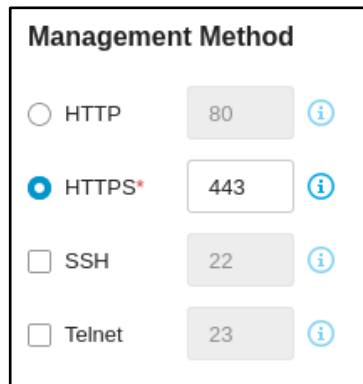


Configuring Management Method and Access Control List

Configuring Management Protocols and Ports

Procedure

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

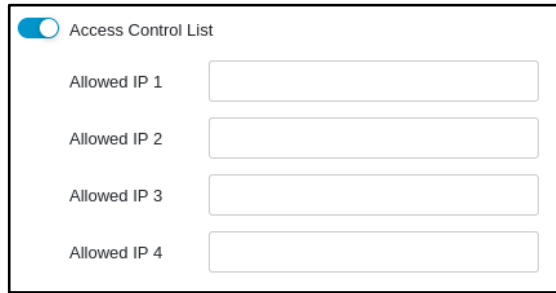


Note: The HTTP and HTTPS protocols are used for connecting to the web management console. The SSH and Telnet protocols are used for connecting to the CLI commands.

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 EdgeIPS Pro 216 and your network is not stable or disconnected, enable the toggle to ping to the Management Interface.



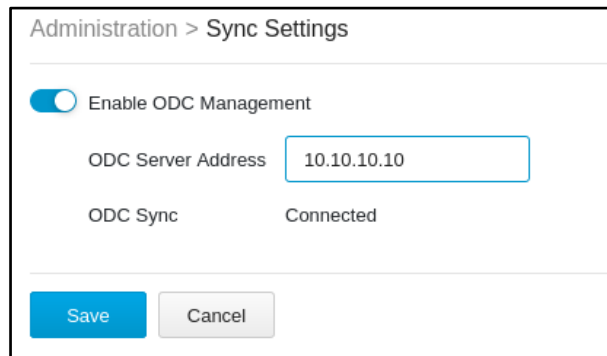
The Sync Setting Tab

EdgeIPS Pro 216 can be managed by a TXOne ODC (Operational Technology Defense Console). Use this tab to register the EdgeIPS Pro 216 to a TXOne ODC.

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.



The Syslog Tab

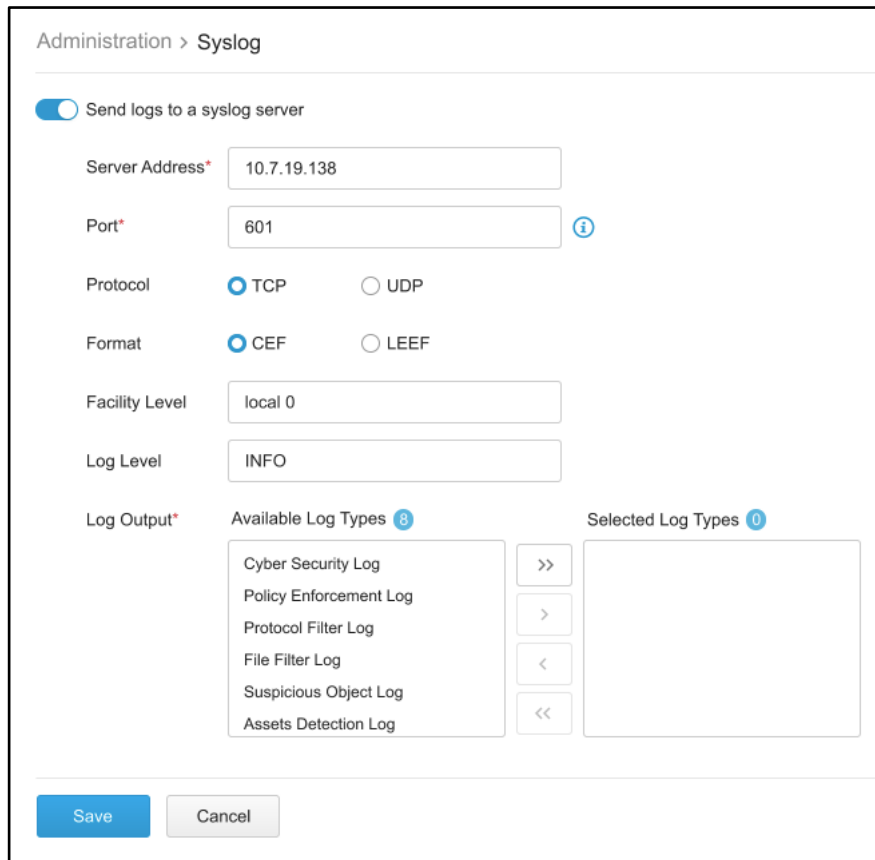
The EdgeIPS Pro 216 system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) and Log Event Extended Format (LEEF) syslog messages are used in EdgeIPS Pro.

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

Configuring Syslog Settings

Procedure

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



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

Fields	Descriptions
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.
Log Level	Select a Syslog severity level. This device only sends logs with the selected severity level or higher to the Syslog servers. For more information, see Syslog Severity Levels on page 85 .

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

Syslog Severity Levels

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

Levels	Severities	Descriptions
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.

Syslog Severity Level Mapping Table

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

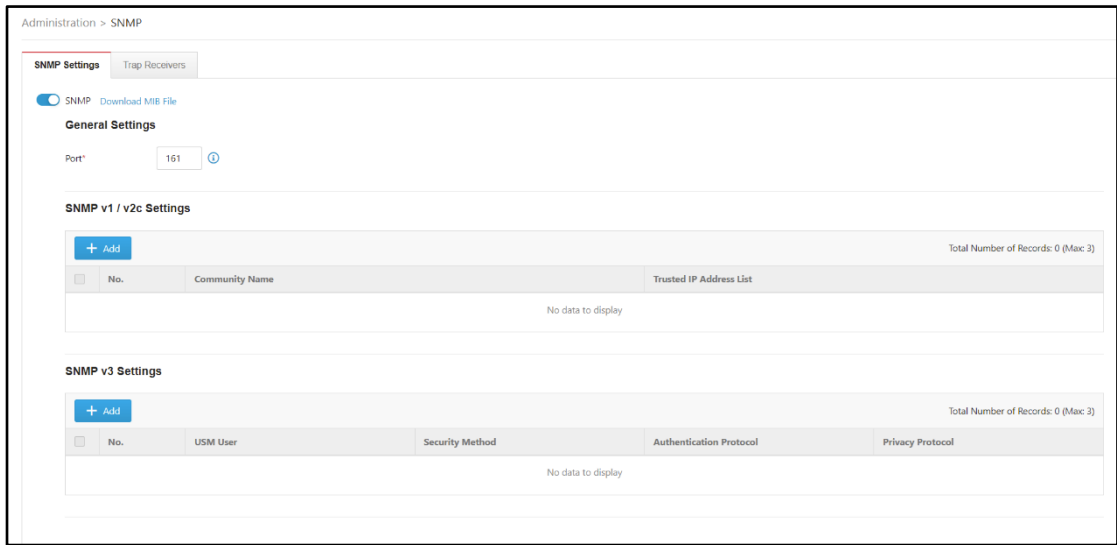
Policy Enforcement / Protocol Filter Actions	Cyber Security Severity Levels	Syslog Severity Levels
		0 - Emergency
	Critical	1 - Alert
	High	2 - Critical
		3 - Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

The SNMP Tab

The Simple Network Management Protocol is a protocol used for exchanging management information between Edge series devices. EdgeIPS Pro 216 supports SNMP v1/v2c and a more secure v3, as well as SNMP traps.

Procedure

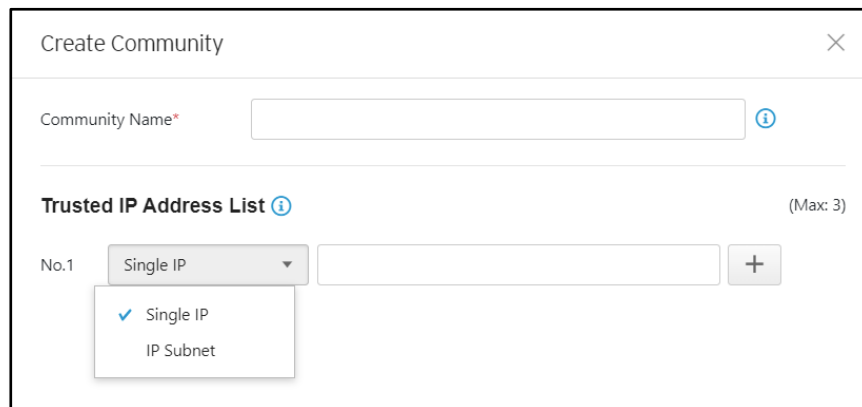
1. Go to [Administration] > [SNMP]
2. Click [Enable] to enable the SNMP function.
3. Under General settings, you can change SNMP port. The default setting is Port 161.
4. You can click the "Download MIB file" link to download the EdgeIPS Pro 216 MIB file.



Configuring SNMP v1/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

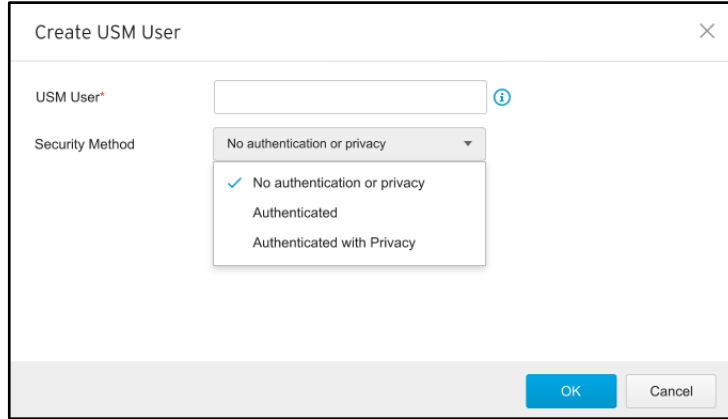


- c. Click [OK] to create a new SNMP v1/v2c community

Configuring SNMP v3

Procedure

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

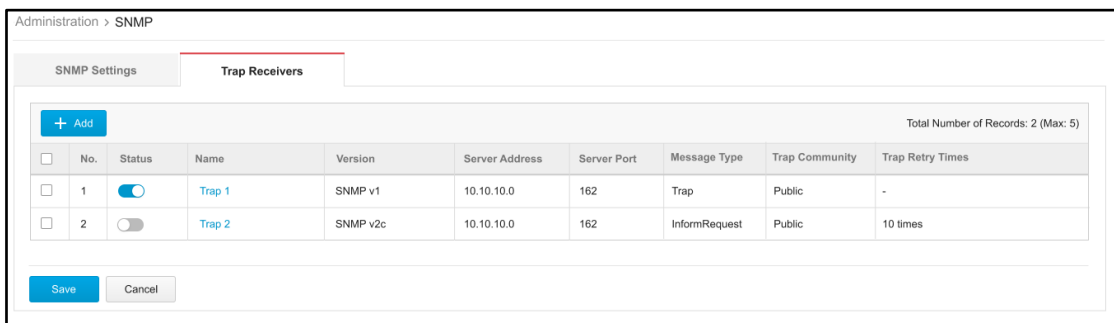


3. Enter USM user.
4. Under [Security Method], select one of the following options:
 - a. No authentication or privacy.
 - b. Authenticated – including SHA and MD5. You can select an appropriate authentication protocol and enter an Authentication Key.
 - c. Authenticated with Privacy – also including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

Configuring SNMP Trap Receivers

Procedure

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



No.	Status	Name	Version	Server Address	Server Port	Message Type	Trap Community	Trap Retry Times
1	<input checked="" type="checkbox"/>	Trap 1	SNMP v1	10.10.10.0	162	Trap	Public	-
2	<input type="checkbox"/>	Trap 2	SNMP v2c	10.10.10.0	162	InformRequest	Public	10 times

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 – options include SNMP v1 and SNMP v2c
 - e. Enter [Server Address].
 - f. Enter [Server Port]. The default setting is port 162.

- g. Select a message type, "Trap" and "informRequest".
- h. Enter Trap Community. The default name is PUBLIC.
- i. Trap Retry Times: The amount of retries ranging from 1 to 10 times.
- k. Select what will trigger an Event Notification.

Create Trap Receiver
✕

Status

Name* ⓘ

Description ⓘ

Version SNMP v1 SNMP v2c

Server Address*

Server Port* ⓘ

Message Type Trap InformRequest

Trap Community*

Trap Retry Times ▼

Event Notification*

- High CPU Usage ⓘ
- High Memory Usage
- Low Disk Space for Logs
- Interface IP Address Changed
- Network Interface Linked Up
- Network Interface Linked Down
- HA Hearbeat Failed

Note: When the CPU usage reaches 70%, 80% or 95%, the system will send an event notification.

Note: When the memory usage reaches 80%, the system will send an event notification.

Note: When the log storage reaches 95%, the system will keep sending event notifications until the log storage is below 95%.

Note: When the fan fails, the system will keep sending event notifications until the fan status is recovered.

Note: When the power fails, the system will keep sending event notifications until the power status is recovered.

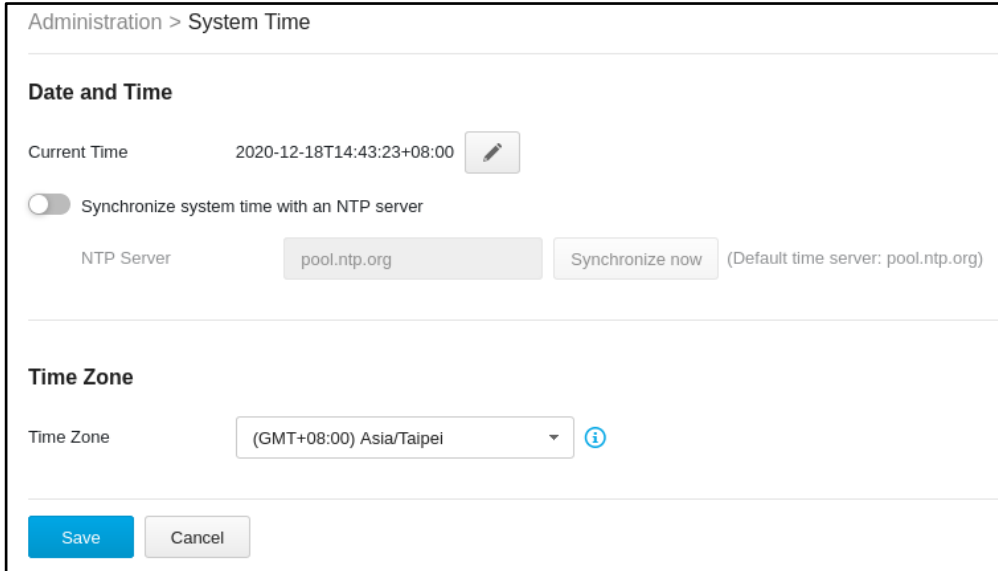
The System Time Tab

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system time.

Configuring System Time

Procedure

1. Go to [Administration] > [System Time].



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

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

The Back Up / Restore Tab

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

We recommend the following:

- Backing up the current configuration before each import operation.
- Performing the backup operation when the EdgeIPS Pro 216 is idle. Importing and exporting configuration settings affects the performance of EdgeIPS Pro.

Backing Up a Configuration

Procedure

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

Administration > Backup / Restore

Backup Configuration

Back up policies and administration settings to a file on your computer.

Restore Configuration

Restore the configuration from a backup file. It is recommended that you back up your current configuration before you replace it.
Note: Restoring replaces current configuration settings.

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

Restoring a Configuration

Follow the steps below to restore the configurations of an EdgeIPS Pro.

Procedure

1. Go to [Administration] > [Backup / Restore].
 2. Under the [Restore Configuration] section, click the [Select File] button, and proceed to import the file.
- All services will restart. It can take some time to restart services after applying imported settings and rules.

The Firmware Management Tab

Use the [Firmware Management] tab to:

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

Viewing Device Firmware Information

Procedure

1. Go to [Administration] > [Firmware Management].
2. The [Firmware Management] pane lists the two partitions available. It shows the [Partition #], [Partition Name], [Partition Status], [Firmware Version] and [Firmware Build Time].

Note: EdgeIPS Pro 216 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.

Administration > Firmware Management

No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPSP_T01_1.0.17	2020-09-01T19:46:42+08:00	
2	boot2	Standby	IPSP_T01_1.0.16	2020-08-26T20:51:34+08:00	⬆️ ⇄

Updating Firmware

Procedure

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

Note: During a firmware upgrade, firmware will always be installed to the [Standby] partition. As such, the firmware upgrade button is only available in the [Standby] partition row.

Administration > Firmware Management

No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPSP_T01_1.0.17	2020-09-01T19:46:42+08:00	
2	boot2	Standby	IPSP_T01_1.0.16	2020-08-26T20:51:34+08:00	⬆️ ⇄

2. Click on the Upgrade Firmware button to install it to the [Standby] partition.
3. In the [Update Firmware] pane, provide the location of the firmware and click [Upload] to install the firmware to the partition on [Standby].

Upgrade Firmware ✕

Firmware Information

Current Firmware Version IPSP_T01_1.0.16

Firmware Build Time 2020-08-26T20:51:34+08:00

Firmware Update

Local Firmware Update

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


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

Rebooting and Applying Firmware

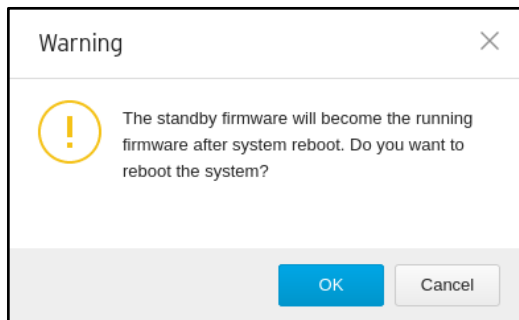
To boot into an upgraded firmware or to revert to previous firmware, you would need to boot into the [Standby] partition and load the firmware from there.

Procedure

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

Administration > Firmware Management					
No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPSP_T01_1.0.17	2020-09-01T19:46:42+08:00	
2	boot2	Standby	IPSP_T01_1.0.16	2020-08-26T20:51:34+08:00	

The below warning will be shown to the user.



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

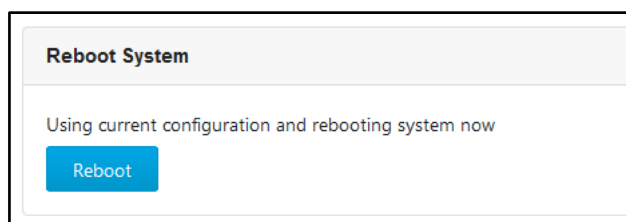
The Reboot System Tab

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

Rebooting the System

Procedure




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



Supported USB Devices

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

#	Models		Device Types
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

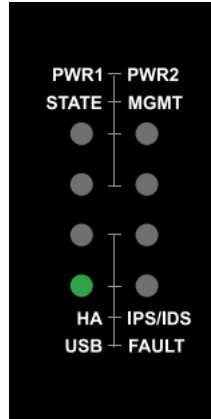
Supported actions via USB Disk

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

Note: Given that this feature allows anyone with a supported USB disk device to perform various operations via the USB, the physical security of the EdgeIPS Pro 216 device must be considered carefully. Only supported USB disk devices may be used for this feature.

To perform any of the above actions:

1. Plug the supported USB disk device into the EdgeIPS Pro 216 device's USB port.
2. Upon successful detection of the USB disk device, the "USB" LED will change to a steady green. The system log can also be checked to confirm that a supported USB disk device was detected when inserted. This state is referred to as the "Default Action" state.



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

- 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 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.
- 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

States/ Actions	LEDs	COLOURS/STATES
Default State – USB Plugged in Backup Configuration	USB LED	Green – Steady
Load/Restore Pattern	STATE	Green – Blinking (1/sec)
Load/Restore Configuration	MGMT	Green – Blinking (1/sec)
Load/Restore Firmware	STATE + MGMT	Green – Blinking (1/sec)

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

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

- While an action is being attempted, if 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	COLOUR/STATE
	USB LED	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	COLOUR/STATE
	FAIL LED	Red – Steady

Note: The 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.

4. 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.
5. 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 LED off), and a log will be available in system logs.

On-demand Configuration backup

1. In the "Default Action" state, on-demand configuration backup to disk can be performed by holding down the reset button for more than 10 seconds. During file transfer the USB LED may blink. However, since configuration files are usually not very large, this process may finish quickly.
 2. This action will save the current running configuration to the disk under the path **"/TXone/config/xxxxxx.acf"**.
 3. After you have saved the config, if successful, the USB app will return to the "Default Action" state. If any error occurs, the FAIL LED will turn red.
- The system logs will also reflect whether the action was successful or not.

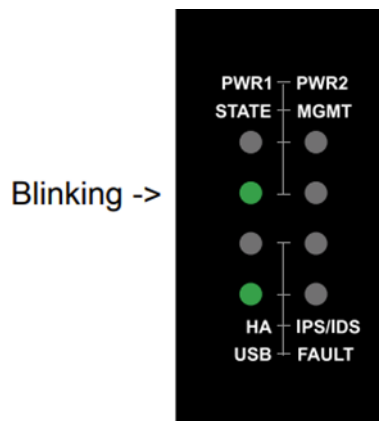
Load Pattern from Disk

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

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

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

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



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

than 3 seconds.

6. After the confirmation, the selected action will be attempted. If successful, the USB app will return to the "Default Action" state. If any errors occur, the FAIL LED will turn red.
7. The system logs will also reflect whether the action was successful or not.

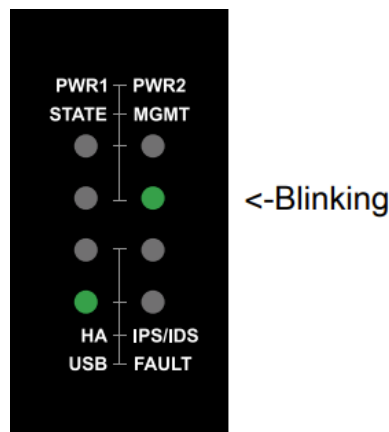
Load Configuration from disk

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

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

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

2. Plug in the USB disk. Enter the "Default Action" state.
3. In the default action state, give the reset button two short presses to toggle to "Load Config" action state.
4. When the device is in the "Load Config" action state, the "MGMT" LED will change to blinking green.



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

Load Firmware from disk

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

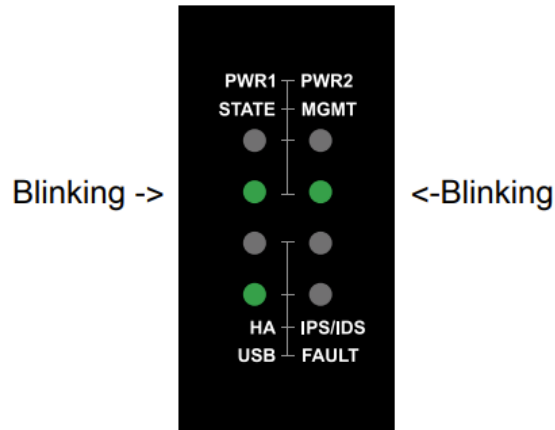
Save the firmware file in a USB disk device under path **"/TXone/firmware/"**. Assuming a firmware file has the name `firmware.acf`, its file path on the USB disk device would be **"/TXone/firmware/firmware.acf"**.

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

Plug in the USB disk. Enter the "Default Action" state.

In the default action state, give the reset button three short presses to toggle to the "Load Firmware" action state.

When the device is in "Load Firmware" action state, the "MGMT" and "STATE" LEDs will change to blinking green.



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

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 FAIL LED will turn red.

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

Note: Various versions of the firmware files can be downloaded at the Trend Micro Download Center at

https://www.trendmicro.com/en_us/business/products/downloads.html.

Terms and Acronyms

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

Terms/Acronyms	Definitions
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