EdgeIPS™

Administrator's Guide

2020-02-04

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

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

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

Table of Contents

About EdgeIPS™

Introduction

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

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

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

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

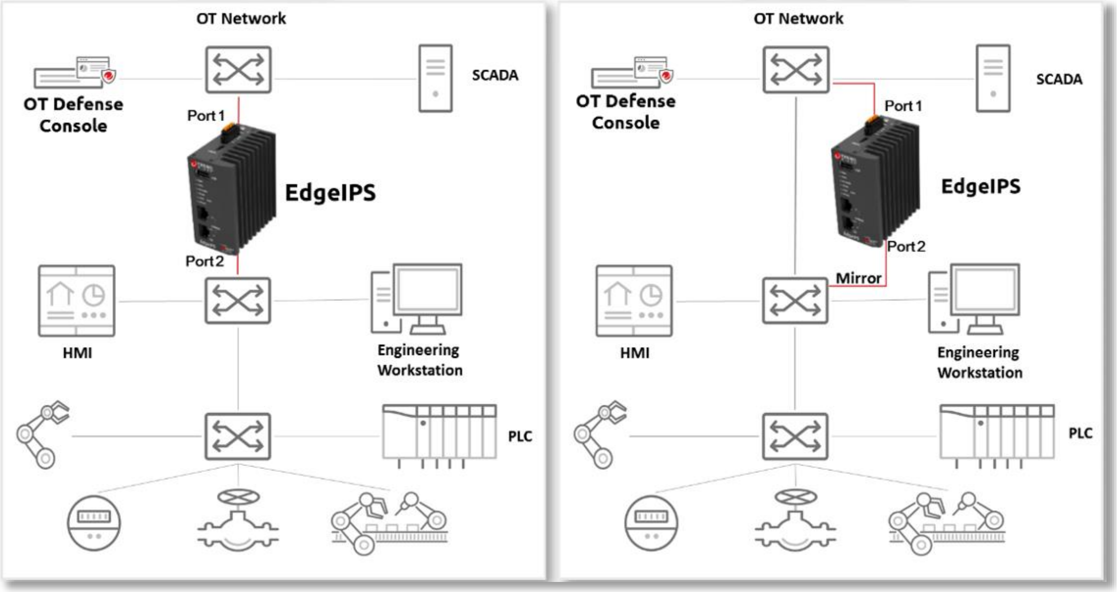


Figure 1. TXOne Networks security solutions for an OT network

Main Functions

EdgeIPS^{tm} is a transparent network security device. The main functions of the product are as follows:

Extensive Support for Industrial Protocols

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

Policy Enforcement for Mission-Critical Machines

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

Improve Shadow OT Visibility by Integrating IT and OT Networks

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

Intrusion Prevention and Intrusion Detection

IPS/IDS provides a powerful, up-to-date first line of defense against known threats. Vulnerability filtering rules provide effective protection against exploits at the network level. Manufacturing personnel manage patching and updating, providing pre-emptive protection against critical production failures and additional protection for old or terminated software.

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

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

Top Threat Intelligence and Analytics

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

Centralized Management

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

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

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

Getting Started

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

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

Getting Started: Task List

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

Procedure

1. Open the management console.
   For more information, see *Opening the Management Console on page 8*.
2. Change the administrator password.
   For more information, see *Changing the Administrator's Password on page 10*.
3. Configure the system time.
   For more information, see *Configuring System Time on page 40* .
4. (Optional) Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings on page 37*.
5. Configure Object Profiles.
   For more information, see *The Object Profiles on page 17*.
6. Configure security policies.
   For more information, see *The Security on page 22*.
7. Configure the device name and device location information.
   For more information, see *Configuring Device Name and Device Location Information on page 35*.
8. (Optional) Configure access control list from management clients.
   For more information, see *Configuring Control List Access from Management Clients on page 36*.
9. Configure management protocols and ports.
   For more information, see *Configuring Management Protocols and Ports on page 36*.
10. (Optional) Update the DPI (Deep Packet Inspection) pattern for the device.
    For more information, see *Manually Updating the Pattern on page 29*.
11. (Optional) Enabling Management by ODC.
    For more information, see *Enabling Management by ODC on page 37*.
12. Configure the network settings and network interface link modes for the device.
    For more information, see *The Device on page 15*.

Opening the Management Console

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

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

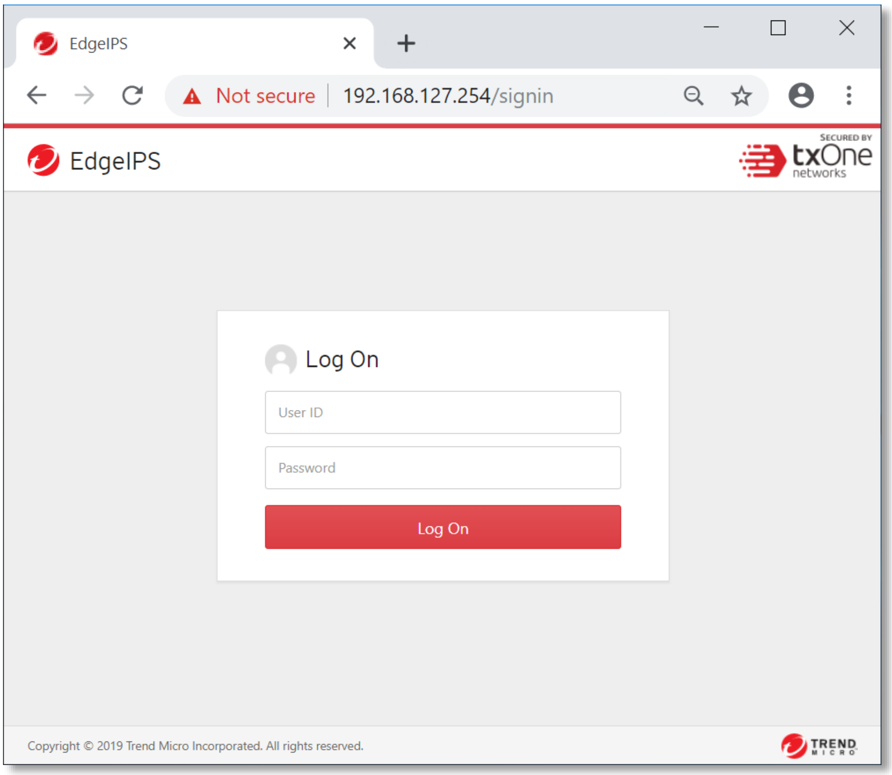
Procedure

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

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

The logon screen will appear.

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

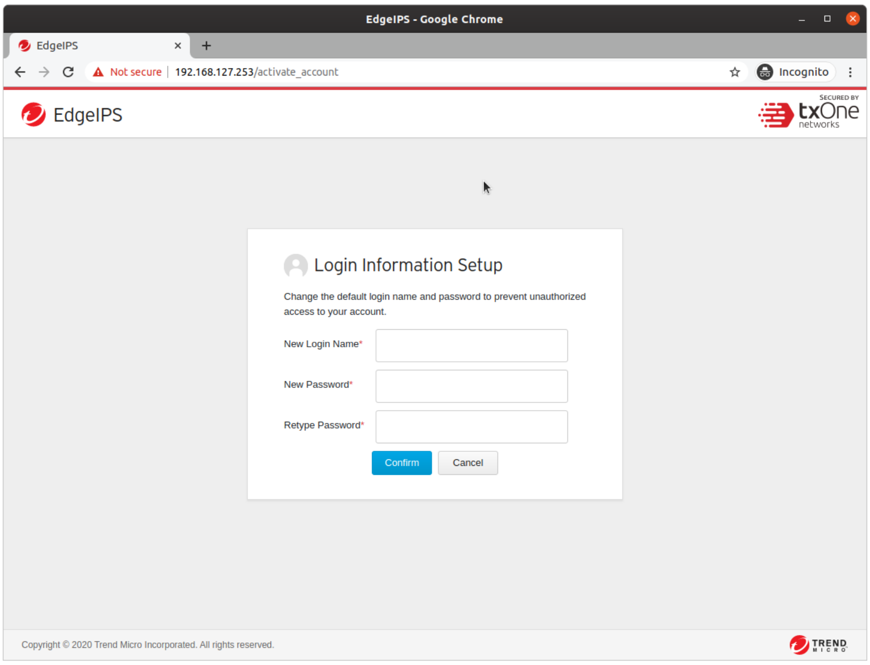

EdgeIPS
Not secure
192.168.127.254/signin
EdgeIPS
SECURED BY txOne networks
Log On
User ID
Password
Log On
Copyright © 2019 Trend Micro Incorporated. All rights reserved.
TREND MICRO

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.


EdgeIPS - Google Chrome
EdgeIPS
Not secure | 192.168.127.253/activate_account
Incognito
EdgeIPS
SECURED BY txOne networks

Login Information Setup

Change the default login name and password to prevent unauthorized access to your account.

New Login Name*

New Password*

Retype Password*

Confirm
Cancel
Copyright © 2020 Trend Micro Incorporated. All rights reserved.
TREND MICRO

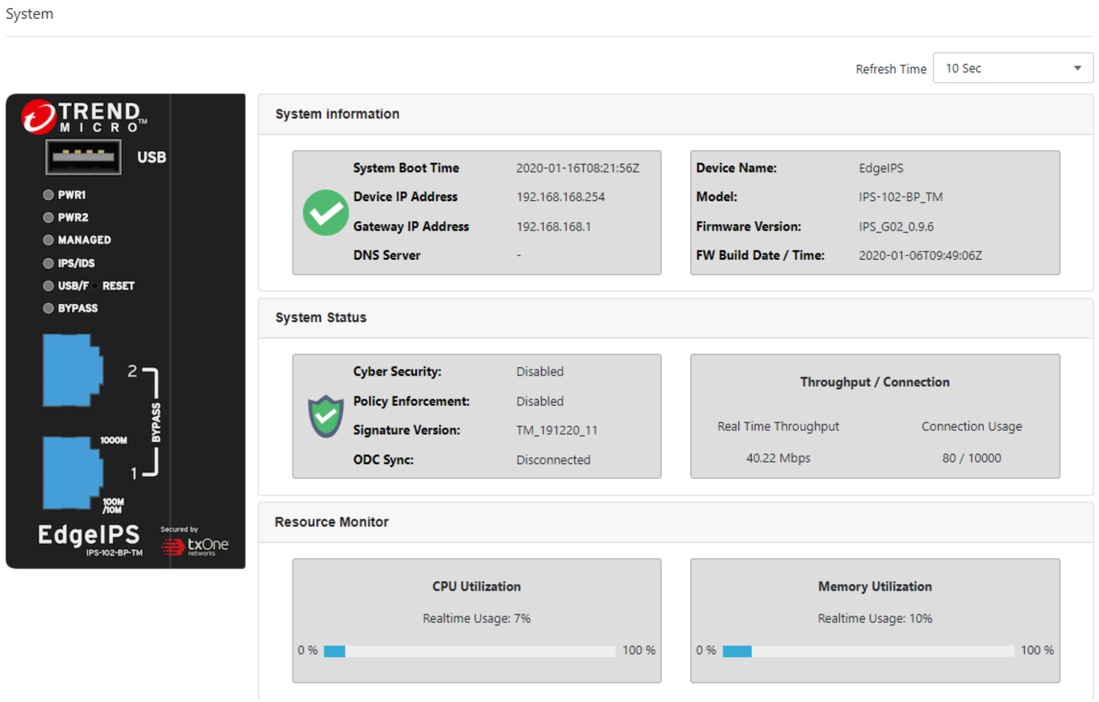
5. Login with newly changed user ID/password credentials.

Changing the Administrator’s Password

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

The System Tab

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



System

Refresh Time: 10 Sec

System information

System Boot Time	2020-01-16T08:21:56Z
Device IP Address	192.168.168.254
Gateway IP Address	192.168.168.1
DNS Server	-

Device Name:	EdgeIPS
Model:	IPS-102-BP_TM
Firmware Version:	IPS_G02_0.9.6
FW Build Date / Time:	2020-01-06T09:49:06Z

System Status

Cyber Security:	Disabled
Policy Enforcement:	Disabled
Signature Version:	TM_191220_11
ODC Sync:	Disconnected

Throughput / Connection

Real Time Throughput	Connection Usage
40.22 Mbps	80 / 10000

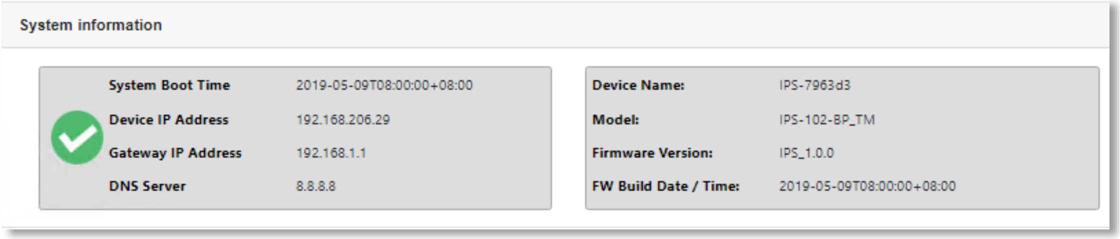
Resource Monitor

CPU Utilization
Realtime Usage: 7%
0 % – 100 %

Memory Utilization
Realtime Usage: 10%
0 % – 100 %

System Information

This widget shows the time when the system started, name of the device, model name of the device, version of the firmware on the device, firmware build date/time, and the IP address settings of the device.



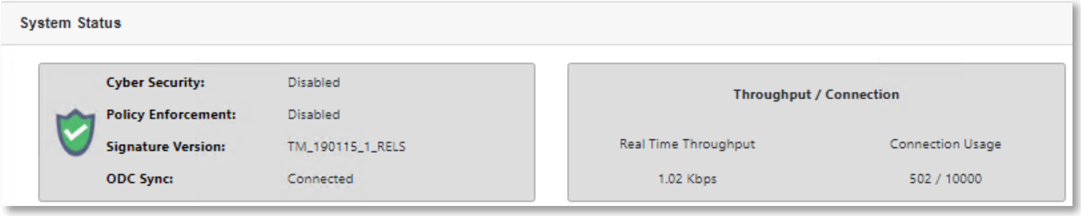
System information

System Boot Time	2019-05-09T08:00:00+08:00
Device IP Address	192.168.206.29
Gateway IP Address	192.168.1.1
DNS Server	8.8.8.8

Device Name:	IPS-7963d3
Model:	IPS-102-BP_TM
Firmware Version:	IPS_1.0.0
FW Build Date / Time:	2019-05-09T08:00:00+08:00

System Status

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



System Status

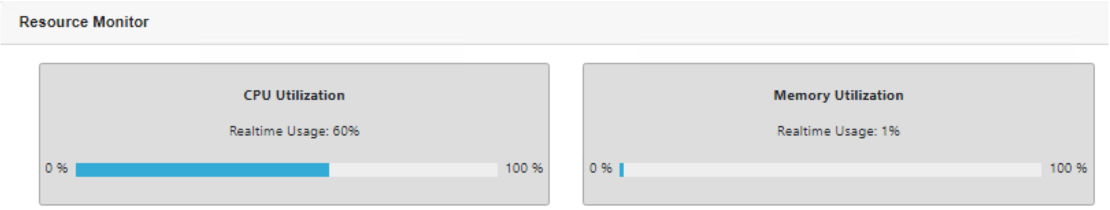
Cyber Security: Disabled
Policy Enforcement: Disabled
Signature Version: TM_190115_1_RELS
ODC Sync: Connected

Throughput / Connection

Real Time Throughput: 1.02 Kbps
Connection Usage: 502 / 10000

Resource Monitor

This widget shows resource usage on the device.



Resource Monitor

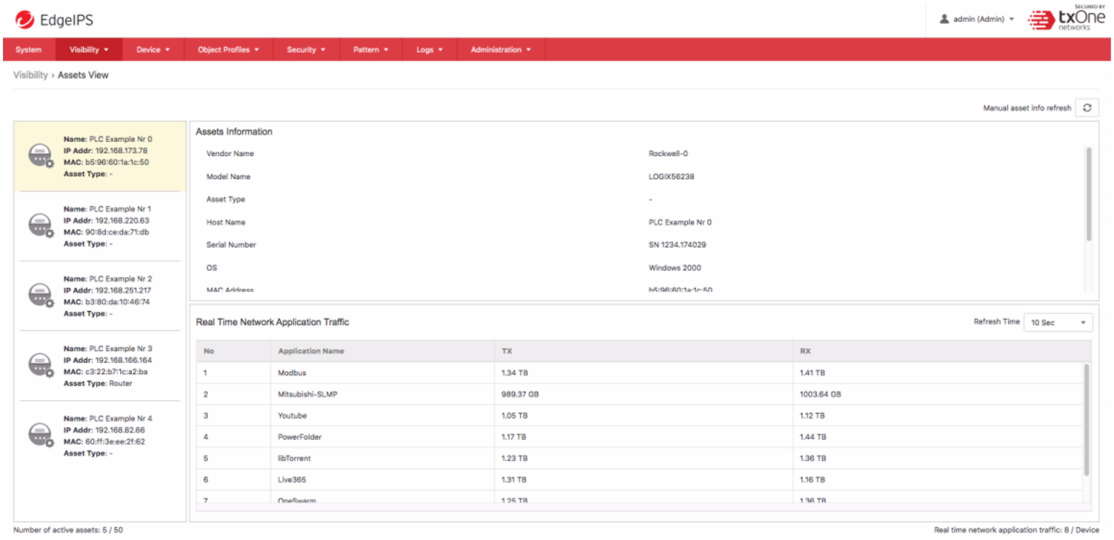
CPU Utilization
Realtime Usage: 60%

Memory Utilization
Realtime Usage: 1%

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

The Visibility Tab

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



Name: PLC Example Nr 0
IP Addr: 192.168.173.78
MAC: b5:96:60:1a:1c:50
Asset Type: -

Name: PLC Example Nr 1
IP Addr: 192.168.220.63
MAC: 90:8d:ce:da:71:db
Asset Type: -

Name: PLC Example Nr 2
IP Addr: 192.168.251.217
MAC: b3:80:da:10:46:74
Asset Type: -

Name: PLC Example Nr 3
IP Addr: 192.168.166.164
MAC: c3:22:b7:1c:a2:ba
Asset Type: Router

Name: PLC Example Nr 4
IP Addr: 192.168.82.66
MAC: 60:ff:3e:ee:2f:62
Asset Type: -

Assets Information

Vendor Name	Rockwell-0
Model Name	LOGIX56238
Asset Type	-
Host Name	PLC Example Nr 0
Serial Number	SN 1234.174029
OS	Windows 2000
MAC Address	b5:96:60:1a:1c:50

Real Time Network Application Traffic

Refresh Time 10 Sec

No	Application Name	TX	RX
1	Modbus	1.34 TB	1.41 TB
2	Mitsubishi-SLMP	989.37 GB	1003.64 GB
3	Youtube	1.05 TB	1.12 TB
4	PowerFolder	1.17 TB	1.44 TB
5	libTorrent	1.23 TB	1.36 TB
6	Live365	1.31 TB	1.16 TB
7	OneSwarm	1.25 TB	1.36 TB

Number of active assets: 5 / 50

Real time network application traffic: 8 / Device

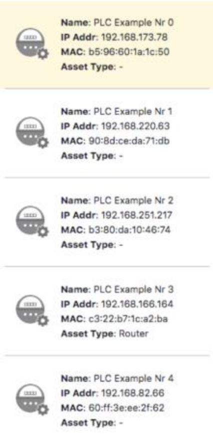
The assets, listed under the tab, are automatically detected by EdgeIPS™ devices.

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

Viewing Asset Information

Procedure

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



Name: PLC Example Nr 0
IP Addr: 192.168.173.78
MAC: b5:96:60:1a:1c:50
Asset Type: -

Name: PLC Example Nr 1
IP Addr: 192.168.220.63
MAC: 90:8d:ce:da:71:db
Asset Type: -

Name: PLC Example Nr 2
IP Addr: 192.168.251.217
MAC: b3:80:da:10:46:74
Asset Type: -

Name: PLC Example Nr 3
IP Addr: 192.168.166.164
MAC: c3:22:b7:1c:a2:ba
Asset Type: Router

Name: PLC Example Nr 4
IP Addr: 192.168.82.66
MAC: 60:ff:3e:ee:2f:62
Asset Type: -

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

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

Viewing Real Time Network Application Traffic

Procedure

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

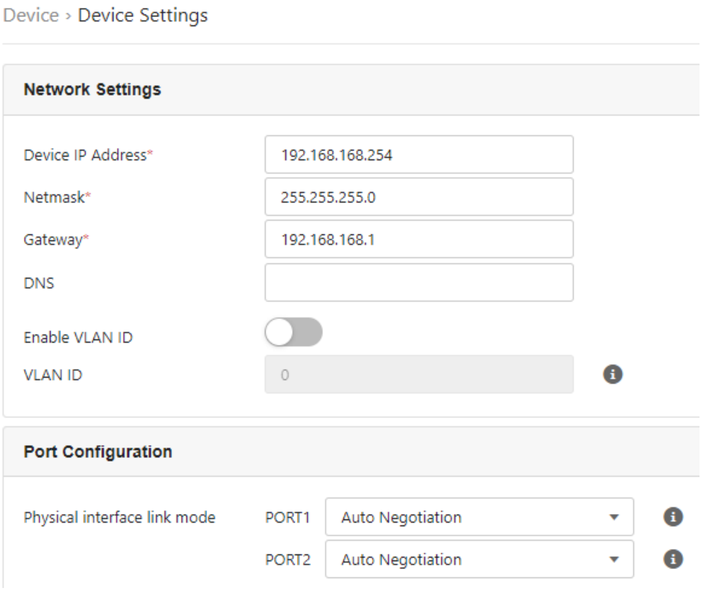
Field	Description
No.	Ordinal number of the application traffic.
Application Name	The application type of the traffic.
TX	The amount of traffic transmitted for this traffic.
RX	The amount of traffic received for this traffic.

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

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

The Device Tab

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



Device › Device Settings

Network Settings

Device IP Address* 192.168.168.254

Netmask* 255.255.255.0

Gateway* 192.168.168.1

DNS

Enable VLAN ID

VLAN ID 0

Port Configuration

Physical interface link mode

PORT1 Auto Negotiation

PORT2 Auto Negotiation

Configuring Network Settings

Procedure

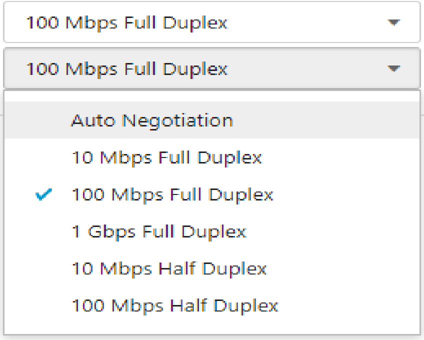
1. Go to [Device] > [Device Settings]
2. In the [Network Settings] pane, configure the network settings for the device:

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

Configuring Interface Link Mode for Ports

Procedure

1. Go to [Device] > [Device Settings]
2. In the [Port Configuration] plane, configure the link modes for the ports of the device:

Task	Action
Port 1 and Port 2	Choose [Auto Negotiation] to specify that the interface should automatically negotiate the highest speed that both sides can work with or specify the configured speed value of the interface.  100 Mbps Full Duplex 100 Mbps Full Duplex Auto Negotiation 10 Mbps Full Duplex ✓ 100 Mbps Full Duplex 1 Gbps Full Duplex 10 Mbps Half Duplex 100 Mbps Half Duplex

The Object Profiles Tab

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

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

- **IP Object Profile**: Contains the IP addresses that you can apply to a policy rule.
- **Service Object Profile**: Contains the service definitions that you can apply to a policy rule. TCP port range, UDP port range, ICMP, and custom protocol number are defined here.
- **Protocol Filter Profile**: Contains more sophisticated and advanced protocol settings that you can apply to a policy rule. Details of ICS (Industrial Control System) protocols are defined here.

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

Task	Description
Add a profile	Click [Add] to create a new profile.
Edit a profile	Click a profile name to edit the settings.
Delete a profile	Select one or more profiles and click [Delete].
Copy a profile	Select on profile and click [Copy].

Configuring IP Object Profile

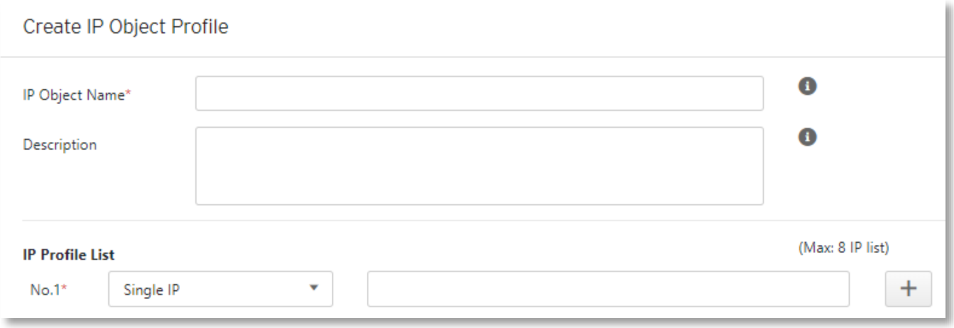
You can configure the IP address in an IP object profile, which can be used by other policy rules.

The types of IP address you can assign are:

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

Procedure

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



Create IP Object Profile

IP Object Name*

Description

IP Profile List

(Max: 8 IP list)

No.1* Single IP

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

Configuring Service Object Profile

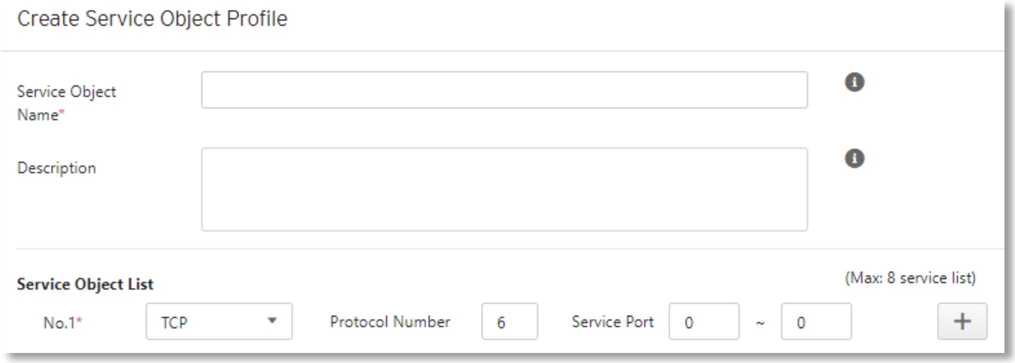
In a service object profile, you can define the following:

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

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

Procedure

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



Create Service Object Profile

Service Object Name*

Description

Service Object List (Max: 8 service list)

No.1* TCP Protocol Number 6 Service Port 0 ~ 0

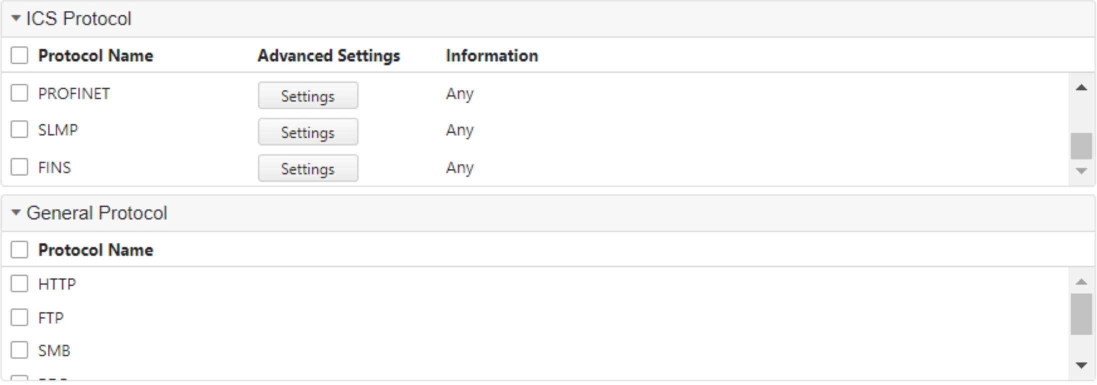
3. Type a descriptive name for the Service Object Profile.
4. Type a description.
5. Provide one of the following definitions:
   a. TCP protocol and its port range
   b. UDP protocol and its port range
   c. ICMP protocol and its type and code
   d. Custom protocol with specified protocol number
6.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

Configuring Protocol Filter Profile

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

The following can be configured in a protocol filter profile:

- Details of ICS protocols, including:
  - Modbus
  - CIP
  - S7COMM
  - S7COMM_PLUS
  - PROFINET
  - SLMP
  - FINS
- General Protocol, including:
  - HTTP
  - FTP
  - SMB
  - RDP
  - MQTT



▾ ICS Protocol

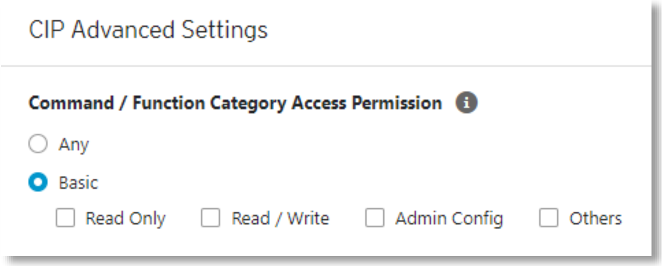
□ Protocol Name	Advanced Settings	Information
□ PROFINET	Settings	Any
□ SLMP	Settings	Any
□ FINS	Settings	Any

▾ General Protocol

□ Protocol Name
□ HTTP
□ FTP
□ SMB

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.



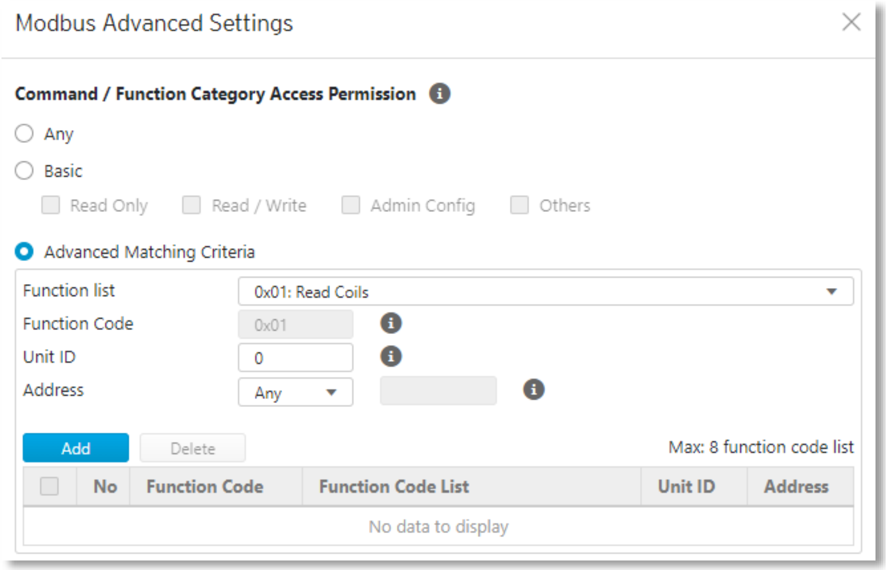
CIP Advanced Settings

Command / Function Category Access Permission

○ Any
● Basic
□ Read Only □ Read / Write □ Admin Config □ Others

Advanced Settings for Modbus Protocol

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



Modbus Advanced Settings

Command / Function Category Access Permission

○ Any

○ Basic

□ Read Only □ Read / Write □ Admin Config □ Others

● Advanced Matching Criteria

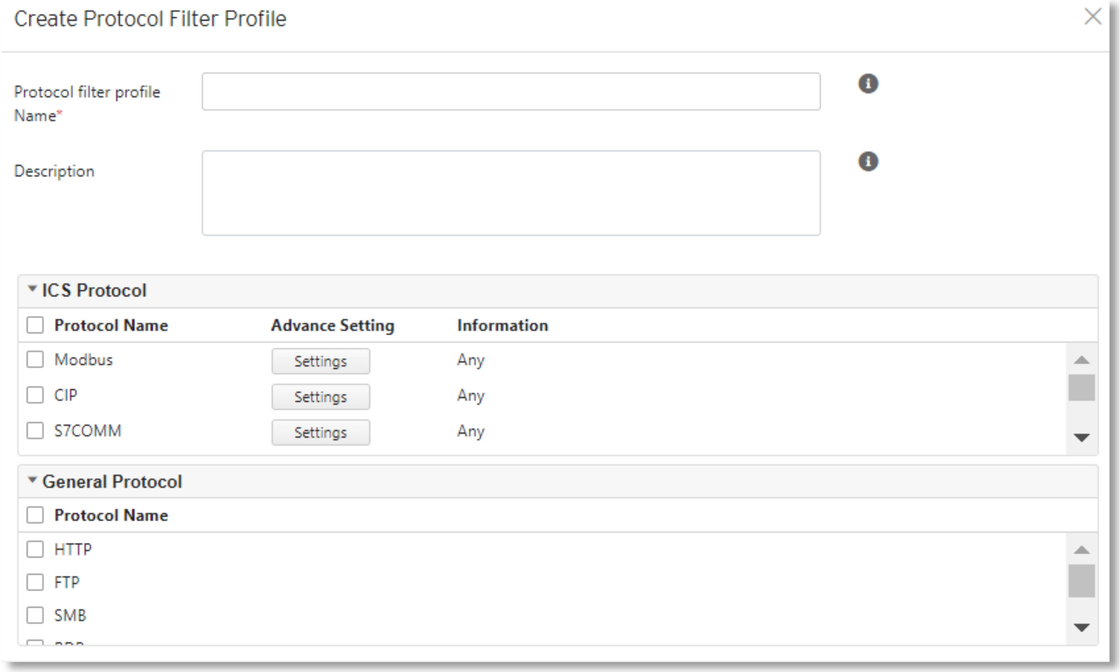
Function list	0x01: Read Coils
Function Code	0x01
Unit ID	0
Address	Any

Max: 8 function code list

□	No	Function Code	Function Code List	Unit ID	Address
No data to display					

Procedure

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



Create Protocol Filter Profile

Protocol filter profile Name*

Description

▾ ICS Protocol

□ Protocol Name	Advance Setting	Information
□ Modbus	Settings	Any
□ CIP	Settings	Any
□ S7COMM	Settings	Any

▾ General Protocol

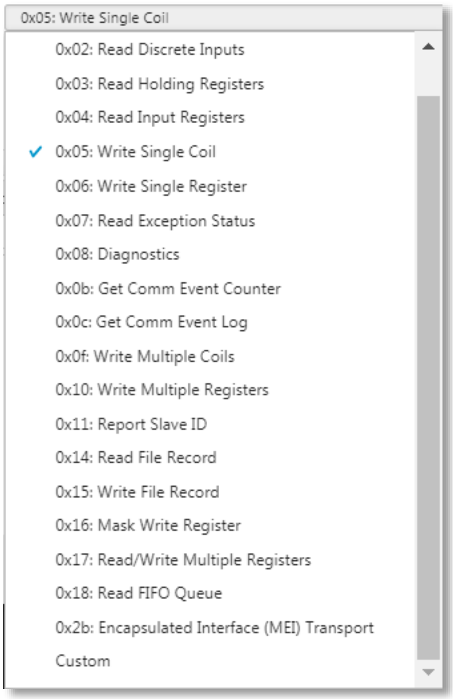
□ Protocol Name
□ HTTP
□ FTP
□ SMB

3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
   a. Click [Settings] next to a protocol, and select one of the following:

    - **Any** - Specify all available commands or function access in this protocol.
    - **Basic** - Multiple selections of the following:
        - **Read Only**: Read commands sent from HMI (Human-Machine Interface) /EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
        - **Read / Write**: Read and write commands sent from HMI/EWS/SCADA to PLC.
        - **Admin Config**: Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands sent from EWS to PLC.
        - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

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

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


0x05: Write Single Coil
0x02: Read Discrete Inputs
0x03: Read Holding Registers
0x04: Read Input Registers
✓ 0x05: Write Single Coil
0x06: Write Single Register
0x07: Read Exception Status
0x08: Diagnostics
0x0b: Get Comm Event Counter
0x0c: Get Comm Event Log
0x0f: Write Multiple Coils
0x10: Write Multiple Registers
0x11: Report Slave ID
0x14: Read File Record
0x15: Write File Record
0x16: Mask Write Register
0x17: Read/Write Multiple Registers
0x18: Read FIFO Queue
0x2b: Encapsulated Interface (MEI) Transport
Custom

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

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

The Security Tab

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

Security General Settings

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

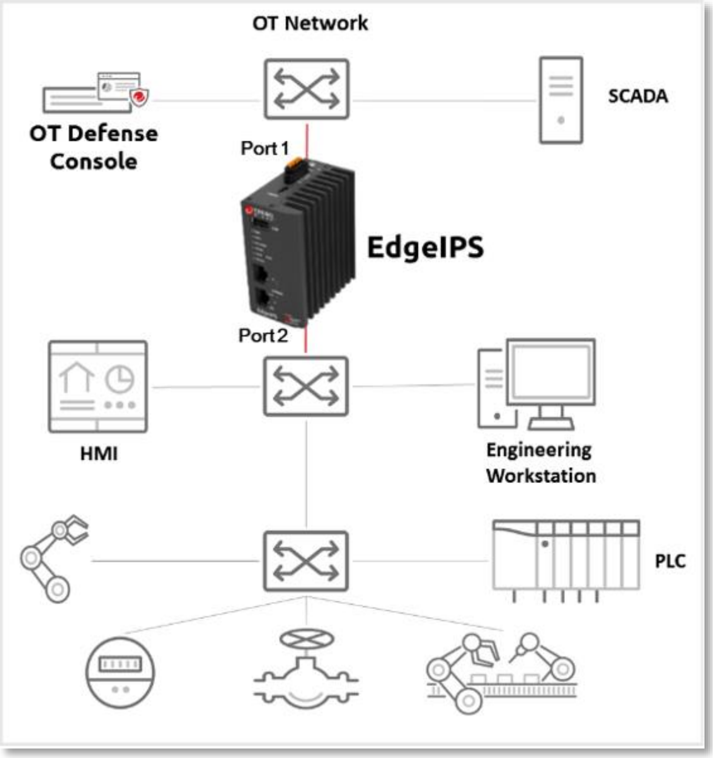
EdgeIPS™ offers two operation modes:

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

The following sections describe these two modes in detail.

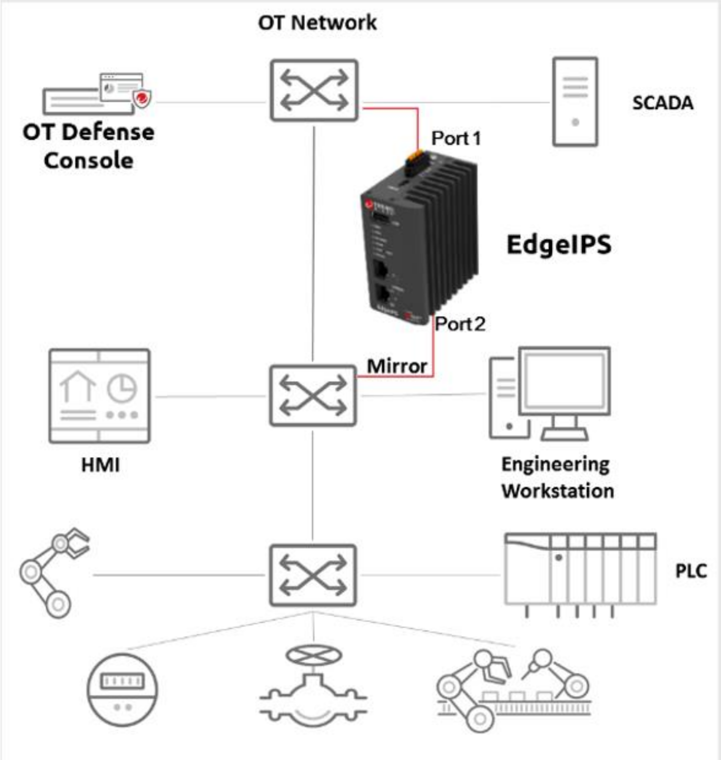
Inline Mode

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



Offline Mode

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

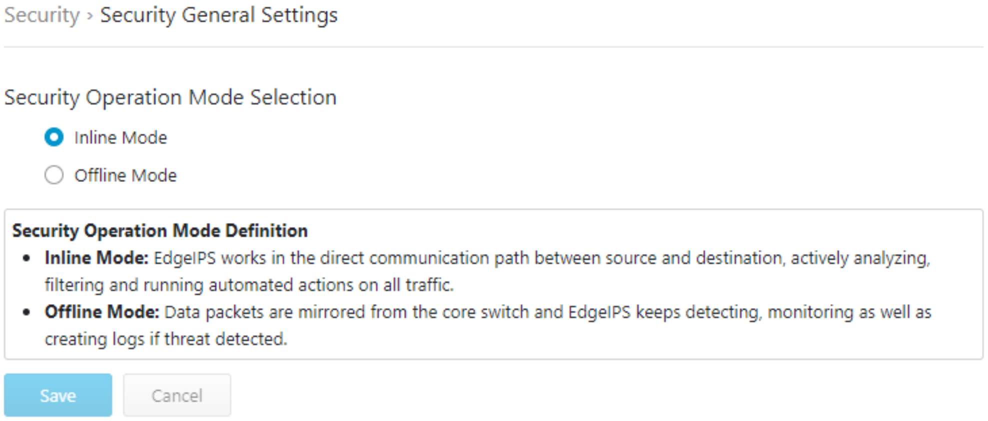


Note: **Port 1** of the EdgeIPS functions as the management port, which connects to another switch, allowing the EdgeIPS to be managed by ODC.

Configuring Security Operation Mode

Procedure

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


Security › Security General Settings

Security Operation Mode Selection

● Inline Mode

○ Offline Mode

Security Operation Mode Definition

- **Inline Mode:** EdgeIPS works in the direct communication path between source and destination, actively analyzing, filtering and running automated actions on all traffic.
- **Offline Mode:** Data packets are mirrored from the core switch and EdgeIPS keeps detecting, monitoring as well as creating logs if threat detected.

3. Choose a desired operation mode for this device.
4. Click [Save].

Warning! Ensure that the operation mode is correctly selected. If EdgeIPS is deployed as inline network topology with the [Security Operation Mode] being set to [Offline Mode], then devices that connect to **port 2** cannot get through outside.

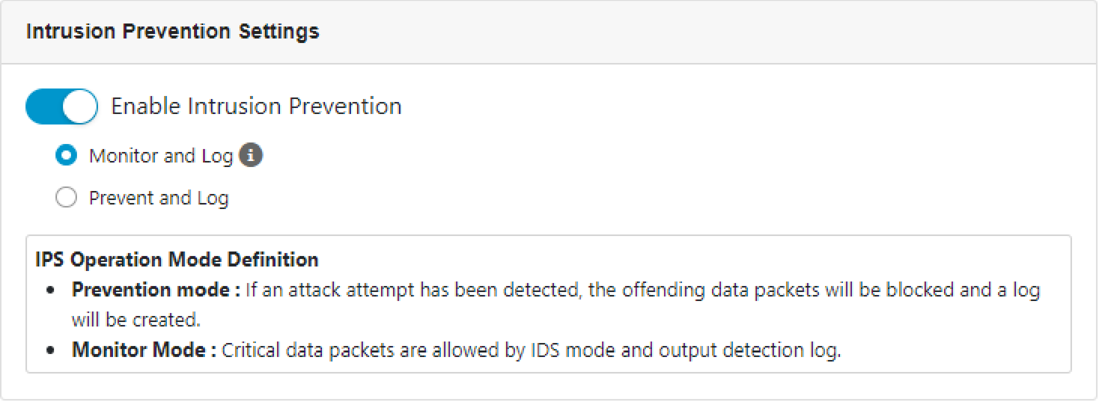
Cyber Security

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

Configuring Cyber Security - Intrusion Prevention Setting

Procedure

1. Go to [Security] > [Cyber Security].
2. At the [Cyber Security] tab you will see the [Intrusion Prevention Settings] pane.
3. Use the toggle to enable or disable the intrusion prevention feature.
4. Select an action ([Monitor and Log] or [Prevent and Log]) for the intrusion prevention feature.



Intrusion Prevention Settings

Enable Intrusion Prevention

● Monitor and Log ℹ

○ Prevent and Log

IPS Operation Mode Definition

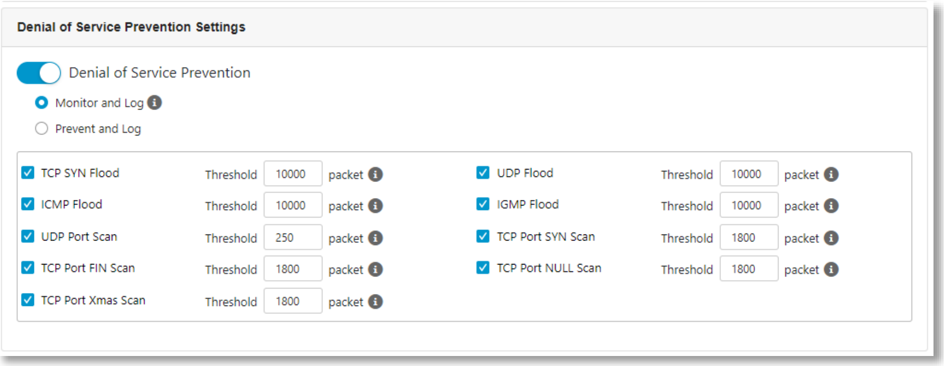
- **Prevention mode :** If an attack attempt has been detected, the offending data packets will be blocked and a log will be created.
- **Monitor Mode :** Critical data packets are allowed by IDS mode and output detection log.

5. Click [Save].

Configuring Cyber Security – Denial of Service Prevention

Procedure

1. Go to [Security] > [Cyber Security].
2. At the [Cyber Security] tab you will see the [Denial of Service Prevention] pane.



Denial of Service Prevention Settings

Denial of Service Prevention

● Monitor and Log ℹ

○ Prevent and Log

☑ TCP SYN Flood	Threshold	10000	packet ℹ	☑ UDP Flood	Threshold	10000	packet ℹ
☑ ICMP Flood	Threshold	10000	packet ℹ	☑ IGMP Flood	Threshold	10000	packet ℹ
☑ UDP Port Scan	Threshold	250	packet ℹ	☑ TCP Port SYN Scan	Threshold	1800	packet ℹ
☑ TCP Port FIN Scan	Threshold	1800	packet ℹ	☑ TCP Port NULL Scan	Threshold	1800	packet ℹ
☑ TCP Port Xmas Scan	Threshold	1800	packet ℹ				

3. Use the toggle to enable or disable the denial of service prevention feature.
4. Select an action ([Monitor and Log] or [Prevent and Log]) for the feature.
5. You can optionally configure the thresholds of the denial of service rules.
6. Click [Save].

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

The following table summarizes the settings:

IPS Operation Mode (Security General Setting)	Action Settings	Action Performed
Inline Mode	Monitor and Log	▪ Detects and monitors network attacks, but does not block network attacks. ▪ Generates logs.
	Prevent and Log	▪ Blocks network attacks. ▪ Generates logs.
Offline Mode	Monitor and Log	▪ Passively detects and monitors network attacks. ▪ Generates logs.

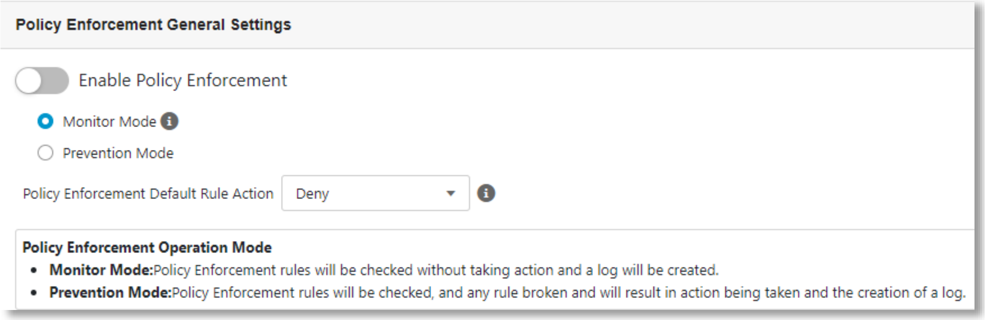
Policy Enforcement

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

Configuring Policy Enforcement

Procedure

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



Policy Enforcement General Settings

Enable Policy Enforcement

● Monitor Mode

○ Prevention Mode

Policy Enforcement Default Rule Action: Deny

Policy Enforcement Operation Mode
- **Monitor Mode:**Policy Enforcement rules will be checked without taking action and a log will be created.
- **Prevention Mode:**Policy Enforcement rules will be checked, and any rule broken and will result in action being taken and the creation of a log.

5. At the [Policy Enforcement Default Rule Action] drop-down menu, select a default action for when no pattern is matched.

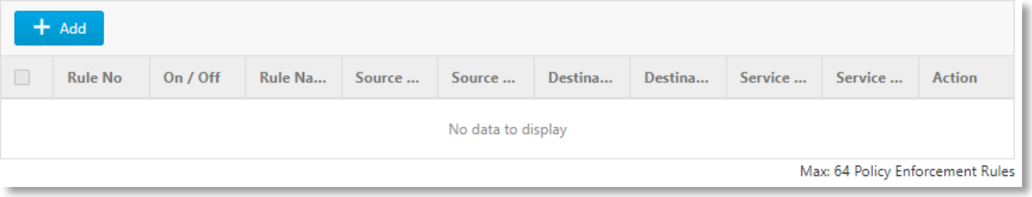
The following table summarizes the settings:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	▪ Detect and monitor abnormal protocol accesses to the OT assets, without blocking network attacks. ▪ Generate logs.
	Prevention Mode	▪ Block abnormal protocol access to OT assets. ▪ Generate logs.
Offline Mode	Monitor and Log	▪ Not supported.

Adding Policy Enforcement Rules

Procedure

1. Configure the required object or objects.
   - IP object profiles
     For more information, see *Configuring IP Object Profile on page 17*.
   - Service object profiles
     For more information, see *Configuring Service Object Profile on page 18*.
   - Protocol filter profiles
     For more information, see *Configuring Protocol Filter Profile on page 19*.
2. Go to [Security] > [Policy Enforcement]
3. Under the [Policy Enforcement] tab you will see the following panes.

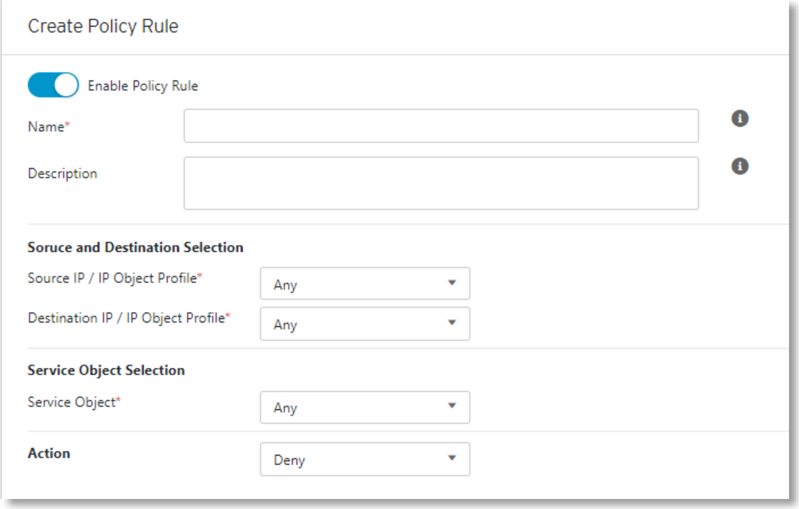


+ Add

□	Rule No	On / Off	Rule Na...	Source ...	Source ...	Destina...	Destina...	Service ...	Service ...	Action
No data to display										

Max: 64 Policy Enforcement Rules

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



Create Policy Rule

Enable Policy Rule

Name*

Description

Soruce and Destination Selection

Source IP / IP Object Profile* Any

Destination IP / IP Object Profile* Any

Service Object Selection

Service Object* Any

Action Deny

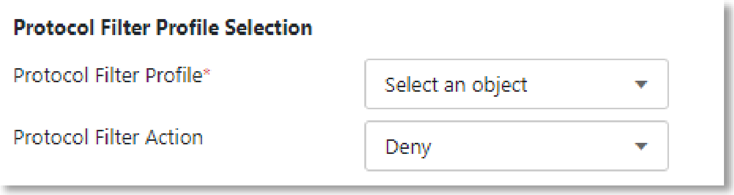
6. Input a descriptive [Rule Name].
7. Input a descriptive [Description] for the rule.
8. At the [Source IP / IP Object Profile] drop-down menu, select either one of the following for the source IP address(es):
   - Any
   - Single IP
   - IP Range
   - IP Subnet
   - Object

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

9. At the [Destination IP / IP Object Profile] drop-down menu, select either one of the following for the destination IP address(es):
   - Any
   - Single IP
   - IP Range
   - IP Subnet
   - Object
10. At the [Service Object] drop-down menu, select either one of the following for the layer 4 criteria:
    - TCP
      You can further specify the port range for this protocol.
    - UDP
      You can further specify the port range for this protocol.
    - ICMP
      You can further specify the Type and Code for this protocol.
    - Custom
      You can further specify the protocol number for this protocol. The term protocol number refers to the one defined in the internet protocol suite.
    - Service Object

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

11. At the [Action] drop-down menu, select one of the following:
    a. Accept: Select this option to allow network traffic that matches this rule.
    b. Deny: Select this option to block network traffic that matches this rule.
    c. Protocol Filter: The node will take further actions based on the protocol filter:
       - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
       - Under the [Protocol Filter Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.



Protocol Filter Profile Selection

Protocol Filter Profile*: Select an object

Protocol Filter Action: Deny

12. Click [Save] to save the configuration.

Managing Policy Enforcement Rules

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

Task	Action
To delete a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the [Delete] button.
To duplicate a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the [Copy] button.
To edit a policy enforcement rule	Click the name of the rule, and an [Edit Policy Rule] window will appear.
To change the priority of a policy enforcement rule	Click the check box in front of the policy enforcement rule, click the [Change Priority] button, and specify a new priority for this rule.

Note: When more than one policy enforcement rule is matched, EdgeIPS™ takes the action of the rule with the highest priority, and ignores the rest of the rules. The rules are listed on the table of the UI screen by priority, with the highest priority rule listed on the first row of the table.

The Pattern Tab

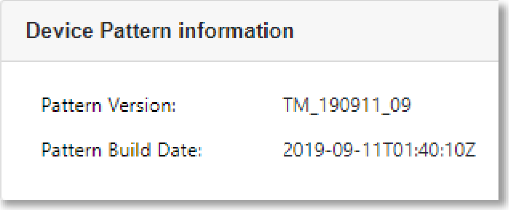
This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the EdgeIPS™ device.

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

Viewing Device Pattern Information

Procedure

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



Device Pattern information

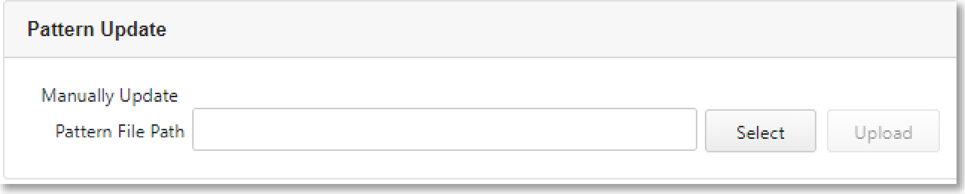
Pattern Version: TM_190911_09

Pattern Build Date: 2019-09-11T01:40:10Z

Manually Updating the Pattern

Procedure

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



Pattern Update

Manually Update

Pattern File Path

5. Click [OK].

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

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**
- **Protocol filter logs**
- **System logs**
- **Assess detection logs**
- **Policy enforcement logs**
- **Audit logs**

Viewing Cyber Security Logs

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

Procedure

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

Field	Description
Time	The time the log entry was created.
Event ID	The ID of the matched signature.
Security Category	The category of the matched signature.
Security Severity	The severity level assigned to the matched signature.
Security Rule Name	The name of the matched signature.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.
Count	The number of detected network packets within the detection period after the detection threshold is reached.

Viewing Policy Enforcement Logs

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

Procedure

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

   The following table describes the log table.

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

Viewing Protocol Filter Logs

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

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Policy Enforcement Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
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, if protocol is selected TCP/UDP. The ICMP type, if protocol is selected ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if protocol is selected TCP/UDP. The ICMP code, if protocol is selected ICMP.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No.	The command or function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing 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 log’s fields.

Field	Description
Time	The time the log entry was created.
Event Type	The log event description.
Asset MAC Address	The MAC address of the asset.
Asset IP Address	The source IP address of the asset.

Viewing System Logs

You can view details about system events on the device.

Procedure

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

   The following table describes the log’s fields.

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

Viewing Audit Logs

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

Procedure

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

   The following table describes the log’s fields.

Field	Description
Time	The time the log entry was created.
User ID	The user account used to execute the task.
Client IP	The IP address of the host used to access the management console.
Severity	The severity level of the logs.
Message	The log event description.

Note: To view the audit logs, please login with the default “audit” account.

The Administration Tab

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

Account Management

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

This system uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.

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

Task	Description
Add account	Click Add to create a new user account. For more information, see *Adding a User Account on page 34*.
Delete existing accounts	Select preexisting user accounts and click Delete.
Edit existing accounts	Click the name of a preexisting user account to view or modify the current account settings.

User Roles

The following table describes the permissions matrix for user roles.

		User Roles			
Sub-Tab	**Action**	**Admin**	**Operator**	**Visitor**	**Auditor**
System	View	Yes	Yes	Yes	Yes
	All operations	Yes	Yes	Yes	Yes
Visibility	View	Yes	Yes	Yes	No
	All operations	Yes	Yes	Yes	No
Device	View	Yes	Yes	No	No
	All operations	Yes	No	No	No
Object Profiles	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Security	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Pattern	View	Yes	Yes	No	No
	All operations	Yes	Yes	No	No
Logs – not including audit log	View	Yes	Yes	Yes	No
Audit Log	View	No	No	No	Yes
Administration	View	Yes	No	No	No
	All operations	Yes	No	No	No

Built-in User Accounts

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

Built-in default Account ID	User Role	Default Password
admin	Admin	txone
auditor	Auditor	txone

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

Note: Ensure that the passwords of the built-in accounts are changed when you first set up the device.

Adding a User Account

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

Procedure

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

Field	Description
ID	Type the user ID to log on to the management console.
Name	Type the name of the user for this account.
Password	Type the account password.
Confirm password	Type the account password again to confirm.
Role	Select a user role for this account. For more information, see *User Roles on page 33*.

4. Click [Save].

Changing Your Password

Procedure

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

Configuring Password Policy Settings

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

- Password complexity settings
  Specify password complexity settings to enforce strong passwords. For example, you can specify users that users must create strong passwords that contain a combination of both

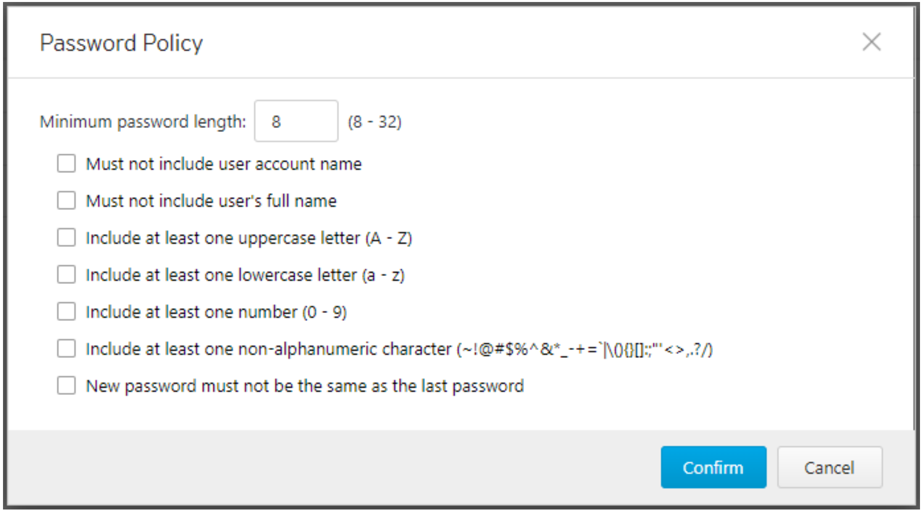
uppercase and lowercase letters, numbers, and symbols, and which are at least eight characters in length.

Note: When strong passwords are required, a user submits a new password, and the password policy determines whether the password meets your company's established requirements. Strict password policies may sometimes increase costs to an organization when users select passwords that are too difficult to remember. Users call the help desk when they forget their passwords, or keep passwords in easily accessible locations and increase their vulnerability to threats. When establishing a password policy, balance your need for strong security against the need to make the policy easy for users to follow.

Procedure

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

   The [Password Policy] screen will appear.



Password Policy

Minimum password length: 8 (8 - 32)

□ Must not include user account name

□ Must not include user's full name

□ Include at least one uppercase letter (A - Z)

□ Include at least one lowercase letter (a - z)

□ Include at least one number (0 - 9)

□ Include at least one non-alphanumeric character (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

□ New password must not be the same as the last password

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

System Management

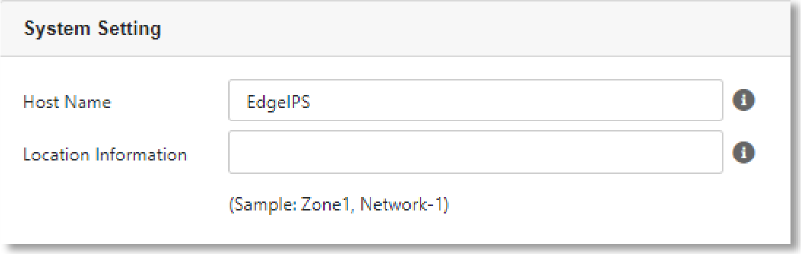
Use the [System Management] tab to do the following:

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

Configuring Device Name and Device Location Information

Procedure

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



System Setting

Host Name: EdgeIPS

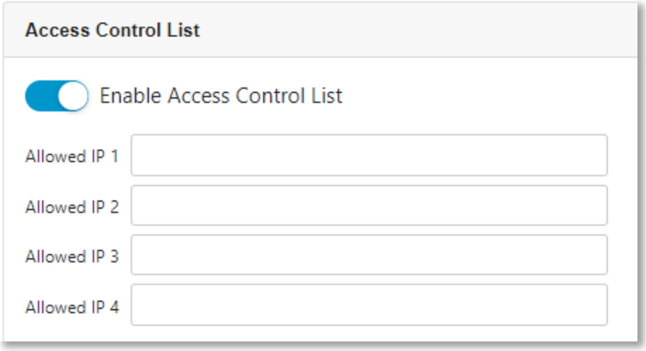
Location Information:

(Sample: Zone1, Network-1)

Configuring Control List Access from Management Clients

Procedure

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



Access Control List

Enable Access Control List

Allowed IP 1:

Allowed IP 2:

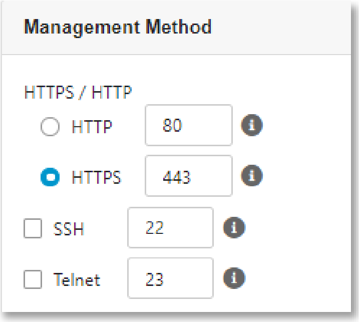
Allowed IP 3:

Allowed IP 4:

Configuring Management Protocols and Ports

Procedure

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



Management Method

HTTPS / HTTP

○ HTTP 80

● HTTPS 443

□ SSH 22

□ Telnet 23

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

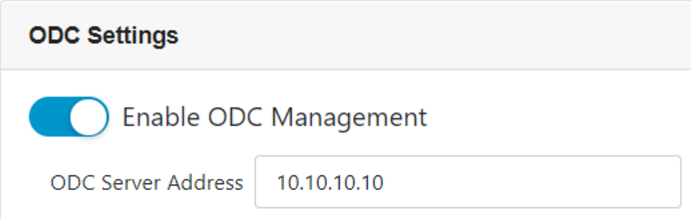
The Sync Setting Tab

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

Enabling Management by ODC

Procedure

1. Go to [Administration] > [Sync Settings].
2. In the [ODC Setting] pane:
   a. Use the toggle to enable management by ODC.
   b. Input the IP address of the ODC server.



ODC Settings

Enable ODC Management

ODC Server Address: 10.10.10.10

The Syslog Tab

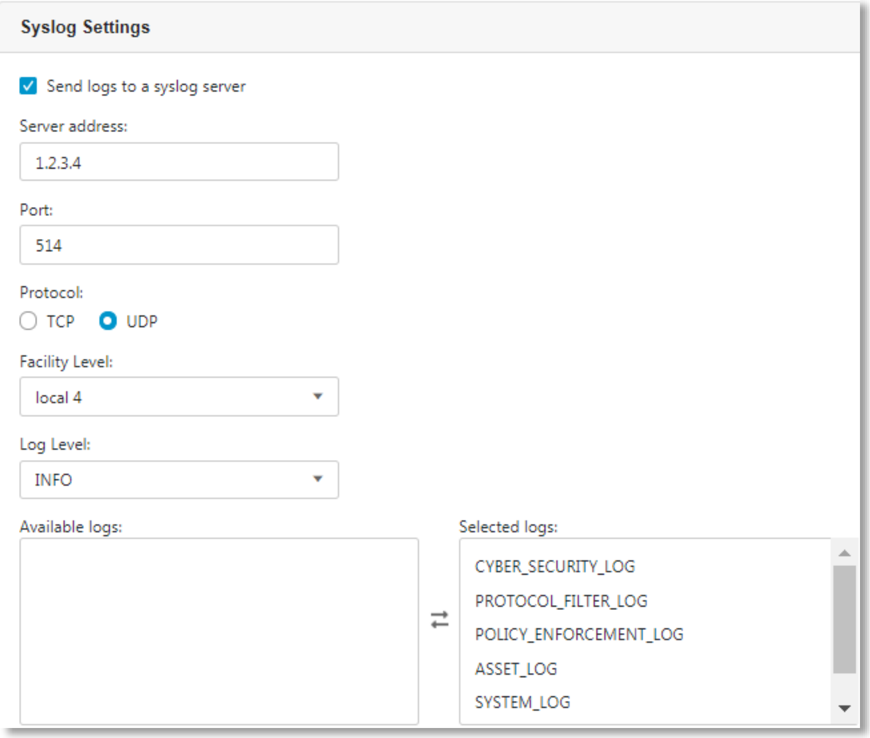
EdgeIPS™ system maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) syslog messages are used in EdgeIPS.

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

Configuring Syslog Settings

Procedure

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



Syslog Settings

☑ Send logs to a syslog server

Server address: 1.2.3.4

Port: 514

Protocol: ○ TCP ● UDP

Facility Level: local 4

Log Level: INFO

Available logs:

Selected logs:
CYBER_SECURITY_LOG
PROTOCOL_FILTER_LOG
POLICY_ENFORCEMENT_LOG
ASSET_LOG
SYSTEM_LOG

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

Field	Description
Server address	Type the IP address of the Syslog server.
Port	Type the port number.
Protocol	Select the protocol for the communication.
Facility level	Select a facility level to determine the source and priority of the logs.
Severity level	Select a Syslog severity level. This device only sends logs with the selected severity level or higher to the Syslog servers. For more information, see *Syslog Severity* Levels *on page 39*.

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

Syslog Severity Levels

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

Level	Severity	Description
0	Emergency	▪ Complete system failure Take immediate action.
1	Critical	▪ Primary system failure Take immediate action.
2	Alert	▪ Urgent failure Take immediate action.
3	Error	▪ Non-urgent failure Resolve issues quickly.
4	Warning	▪ Error pending Take action to avoid errors.
5	Notice	▪ Unusual events Immediate action is not required.
6	Informational	▪ Normal operational messages useful for reporting, measuring throughput, and other purposes No action is required.
7	Debug	▪ Useful information when debugging the application. **Note:** Setting the debug level can generate a large amount of Syslog traffic in a busy network. Use with caution.

Syslog Severity Level Mapping Table

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

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

The System Time Tab

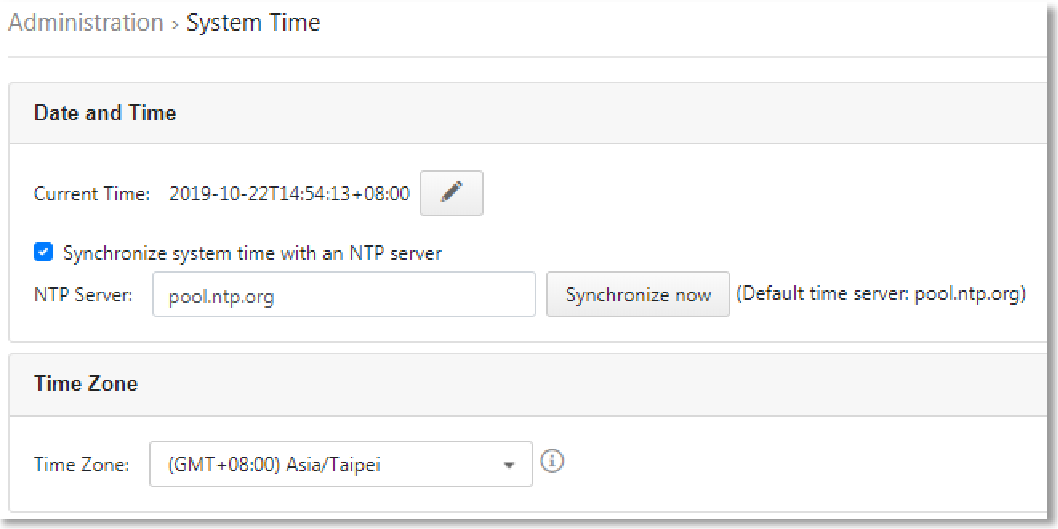
Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure

NTP settings to synchronize the server clock with an NTP server, or manually set the system time.

Configuring System Time

Procedure

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



Administration › System Time

Date and Time

Current Time: 2019-10-22T14:54:13+08:00

☑ Synchronize system time with an NTP server

NTP Server: pool.ntp.org

(Default time server: pool.ntp.org)

Time Zone

Time Zone: (GMT+08:00) Asia/Taipei

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

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

The Back Up / Restore Tab

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

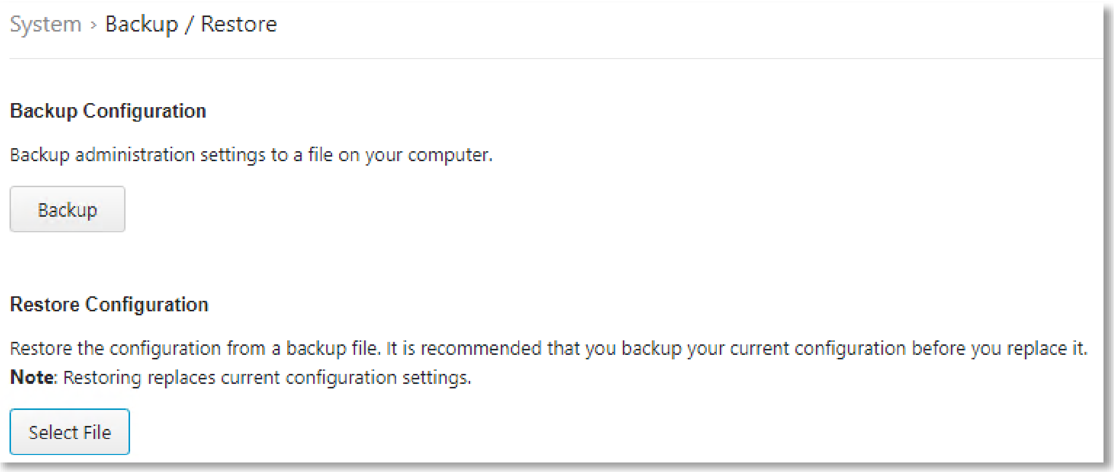
We recommend the following:

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

Backing Up a Configuration

Procedure

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



System › Backup / Restore

Backup Configuration

Backup administration settings to a file on your computer.

Restore Configuration

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

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

Restoring a Configuration

Follow the steps to restore the configurations of the EdgeIPS.

Procedure

1. Go to [Administration] > [Back Up / Restore].
2. Under the [Restore Configuration] section, click the [Select File] button, and proceed to import the file.

All services will restart. It can take some time to restart services after applying imported settings and rules.

The Firmware Management Tab

Use the [Firmware Management] tab to:

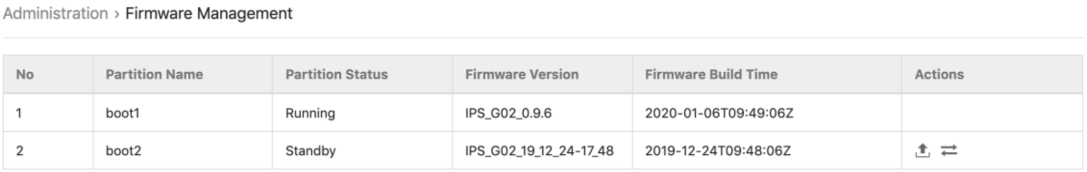
- View the firmware information for the device
- Upgrade the firmware of the device
- Boot into standby partition and firmware

Viewing Device Firmware Information

Procedure

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

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



Administration › Firmware Management

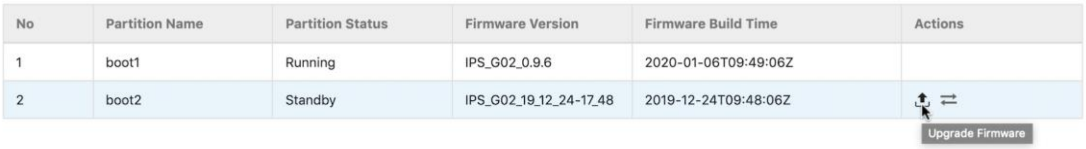
No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPS_G02_0.9.6	2020-01-06T09:49:06Z	
2	boot2	Standby	IPS_G02_19_12_24-17_48	2019-12-24T09:48:06Z	⇧ ⇄

Updating Firmware

Procedure

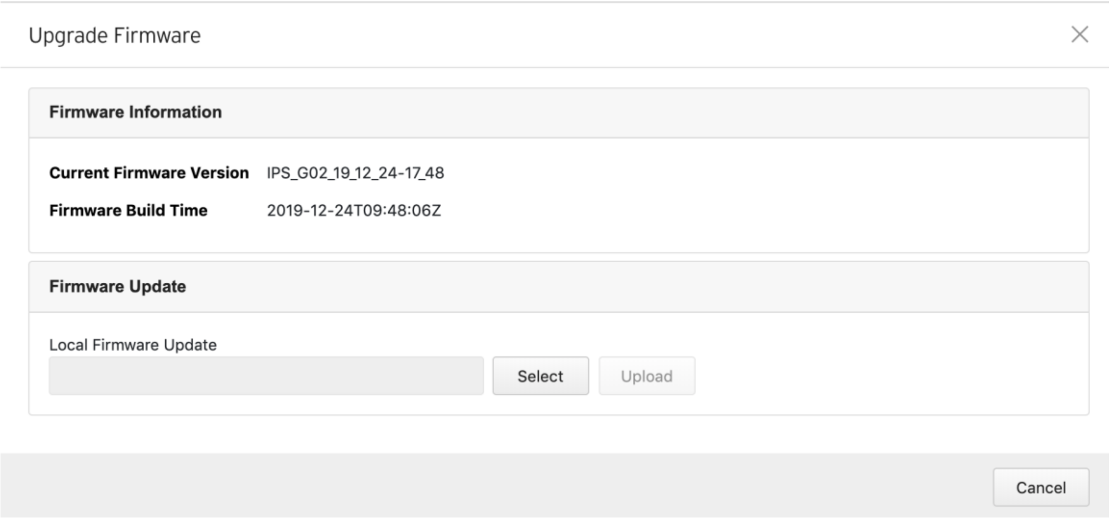
1. Go to [Administration] > [Firmware Management].

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.



No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPS_G02_0.9.6	2020-01-06T09:49:06Z	
2	boot2	Standby	IPS_G02_19_12_24-17_48	2019-12-24T09:48:06Z	⇧ ⇄

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



Upgrade Firmware

Firmware Information

Current Firmware Version IPS_G02_19_12_24-17_48

Firmware Build Time 2019-12-24T09:48:06Z

Firmware Update

Local Firmware Update

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

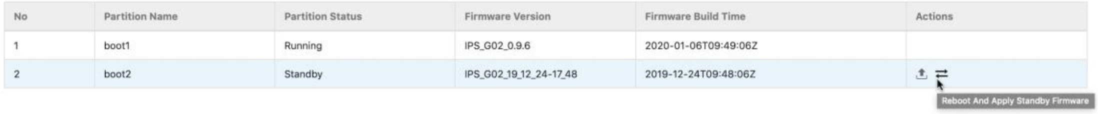
Note: Various versions of the firmware can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

Rebooting and Applying Firmware

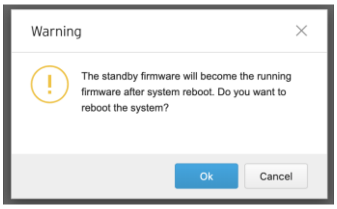
To boot into upgraded firmware or to revert to previous firmware, a user may need to boot into the [Standby] partition and load the firmware from there.

Procedure

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



No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IPS_G02_0.9.6	2020-01-06T09:49:06Z	
2	boot2	Standby	IPS_G02_19_12_24-17_48	2019-12-24T09:48:06Z	



Warning

The standby firmware will become the running firmware after system reboot. Do you want to reboot the system?

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

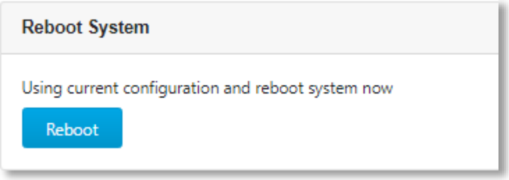
The Reboot System Tab

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

Rebooting the System

Procedure

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



Reboot System

Using current configuration and reboot system now

Supported USB Devices

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

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

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

Pattern Loading Function

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

Note: Given that this feature allows anyone with a supported USB disk device to update the pattern file, the physical security of the EdgeIPS device must be considered carefully.

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

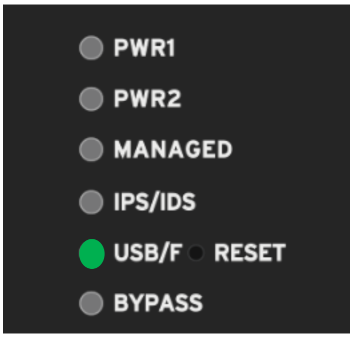
Procedure

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.

Note: If multiple pattern files exist in the folder, the newest will be selected in subsequent steps.

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

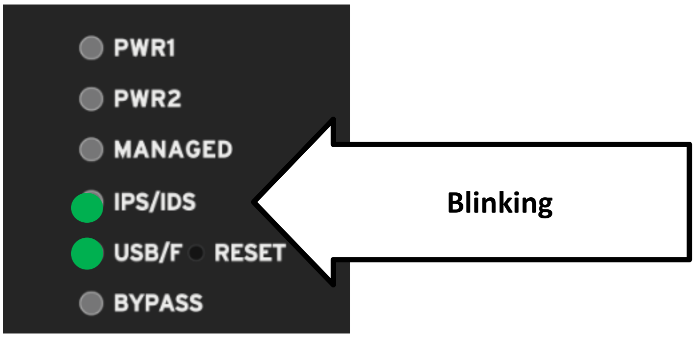


Note: If an unsupported USB device is plugged in, it will simply be ignored and no further action will be taken.

4. The functionality of the reset button will also change to support this function until the USB device is unplugged out. The reset button will at this time not serve the as reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken when a USB device is plugged in.
5. The user can use the reset button to cycle through a set of possible actions. By default, no action is selected. The user must press the reset button at least once to make selection. The LEDs will indicate which action is currently selected.

Action	LED	COLOUR/STATE
Default – No action selected but USB plugged in	USB LED	Green – Steady
Load/Restore Pattern from USB Disk Device	IPS/IDS LED	Green – Blinking (1/sec)

6. From the default state, press the reset button once to select "Load/Restore Pattern from USB Disk Device". The IPS/IDS LED will turn green and start blinking.



7. After ensuring the correct action is selected, the action must be confirmed by holding down the reset button for more than 3 seconds.

Note: The action must be confirmed within 10 seconds. If the action is not confirmed within 10 seconds, the LEDs will be return to their default state (no action selected) and an action must be selected once again if desired.

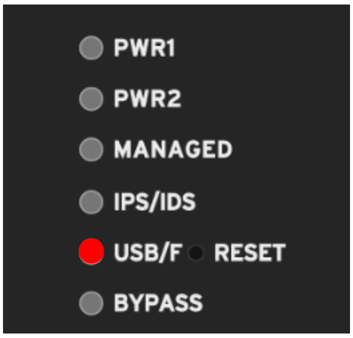
8. While an action is being attempted, if there is a USB disk data transfer, the following LEDs will indicate it as shown here and then return to previous state after data transfer is complete.

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

9. If any error occurs when action is being attempted, the following LEDS will indicate show it like so:

Error Indication (on any	LED	COLOUR/STATE
	Fault LED	Red – Steady

error while action was being processed)		



Note: The error can only be cleared if: (1) the reset button is pressed once more (LEDs return to default state with no action selected) or (2) the USB disk is unplugged

10. Relevant system logs can be checked to verify whether action was completed successfully or failed. If an action is successful, LEDs will be restored to their default state when the USB disk device was first plugged in and no action was selected.
11. The USB disk device may be unplugged, after which LEDs will return to their state prior to the USB disk device being plugged in (USB LED off), and a log will be available in system logs.

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

Terms and Acronyms

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

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