EdgeFire™

Administrator's Guide

2021-12-24

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 EdgeFire™

Introduction

EdgeFire™, a next generation firewall, is a highly integrated industrial multiport secure router with firewall, NAT, and IPS functions. It is designed for Ethernet-based security applications on factory networks, and it provides an electronic security perimeter for the protection of critical cyber assets including pump-and-treat systems in water stations, DCS systems in oil and gas applications, and PLC/SCADA systems in factory automation. Users can access its web-based 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.

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 making provisioning timely security updates or patches 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

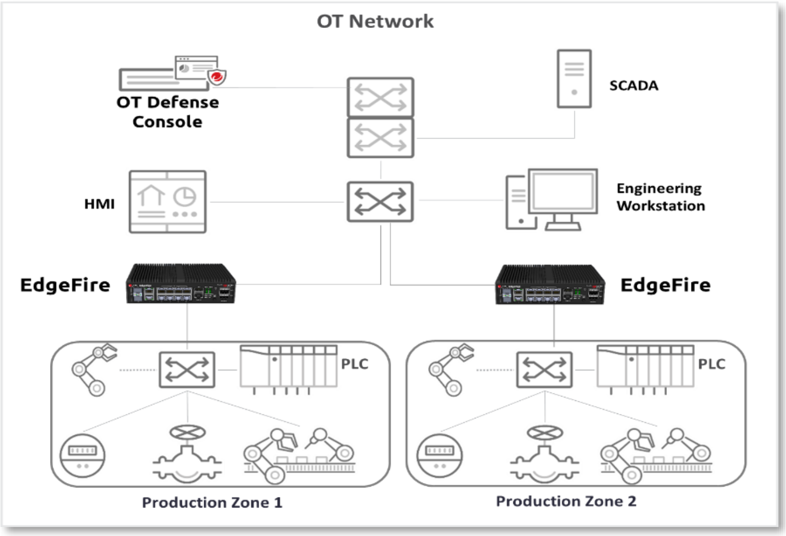


Figure 1. Trend Micro security solutions for OT networks

Main Functions

EdgeFire™ is a security device which can be managed by the OT Defense Console. The main functions of the product are as follows:

Extensive Support for Industrial Protocols

EdgeFire™ 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

EdgeFire™'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.

Intelligence Learning and Rule Generation for Daily Network Traffic

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

Improve Shadow OT Visibility by Integrating IT and OT Networks

EdgeFire™ 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 all 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

EdgeFire™ 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, EdgeFire™ offers your systems exclusive protection from undisclosed and zero-day threats.

Centralized Management

Trend Micro'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

Flexible Segmentation and Isolation

EdgeFire™ is the ideal solution for segmenting a network into easily managed security zones. It segments networks and isolates connectivity both to and between facilities as well as production zones. EdgeFire™ 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.

Getting Started

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

> **Note:** For an overview of the physical hardware and characteristics or a condensed version of help with initial setup of the device, please refer to the EdgeFire™ Quick Setup Guide

Getting Started: Task List

The Getting Started Task List provides a high-level overview of all procedures required to get EdgeFire™ up and running as quickly as possible. Each step links to more detailed instructions later in the document.

Procedure

1. Open the management console.

   For more information, see *Opening the Management Console on page 13*.

2. Change the administrator password.

   For more information, see *Changing the Administrator's Password on page 14*.

3. Ensure that the link speed modes of the network ports are correct for your environment.

   For more information, see *Configuring the Ports on page 22*.

4. Change the default web management console IP address.

   The default web management console IP address is **192.168.127.254**. The IP address is bound to **LAN1** network interface. To change the default IP address, see *Configuring LAN Network Interface on page 24*.

5. Configure the network interfaces.

   For more information, see *The Network on page 24*.

6. Configure the system time.

   For more information, see *Configuring System Time on page 115*.

7. (Optional) Configure the Syslog settings.

   For more information, see *Configuring Syslog Settings on page 112*.

8. Configure Object Profiles.

   For more information, see *The Object Profiles on page 48*.

9. Configure security policies.

   For more information, see *The Security on page 81*.

10. Configure the device name and device location information.

    For more information, see *Configuring Device Name and Device Location Information on page 110*.

11. (Optional) Configure management protocols and ports.

    For more information, see *Configuring Management Protocols and Ports on page 110*.

(Optional) Configure access control list from management clients.

For more information, see *Configuring Access Control List from Management Clients on page 111*.

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

    For more information, see *Manually Updating the Pattern on page 96*.

13. (Optional) Enabling Management by ODC.

    For more information, see *The Sync Settings Tab on page 111*.

14. (Optional) Configuring password policy.

For more information, see *Configuring Password Policy Settings on page 108*.

Opening the Management Console

EdgeFire™ 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.

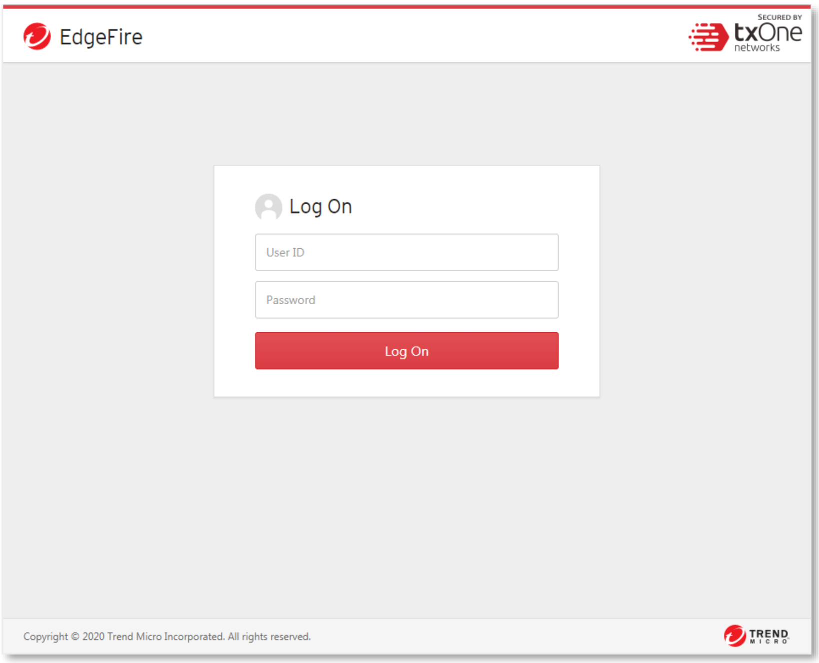
Procedure

1. In a web browser, type enter the address of the EdgeFire™ in the following format:

   `https://192.168.127.254`

   The logon screen will appear.

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



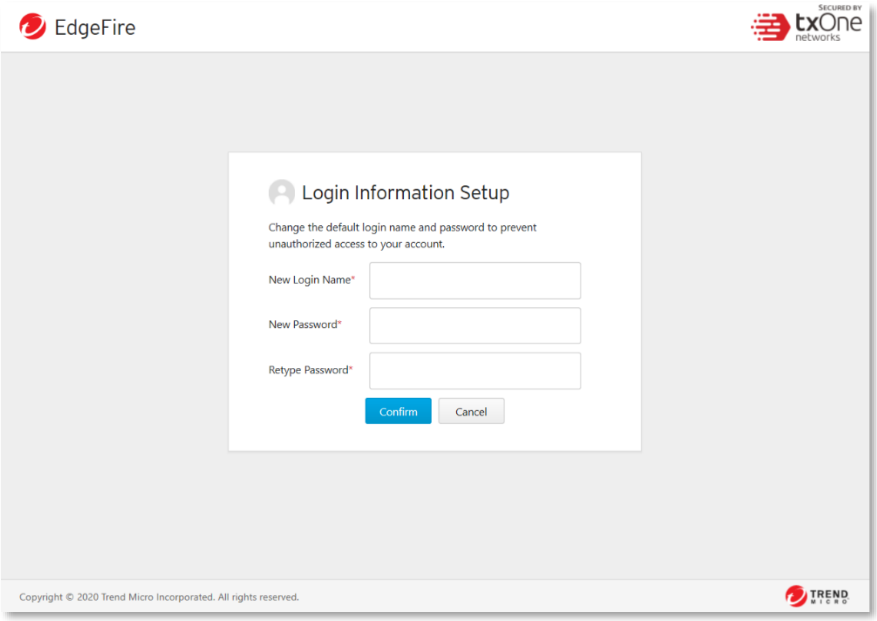
Copyright © 2020 Trend Micro Incorporated. All rights reserved.

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

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

   - User name: `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.



Login Information Setup

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

New Login Name*

New Password*

Retype Password*

Copyright © 2020 Trend Micro Incorporated. All rights reserved.

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

Changing the Administrator's Password

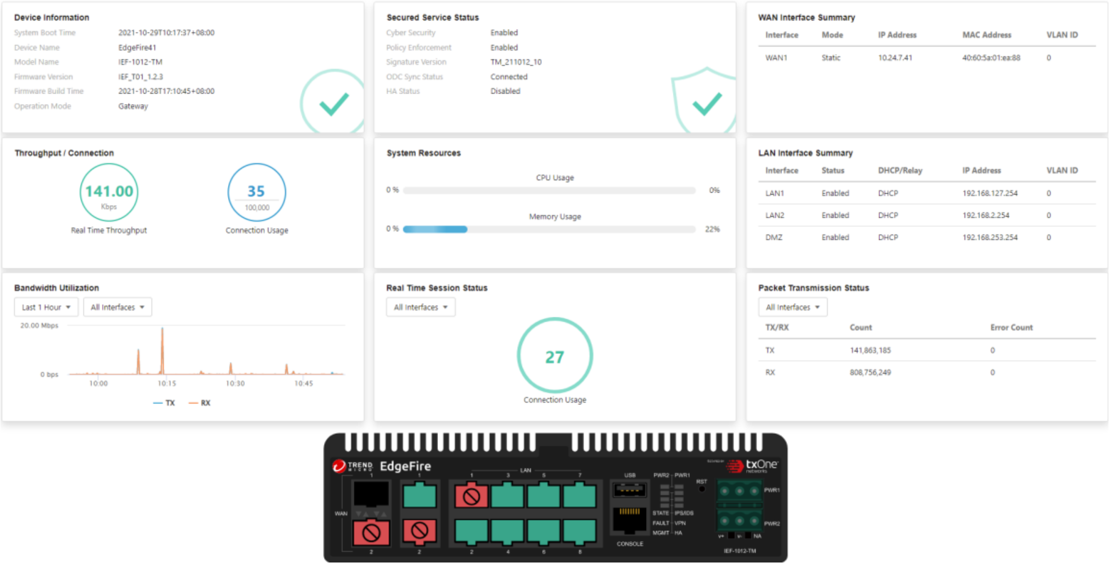
Refer to chapter "The Administration Tab", under sub-topic Account Management > Changing Your Password.

The System Tab

Monitor the following on the [System] tab:

- Device information
- Status of secured services
- System resource usage
- WAN interface information
- LAN interface information
- Throughput/connection information for this device
- Bandwidth utilization (in gateway mode)
- Real time session status (in gateway mode)
- Packet transmission status (in gateway mode)

The System tab in gateway mode is shown as below:



Device Information

System Boot Time	2021-10-29T10:17:37+08:00
Device Name	EdgeFire41
Model Name	IEF-1012-TM
Firmware Version	IEF_T01_1.2.3
Firmware Build Time	2021-10-28T17:10:45+08:00
Operation Mode	Gateway

Secured Service Status

Cyber Security	Enabled
Policy Enforcement	Enabled
Signature Version	TM_211012_10
ODC Sync Status	Connected
HA Status	Disabled

WAN Interface Summary

Interface	Mode	IP Address	MAC Address	VLAN ID
WAN1	Static	10.24.7.41	40:60:5a:01:ea:88	0

Throughput / Connection

System Resources

CPU Usage 0 % 0%

Memory Usage 0 % 22%

LAN Interface Summary

Interface	Status	DHCP/Relay	IP Address	VLAN ID
LAN1	Enabled	DHCP	192.168.127.254	0
LAN2	Enabled	DHCP	192.168.2.254	0
DMZ	Enabled	DHCP	192.168.253.254	0

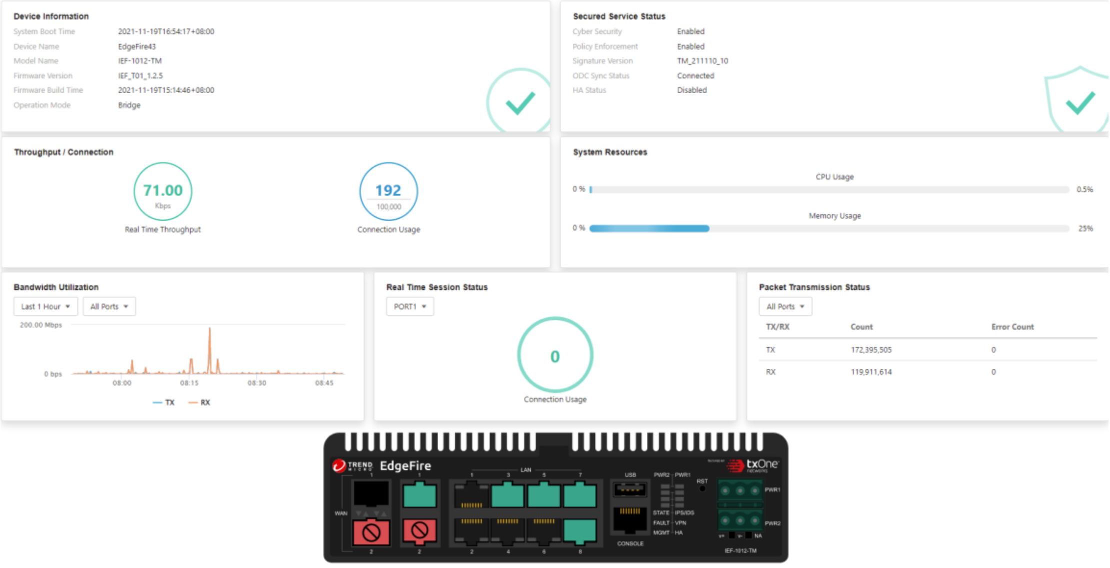
Bandwidth Utilization

Real Time Session Status

Packet Transmission Status

TX/RX	Count	Error Count
TX	141,863,185	0
RX	808,756,249	0

The System tab in bridge mode is shown as below:



Device Information

System Boot Time	2021-11-19T16:54:17+08:00
Device Name	EdgeFire43
Model Name	IEF-1012-TM
Firmware Version	IEF_T01_1.2.5
Firmware Build Time	2021-11-19T15:14:46+08:00
Operation Mode	Bridge

Secured Service Status

Cyber Security	Enabled
Policy Enforcement	Enabled
Signature Version	TM_211110_10
ODC Sync Status	Connected
HA Status	Disabled

Throughput / Connection

71.00 Kbps Real Time Throughput

192 / 100,000 Connection Usage

System Resources

CPU Usage 0 % 0.5%

Memory Usage 0 % 25%

Bandwidth Utilization

Last 1 Hour ▾ All Ports ▾

Real Time Session Status

PORT1 ▾

0 Connection Usage

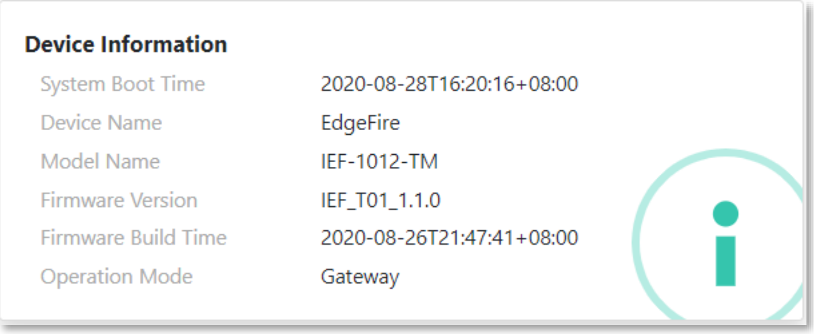
Packet Transmission Status

All Ports ▾

TX/RX	Count	Error Count
TX	172,395,505	0
RX	119,911,614	0

Device Information

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

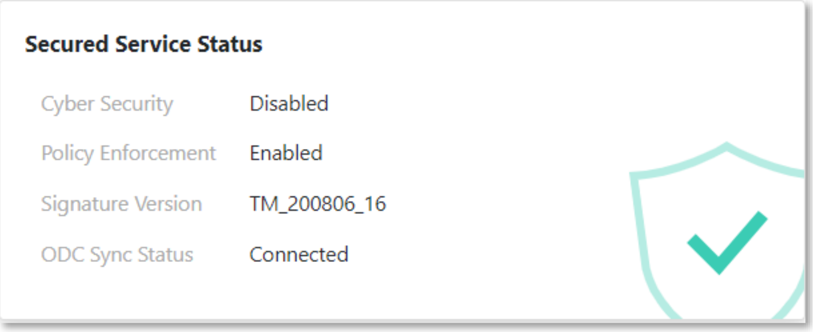


Device Information

System Boot Time	2020-08-28T16:20:16+08:00
Device Name	EdgeFire
Model Name	IEF-1012-TM
Firmware Version	IEF_T01_1.1.0
Firmware Build Time	2020-08-26T21:47:41+08:00
Operation Mode	Gateway

Secured Service Status

This widget shows the statuses (enabled/disabled) of the security services the device provides, as well as the signature version used and sync status with ODC.



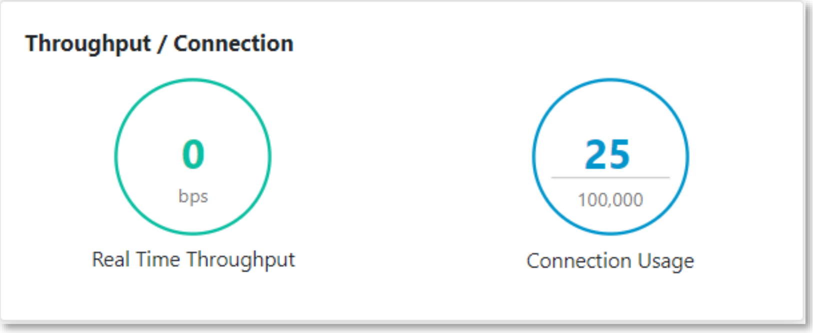
Secured Service Status

Cyber Security	Disabled
Policy Enforcement	Enabled
Signature Version	TM_200806_16
ODC Sync Status	Connected

System Resources

This widget shows the following:

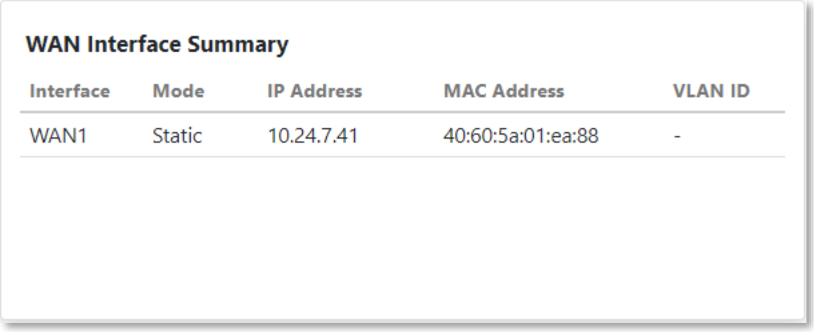
- CPU Utilization - Real time CPU utilization % (according to refresh time settings).
- Memory Utilization - Real time memory utilization % (according to refresh time settings).



Throughput / Connection

WAN Interface Summary

This widget shows a summary of information for the WAN interface.

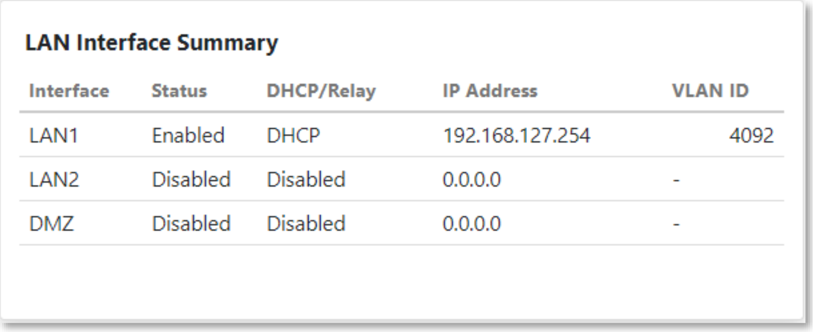


WAN Interface Summary

Interface	Mode	IP Address	MAC Address	VLAN ID
WAN1	Static	10.24.7.41	40:60:5a:01:ea:88	-

LAN Interface Summary

This widget shows a summary of information for the LAN, LAN2 interfaces.

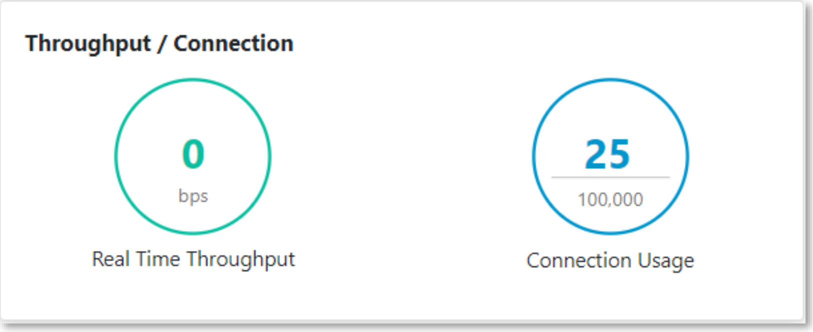


LAN Interface Summary

Interface	Status	DHCP/Relay	IP Address	VLAN ID
LAN1	Enabled	DHCP	192.168.127.254	4092
LAN2	Disabled	Disabled	0.0.0.0	-
DMZ	Disabled	Disabled	0.0.0.0	-

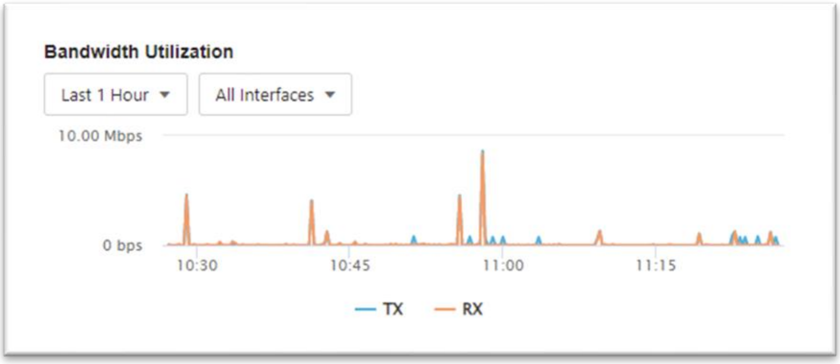
Throughput / Connection

This widget shows the throughput/connection (real time throughput and connection usage) of the device.



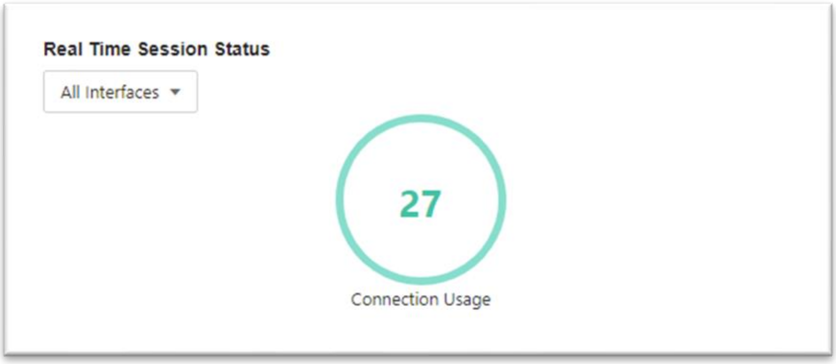
Bandwidth Utilization (In Gateway Mode)

This widget shows the amount of bandwidth consumed on the network via different interfaces in the regular time interval.



Real Time Session Status (In Gateway Mode)

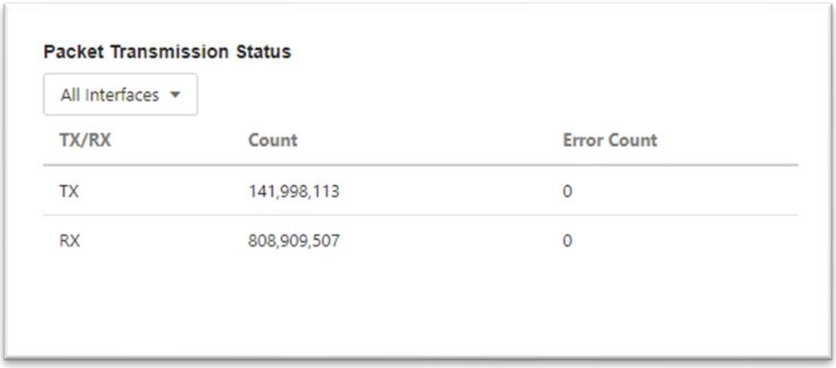
This widget shows the status of real time session with the percentage of connection.



Real Time Session Status

Device Information (In Gateway Mode)

This widget shows the packet transmission status via error(s) in the total counts.



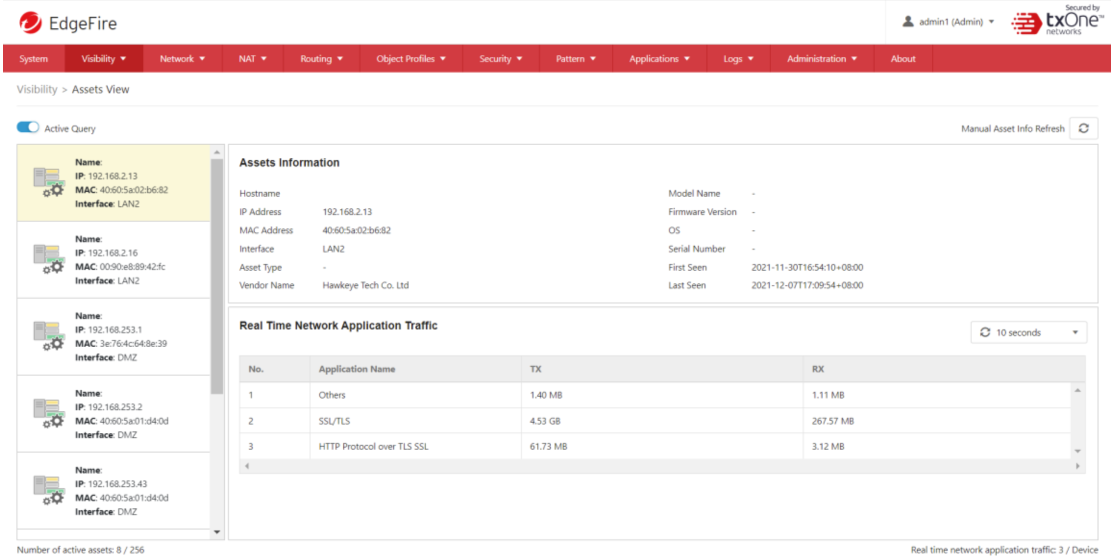
Packet Transmission Status

TX/RX	Count	Error Count
TX	141,998,113	0
RX	808,909,507	0

Chapter 4

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 EdgeFire™.



Name:
IP: 192.168.2.13
MAC: 40:60:5a:02:b6:82
Interface: LAN2

Name:
IP: 192.168.2.16
MAC: 00:90:e8:89:42:fc
Interface: LAN2

Name:
IP: 192.168.253.1
MAC: 3e:76:4c:64:8e:39
Interface: DMZ

Name:
IP: 192.168.253.2
MAC: 40:60:5a:01:d4:0d
Interface: DMZ

Name:
IP: 192.168.253.43
MAC: 40:60:5a:01:d4:0d
Interface: DMZ

Number of active assets: 8 / 256

Assets Information

Hostname		Model Name	-
IP Address	192.168.2.13	Firmware Version	-
MAC Address	40:60:5a:02:b6:82	OS	-
Interface	LAN2	Serial Number	-
Asset Type	-	First Seen	2021-11-30T16:54:10+08:00
Vendor Name	Hawkeye Tech Co. Ltd	Last Seen	2021-12-07T17:09:54+08:00

Real Time Network Application Traffic

No.	Application Name	TX	RX
1	Others	1.40 MB	1.11 MB
2	SSL/TLS	4.53 GB	267.57 MB
3	HTTP Protocol over TLS SSL	61.73 MB	3.12 MB

Real time network application traffic: 3 / Device

The assets, listed on the tab, are automatically detected by the EdgeFire™ device.

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

Active Query

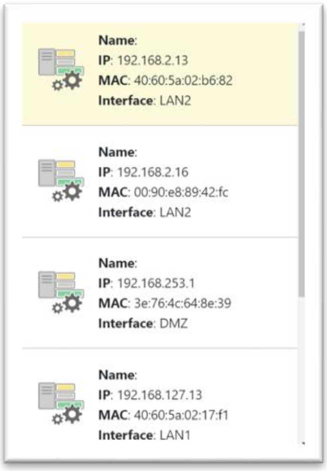
Active query can detect inactive or dormant assets or passive assets in the network.

Note: In firmware 1.1, Active query supports 4 protocols (Modbus, CIP, OMRON FINS and SMB)

Viewing Asset Information

Procedure

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



Name:
IP: 192.168.2.13
MAC: 40:60:5a:02:b6:82
Interface: LAN2

Name:
IP: 192.168.2.16
MAC: 00:90:e8:89:42:fc
Interface: LAN2

Name:
IP: 192.168.253.1
MAC: 3e:76:4c:64:8e:39
Interface: DMZ

Name:
IP: 192.168.127.13
MAC: 40:60:5a:02:17:f1
Interface: LAN1

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

Field	Description
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 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 statistics for the asset

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

Note: Click the [Manual asset info refresh] to refresh the information displayed.

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

The Network Tab

This chapter describes how to configure the physical ports and network interfaces for your EdgeFire™.

Port Settings

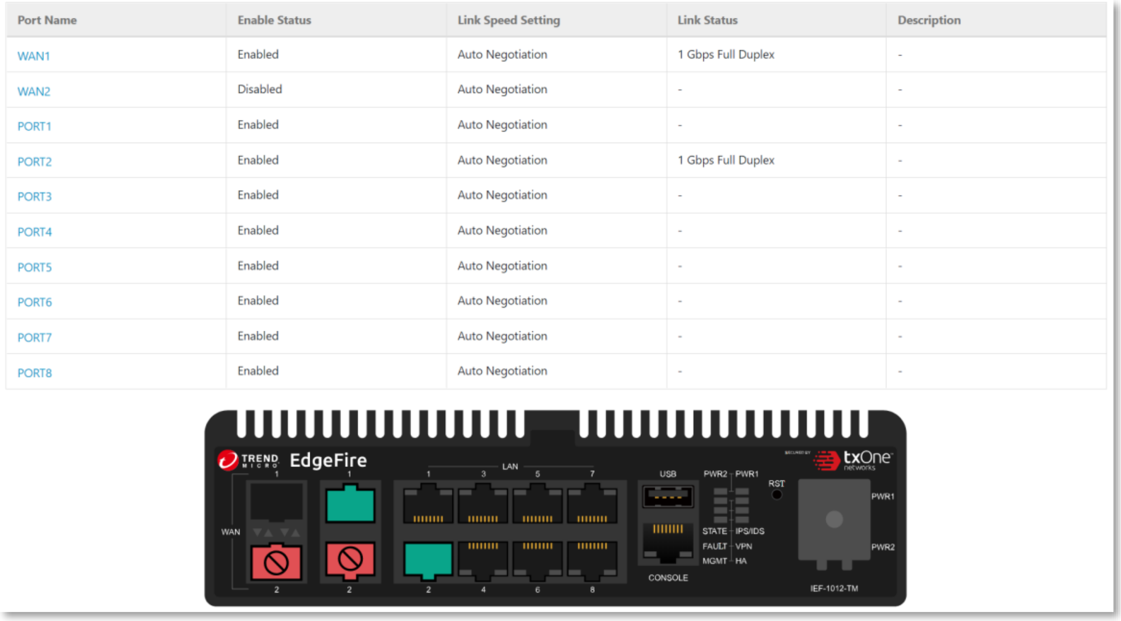
The [Port Settings] option allows you to enable/disable the ports and select the desired link speed for the ports.

> **Note:** The term **Port** in this document refers to the physical port to which the network cable is connected.

Configuring the Ports

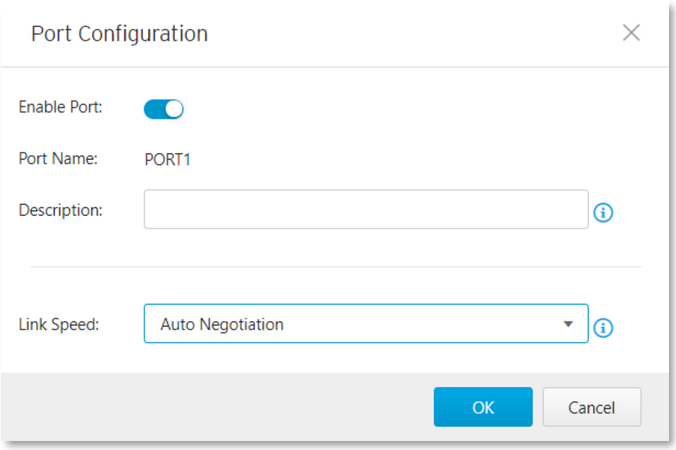
Procedure

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



Port Name	Enable Status	Link Speed Setting	Link Status	Description
WAN1	Enabled	Auto Negotiation	1 Gbps Full Duplex	-
WAN2	Disabled	Auto Negotiation	-	-
PORT1	Enabled	Auto Negotiation	-	-
PORT2	Enabled	Auto Negotiation	1 Gbps Full Duplex	-
PORT3	Enabled	Auto Negotiation	-	-
PORT4	Enabled	Auto Negotiation	-	-
PORT5	Enabled	Auto Negotiation	-	-
PORT6	Enabled	Auto Negotiation	-	-
PORT7	Enabled	Auto Negotiation	-	-
PORT8	Enabled	Auto Negotiation	-	-

2. Click a port in the [Port Name] column to configure the port:
   a. Use the toggle to enable or disable the port.
   b. Under the [Link Speed] drop down menu, select the speed and negotiation method of the port.



Port Configuration

Enable Port: ●

Port Name: PORT1

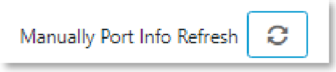
Description:

Link Speed: Auto Negotiation

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

Note: Dual WAN is currently not supported. The WAN2 is disabled.

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



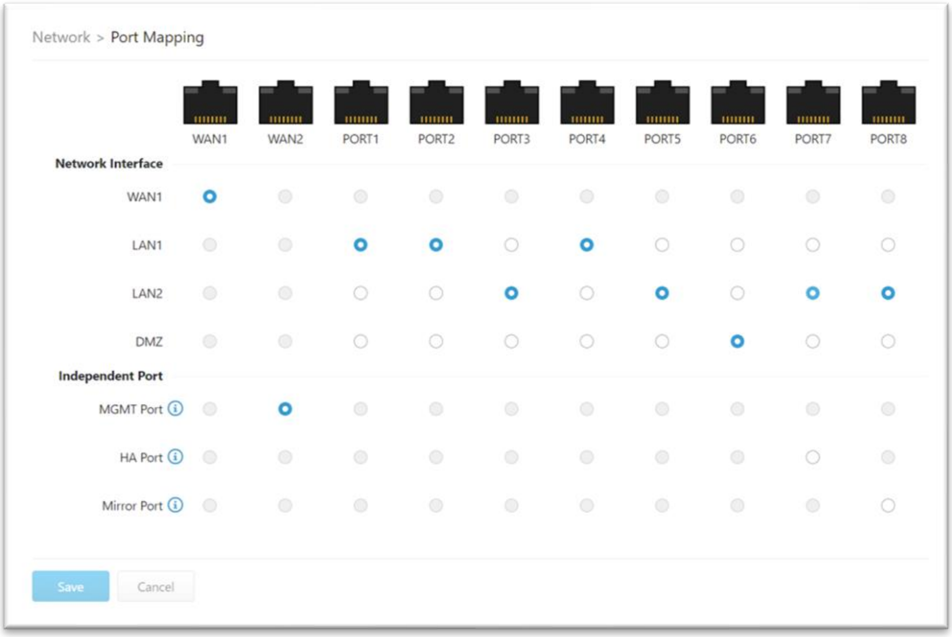
Port Mapping

Use the [Port Mapping] tab to view the mapping between the ports and the interfaces.

Viewing the Port Mapping (In Gateway Mode)

Procedure

1. Go to [Network] > [Port Mapping].
2. The Port Mapping tab will appear. This tab shows the mapping between the physical ports and the network interfaces (WAN interface, LAN interfaces or independent ports).



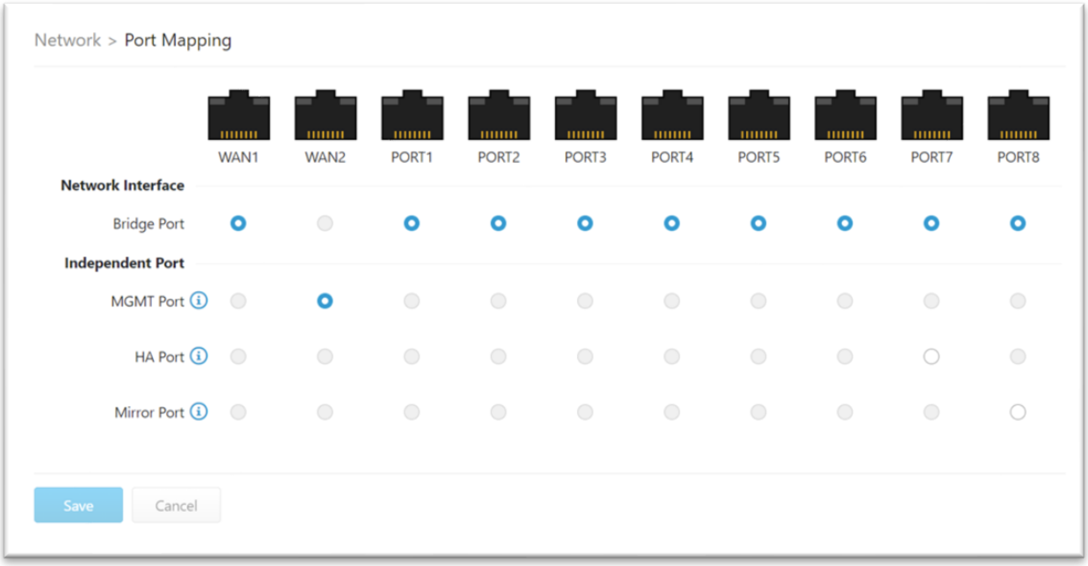
Network > Port Mapping

	WAN1	WAN2	PORT1	PORT2	PORT3	PORT4	PORT5	PORT6	PORT7	PORT8
Network Interface										
WAN1	●	○	○	○	○	○	○	○	○	○
LAN1	○	○	●	●	○	●	○	○	○	○
LAN2	○	○	○	○	●	○	●	○	●	●
DMZ	○	○	○	○	○	○	○	●	○	○
Independent Port										
MGMT Port	○	●	○	○	○	○	○	○	○	○
HA Port	○	○	○	○	○	○	○	○	○	○
Mirror Port	○	○	○	○	○	○	○	○	○	○

Viewing the Port Mapping (In Bridge Mode)

Procedure

3. Go to [Network] > [Port Mapping].
4. The Port Mapping tab will appear. This tab shows the mapping between the physical ports and the interfaces (Bridge port or independent ports).



Network > Port Mapping

	WAN1	WAN2	PORT1	PORT2	PORT3	PORT4	PORT5	PORT6	PORT7	PORT8
Network Interface										
Bridge Port	●	○	●	●	●	●	●	●	●	●
Independent Port										
MGMT Port ⓘ	○	●	○	○	○	○	○	○	○	○
HA Port ⓘ	○	○	○	○	○	○	○	○	○	○
Mirror Port ⓘ	○	○	○	○	○	○	○	○	○	○

Network Interface (In Gateway Mode Only)

Use the [Network Interface] tab to configure the following:

- Network settings of the network interfaces of the device
- DHCP settings on the LAN network interface, including:
  - Disabling DHCP service
  - Enabling DHCP service
  - Configuring DHCP Relay
- Connection type for the WAN network interface, including:
  - Static IP address settings
  - DHCP client

Note: The term **Network Interface** or **Interface** in this document refers to the logical interface that maps to one or more physical ports.

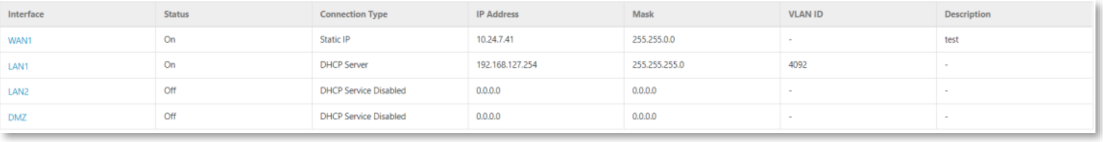
Note: The default web management console IP address is **192.168.127.254**. The IP address is bound to **LAN1** network interface. To change the default IP address, see *Configuring LAN Network Interface on page 24*.

Configuring LAN Network Interface

Procedure

1. Go to [Network] > [Network Interface].

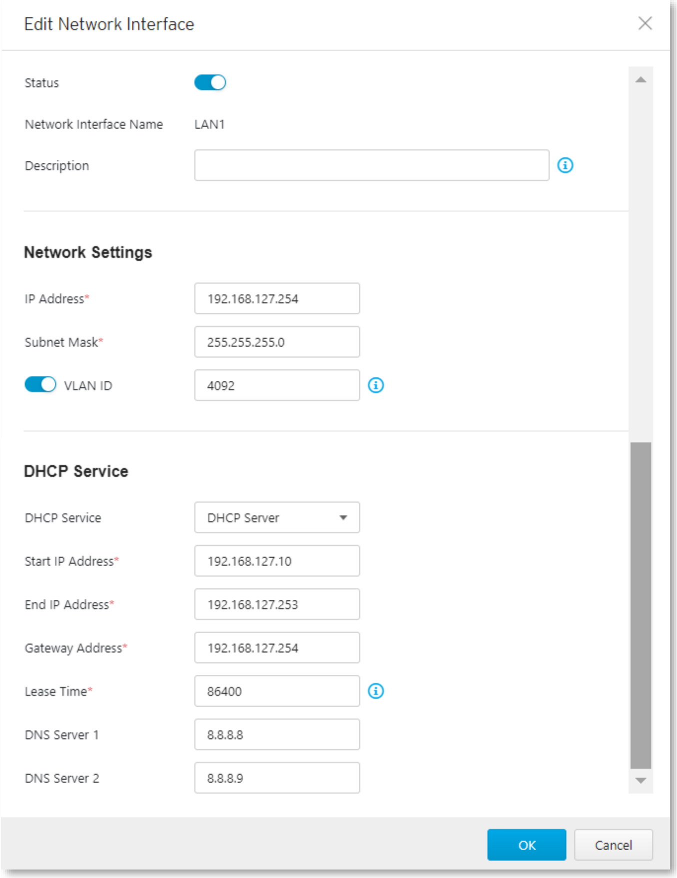
   The [Network Interface] tab will appear.



Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	Static IP	10.24.7.41	255.255.0.0	-	test
LAN1	On	DHCP Server	192.168.127.254	255.255.255.0	4092	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click an LAN interface.

   The [Edit Network Interface] tab will appear.



Edit Network Interface

Status	On
Network Interface Name	LAN1
Description	

Network Settings

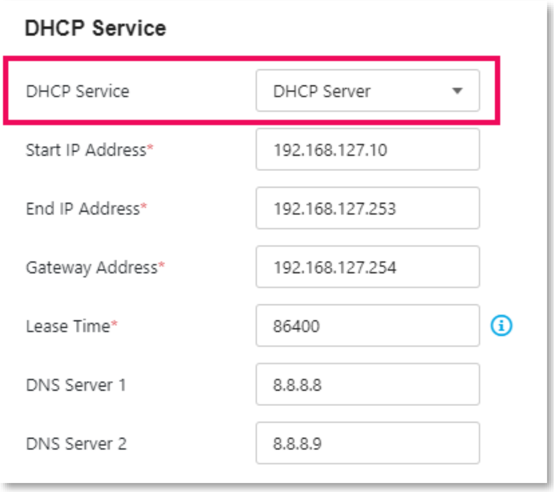
IP Address*	192.168.127.254
Subnet Mask*	255.255.255.0
VLAN ID (On)	4092

DHCP Service

DHCP Service	DHCP Server
Start IP Address*	192.168.127.10
End IP Address*	192.168.127.253
Gateway Address*	192.168.127.254
Lease Time*	86400
DNS Server 1	8.8.8.8
DNS Server 2	8.8.8.9

3. Use the toggle to enable or disable the network interface.
4. Input a descriptive name for the network interface.
5. In the [Network Setting] section, configure the network settings for the interface:
   a. Input an IP address.
   b. Input a subnet mask.
   c. (Optional) Use the toggle to enable or disable VLAN ID. If VNLAN ID is enabled, input the VLAN ID.
6. In the [DHCP] section, configure the DHCP settings for the interface. Possible choices are:
   a. **Disabled**. No DHCP service will be provided at this interface.
   b. **DHCP Server**. This interface will provide DHCP service to the devices that connect to the interface. Once this is selected, you need to provide the following information:

- Start IP address of the DHCP service
- End IP address of the DHCP service
- Gateway IP address that will be assigned to the clients
- Lease time - The amount of time in seconds that a client device can use the IP address settings assigned by the DHCP server
- DNS server IP addresses that will be assigned to the clients

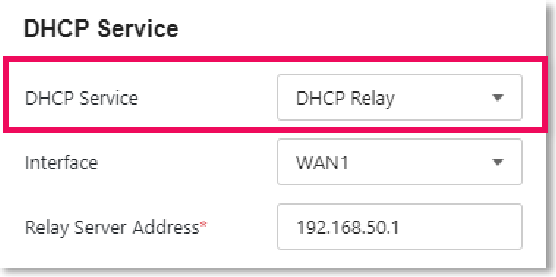


DHCP Service

DHCP Service	DHCP Server
Start IP Address*	192.168.127.10
End IP Address*	192.168.127.253
Gateway Address*	192.168.127.254
Lease Time*	86400
DNS Server 1	8.8.8.8
DNS Server 2	8.8.8.9

c. **DHCP Relay**. This interface will relay the traffic from the clients to a relayed server for DHCP service. Once this is selected, you need to provide the following information:

- Relay Server Address: The IP address of the server that will provide DHCP service



DHCP Service

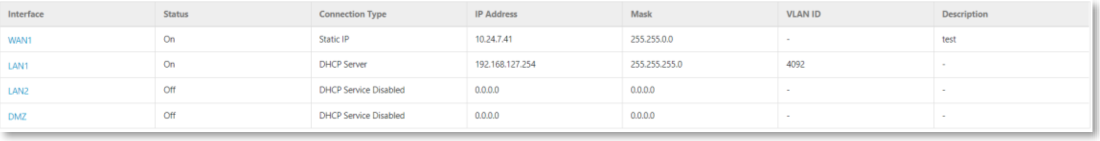
DHCP Service	DHCP Relay
Interface	WAN1
Relay Server Address*	192.168.50.1

Configuring DMZ Network Interface

Procedure

1. Go to [Network] > [Network Interface].

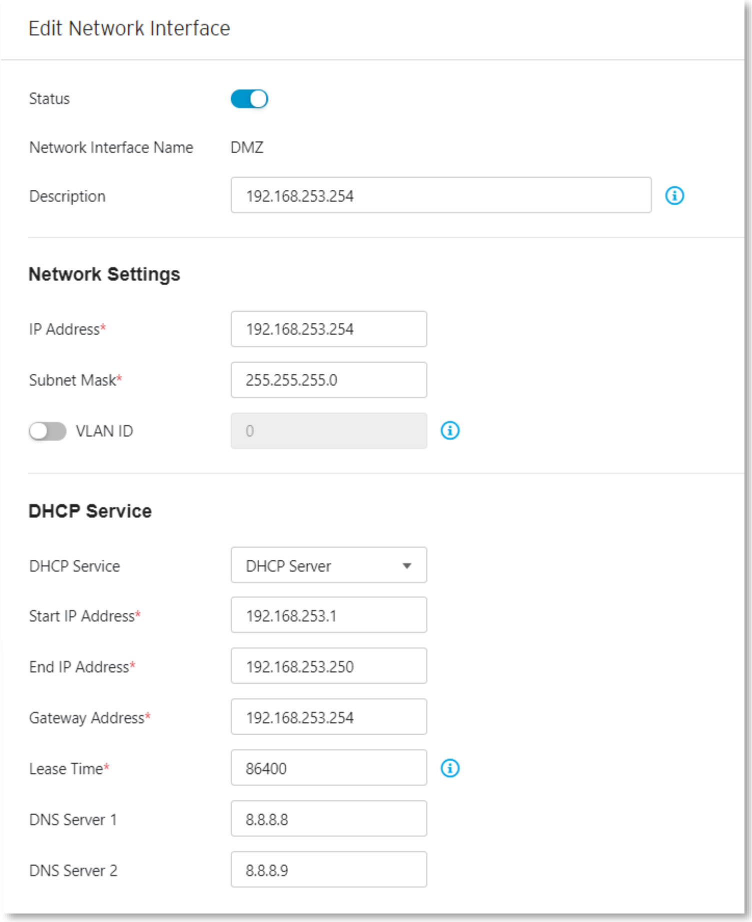
   The [Network Interface] tab will appear.



Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	Static IP	10.24.7.41	255.255.0.0	-	test
LAN1	On	DHCP Server	192.168.127.254	255.255.255.0	4092	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click an DMZ interface.

   The [Edit Network Interface] tab will appear.



Edit Network Interface

Status: ●

Network Interface Name: DMZ

Description: 192.168.253.254

Network Settings

IP Address*: 192.168.253.254

Subnet Mask*: 255.255.255.0

○ VLAN ID: 0

DHCP Service

DHCP Service: DHCP Server

Start IP Address*: 192.168.253.1

End IP Address*: 192.168.253.250

Gateway Address*: 192.168.253.254

Lease Time*: 86400

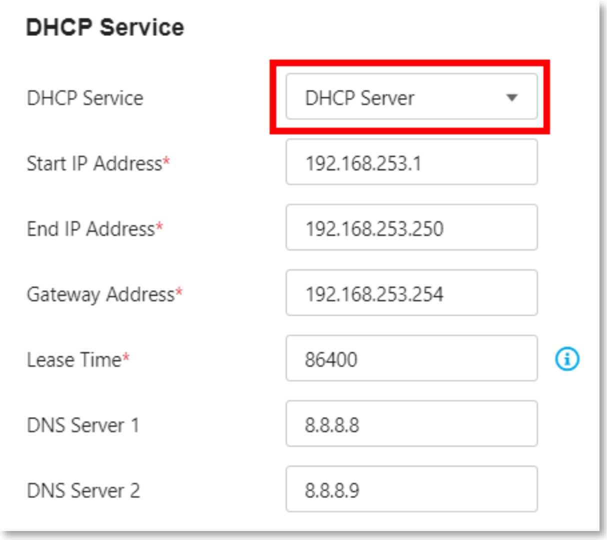
DNS Server 1: 8.8.8.8

DNS Server 2: 8.8.8.9

3. Use the toggle to enable or disable the network interface.
4. Input a descriptive name for the network interface.
5. In the [Network Setting] section, configure the network settings for the interface:
   a. Input an IP address.
   b. Input a subnet mask.
   c. (Optional) Use the toggle to enable or disable VLAN ID. If VNLAN ID is enabled, input the VLAN ID.
6. In the [DHCP] section, configure the DHCP settings for the interface. Possible choices are:
   a. **Disabled**. No DHCP service will be provided at this interface.

b. **DHCP Server**. This interface will provide DHCP service to the devices that connect to the interface. Once this is selected, you need to provide the following information:

- Start IP address of the DHCP service
- End IP address of the DHCP service
- Gateway IP address that will be assigned to the clients
- Lease time - The amount of time in seconds that a client device can use the IP address settings assigned by the DHCP server
- DNS server IP addresses that will be assigned to the clients



DHCP Service

DHCP Service: DHCP Server

Start IP Address*: 192.168.253.1

End IP Address*: 192.168.253.250

Gateway Address*: 192.168.253.254

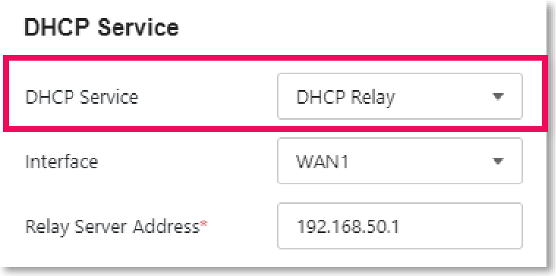
Lease Time*: 86400

DNS Server 1: 8.8.8.8

DNS Server 2: 8.8.8.9

c. **DHCP Relay**. This interface will relay the traffic from the clients to a relayed server for DHCP service. Once this is selected, you need to provide the following information:

- Relay Server Address: The IP address of the server that will provide DHCP service



DHCP Service

DHCP Service: DHCP Relay

Interface: WAN1

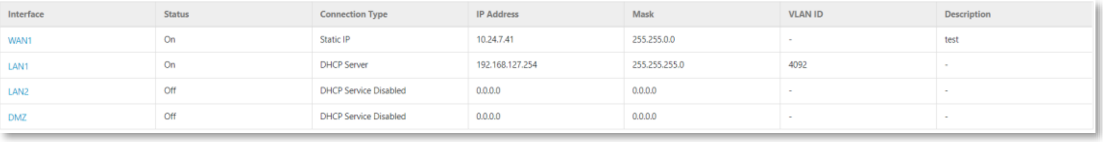
Relay Server Address*: 192.168.50.1

Configuring WAN Network Interface

Procedure

1. Go to [Network] > [Network Interface].

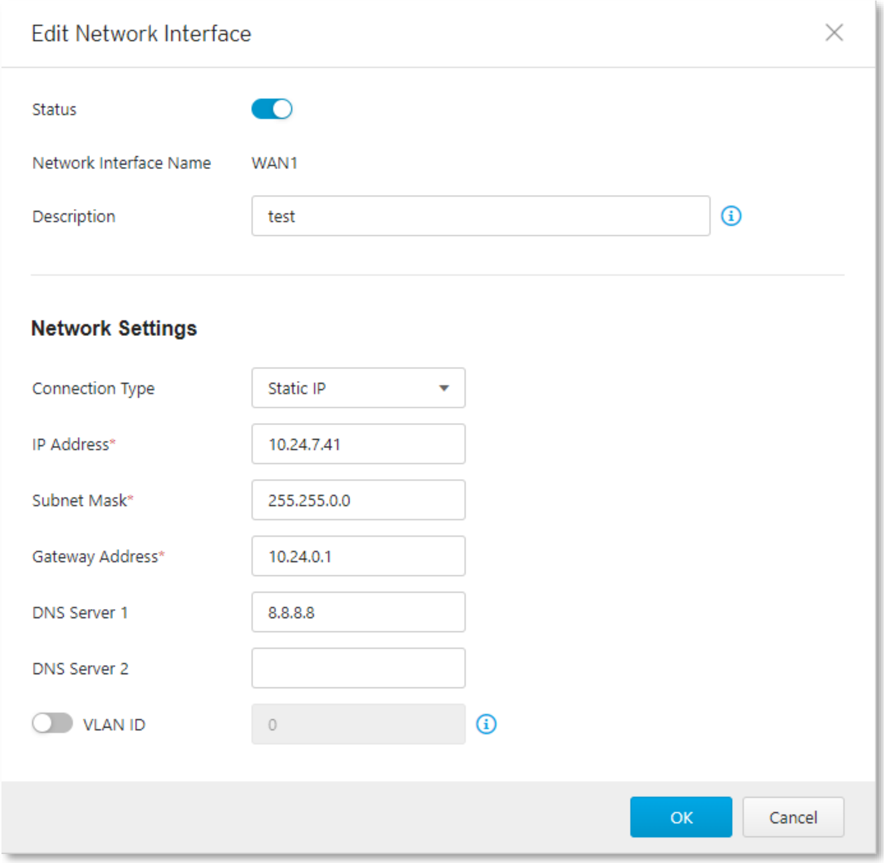
   The [Network Interface] tab will appear.



Interface	Status	Connection Type	IP Address	Mask	VLAN ID	Description
WAN1	On	Static IP	10.24.7.41	255.255.0.0	-	test
LAN1	On	DHCP Server	192.168.127.254	255.255.255.0	4092	-
LAN2	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-
DMZ	Off	DHCP Service Disabled	0.0.0.0	0.0.0.0	-	-

2. Click a WAN interface.

   The [Edit Network Interface] tab will appear.



Edit Network Interface

Status: On

Network Interface Name: WAN1

Description: test

Network Settings

Connection Type: Static IP

IP Address*: 10.24.7.41

Subnet Mask*: 255.255.0.0

Gateway Address*: 10.24.0.1

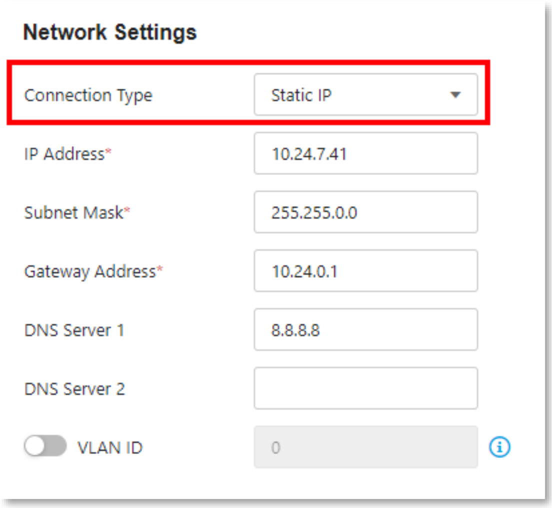
DNS Server 1: 8.8.8.8

DNS Server 2:

VLAN ID: 0

3. Use the toggle to enable or disable the network interface.
4. Input a descriptive name for the network interface.
5. In the [Network Settings] section, choose a [Connection Type] for the interface. Possible choices are:
   a. **Static IP**: This device will use a static IP address for this interface. Once selected, you need to provide the following information:

- IP Address: IP address of the interface
- Subnet Mask: Subnet mask of the interface
- Gateway Address: Gateway IP address of the interface
- DNS server: DNS server IP address of the interface
- (Optional) Use the toggle to enable VLAN ID. Once enabled, input the VLAN ID for the interface.



Network Settings

Connection Type: Static IP

IP Address*: 10.24.7.41

Subnet Mask*: 255.255.0.0

Gateway Address*: 10.24.0.1

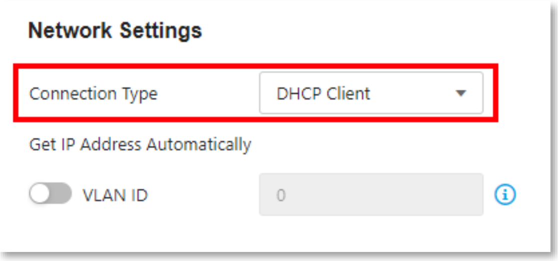
DNS Server 1: 8.8.8.8

DNS Server 2:

VLAN ID: 0

b. **DHCP Client**: The interface will function as a DHCP client to get an IP address from a DHCP server. Once selected, you need to provide the following information:

- (Optional) Use the toggle to enable VLAN ID. Once enabled, input the VLAN ID for the interface.



Network Settings

Connection Type: DHCP Client

Get IP Address Automatically

VLAN ID: 0

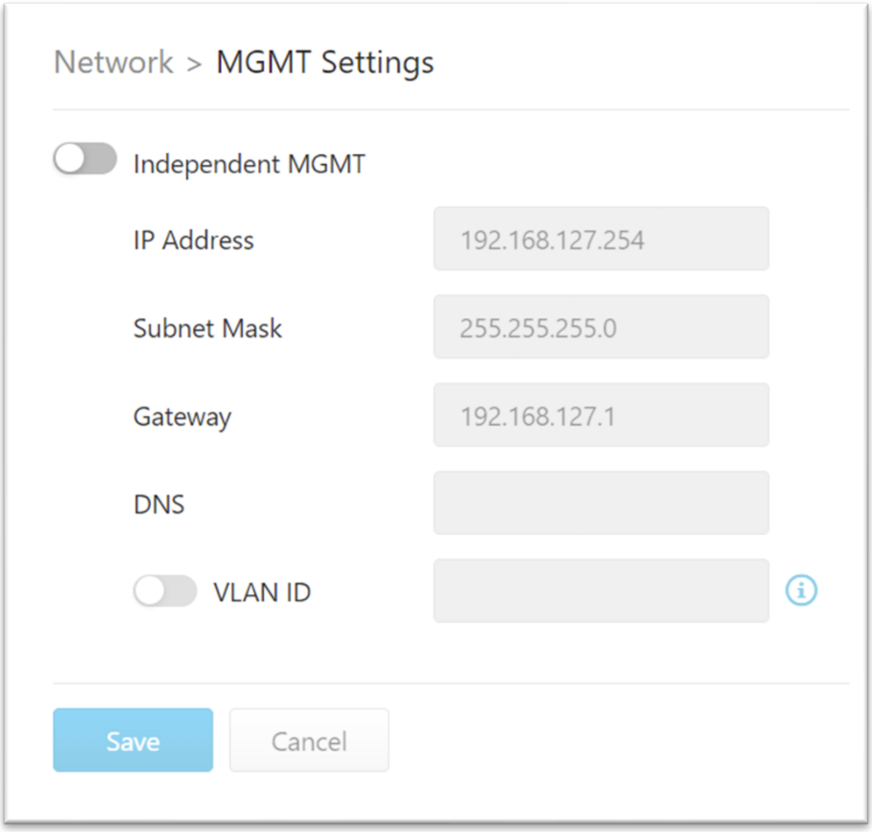
MGMT Settings (In Gateway Mode)

MGMT Settings are the settings for the MGMT Port, which is the reserved port used for the remote system management and the configuration of the network device(s).

Configuring MGMT Port

Procedure

1. Go to [Network] > [MGMT Settings].
   The [MGMT Settings] tab will appear.



Network > MGMT Settings

○ Independent MGMT

IP Address: 192.168.127.254

Subnet Mask: 255.255.255.0

Gateway: 192.168.127.1

DNS:

○ VLAN ID:

2. Use the toggle to enable or disable the [Independent MGMT] function.
3. If Independent MGMT is enabled, configure the following MGMT port settings:
   a. Input an IP address.
   b. Input a subnet mask.
   c. Input a gateway.
   d. Input a DNS.
4. (Optional) Use the toggle to enable or disable VLAN ID. If VNLAN ID is enabled, input the VLAN ID. (VLAN ID: 1~4094)

Note: MGMT Port is WAN2 by default.

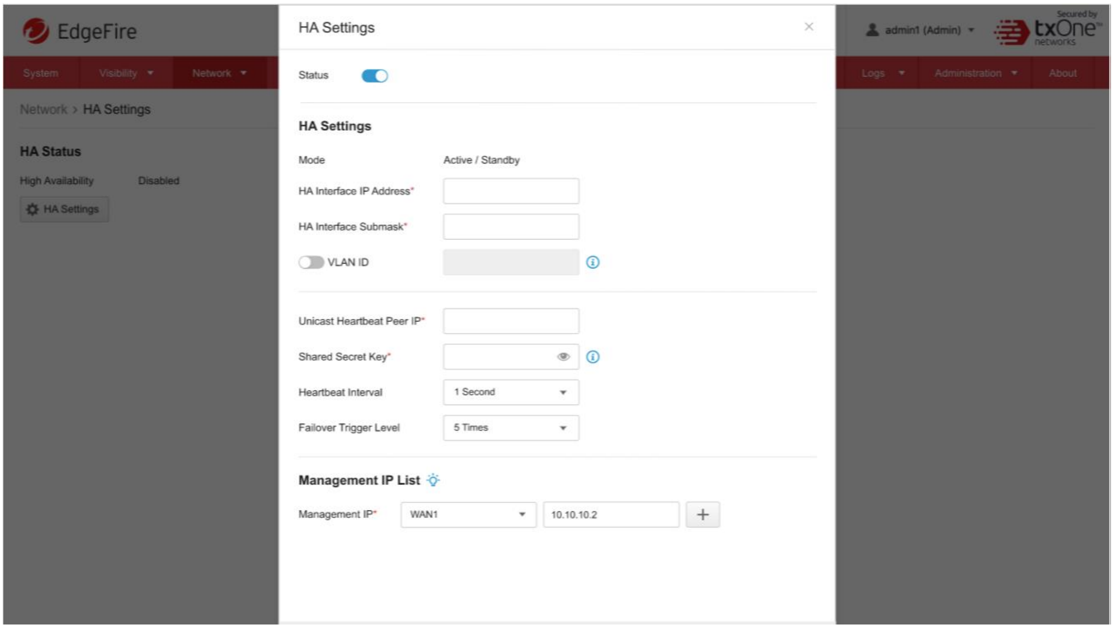
HA Settings

Using a single device for network security and traffic flow can create a single point of failure. EdgeFire™ 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 the primary device to the secondary backup in case of the primary device failure. It thus allows for the planning and building of a fault-tolerant, resilient, and secure network to minimize any OT operational downtime.

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

Procedure

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



HA Settings

Status ●

HA Settings

Mode: Active / Standby

HA Interface IP Address*

HA Interface Submask*

VLAN ID

Unicast Heartbeat Peer IP*

Shared Secret Key*

Heartbeat Interval: 1 Second

Failover Trigger Level: 5 Times

Management IP List

Management IP*: WAN1 10.10.10.2 +

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

Field	Description
Status	Shows HA sync status between two EdgeFire™ devices in the same HA group. This also displays the sync progress.
Mode	**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.
HA Interface IP 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/Disable VLAN ID	VLAN ID of the HA Interface
Unicast Heartbeat Peer IP	The IP address of the HA peer

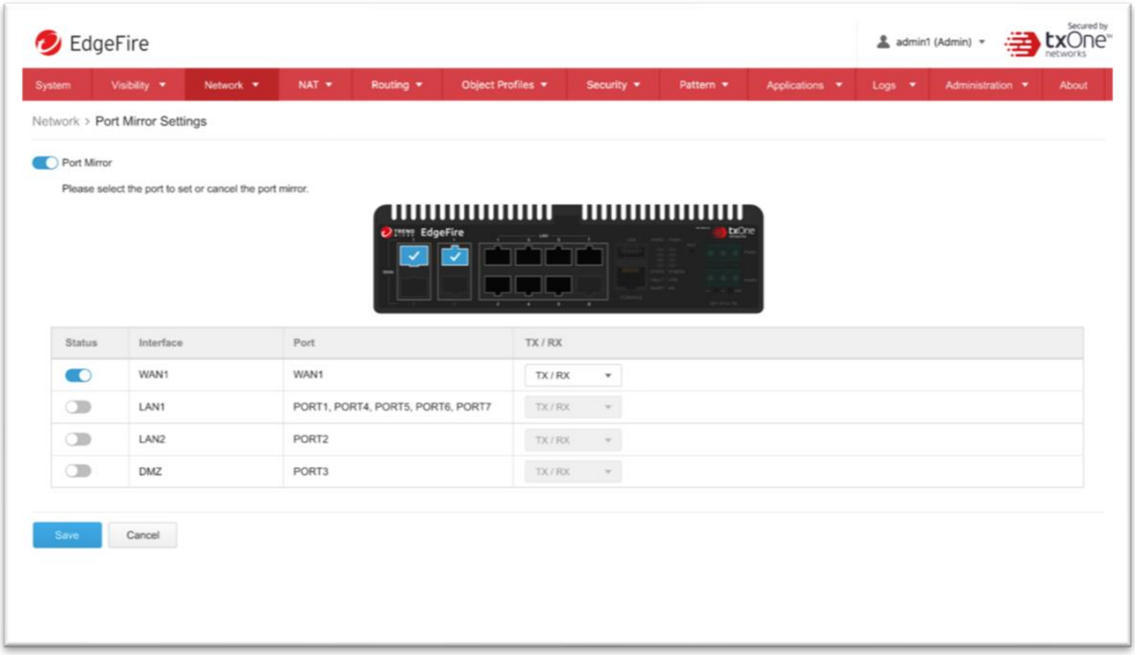
Shared Secret key	Shared secret key to allow for two HA peers to authenticate and communciate with each other
Heartbeat Interval	Interval between sent heartbeats – supported range of: 1-10 seconds
Failover Trigger Level	Failover retry time – supported range of 1-10 heartbeats: Maximum number of consecutive missed hearbeats before secondary to primary switch is triggered

Port Mirror Settings

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

Procedure

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



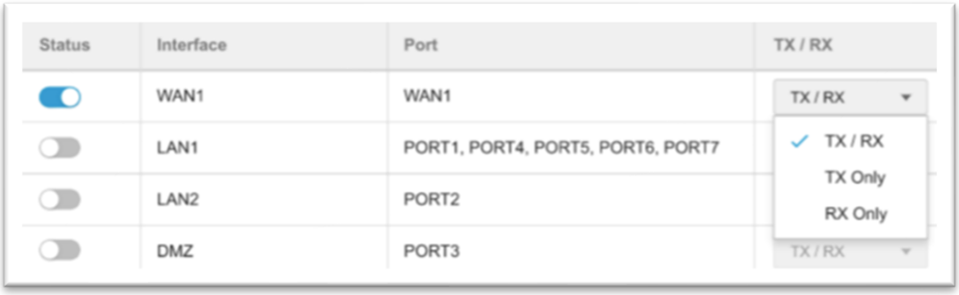
Network > Port Mirror Settings

● Port Mirror

Please select the port to set or cancel the port mirror.

Status	Interface	Port	TX / RX
●	WAN1	WAN1	TX / RX
○	LAN1	PORT1, PORT4, PORT5, PORT6, PORT7	TX / RX
○	LAN2	PORT2	TX / RX
○	DMZ	PORT3	TX / RX

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



Status	Interface	Port	TX / RX
●	WAN1	WAN1	TX / RX
○	LAN1	PORT1, PORT4, PORT5, PORT6, PORT7	
○	LAN2	PORT2	
○	DMZ	PORT3	TX / RX

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

Operation Mode

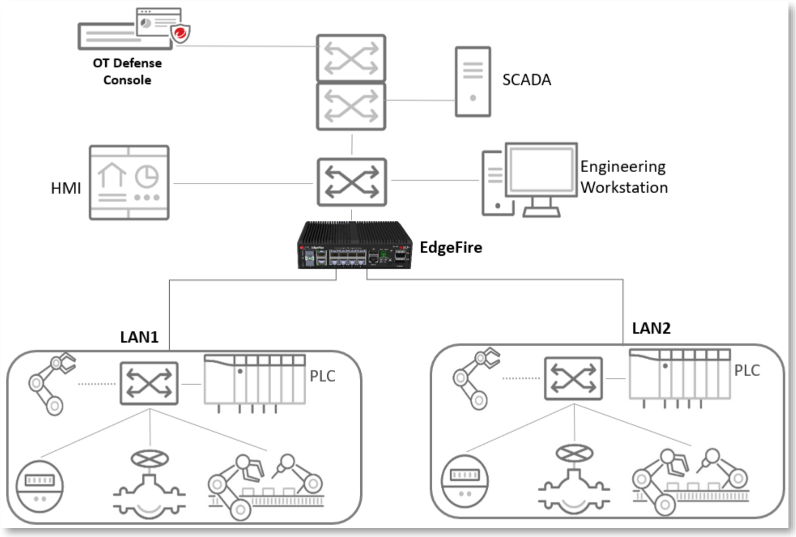
EdgeFire™ offers two system operation modes:

- **Gateway Mode**
- **Bridge Mode**

The following sections describe these two modes in detail.

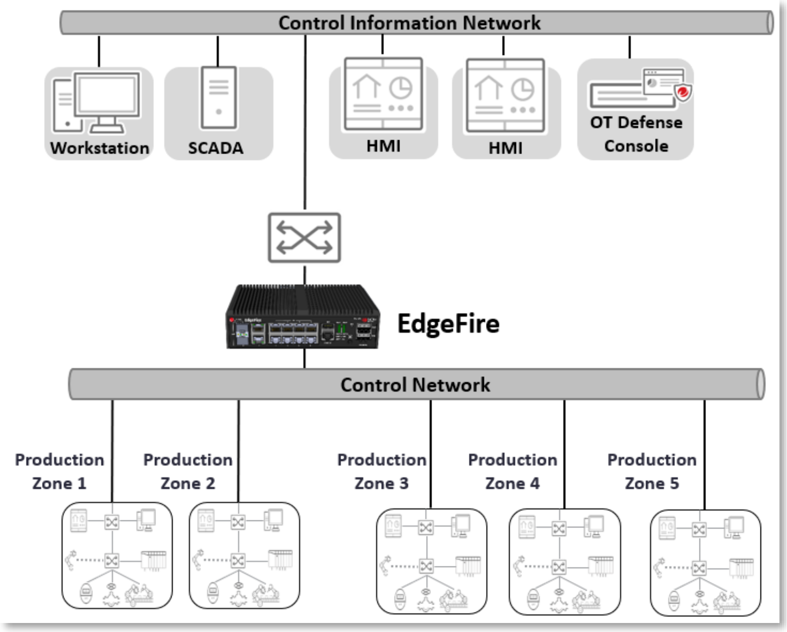
Gateway Mode

EdgeFire™ operates as a gateway with NAT and routing main features between multiple different network segments, actively analyzing, filtering, and taking actions on all traffic that passes through it.



Bridge Mode

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



Use the [Operation Mode] tab to configure or view the following:

- Select Gateway mode or Bridge mode of the device
- Enable or disable LLDP (Link Layer Discovery Protocol) settings

Switch to Gateway Mode

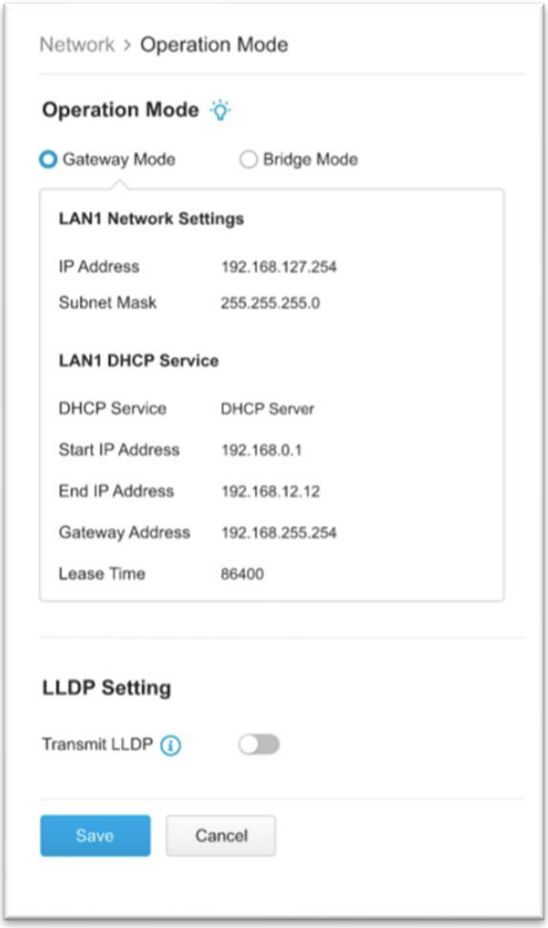
Procedure

1. Go to [Network] > [Operation Mode].

   The [Operation Mode] tab will appear.

2. Click the radio button [Gateway Mode].

   The [LAN1 Network Settings and LAN1 DHCP Service] pane for the gateway mode will appear.



Network > Operation Mode

Operation Mode

● Gateway Mode ○ Bridge Mode

LAN1 Network Settings

IP Address	192.168.127.254
Subnet Mask	255.255.255.0

LAN1 DHCP Service

DHCP Service	DHCP Server
Start IP Address	192.168.0.1
End IP Address	192.168.12.12
Gateway Address	192.168.255.254
Lease Time	86400

LLDP Setting

Transmit LLDP ⓘ

3. In the [LAN1 Network Settings] section, configure the network settings for gateway mode:
   a. Input an IP address.
   b. Input a subnet mask.

4. In the [LAN1 DHCP Service Settings] section, configure the network settings for gateway mode:
   a. Showing the status of DHCP service.

b. Input a start IP address.

c. Input an end IP address.

d. Input a gateway address.

e. Input the lease time (86400 seconds by default).

5. Click [Save] to save the settings.

> **Note:** In bridge mode, the LAN1 network settings / LAN1 DHCP Service for Gateway mode is for viewing only.
>
> **Note:** The configuration of the policy enforcement rule is not compatible between Gateway mode and Bridge mode. Therefore, the policy enforcement rule needs to be reconfigured after switching from Bridge mode to Gateway mode.

Switch to Bridge Mode

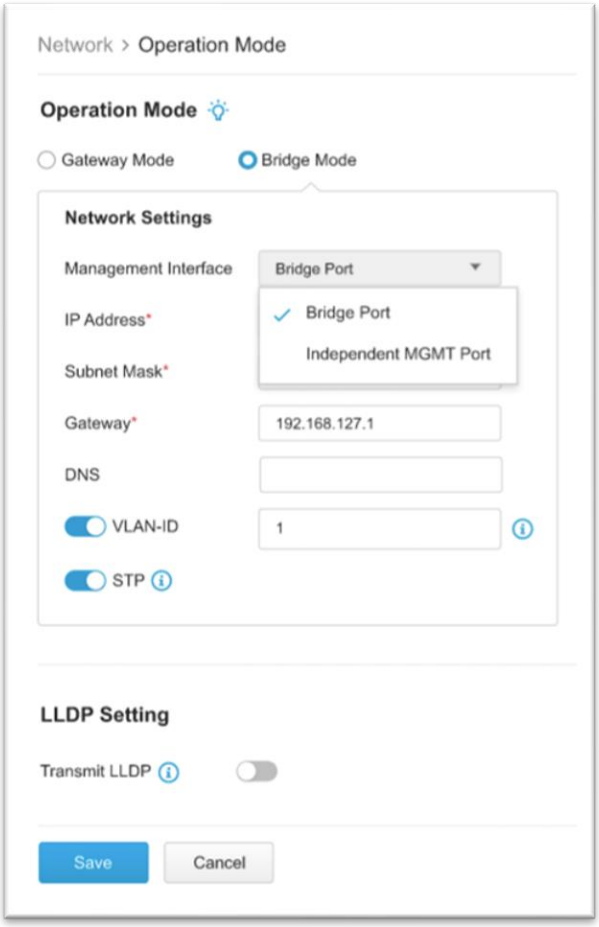
Procedure

1. Go to [Network] > [Operation Mode].

   The [Operation Mode] tab will appear.

2. Click the radio button [Bridge Mode].

   The [Network Settings] section for bridge mode will appear.



Network > Operation Mode

Operation Mode

○ Gateway Mode ● Bridge Mode

Network Settings

Management Interface: Bridge Port

✓ Bridge Port

Independent MGMT Port

IP Address*

Subnet Mask*

Gateway*: 192.168.127.1

DNS:

● VLAN-ID: 1

● STP

LLDP Setting

Transmit LLDP ○

3. In the [Network Settings] section, configure the network settings for bridge mode:
   f. Select a management interface: Bridge Port or Independent MGMT Port.
   g. Input an IP address.
   h. Input a subnet mask.
   i. Input a gateway address.
   j. Input a DNS address.
   k. (Optional) Use the toggle to enable or disable VLAN ID. If VNLAN ID is enabled, input the VLAN ID.
   l. (Optional) Use the toggle to enable or disable STP (Spanning Tree Protocol).
   m. Click [Save] to save the settings.

4. Click [Save] to save the settings.

Note: When EdgeFire™ is switched from gateway mode to Bridge mode, the features of Port Mapping, Network Interface, NAT Rules, ALG, and Static Route will not operate and not be configurable.

Note: The configuration of the policy enforcement rule is not compatible between Gateway mode and Bridge mode. Therefore, the policy enforcement rule needs to be reconfigured after switching from Gateway mode to Bridge mode.

The NAT Tab

Use the NAT (Network Address Translation) tab to view and configure NAT rules, and enable or disable application layer gateways.

NAT Rule

Use the NAT tab to configure the following:

- 1 to 1 network address translation for the incoming traffic on the specific interface
- Multiple 1 to 1 network address translation for the incoming traffic on the specific interface (CIDR, Classless Inter-Domain Routing)
- Multiple 1 to 1 network address translation for the incoming traffic on the specific interface (IP range)
- Port forwarding address translation for the incoming traffic on the specific interface

The following table describes the tasks you can perform on the [NAT Rule] tab.

Task	Description
Add a NAT rule	Click [Add] to create a new NAT rule.
Edit a NAT rule	Click a NAT Rule Name to edit its settings.
Delete a NAT rule	Select one or more NAT rules and click [Delete].
Copy a NAT rule	Select one NAT rule and click [Copy].
Change Priority	Select one NAT rule and click [Change Priority].

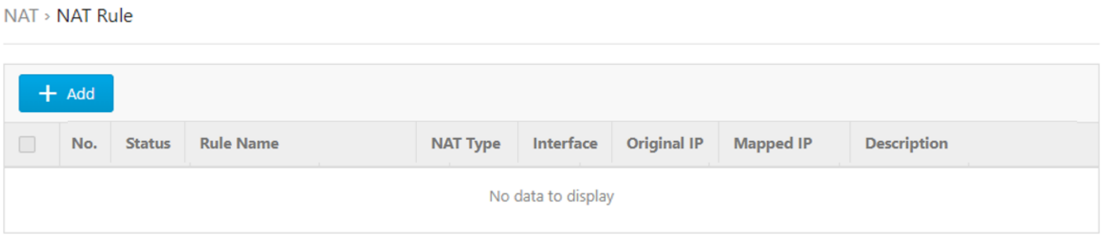
Configuring a 1 to 1 NAT Rule

A 1 to 1 NAT rule allows you to map a destination IP address in the incoming traffic to another IP address located in the specific network.

Procedure

1. Go to [NAT] > [NAT Rule].

   The [NAT] tab will appear.



NAT › NAT Rule

□	No.	Status	Rule Name	NAT Type	Interface	Original IP	Mapped IP	Description

No data to display

2. Do one of the following:
   - Click [Add] to create a NAT rule.
   - Click a NAT rule name to edit its settings.
3. Configuring a NAT rule:

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

b. Under the [NAT Type] drop-down menu, select [1 to 1 NAT].

c. Input a name for the rule.

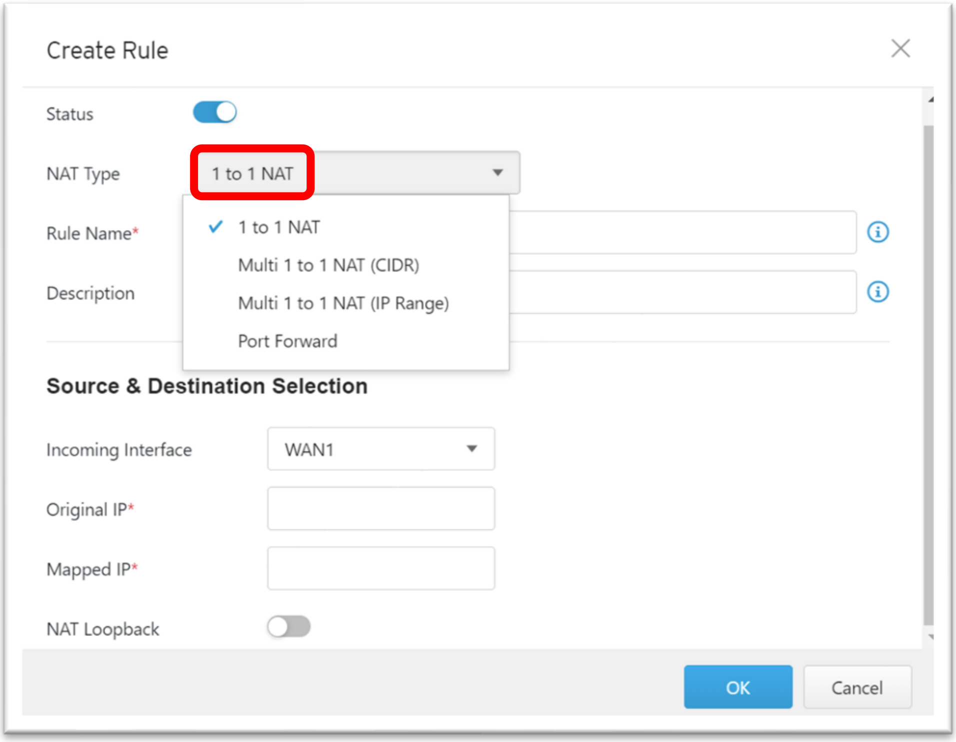
d. Input a description for the rule.

e. Under the [Incoming Interface] drop-down menu, select the interface that will process the incoming traffic for this rule.

f. In the [Original IP] field, input the destination IP address that will be translated. When the device receives an incoming packet going through the interface specified in the [Incoming Interface], the destination IP address in the packet that matches this [Original IP] field will be mapped another IP address.

g. In the [Mapped IP] field, input the IP address you will map to. This IP address is usually a private IP address in your local network.

h. (Optional) Use the toggle to enable NAT loopback.



Create Rule

Status

NAT Type: 1 to 1 NAT

Rule Name*

Description

Source & Destination Selection

Incoming Interface: WAN1

Original IP*

Mapped IP*

NAT Loopback

4. Click [OK] to accept the rule.

5. Click [Save] to save the settings.

Note: Starting from firmware 1.1, [Network Interface] now can support WAN1, LAN1, LAN2 and DMZ interface when [NAT Type] is selected to “1 to 1 NAT”.

Configuring a Multiple 1 to 1 NAT Rule: CIDR

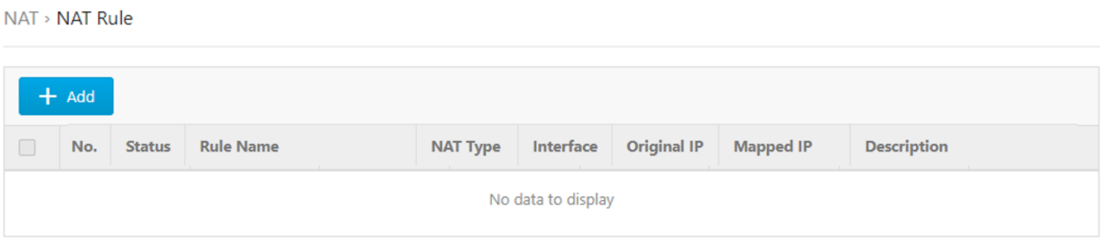
A multiple 1 to 1 NAT rule (CIDR) allows you to map the destination IP addresses in the incoming traffic to different IP addresses located in the specific network. The following table shows an example.

Original Destination IP Addresses	... Are Mapped to These Destination IP Addresses
172.1.1.5	192.168.100.5
172.1.1.20	192.168.100.20
172.1.1.50	192.168.100.50
172.1.1.69	192.168.100.69

Procedure

1. Go to [NAT] > [NAT Rule].

   The [NAT] tab will appear.



NAT › NAT Rule

+ Add

☐	No.	Status	Rule Name	NAT Type	Interface	Original IP	Mapped IP	Description

No data to display

2. Do one of the following:
   - Click [Add] to create a NAT rule.
   - Click a NAT rule name to edit its settings.
3. Configuring the NAT rule:
   a. Use the toggle to enable or disable the rule.

   b. Under the [NAT Type] drop-down menu, select [Multi 1 to 1 NAT (CIDR)].

   c. Input a name for the rule.

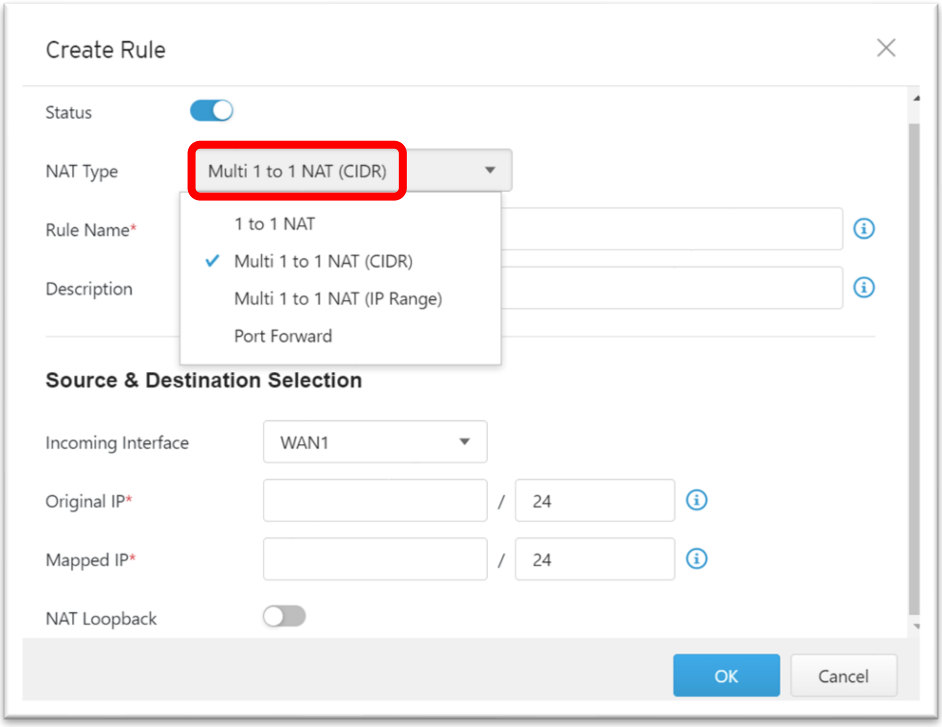
   d. Input a description for the rule.

   e. Under the [Incoming Interface] drop-down menu, select the interface that will process the incoming traffic for this rule.

   f. In the [Original IP] field, input with the CIDR (Classless Inter-Domain Routing) format to present the IP addresses that will be translated; for example, 172.1.1.0 / 24. When the device receives an incoming packet going through the interface specified in the [Incoming Interface], the destination IP address in the packet that matches this [Original IP] field will be mapped to another IP address. These IP addresses are usually the ones assigned by an ISP (Internet Service Provider).

   g. In the [Mapped IP] field, input with the CIDR (Classless Inter-Domain Routing) format to present the IP addresses that will be mapped to; for example, 192.168.100.0 / 24.

   h. (Optional) Use the toggle to enable NAT loopback.



Create Rule

Status: on

NAT Type: Multi 1 to 1 NAT (CIDR)

Rule Name*

Description

Source & Destination Selection

Incoming Interface: WAN1

Original IP* / 24

Mapped IP* / 24

NAT Loopback: off

4. Click [OK] to accept the rule.
5. Click [Save] to save the settings.

Note: Starting from firmware 1.1, [Network Interface] now can support WAN1, LAN1, LAN2 and DMZ interface when [NAT Type] is selected to “Multi 1 to 1 NAT”.

Configuring a Multiple 1 to 1 NAT Rule: IP Range

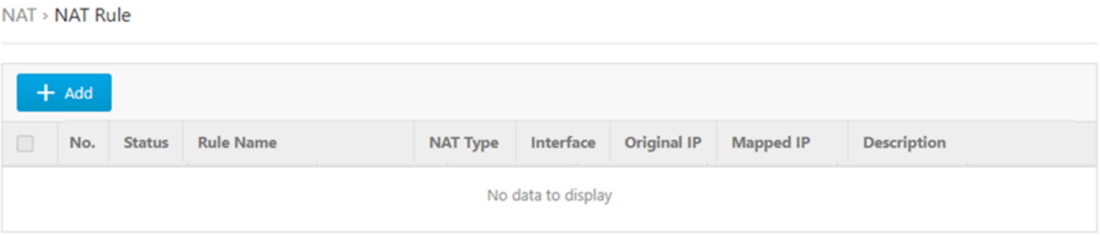
A multiple 1 to 1 NAT rule (IP range) allows you to map the destination IP addresses in the incoming traffic to different IP addresses located in the specific network. The following table shows an example.

Original Destination IP Addresses	... Are Mapped to These Destination IP Addresses
172.1.1.5	192.168.100.5
172.1.1.20	192.168.100.20
172.1.1.50	192.168.100.50
172.1.1.69	192.168.100.69

Procedure

1. Go to [NAT] > [NAT Rule].

   The [NAT] tab will appear.

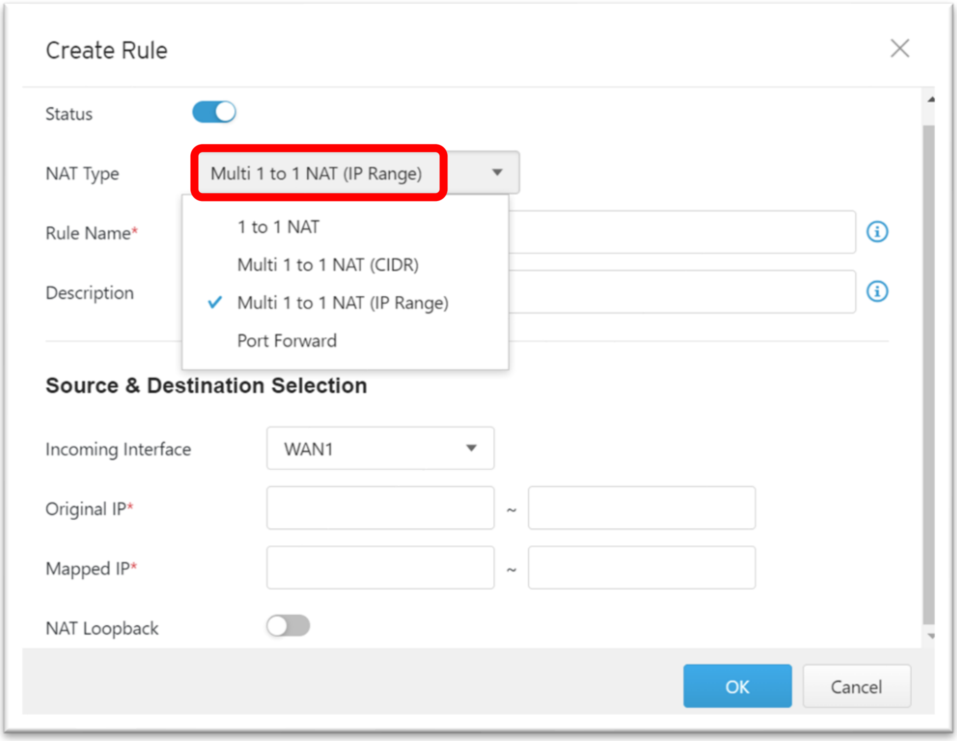


NAT › NAT Rule

□	No.	Status	Rule Name	NAT Type	Interface	Original IP	Mapped IP	Description

No data to display

2. Do one of the following:
   - Click [Add] to create a NAT rule.
   - Click a NAT rule name to edit its settings.
3. Configuring the NAT rule:
   a. Use the toggle to enable or disable the rule.
   b. Under the [NAT Type] drop-down menu, select [Multi 1 to 1 NAT (IP Range)].
   c. Input a name for the rule.
   d. Input a description for the rule.
   e. Under the [Incoming Interface] drop-down menu, select the interface that will process the incoming traffic for this rule.
   f. In the [Original IP] field, input with the IP Range format to present the IP addresses that will be translated; for example, 172.1.1.0 / 24. When the device receives an incoming packet going through the interface specified in the [Incoming Interface], the destination IP address in the packet that matches this [Original IP] field will be mapped to another IP address. These IP addresses are usually the ones assigned by an ISP (Internet Service Provider).
   g. In the [Mapped IP] field, input with the IP Range format to present the IP addresses that will be mapped to; for example, 192.168.100.0 / 24.
   h. (Optional) Use the toggle to enable NAT loopback.



Create Rule

Status ●

NAT Type: Multi 1 to 1 NAT (IP Range)

Rule Name*

Description

Source & Destination Selection

Incoming Interface: WAN1

Original IP* ~

Mapped IP* ~

NAT Loopback ○

4. Click [OK] to accept the rule.

5. Click [Save] to save the settings.

Note: Starting from firmware 1.1, [Network Interface] now can support WAN1, LAN1, LAN2 and DMZ interface when [NAT Type] is selected to “Multi 1 to 1 NAT”.

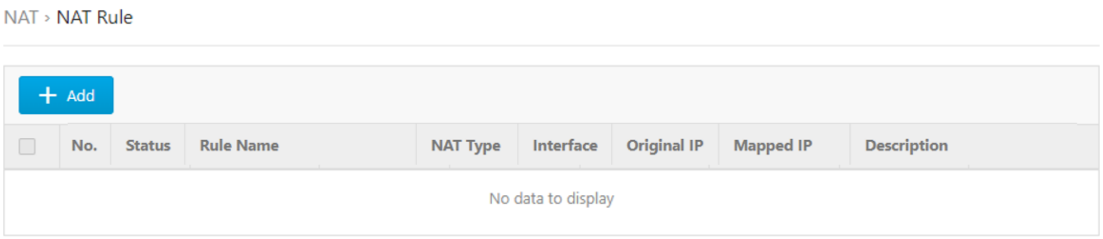
Configuring Port Forwarding

A port forwarding rule allows you to map a host IP address in the incoming traffic to another IP address located in your local network.

Procedure

1. Go to [NAT] > [NAT Rule].

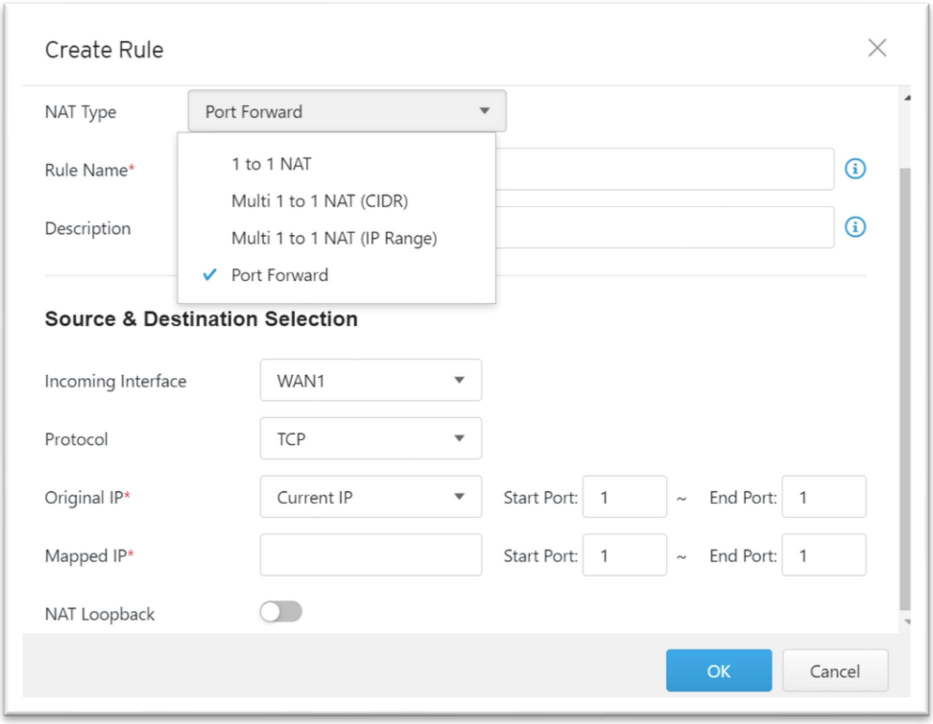
   The [NAT] tab will appear.



NAT › NAT Rule

☐	No.	Status	Rule Name	NAT Type	Interface	Original IP	Mapped IP	Description
No data to display								

2. Do one of the following:
   - Click [Add] to create a NAT rule.
   - Click a NAT rule name to edit its settings.
3. Configuring a NAT rule:
   a. Use the toggle to enable or disable the rule.
   b. Under the [NAT Type] drop down menu, select [Port Forward].
   c. Input a descriptive name for the rule.
   d. Input a description for the rule.
   e. Under the [Incoming Interface] drop-down menu, select the interface that will process the incoming traffic for this rule.
   f. Under the [Protocol] drop-down menu, select the protocol that will process the incoming traffic for this rule.
   g. In the [Original IP] field, input the start port and the end port that will be translated. When the device receives an incoming packet going through the interface specified in the [Incoming Interface], the destination IP address in the packet that matches this [Original IP] field will be mapped another IP and port address.
   h. In the [Mapped IP] field, input the IP address and port range you will map to. This IP address is usually a private IP address in your local network.
   i. (Optional) Use the toggle to enable NAT loopback.



Create Rule

NAT Type: Port Forward

1 to 1 NAT
Multi 1 to 1 NAT (CIDR)
Multi 1 to 1 NAT (IP Range)
✓ Port Forward

Rule Name*

Description

Source & Destination Selection

Incoming Interface: WAN1

Protocol: TCP

Original IP*: Current IP Start Port: 1 ~ End Port: 1

Mapped IP*: Start Port: 1 ~ End Port: 1

NAT Loopback

4. Click [OK] to accept the rule.
5. Click [Save] to save the settings.

ALG

An ALG or Application Layer Gateway allows the client applications to communicate with the server applications when the server ports are dynamically opened to client applications. These ports are usually dynamically assigned in the application protocol. An ALG understands application protocols, recognizes application specific commands, and helps open the ports dynamically on the device for communication. Without ALG, client applications like FTP would not be able to transfer files when the FTP client is in an NAT network.

Use the ALG (Application Layer Gateway) tab to configure the following:

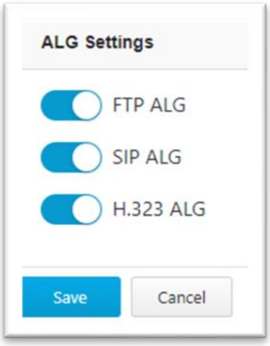
- FTP ALG
- SIP ALG
- H.323 ALG

Configuring ALG Settings

Procedure

1. Go to [NAT] > [ALG].

   The [ALG Settings] tab will appear.
2. Use the toggle to enable or disable FTP, SIP and H.323 ALG.
3. Click [Save].



ALG Settings

FTP ALG

SIP ALG

H.323 ALG

The Routing Tab

Use the [Routing] tab to view and configure static routes on the device.

Static Route

Static routes are generally used when no appropriate dynamic route is present, or when you want the traffic to follow the static route you specify as opposed to following the dynamic route that is automatically learned and generated by the device.

Use the [Static Route] tab to view a list of current static routes on the device and configure their settings.

The following table describes the tasks you can perform on the [Static Route] tab.

Task	Description
Add a static route	Click [Add] to create a new static route.
Edit a static route	Click a static route name to edit the rule settings.
Delete a static route	Select one or more static routes and click [Delete].
Copy a static route	Select one static route and click [Copy].

Configuring a Static Route

Procedure

1. Go to [Routing] > [Static Route].
2. Do one of the following:
   - Click [Add] to create a static route.
   - Click a static route name to edit settings.
3. Configuring the static route:
   a. Use the toggle to enable or disable the route.
   b. Input a name for the rule.
   c. Input a description for the rule.
   d. Configure the destination:
   - In the [Destination Address] field, input IP address.
   - In the [Subnet Mask] field, input the subnet mask.

Tip: If the destination is a single IP address, then input 255.255.255.255 in the [Subnet Mask] field. If the destination is a subnet of IP addresses, then input, for example, 255.255.255.0, in the [Subnet Mask] to present the destination IP address range.

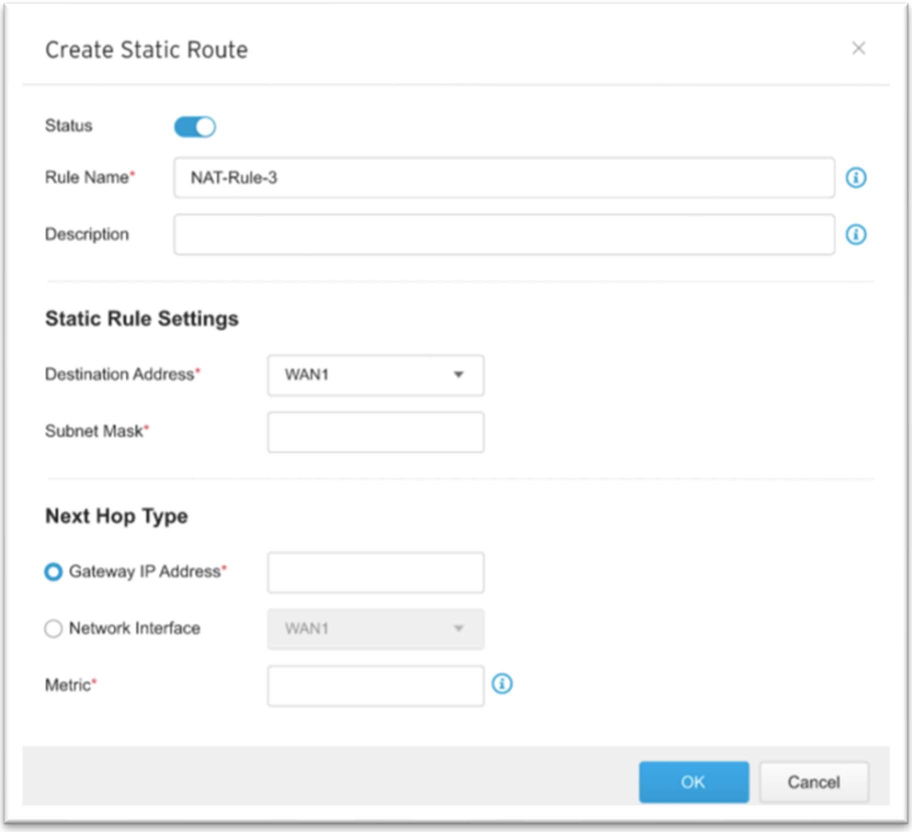
   e. Configure the next hop:
   - If the next hop is a gateway, then under [Next Hop Type], select [Gateway IP Address] and input the IP address. The gateway needs to be on the same network as the interface.
   - If the next hop is a network interface on the device, then under [Next Hop Type], select [Network Interface], and select a network interface from the drop-down menu. [Note]

For this firmware of the device, the available network interface to be selected is fixed to [WAN 1].

Tip: For more information about the network interface, see *Network Interface on page 22*.

f. Input the metric value:

- In the [Metric] field, input a metric value for this static route. The device determines which static route to use based on the metric value, with the lower number representing higher priority.



Create Static Route

Status: ●

Rule Name*: NAT-Rule-3

Description:

Static Rule Settings

Destination Address*: WAN1

Subnet Mask*:

Next Hop Type

● Gateway IP Address*:

○ Network Interface: WAN1

Metric*:

g. Click [OK] to accept the settings.

h. Click [Save] to save the rule.

The Object Profiles Tab

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

You can configure the following types of object profiles in 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 profiles or edit profiles to apply on a policy rule. Details of ICS (Industrial Control System) protocols are defined here.
- **File Filter Profiles**: Contains the settings of file filter profiles that you can apply on a policy rule. Details of file filter by protocol are defined here.

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

- **Device Profiles**: Contains the IP Object(s), Service Object(s), Protocol Filter Profile(s), IPS Profile(s) and File Filter Profile(s) that users with local account privileges for EdgeFire™ can apply to a policy rule.

- **Master Profiles**: Contains the IP Object(s), Service Object(s), Protocol Filter Profile(s), IPS Profile(s), and File Filter Profile(s) synced from ODC that users with local account privilege in ODC can apply to a policy rule. Users with local account privilege for EdgeFire™ can only view and copy profiles(s) from Master Profiles(s) to Device Profiles.

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

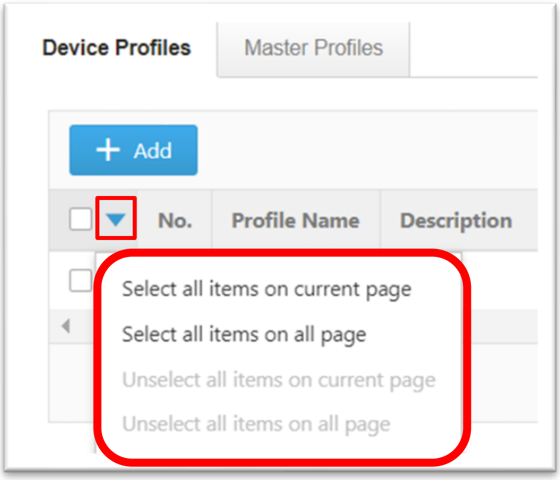
- **Device Profiles:**

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

- **Master Profiles:**

Task	Description
Copy a profile	Select one or more profiles and click [Copy Master Profiles to Device Profiles].

Click the down arrow icon next to the checkbox and the drop-down menu to select the profile(s) will be shown:


Device Profiles
Master Profiles
+ Add
No.
Profile Name
Description
Select all items on current page
Select all items on all page
Unselect all items on current page
Unselect all items on all page

Configuring IP Object Profiles

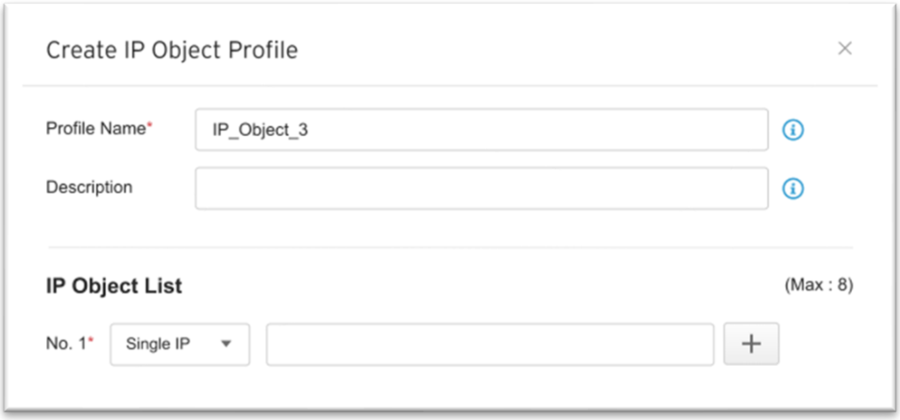
You can configure the IP address in an IP object profile, which can be used by other policy rules.

The types of IP address you can assign are:

- Single IP
- IP range
- IP subnet

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*: IP_Object_3

Description:

IP Object List (Max : 8)

No. 1*: Single IP

3. Type a name for the IP Object Profile.
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

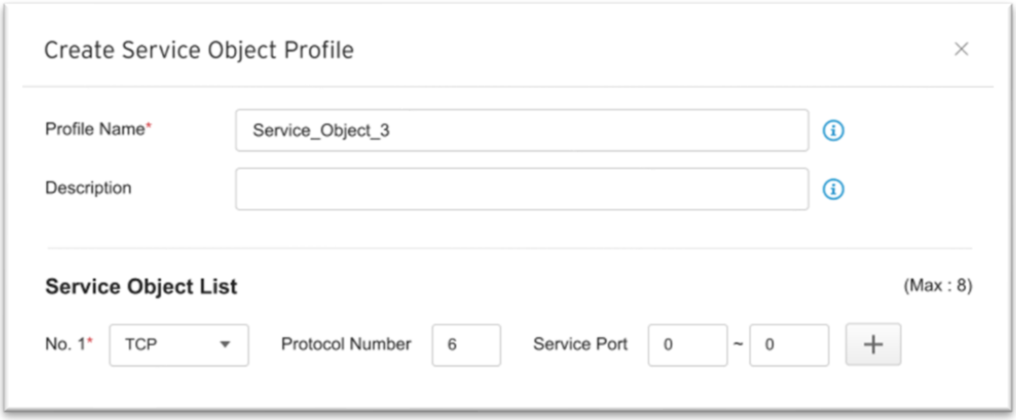
In a service object profile, you can define the following:

- TCP protocol port range
- UDP protocol port range
- ICMP protocol type and code
- Custom protocol with the specified protocol number

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*: Service_Object_3

Description:

Service Object List (Max : 8)

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

3. Type a 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 the specified protocol number

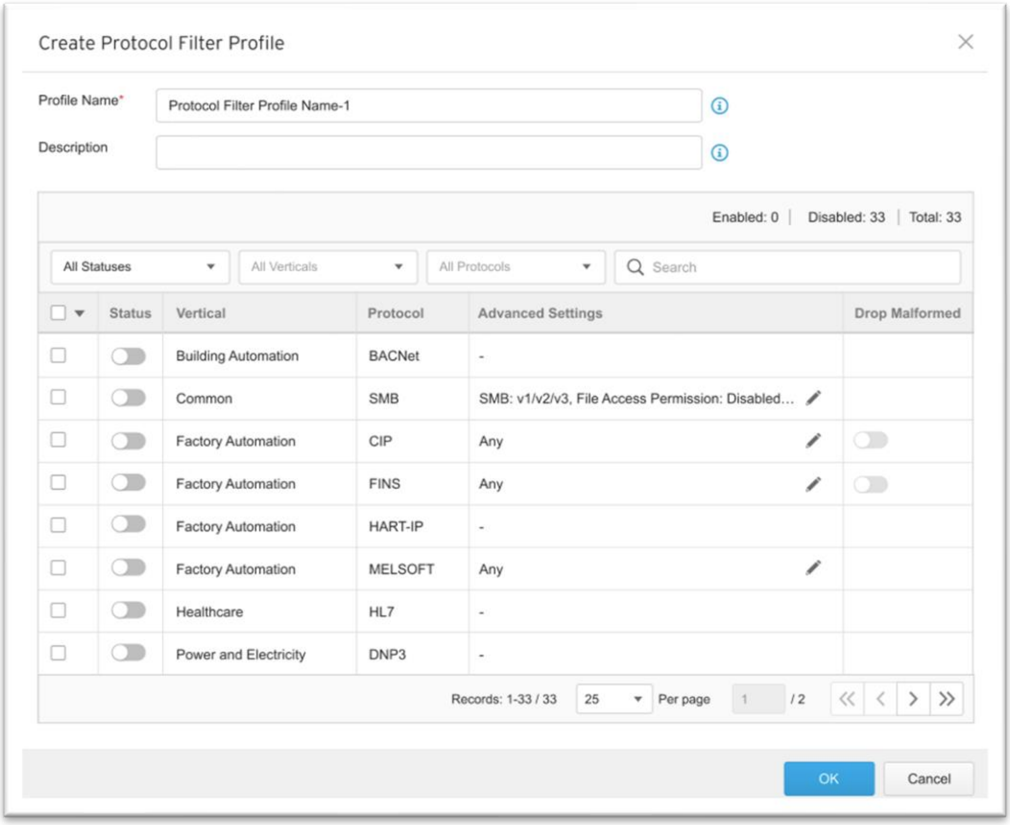
    3. If you want to add another entry, click the + button.
    4. Click [OK].

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
    - BACnet
- HealthCare
    - DICOM
    - HL7
- Power and Electricity
    - DNP3
    - IEC104
    - IEC61850-MMS
- General Protocol, including:
    - HTTP
    - FTP
    - SMB
    - RDP
    - MQTT
    - MSRPC
    - SIP
    - SMTP
    - SNMP
    - SSH
    - TELNET
    - TFTP
    - VNC
    - DNS



Create Protocol Filter Profile

Profile Name*: Protocol Filter Profile Name-1

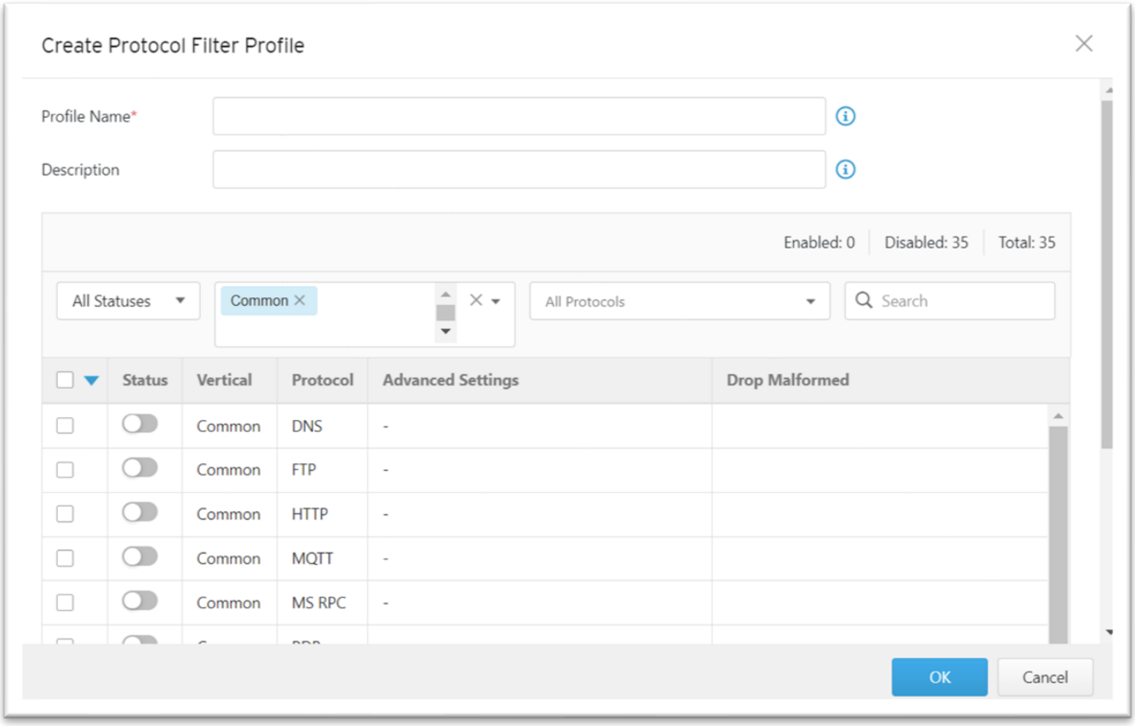
Description:

Enabled: 0 | Disabled: 33 | Total: 33

All Statuses | All Verticals | All Protocols | Search

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	○	Building Automation	BACNet	-	
□	○	Common	SMB	SMB: v1/v2/v3, File Access Permission: Disabled… ✎	
□	○	Factory Automation	CIP	Any ✎	○
□	○	Factory Automation	FINS	Any ✎	○
□	○	Factory Automation	HART-IP	-	
□	○	Factory Automation	MELSOFT	Any ✎	
□	○	Healthcare	HL7	-	
□	○	Power and Electricity	DNP3	-	

Records: 1-33 / 33 | 25 Per page | 1 / 2



Create Protocol Filter Profile

Profile Name*:

Description:

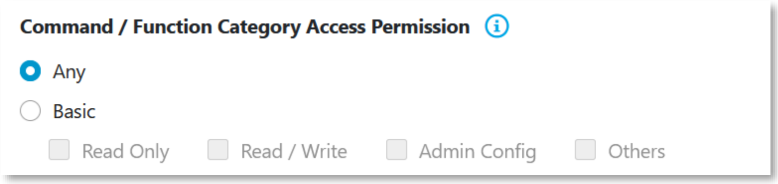
Enabled: 0 | Disabled: 35 | Total: 35

All Statuses | Common × | All Protocols | Search

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	○	Common	DNS	-	
□	○	Common	FTP	-	
□	○	Common	HTTP	-	
□	○	Common	MQTT	-	
□	○	Common	MS RPC	-	

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.



Command / Function Category Access Permission ⓘ

● Any

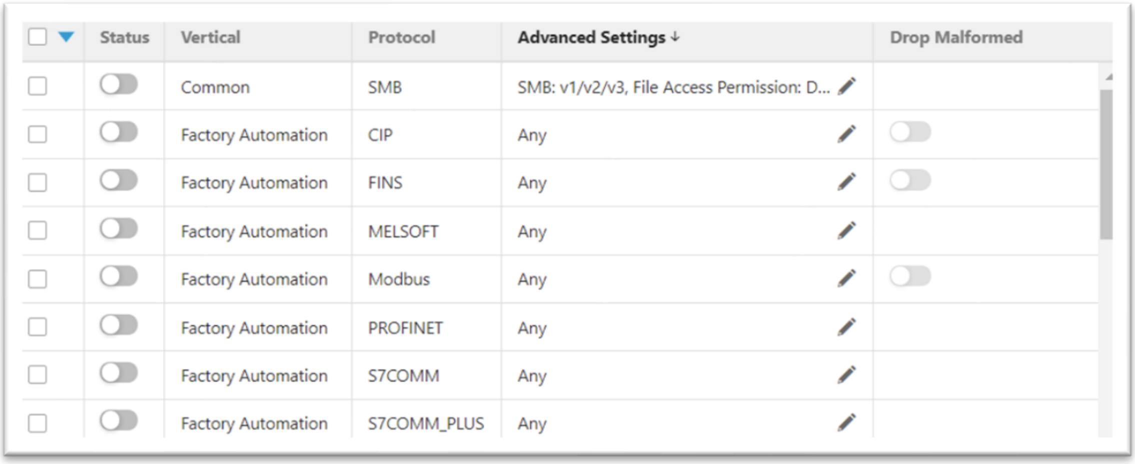
○ Basic

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

Applying the Drop Malformed Option to an ICS Protocol

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

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



□	Status	Vertical	Protocol	Advanced Settings ↓	Drop Malformed
□	○	Common	SMB	SMB: v1/v2/v3, File Access Permission: D... ✎	
□	○	Factory Automation	CIP	Any ✎	○
□	○	Factory Automation	FINS	Any ✎	○
□	○	Factory Automation	MELSOFT	Any ✎	
□	○	Factory Automation	Modbus	Any ✎	○
□	○	Factory Automation	PROFINET	Any ✎	
□	○	Factory Automation	S7COMM	Any ✎	
□	○	Factory Automation	S7COMM_PLUS	Any ✎	

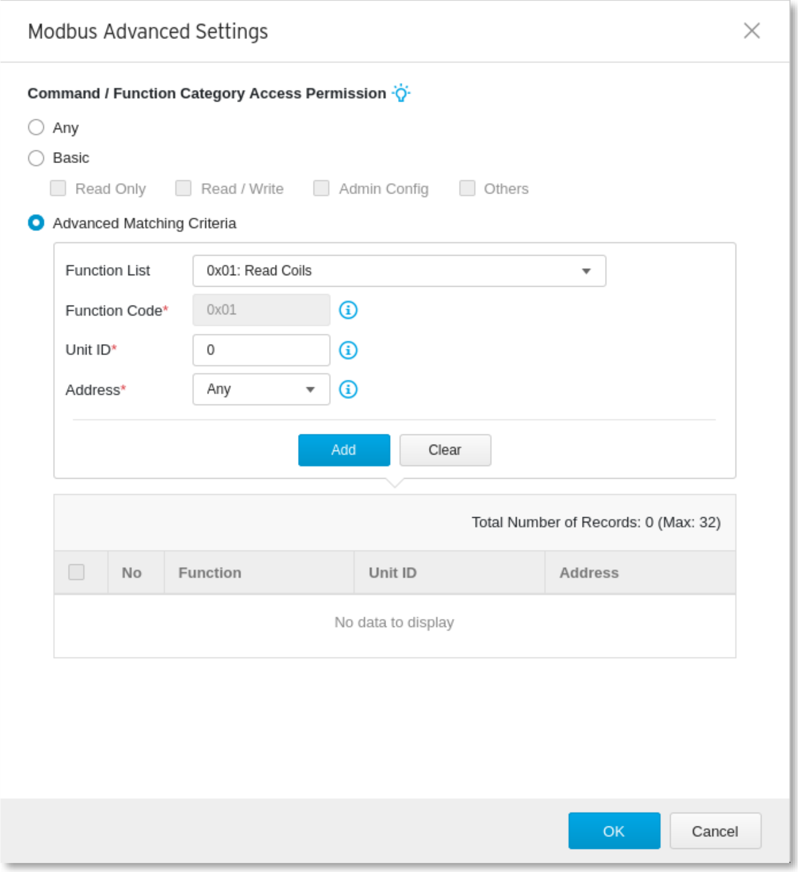
Note: In firmware 1.1, Drop Malformed supports 4 protocols (Modbus, CIP, OMRON FINS and TOYOPUC)

Advanced Settings

Below is a list of advanced settings for OT protocols supported by EdgeFire™.

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

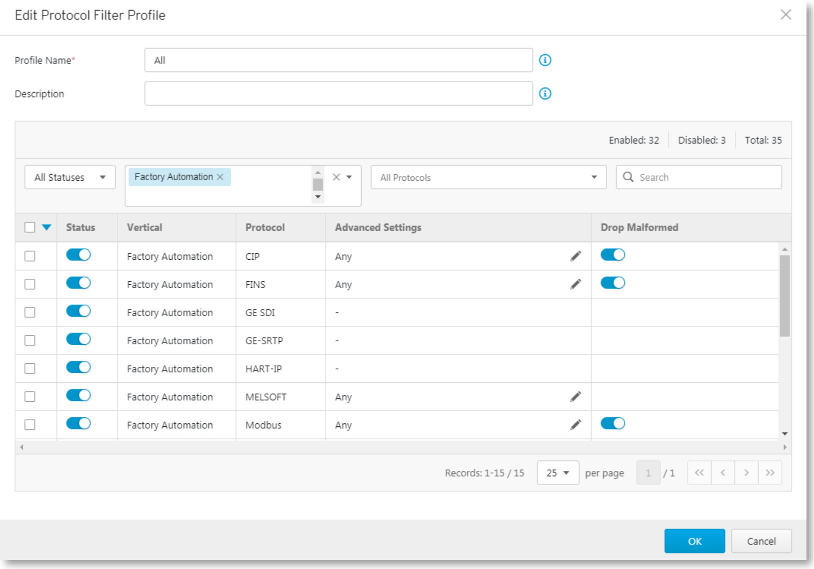
Total Number of Records: 0 (Max: 32)

□	No	Function	Unit ID	Address

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.



Edit Protocol Filter Profile

Profile Name*	All
Description	

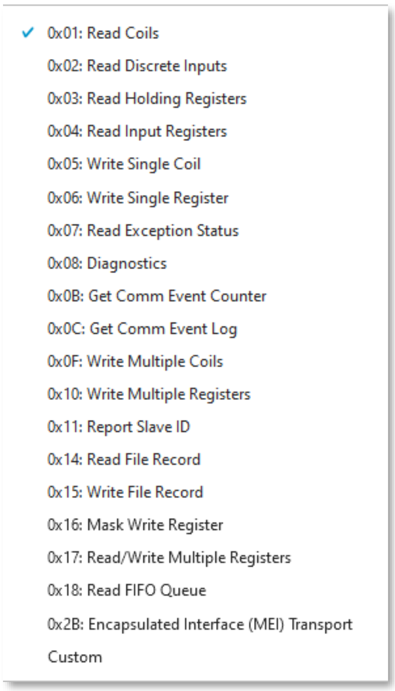
Enabled: 32 | Disabled: 3 | Total: 35

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any	●
□	●	Factory Automation	FINS	Any	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any	
□	●	Factory Automation	Modbus	Any	●

Records: 1-15 / 15 25 per page 1 / 1

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

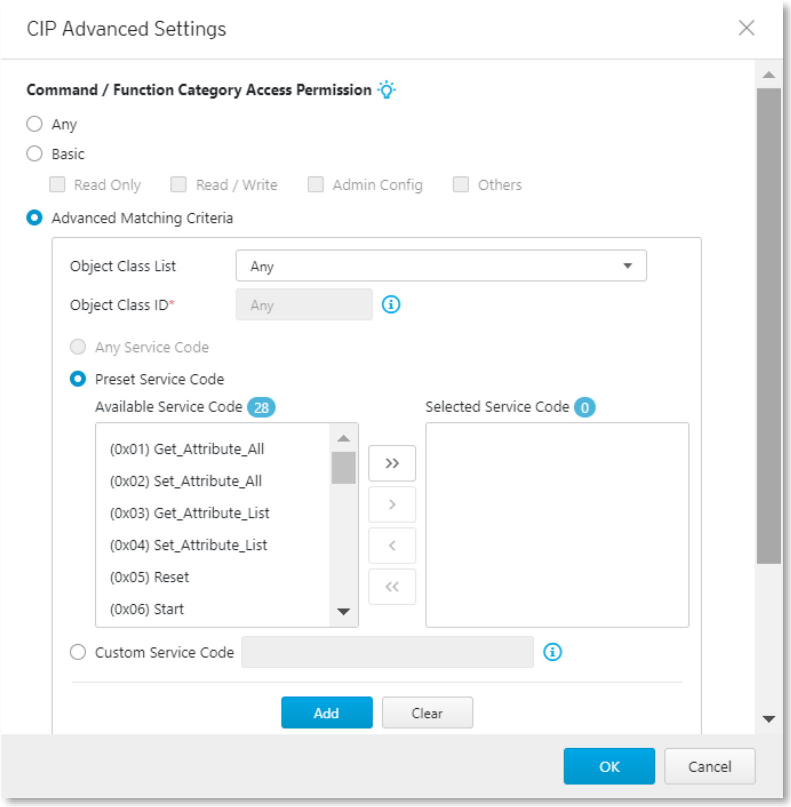

✓ 0x01: Read Coils
0x02: Read Discrete Inputs
0x03: Read Holding Registers
0x04: Read Input Registers
0x05: Write Single Coil
0x06: Write Single Register
0x07: Read Exception Status
0x08: Diagnostics
0x0B: Get Comm Event Counter
0x0C: Get Comm Event Log
0x0F: Write Multiple Coils
0x10: Write Multiple 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. Click [OK].

Advanced Settings for CIP Protocol

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



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

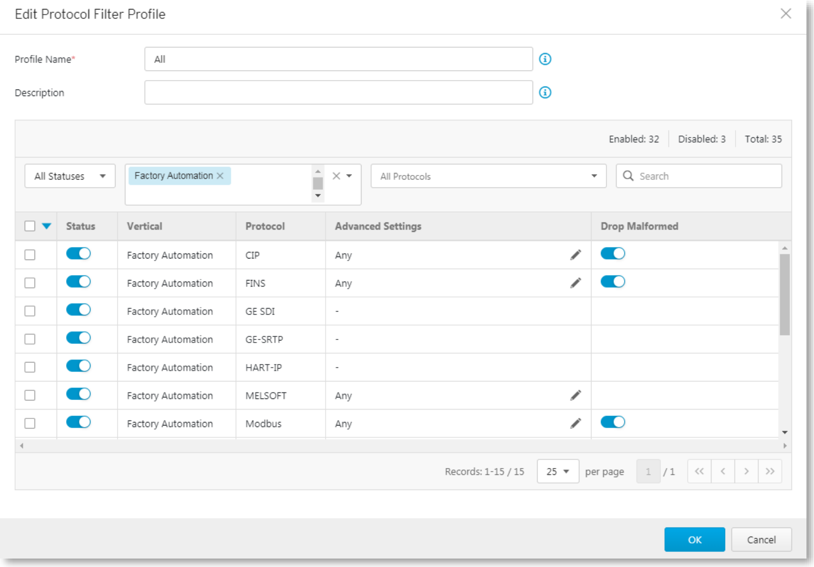
Available Service Code 28
(0x01) Get_Attribute_All
(0x02) Set_Attribute_All
(0x03) Get_Attribute_List
(0x04) Set_Attribute_List
(0x05) Reset
(0x06) Start

Selected Service Code 0

○ Custom Service Code

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.



Edit Protocol Filter Profile

Profile Name*: All

Description:

Enabled: 32 | Disabled: 3 | Total: 35

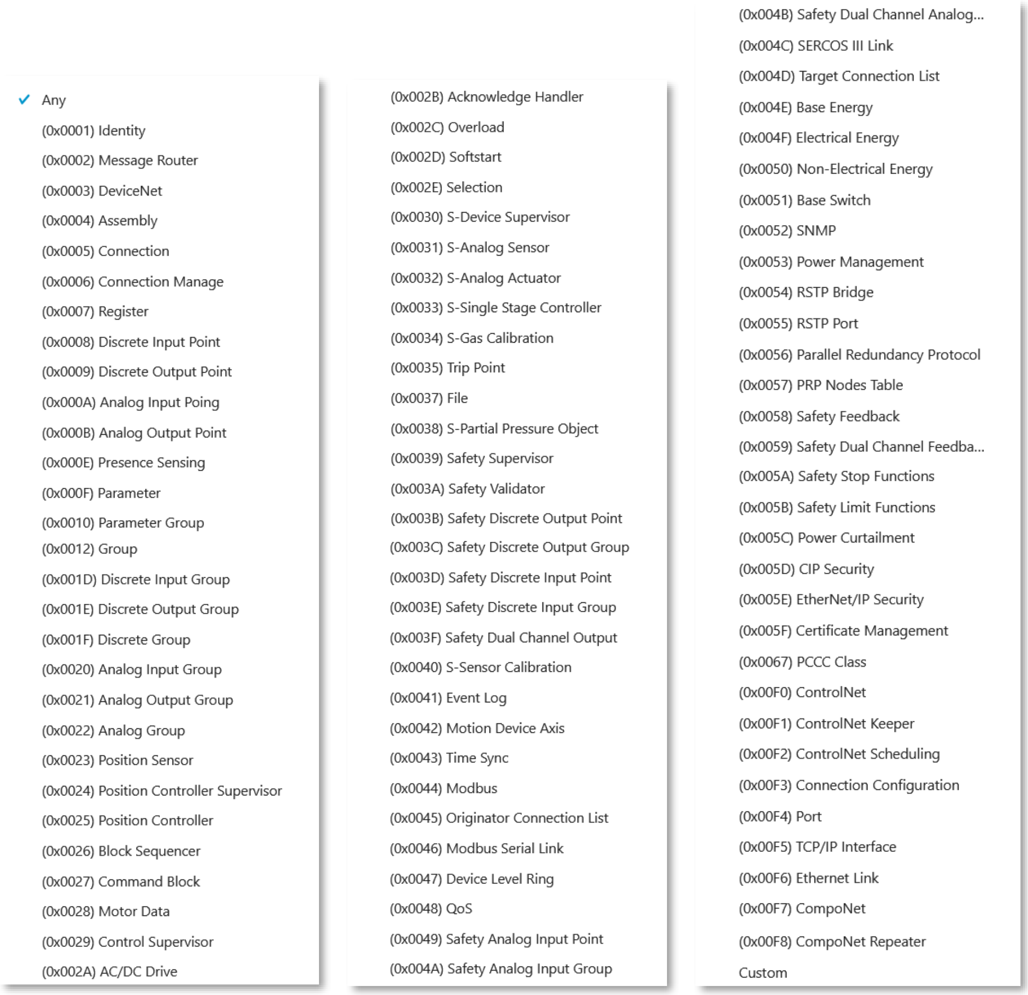
All Statuses | Factory Automation | All Protocols | Search

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any ✎	●
□	●	Factory Automation	FINS	Any ✎	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any ✎	
□	●	Factory Automation	Modbus	Any ✎	●

Records: 1-15 / 15 | 25 per page | 1 / 1

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 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.
    - 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].
- At the [Object Class List] drop down menu, select a function of this protocol.



✓ 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

(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

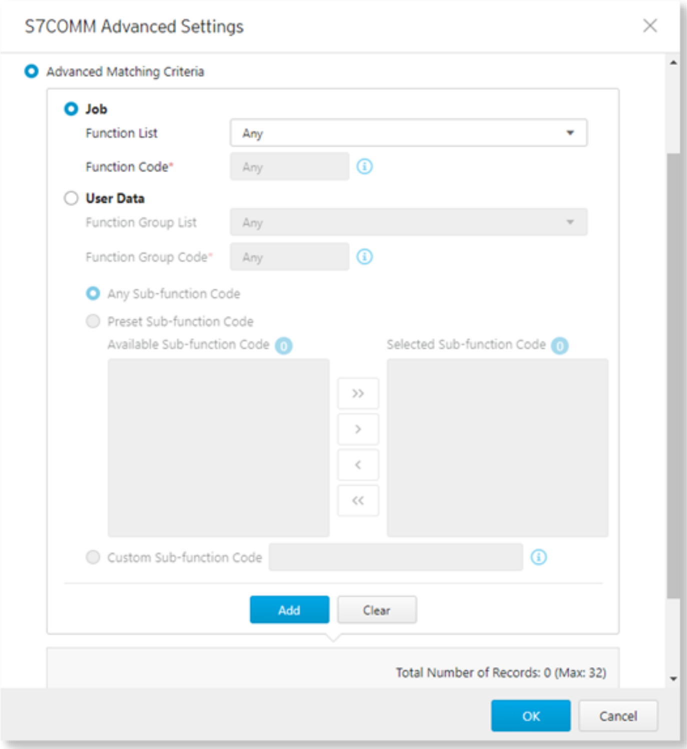
(0x004B) Safety Dual Channel Analog...
(0x004C) SERCOS III Link
(0x004D) Target Connection List
(0x004E) Base Energy
(0x004F) Electrical Energy
(0x0050) Non-Electrical Energy
(0x0051) Base Switch
(0x0052) SNMP
(0x0053) Power Management
(0x0054) RSTP Bridge
(0x0055) RSTP Port
(0x0056) Parallel Redundancy 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 to all the service codes within the function you specified to be applied, then select [Any Service Code]
- If you want to specify one service code or multiple service codes, then select [Preset Service Code] and move the service code(s) from the [Available Service Code] field to the [Selected Service Code] field.
- If you want to specify a service code by yourself, then select [Custom Service Code] and input a service code in the [Custom Service Code] field.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

Advanced Settings for S7COMM

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



S7COMM Advanced Settings

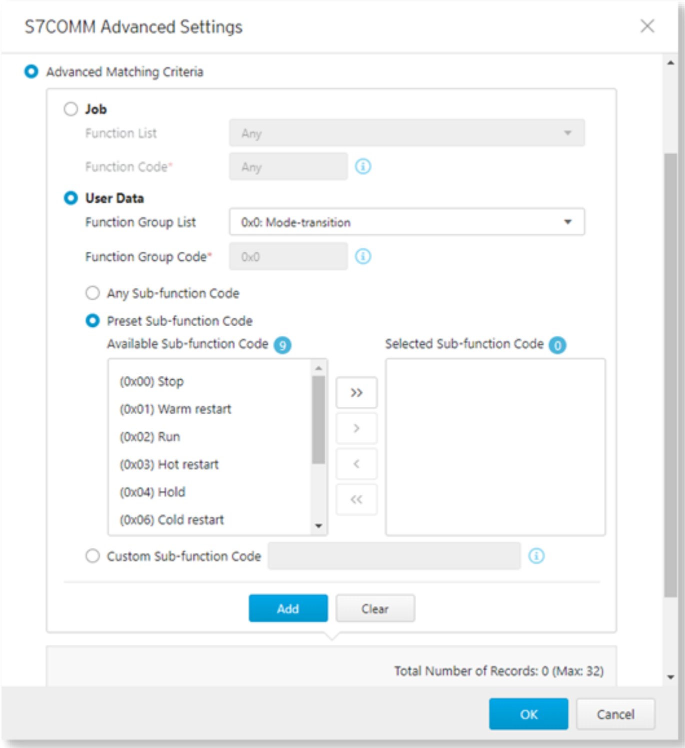
● Advanced Matching Criteria

● 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

Total Number of Records: 0 (Max: 32)



S7COMM Advanced Settings

● Advanced Matching Criteria

○ Job
Function List: Any
Function Code*: Any

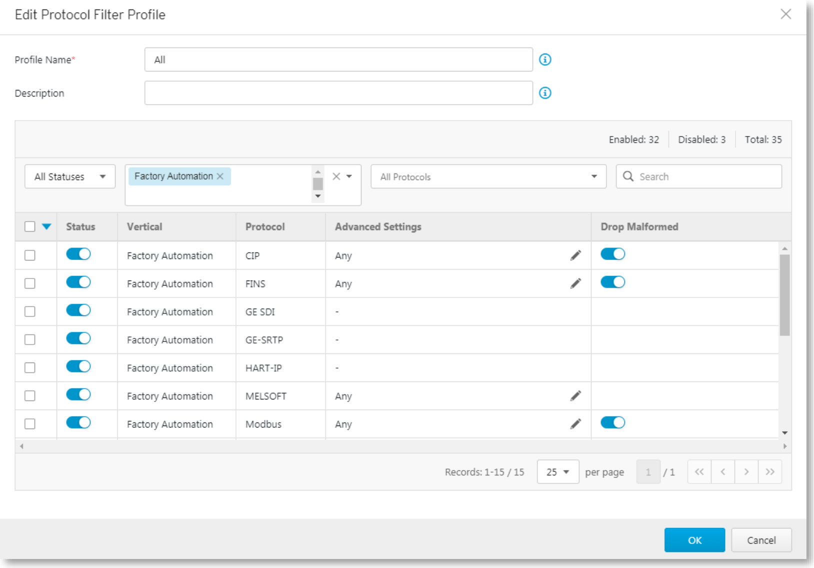
● User Data
Function Group List: 0x0: Mode-transition
Function Group Code*: 0x0

○ Any Sub-function Code
● Preset Sub-function Code
Available Sub-function Code 9
(0x00) Stop
(0x01) Warm restart
(0x02) Run
(0x03) Hot restart
(0x04) Hold
(0x06) Cold restart
Selected Sub-function Code 0
○ Custom Sub-function Code

Total Number of Records: 0 (Max: 32)

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.



Edit Protocol Filter Profile

Profile Name*: All

Description:

Enabled: 32 | Disabled: 3 | Total: 35

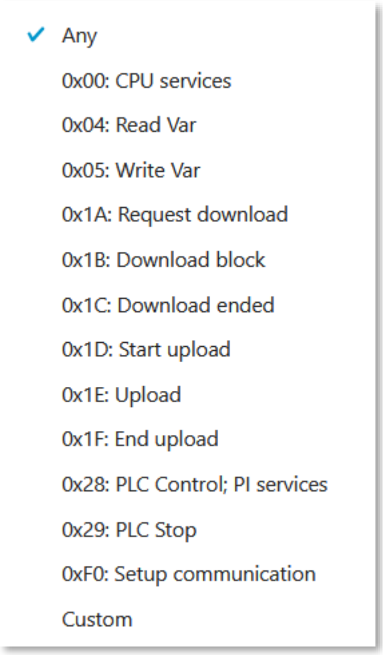
All Statuses ▾ | Factory Automation ✕ | All Protocols ▾ | Search

☐	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
☐	●	Factory Automation	CIP	Any ✎	●
☐	●	Factory Automation	FINS	Any ✎	●
☐	●	Factory Automation	GE SDI	-	
☐	●	Factory Automation	GE-SRTP	-	
☐	●	Factory Automation	HART-IP	-	
☐	●	Factory Automation	MELSOFT	Any ✎	
☐	●	Factory Automation	Modbus	Any ✎	●

Records: 1-15 / 15 | 25 ▾ per page | 1 / 1

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 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.
   - 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 at the [Function list] drop down menu.



✓ Any

0x00: CPU services

0x04: Read Var

0x05: Write Var

0x1A: Request download

0x1B: Download block

0x1C: Download ended

0x1D: Start upload

0x1E: Upload

0x1F: End upload

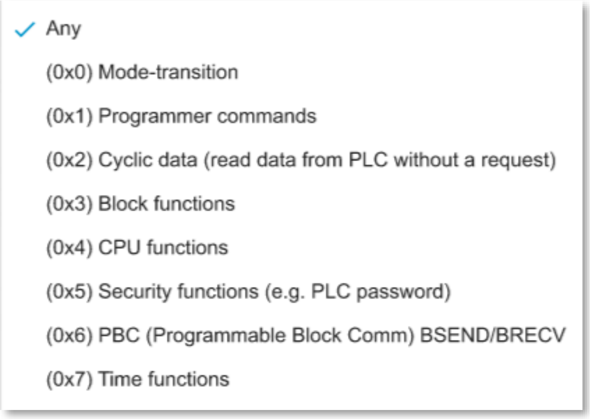
0x28: PLC Control; PI services

0x29: PLC Stop

0xF0: Setup communication

Custom

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



✓ Any

(0x0) Mode-transition

(0x1) Programmer commands

(0x2) Cyclic data (read data from PLC without a request)

(0x3) Block functions

(0x4) CPU functions

(0x5) Security functions (e.g. PLC password)

(0x6) PBC (Programmable Block Comm) BSEND/BRECV

(0x7) Time functions

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

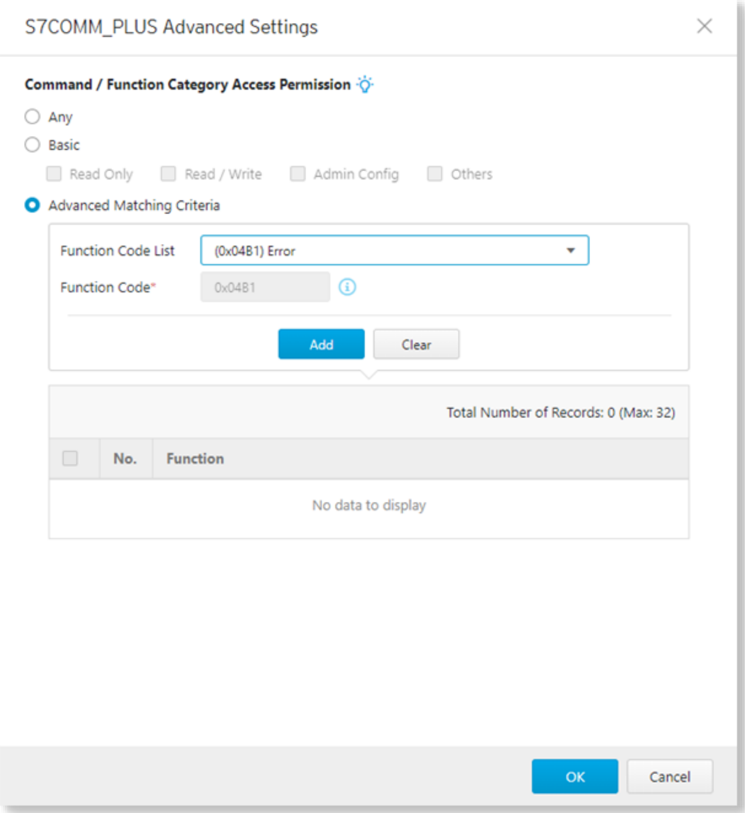
code(s) from the [Available Sub-function Code] to the [Selected Sub-function Code] field.

- If you want to specify a service code by yourself, then select [Custom Sub-function Code] and input a sub-function code in the [Custom Sub-function Code] field.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

Advanced Settings for S7COMM_PLUS

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



S7COMM_PLUS Advanced Settings

Command / Function Category Access Permission

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

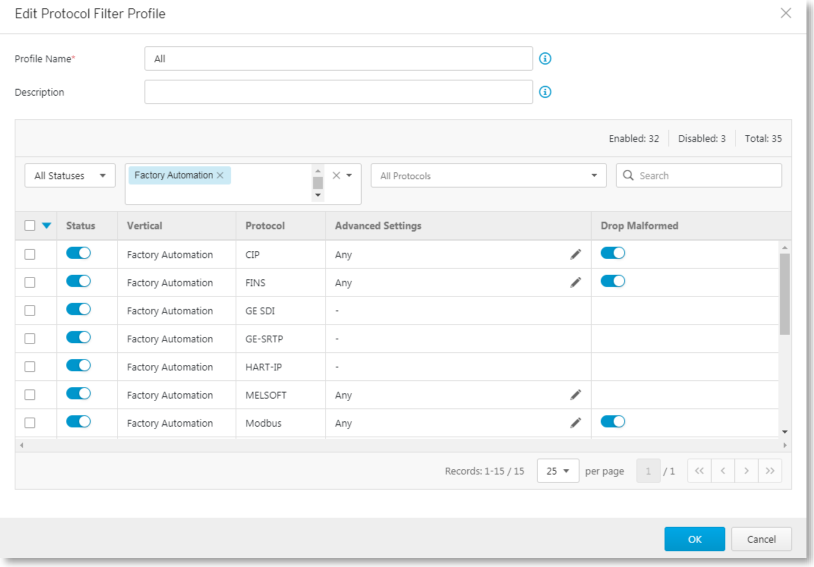
Function Code List: (0x04B1) Error
Function Code*: 0x04B1

Total Number of Records: 0 (Max: 32)

□	No.	Function
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.



Edit Protocol Filter Profile

Profile Name*: All

Description:

Enabled: 32 | Disabled: 3 | Total: 35

All Statuses | Factory Automation × | All Protocols | Search

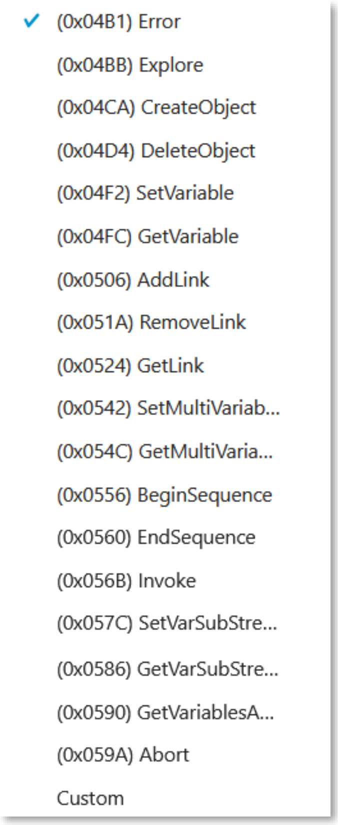
□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any ✎	●
□	●	Factory Automation	FINS	Any ✎	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any ✎	
□	●	Factory Automation	Modbus	Any ✎	●

Records: 1-15 / 15 | 25 per page | 1 / 1

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

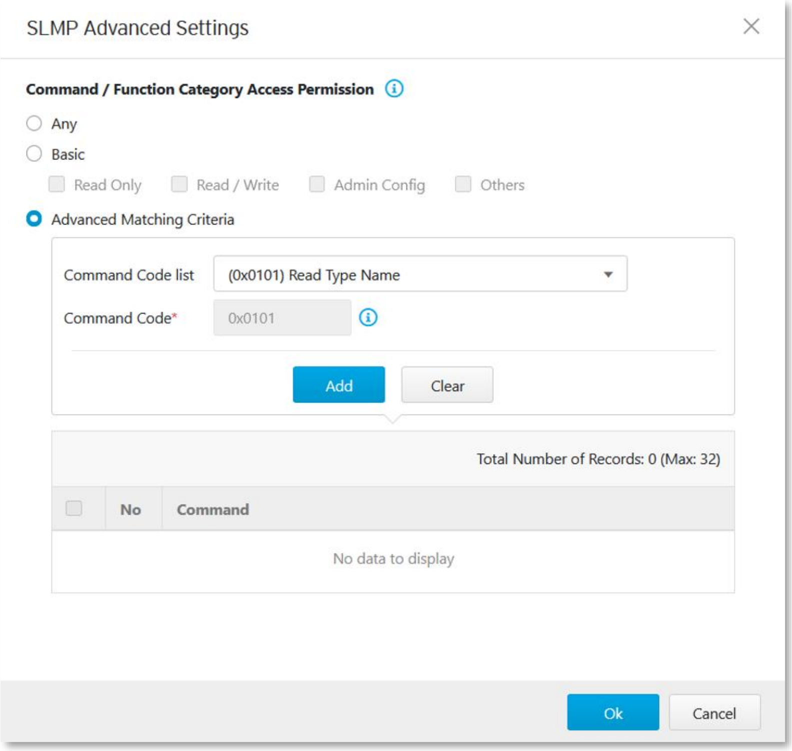


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

Advanced Settings for SLMP

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



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

Add | Clear

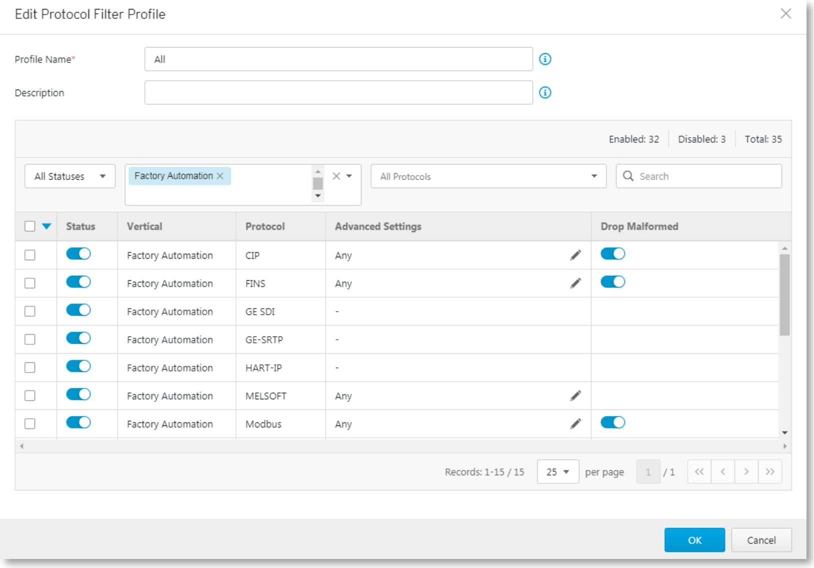
Total Number of Records: 0 (Max: 32)

□	No	Command
		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.



Edit Protocol Filter Profile

Profile Name*: All
Description:

Enabled: 32 | Disabled: 3 | Total: 35

All Statuses | Factory Automation | All Protocols | Search

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any	●
□	●	Factory Automation	FINS	Any	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any	
□	●	Factory Automation	Modbus	Any	●

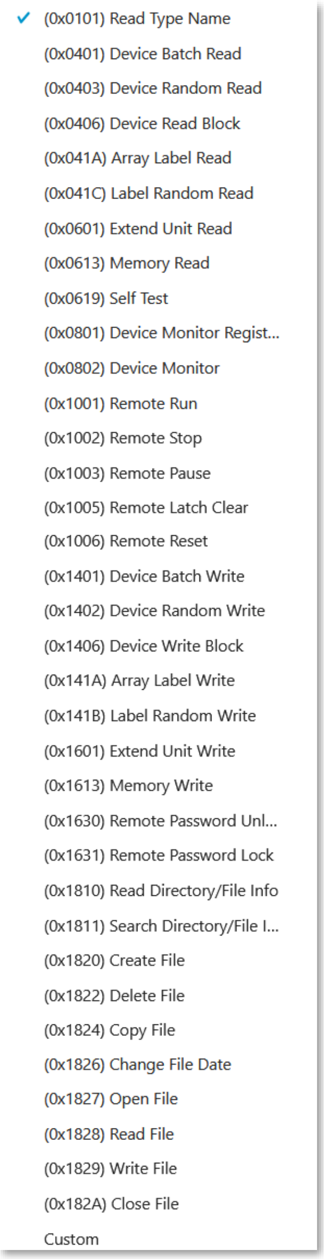
Records: 1-15 / 15 | 25 per page | 1 / 1

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

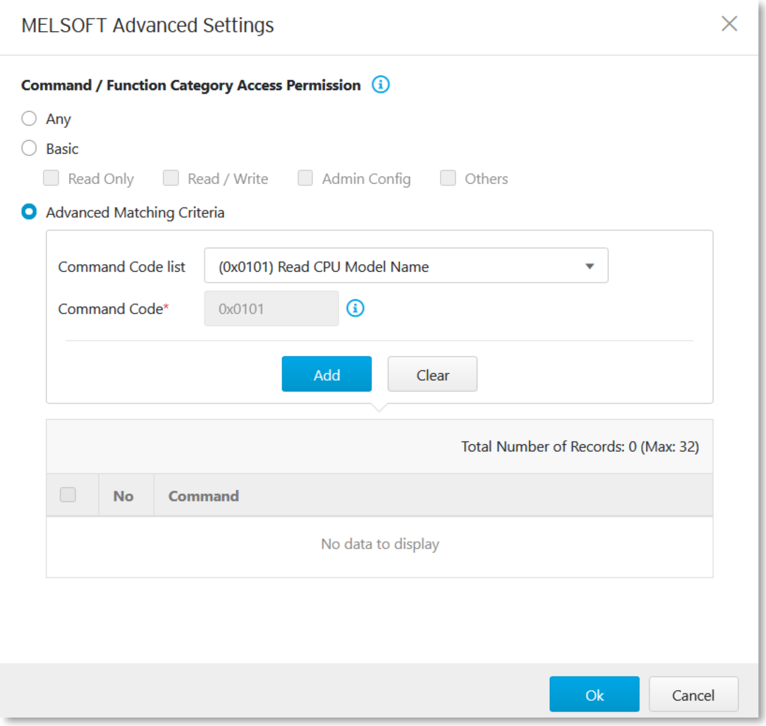

✓ (0x0101) Read Type Name
(0x0401) Device Batch Read
(0x0403) Device Random Read
(0x0406) Device Read Block
(0x041A) Array Label Read
(0x041C) Label Random Read
(0x0601) Extend Unit Read
(0x0613) Memory Read
(0x0619) Self Test
(0x0801) Device Monitor Regist...
(0x0802) Device Monitor
(0x1001) Remote Run
(0x1002) Remote Stop
(0x1003) Remote Pause
(0x1005) Remote Latch Clear
(0x1006) Remote Reset
(0x1401) Device Batch Write
(0x1402) Device Random Write
(0x1406) Device Write Block
(0x141A) Array Label Write
(0x141B) Label Random Write
(0x1601) Extend Unit Write
(0x1613) Memory Write
(0x1630) Remote Password Unl...
(0x1631) Remote Password Lock
(0x1810) Read Directory/File Info
(0x1811) Search Directory/File I...
(0x1820) Create File
(0x1822) Delete File
(0x1824) Copy File
(0x1826) Change File Date
(0x1827) Open File
(0x1828) Read File
(0x1829) Write File
(0x182A) Close File
Custom

- 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 [Advanced Settings] pane, you can further specify the command code against which the function will operate.



MELSOFT Advanced Settings

Command / Function Category Access Permission

○ Any

○ Basic

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

● Advanced Matching Criteria

Command Code list: (0x0101) Read CPU Model Name

Command Code*: 0x0101

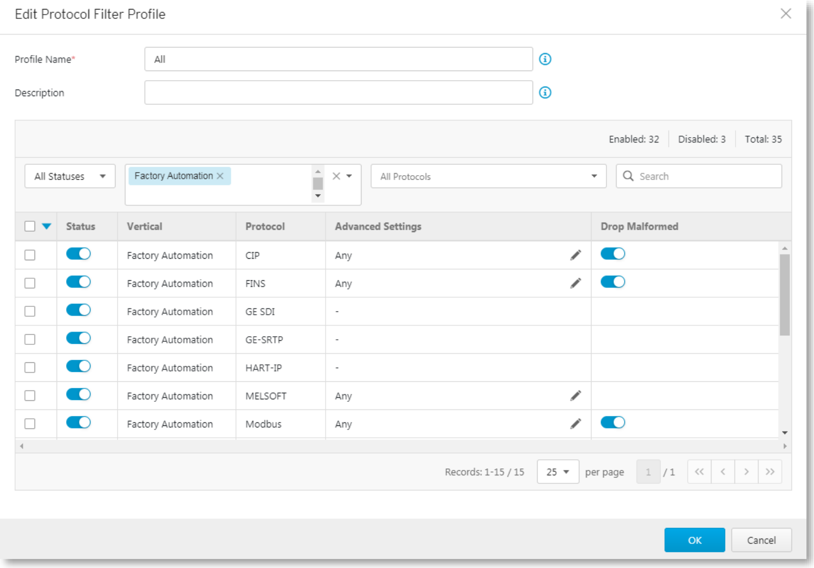
Total Number of Records: 0 (Max: 32)

□	No	Command

No data to display

Procedure

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



Edit Protocol Filter Profile

Profile Name*: All

Description:

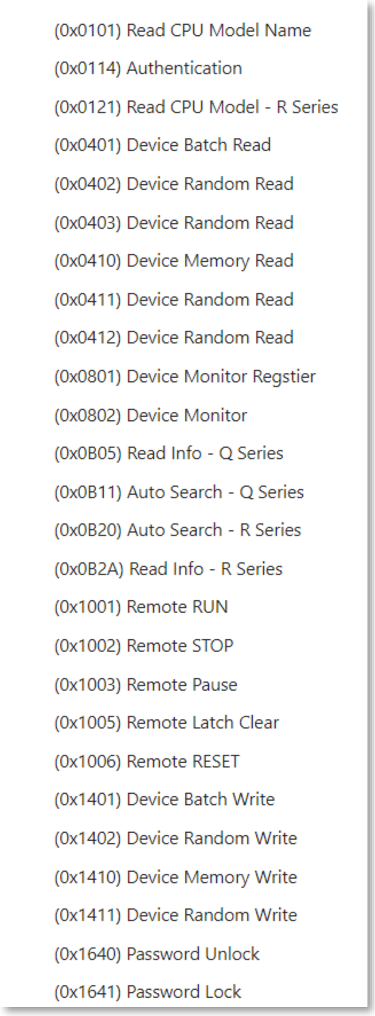
Enabled: 32 | Disabled: 3 | Total: 35

□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any	●
□	●	Factory Automation	FINS	Any	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any	
□	●	Factory Automation	Modbus	Any	●

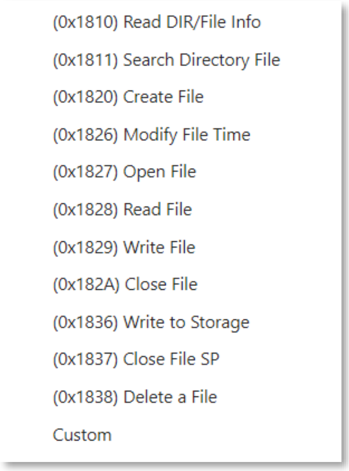
Records: 1-15 / 15 25 per page 1 / 1

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

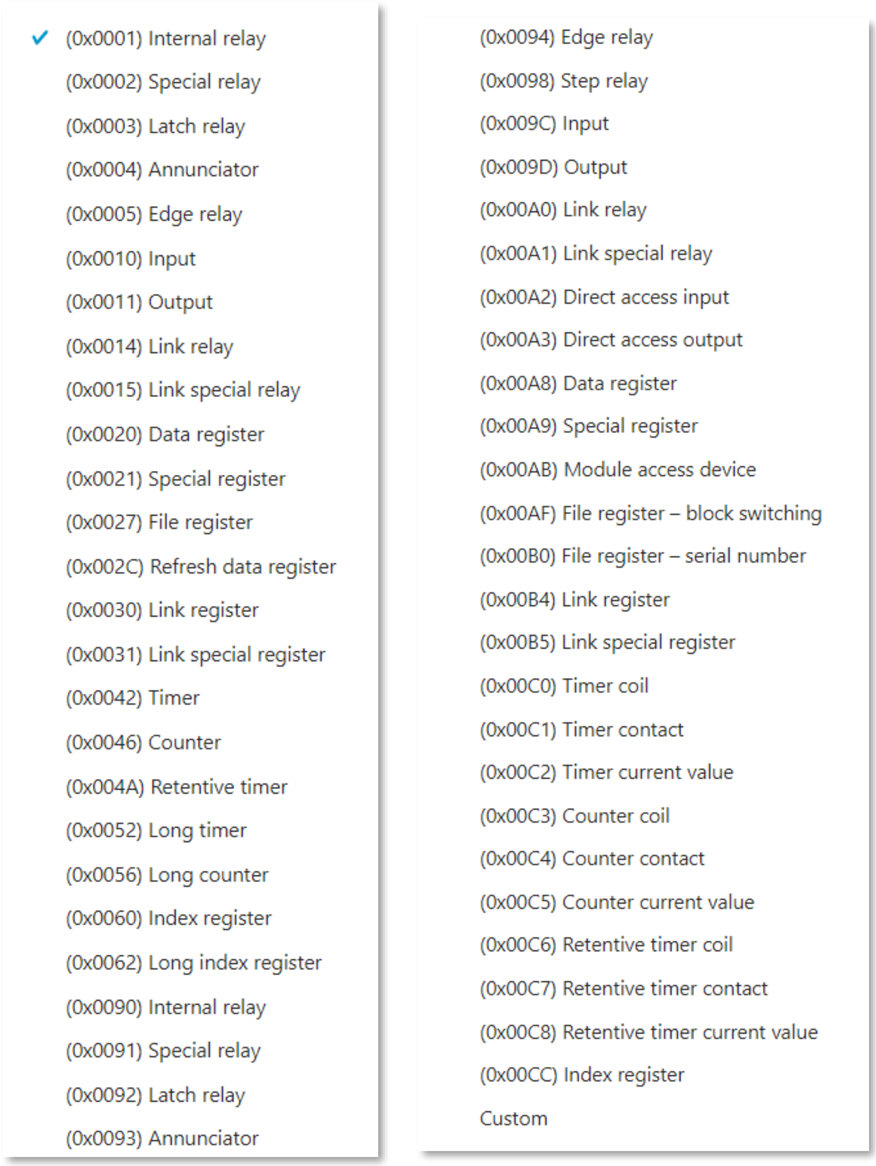


(0x0101) Read CPU Model Name
(0x0114) Authentication
(0x0121) Read CPU Model - R Series
(0x0401) Device Batch Read
(0x0402) Device Random Read
(0x0403) Device Random Read
(0x0410) Device Memory Read
(0x0411) Device Random Read
(0x0412) Device Random Read
(0x0801) Device Monitor Regstier
(0x0802) Device 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 code(s) from the drop list.



✓ (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

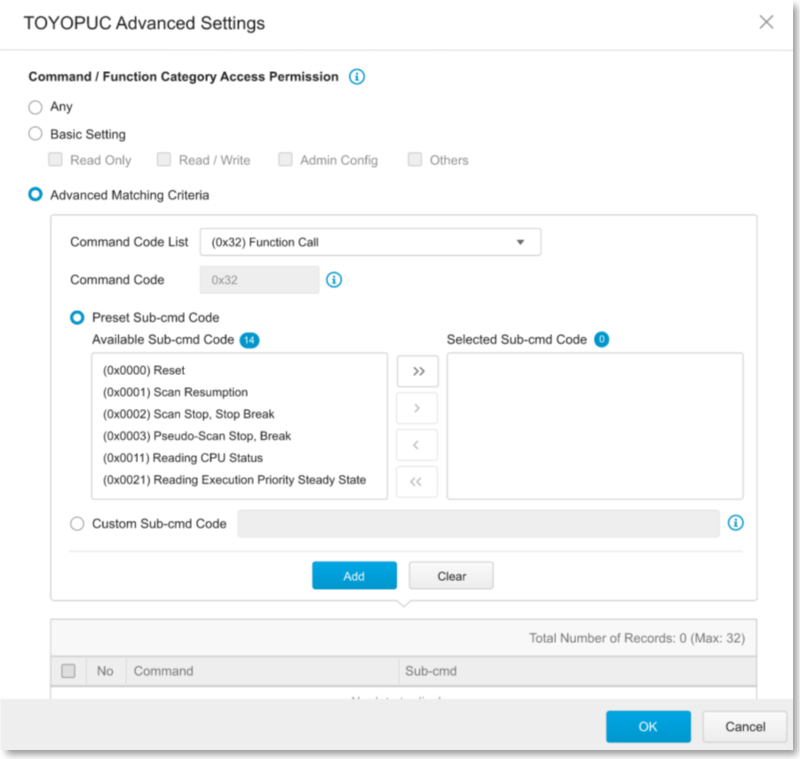
(0x0094) Edge relay
(0x0098) Step relay
(0x009C) Input
(0x009D) Output
(0x00A0) Link relay
(0x00A1) Link special relay
(0x00A2) Direct access input
(0x00A3) Direct access output
(0x00A8) Data register
(0x00A9) Special register
(0x00AB) Module access device
(0x00AF) File register – block switching
(0x00B0) 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 criteria, then select [Any] from the drop list.
- If you want to specify a device number, then select [Single] from the drop list.
- If you want to specify a range of device numbers, then select [Range] from the drop list.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

6. Click [OK].

Advanced Settings for TOYOPUC

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



TOYOPUC Advanced Settings

Command / Function Category Access Permission

○ Any

○ Basic Setting

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

● Advanced Matching Criteria

Command Code List (0x32) Function Call

Command Code 0x32

● Preset Sub-cmd Code

Available Sub-cmd Code 14

- (0x0000) Reset
- (0x0001) Scan Resumption
- (0x0002) Scan Stop, Stop Break
- (0x0003) Pseudo-Scan Stop, Break
- (0x0011) Reading CPU Status
- (0x0021) Reading Execution Priority Steady State

Selected Sub-cmd Code 0

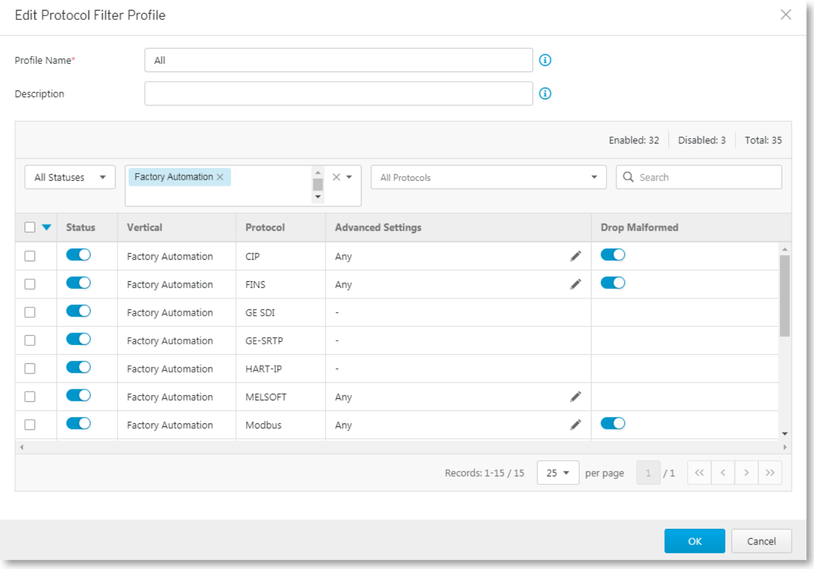
○ Custom Sub-cmd Code

Total Number of Records: 0 (Max: 32)

□	No	Command	Sub-cmd

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.



Edit Protocol Filter Profile

Profile Name* All

Description

Enabled: 32 | Disabled: 3 | Total: 35

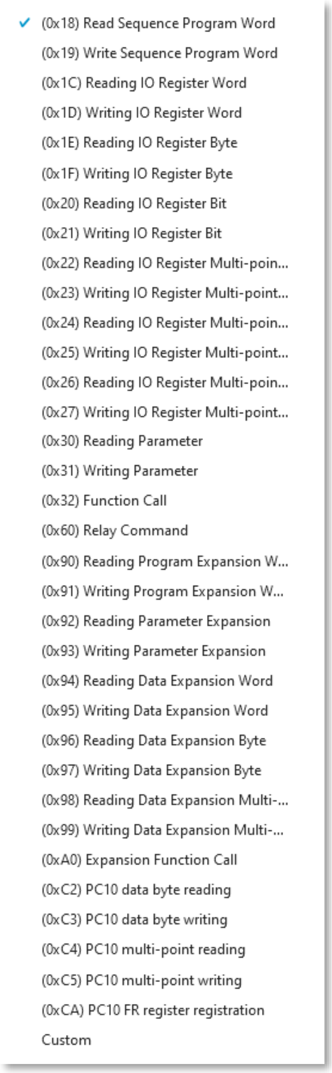
□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any	●
□	●	Factory Automation	FINS	Any	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any	
□	●	Factory Automation	Modbus	Any	●

Records: 1-15 / 15 25 per page 1 / 1

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 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.

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


✓ (0x18) Read Sequence Program Word
(0x19) Write Sequence Program Word
(0x1C) Reading IO Register Word
(0x1D) Writing IO Register Word
(0x1E) Reading IO Register Byte
(0x1F) Writing IO Register Byte
(0x20) Reading IO Register Bit
(0x21) Writing IO Register Bit
(0x22) Reading IO Register Multi-poin...
(0x23) Writing IO Register Multi-point...
(0x24) Reading IO Register Multi-poin...
(0x25) Writing IO Register Multi-point...
(0x26) Reading IO Register Multi-poin...
(0x27) Writing IO Register Multi-point...
(0x30) Reading Parameter
(0x31) Writing Parameter
(0x32) Function Call
(0x60) Relay Command
(0x90) Reading Program Expansion W...
(0x91) Writing Program Expansion W...
(0x92) Reading Parameter Expansion
(0x93) Writing Parameter Expansion
(0x94) Reading Data Expansion Word
(0x95) Writing Data Expansion Word
(0x96) Reading Data Expansion Byte
(0x97) Writing Data Expansion Byte
(0x98) Reading Data Expansion Multi-...
(0x99) Writing Data Expansion Multi-...
(0xA0) Expansion Function Call
(0xC2) PC10 data byte reading
(0xC3) PC10 data byte writing
(0xC4) PC10 multi-point reading
(0xC5) PC10 multi-point writing
(0xCA) PC10 FR register registration
Custom

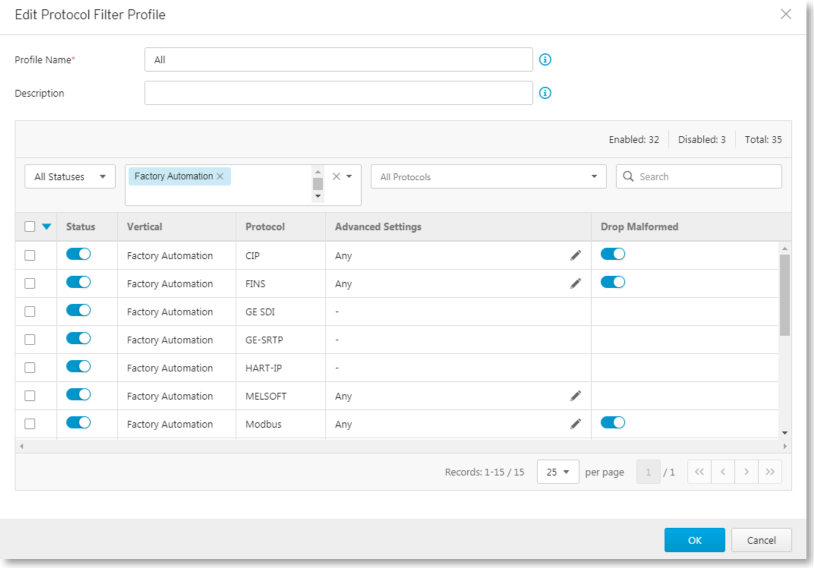
- If you want to specify one sub-command code or multiple sub-command codes, then select [Preset Sub-command Code] and move the sub-function code(s) from the [Available Sub-command Code] field to the [Selected Sub-command Code] field.
- If you want to specify a sub-command code by yourself, then select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

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

6. Click [OK].

Advanced Settings for SMB

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



Edit Protocol Filter Profile

Profile Name*: All

Description:

Enabled: 32 | Disabled: 3 | Total: 35

All Statuses | Factory Automation | All Protocols | Search

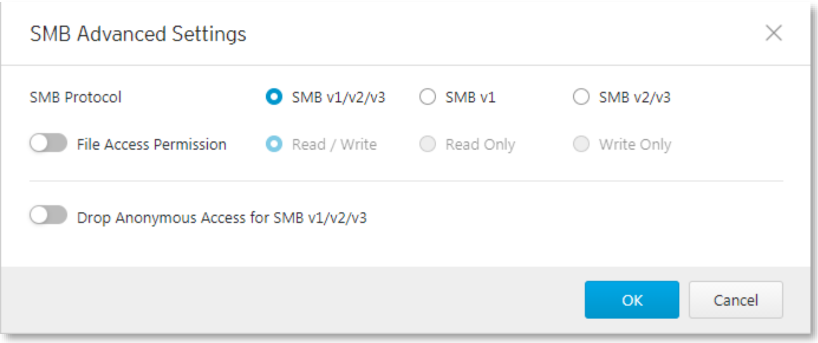
□	Status	Vertical	Protocol	Advanced Settings	Drop Malformed
□	●	Factory Automation	CIP	Any	●
□	●	Factory Automation	FINS	Any	●
□	●	Factory Automation	GE SDI	-	
□	●	Factory Automation	GE-SRTP	-	
□	●	Factory Automation	HART-IP	-	
□	●	Factory Automation	MELSOFT	Any	
□	●	Factory Automation	Modbus	Any	●

Records: 1-15 / 15 | 25 per page | 1 / 1

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.



SMB Advanced Settings

SMB Protocol: ● SMB v1/v2/v3 ○ SMB v1 ○ SMB v2/v3

File Access Permission (off): ● Read / Write ○ Read Only ○ Write Only

Drop Anonymous Access for SMB v1/v2/v3 (off)

OK | 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 button in the [Status] column.
   - Click the [✎] icon in the [Advanced Settings] column, then select one of the following:
   - **SMB Protocol** - Specify SMB the protocol version combination – options include SMBv1/v2/v3, SMBv1 and SMB v2/v3.
   - **File Access** – Select access permission behavior:
     - **Read / Write**: Read and write file access
     - **Read Only**: File access for reading only
     - **Write Only**: File access for writing only

- **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 you can do granular control and apply to a policy rule.

The following can be configured in an IPS profile:

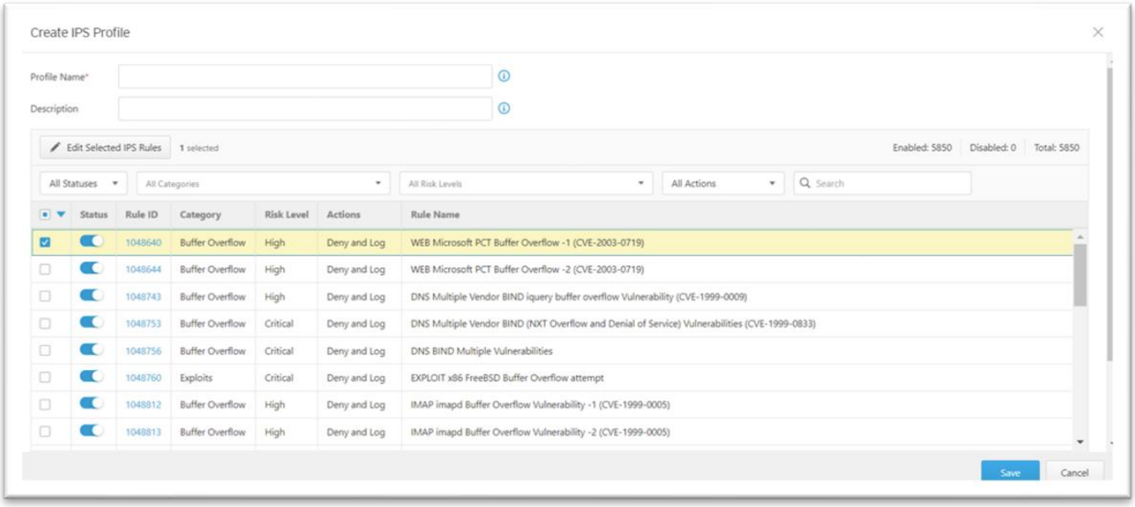
- Details of IPS protocol category, including:
  - File Vulnerabilities
  - Buffer Overflow
  - DoS Attacks
  - Exploits
  - Malware Traffic
  - Reconnaissance
  - Web Threats
  - ICS Threats
  - Others
  - Misc.

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

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

Configuring a Pattern Rule for Granular Control

When configuring an IPS pattern rule, you can specify which action should be taken for the specific category/risk level of pattern and add it in the IPS profile, as the following picture shows.



Create IPS Profile

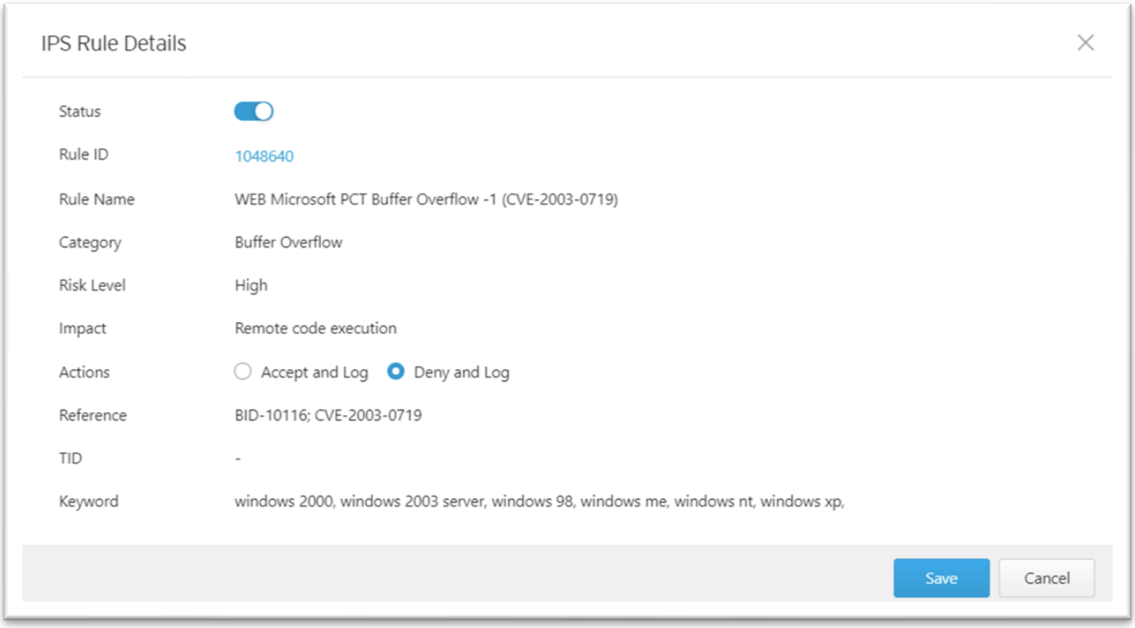
Profile Name*

Description

Edit Selected IPS Rules 1 selected — Enabled: 5850 | Disabled: 0 | Total: 5850

All Statuses ▾ | All Categories ▾ | All Risk Levels ▾ | All Actions ▾ | Search

■	Status	Rule ID	Category	Risk Level	Actions	Rule Name
☑	●	1048640	Buffer Overflow	High	Deny and Log	WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719)
□	●	1048644	Buffer Overflow	High	Deny and Log	WEB Microsoft PCT Buffer Overflow -2 (CVE-2003-0719)
□	●	1048743	Buffer Overflow	High	Deny and Log	DNS Multiple Vendor BIND iquery buffer overflow Vulnerability (CVE-1999-0009)
□	●	1048753	Buffer Overflow	Critical	Deny and Log	DNS Multiple Vendor BIND (NXT Overflow and Denial of Service) Vulnerabilities (CVE-1999-0833)
□	●	1048756	Buffer Overflow	Critical	Deny and Log	DNS BIND Multiple Vulnerabilities
□	●	1048760	Exploits	Critical	Deny and Log	EXPLOIT x86 FreeBSD Buffer Overflow attempt
□	●	1048812	Buffer Overflow	High	Deny and Log	IMAP imapd Buffer Overflow Vulnerability -1 (CVE-1999-0005)
□	●	1048813	Buffer Overflow	High	Deny and Log	IMAP imapd Buffer Overflow Vulnerability -2 (CVE-1999-0005)

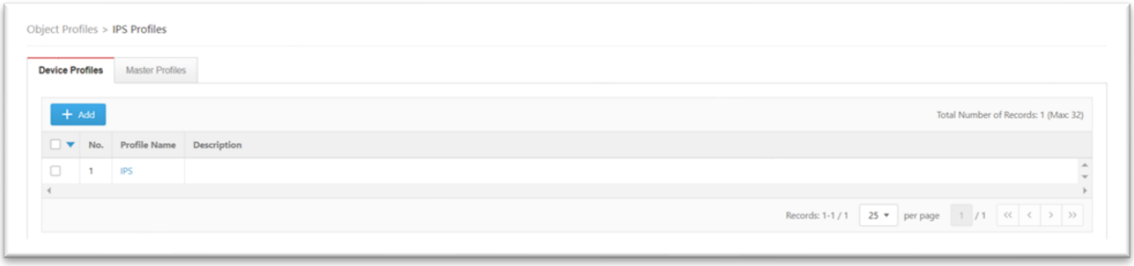


IPS Rule Details

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].



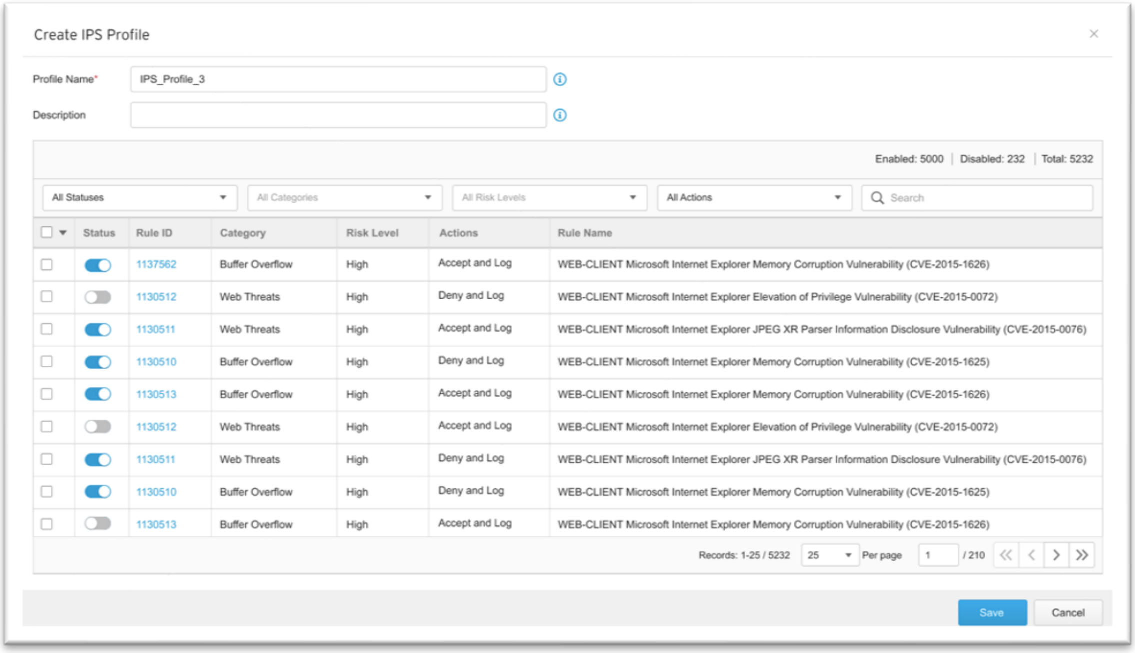
Object Profiles > IPS Profiles

Total Number of Records: 1 (Max: 32)

□	No.	Profile Name	Description
□	1	IPS	

Records: 1-1 / 1 25 ▾ per page 1 / 1

2. Click [Add] to add an IPS profile.
   The [Create IPS Profile] screen will appear.



Create IPS Profile

Profile Name*: IPS_Profile_3

Description:

Enabled: 5000 | Disabled: 232 | Total: 5232

☐	Status	Rule ID	Category	Risk Level	Actions	Rule Name
☐	●	1137562	Buffer Overflow	High	Accept and Log	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)
☐	○	1130512	Web Threats	High	Deny and Log	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)
☐	●	1130511	Web Threats	High	Accept and Log	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)
☐	●	1130510	Buffer Overflow	High	Deny and Log	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)
☐	●	1130513	Buffer Overflow	High	Accept and Log	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)
☐	○	1130512	Web Threats	High	Accept and Log	WEB-CLIENT Microsoft Internet Explorer Elevation of Privilege Vulnerability (CVE-2015-0072)
☐	●	1130511	Web Threats	High	Deny and Log	WEB-CLIENT Microsoft Internet Explorer JPEG XR Parser Information Disclosure Vulnerability (CVE-2015-0076)
☐	●	1130510	Buffer Overflow	High	Deny and Log	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1625)
☐	○	1130513	Buffer Overflow	High	Accept and Log	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-1626)

Records: 1-25 / 5232 | 25 Per page | 1 / 210

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

Field	Description
Status	The operational status of the pattern rule
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 cause to the target network device if the cyberattack succeeds
Actions	The preset action for the cyber attacks
Reference	The vulnerability ID of the cyber attacks (e.g. CVE-2017-0147)
TID	MITRE ID information
keyword	The word(s) for searching the pattern rules

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

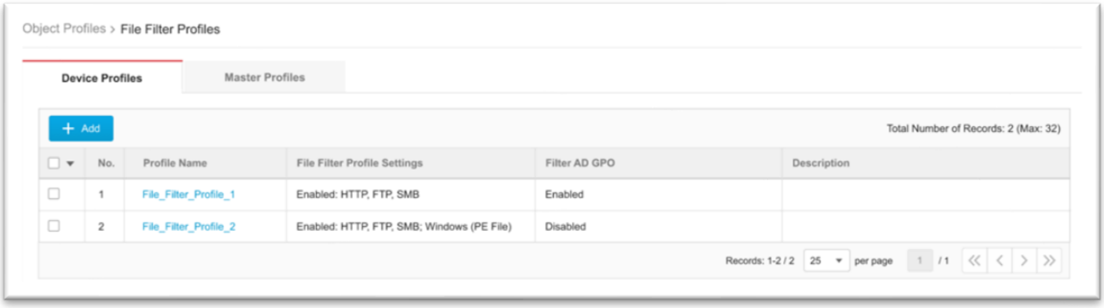
Configuring File Filter Profiles

The File Filter Profiles contains the detailed access protocols, dropping executable file types and Active Directory (AD) GPO dispatch settings, 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 the Executable File(s)

  Includes: Windows (PE files) and Linux (ELF file)
- Filter AD GPO
  Enable or disable Drop Active Directory (AD) GPO



Object Profiles > File Filter Profiles

Device Profiles | Master Profiles

+ Add

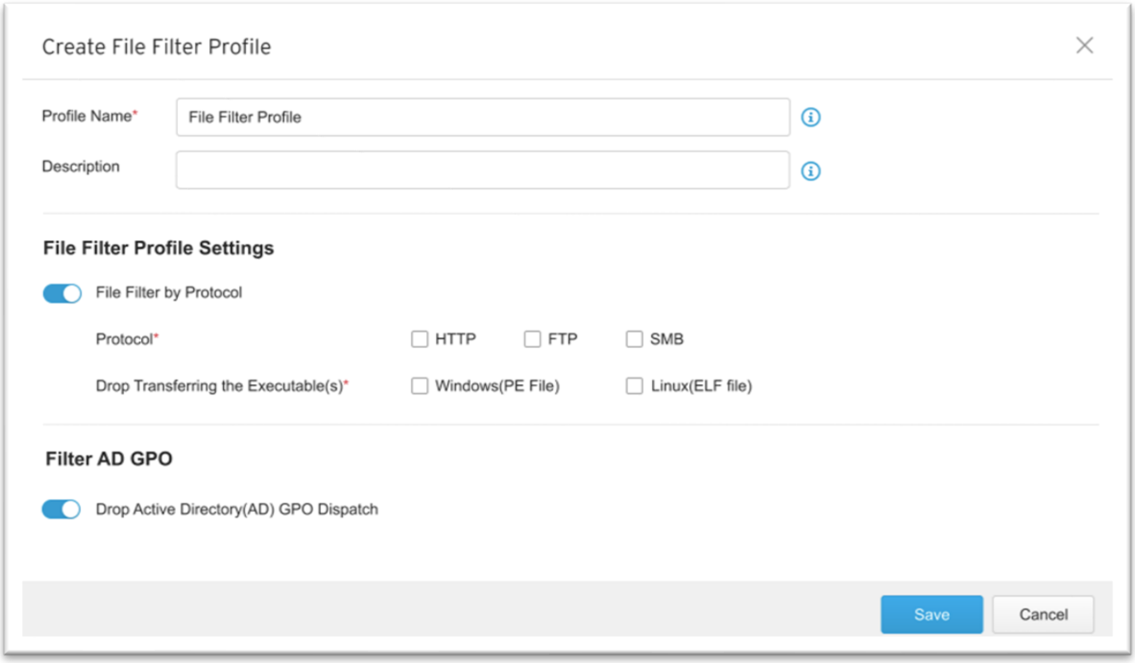
Total Number of Records: 2 (Max: 32)

□	No.	Profile Name	File Filter Profile Settings	Filter AD GPO	Description
□	1	File_Filter_Profile_1	Enabled: HTTP, FTP, SMB	Enabled	
□	2	File_Filter_Profile_2	Enabled: HTTP, FTP, SMB; Windows (PE File)	Disabled	

Records: 1-2 / 2 25 per page 1 / 1

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.



Create File Filter Profile

Profile Name*: File Filter Profile

Description:

File Filter Profile Settings

● File Filter by Protocol

Protocol*: □ HTTP □ FTP □ SMB

Drop Transferring the Executable(s)*: □ Windows(PE File) □ Linux(ELF file)

Filter AD GPO

● Drop Active Directory(AD) GPO Dispatch

Save | Cancel

3. Type a name for the File Filter Profile.
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 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.

Note: The support list of archive file type include zip and gzip file types.

Chapter 9

The Security Tab

This chapter describes the following configurations:

- **Cyber Security configuration**, which allows you to define denial of service attack prevention settings.
- **Policy Enforcement configuration**, which allows you to define a custom protocol that matches to industrial protocol(s), and then allow or block activities fitting that protocol in your network environment.
- **Policy Rule Auto-Learning**, which allows you to create a learning task with a scheduled period of time, generating a trust list for policy enforcement in your network.
- **Suspicious Objects**, which allows you to sync the node-based list that matches to the hash value of a network node with the ODC, and then allow or block activities fitting that network node/network link in your network environment

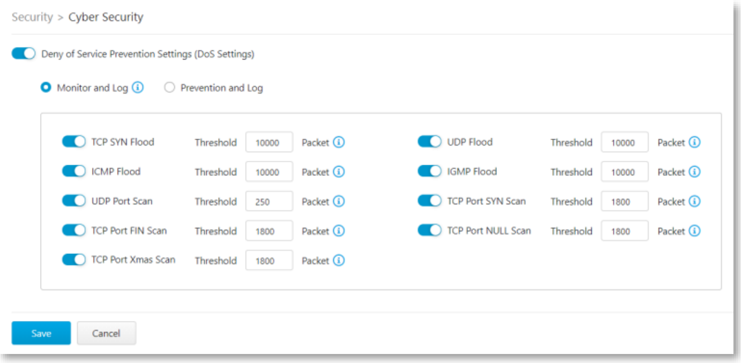
Cyber Security

The feature, Cyber Security, is used to deny the 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 as through the manual import on the web management UI of the device.

Configuring Cyber Security – Denial of Service Prevention

Procedure

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



Security > Cyber Security

Deny of Service Prevention Settings (DoS Settings)

● Monitor and Log ○ Prevention and Log

TCP SYN Flood	Threshold	10000	Packet	UDP Flood	Threshold	10000	Packet
ICMP Flood	Threshold	10000	Packet	IGMP Flood	Threshold	10000	Packet
UDP Port Scan	Threshold	250	Packet	TCP Port SYN Scan	Threshold	1800	Packet
TCP Port FIN Scan	Threshold	1800	Packet	TCP Port NULL Scan	Threshold	1800	Packet
TCP Port Xmas Scan	Threshold	1800	Packet				

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.

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 the subsequent anomalous packets until the end of the detection period. After the detection period, the security node allows anomalous packets until it reached the threshold again.

6. Click [Save].

The following table summarizes the settings:

Mode (Cyber Security)	Action Performed
Monitor and Log	▪ Detects and monitors network attacks, but does not block network attacks. ▪ Generates logs.
Prevention and Log	▪ Blocks network attacks. ▪ Generates logs.

Policy Enforcement

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

There are two types of policy enforcement rule list for this device:

- **Device Rule List**: Contains the policy rule(s) created and configured by users with local account privileges for EdgeFire™.
- **Master Rule List**: Contains the policy rule(s) synced from ODC that the user who has local account privileges in ODC can apply to a policy rule. Users with local account privileges for EdgeFire™ can only view policy rules.

Note: For rule checking, the device rule list is of higher priority than the master rule list.

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

- **Device Rule List:**

Task	Description
Add a policy rule	Click [Add] to create a new policy rule.
Edit a policy rule	Click a policy rule name to edit the settings.
Delete a policy rule	Select one or more policy rules and click [Delete].
Copy a policy rule	Select a policy rule and click [Copy].
Change priority	Select a policy rule and click [Change Priority].

- **Master Rule List:**

Task	Description
N/A	The rule(s) on the Master Rule List are view-only.

Configuring Policy Enforcement

Procedure

1. Go to [Security] > [Policy Enforcement]
2. In 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. From the [Policy Enforcement Operation Mode] drop-down menu, select a mode, [Monitor Mode] or [Prevention Mode] for the policy enforcement.
5. From the [Policy Enforcement Default Rule Action] drop-down menu, select a default action, [Accept], [Accept and Log] or [Deny and Log] when no user-defined policy enforcement rule is matched.

The following table summarizes the settings:

Mode (Policy Enforcement)	Action Performed
Monitor Mode	▪ Detects and monitors protocol access to OT assets, but does not block network attacks. ▪ Generates logs.
Prevention Mode	▪ Blocks abnormal protocol access to OT assets. ▪ Generates logs.

Adding Policy Enforcement Rules (In Gateway Mode)

Procedure

1. Configure the required object(s).
   - IP object profiles

     For more information, see *Configuring IP Object Profile on* page 49.
   - Service object profiles

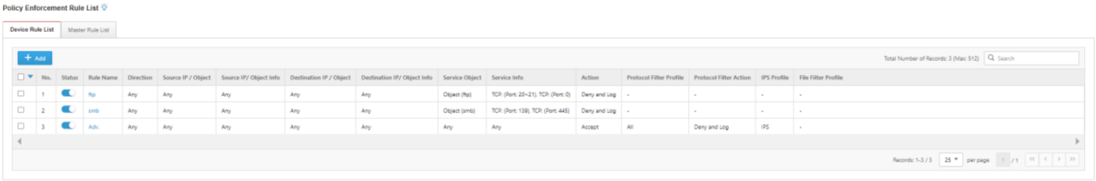
     For more information, see *Configuring Service Object Profile on page 50*.
   - Protocol filter profiles

     For more information, see *Configuring Protocol Filter Profile on page 50*.
   - IPS profiles

     For more information, see *Configuring IPS Profiles on page 76.*
   - File filter profiles

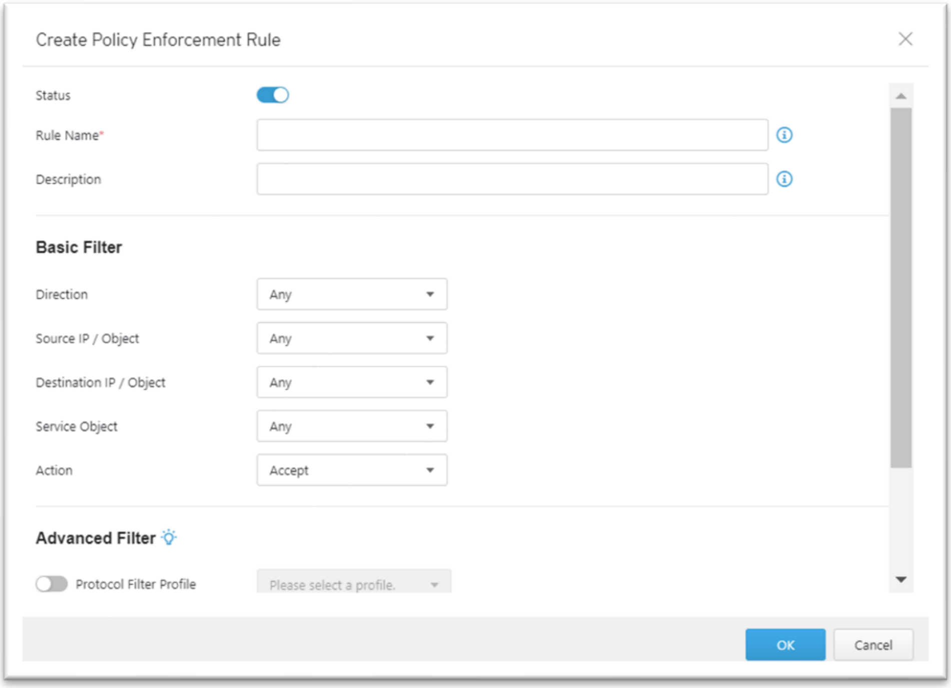
     For more information, see *Configuring File Filter Profiles on page 79*.

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



□	No.	Status	Rule Name	Direction	Source IP / Object	Source IP/ Object Info	Destination IP / Object	Destination IP/ Object Info	Service Object	Service Info	Action	Protocol Filter Profile	Protocol Filter Action	IPS Profile	File Filter Profile
□	1		ftp	Any	Any	Any	Any	Any	Object (ftp)	TCP: (Port: 20~21), TCP: (Port: 0)	Deny and Log	-	-	-	-
□	2		smb	Any	Any	Any	Any	Any	Object (smb)	TCP: (Port: 139), TCP: (Port: 445)	Deny and Log	-	-	-	-
□	3		Adv.	Any	Any	Any	Any	Any	Any	Any	Accept	All	Deny and Log	IPS	-

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



Create Policy Enforcement Rule

Status: On

Rule Name*:

Description:

Basic Filter

Direction: Any

Source IP / Object: Any

Destination IP / Object: Any

Service Object: Any

Action: Accept

Advanced Filter

Protocol Filter Profile: Please select a profile.

6. Input a name for the rule.
7. Input a description for the rule.

8. Under the caption of **[Basic Filter]**, the basic networking setting should be configured. Under the [Interface Direction] drop-down menu, select one of the following for the network traffic direction:
   - Any
   - WAN to LAN
   - LAN to WAN
   - WAN to DMZ
   - DMZ to WAN
   - LAN to DMZ
   - DMZ to LAN
   - LAN to LAN

Note: The network interface in the drop-down menu does not specify which exact network interface, but two or more network interfaces of a kind from the broad view. For example, if you select [WAN to LAN], then the policy enforcement rule will be effective on the traffic from WAN1 interface to LAN1 interface or WAN1 interface to LAN2 interface. If you select [LAN to LAN], then the policy enforcement rule will be effective on the traffic from LAN1 interface to LAN2 interface or LAN2 interface to LAN1 interface.

Note: If you select [Any], then the policy enforcement rule will be effective on the traffic from all network interfaces.

9. Under the [Source IP / IP Object] drop-down menu, select 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 the IP object from an IP object profiles that have been created beforehand.

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

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

10. 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 generate log(s).
    - **Deny and Log**: Select this option to block network traffic that matches this rule and generate log(s).

11. Under the caption of **[Advanced Filter]**, the following settings of profiles will be configured. The node will further take actions based on the protocol filter, the IPS profile or the File filter Profile.
    - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand. From the [Action] drop-down menu, select one of the following:
      a. **Accept**: Select this option to allow network traffic that matches this rule.
      b. **Accept and Log**: Select this option to allow network traffic that matches this rule and generate log(s).

c. **Deny and Log**: Select this option to block network traffic that matches this rule and generate log(s).

- 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.

12. Click [OK] to save the configurations.

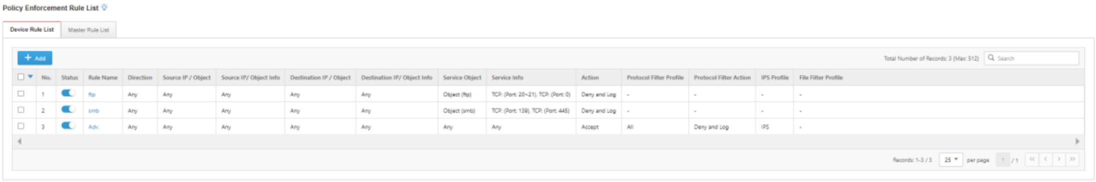
Note: The policy enforcement rule in gateway mode is effective on the level of network interface only, not on the level of network physical ports. The policy enforcement rule cannot inspect the traffic between the physical ports under the same network interface.

Adding Policy Enforcement Rules (In Bridge Mode)

Procedure

1. Configure the required object or objects(s).
   - IP object profiles
     For more information, see *Configuring IP Object Profile on* page 49.
   - Service object profiles
     For more information, see *Configuring Service Object Profile on page 50*.
   - Protocol filter profiles
     For more information, see *Configuring Protocol Filter Profile on page 50*.
   - IPS profiles
     For more information, see *Configuring IPS Profiles on page 76*.
   - File filter profiles
     For more information, see *Configuring File Filter Profiles on page 79*.

2. Go to [Security] > [Policy Enforcement]
3. In the [Policy Enforcement] tab, you will see the following pane.



Policy Enforcement Rule List

Device Rule List | Master Rule List

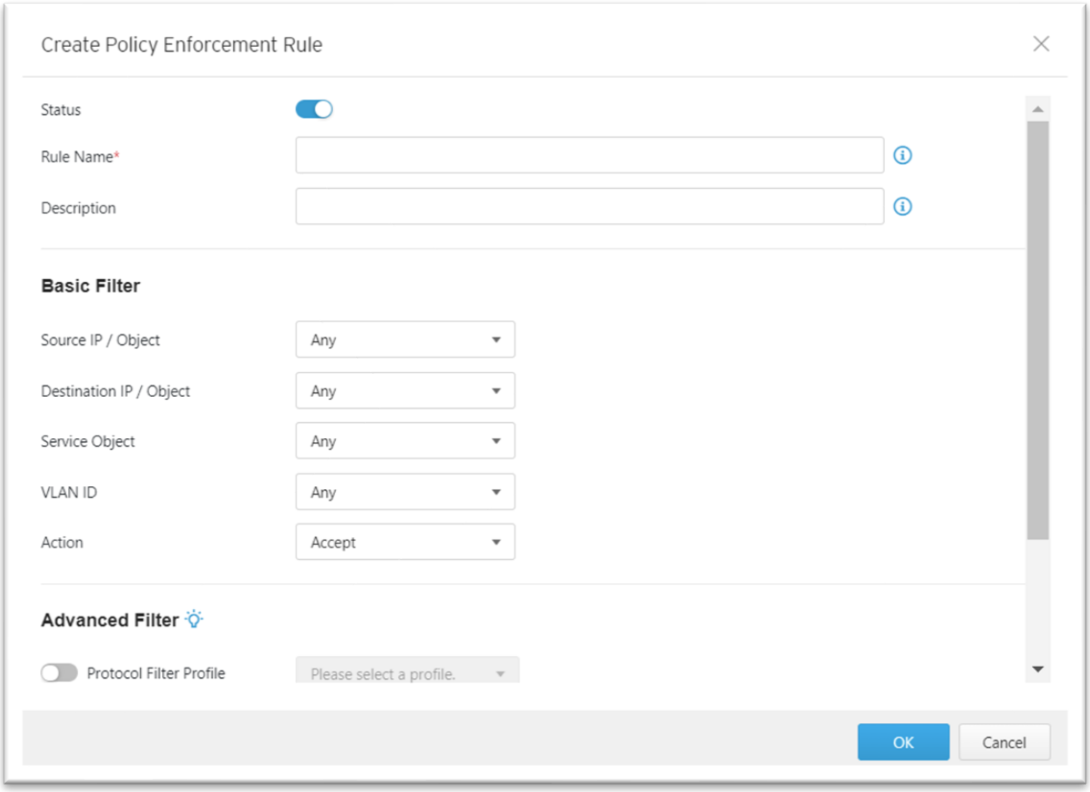
+ Add

Total Number of Records: 3 (Max: 512)

□	No.	Status	Rule Name	Direction	Source IP / Object	Source IP/ Object Info	Destination IP / Object	Destination IP/ Object Info	Service Object	Service Info	Action	Protocol Filter Profile	Protocol Filter Action	IPS Profile	File Filter Profile
□	1	●	ftp	Any	Any	Any	Any	Any	Object (ftp)	TCP: (Port: 20~21), TCP: (Port: 0)	Deny and Log	-	-	-	-
□	2	●	smb	Any	Any	Any	Any	Any	Object (smb)	TCP: (Port: 139), TCP: (Port: 445)	Deny and Log	-	-	-	-
□	3	●	Adv.	Any	Any	Any	Any	Any	Any	Any	Accept	All	Deny and Log	IPS	-

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

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



Create Policy Enforcement Rule

Status: on

Rule Name*

Description

Basic Filter

Source IP / Object: Any

Destination IP / Object: Any

Service Object: Any

VLAN ID: Any

Action: Accept

Advanced Filter

Protocol Filter Profile: Please select a profile.

6. Input a name for the rule.
7. Input a description for the rule.

8. Under the caption of **[Basic Filter]**, the basic networking setting should be configured. From the [Source IP / IP Object Profile] drop-down menu, select 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 the IP object from an IP object profiles that have been created beforehand.

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

      You can further specify the port range for this protocol.

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

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

11. From the [VLAN ID] drop-down menu, select one of the following:
    - **Any**: Select this option to configure any VLAN ID(s).
    - **Custom**: Select this option to configure custom VLAN ID(s).

Note: You can input up to 5 VLAN IDs in one policy enforcement rule.

12. 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 generate log(s).
    - **Deny and Log**: Select this option to block network traffic that matches this rule and generate log(s).

13. Under the caption of **[Advanced Filter]**, the following settings of profiles will be configured. The node will further take actions based on the protocol filter, the IPS profile or the File filter Profile.
    - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand. From the [Action] drop-down menu, select one of the following:
      a. **Accept**: Select this option to allow network traffic that matches this rule.
      b. **Accept and Log**: Select this option to allow network traffic that matches this rule and generate log(s).
      c. **Deny and Log**: Select this option to block network traffic that matches this rule and generate log(s).
    - Under the [IPS Profile] drop-down menu, select an IPS profile you have defined beforehand.
    - Under the [File Filter Profile] drop-down menu, select a file filter profile you have defined beforehand.
14. Click [OK] to save the configurations.

Managing Policy Enforcement Rules

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

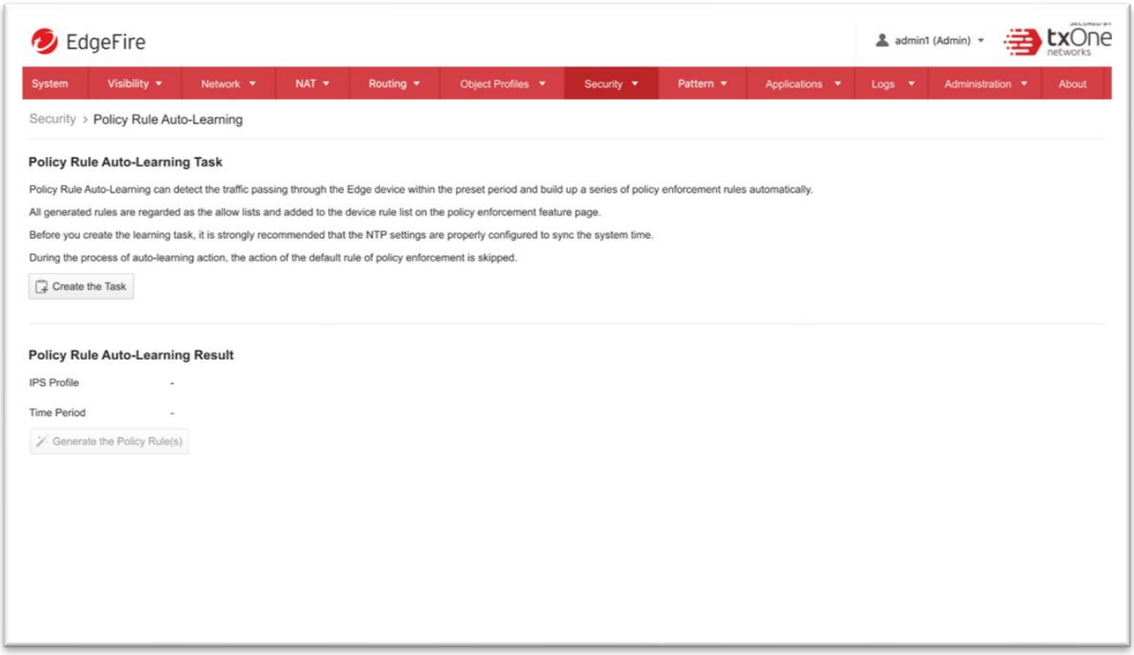
Task	Action
To delete a policy enforcement rule	Click the check box in front of the policy enforcement rule and click the [Delete] button.

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, the device takes the action of the rule with the highest priority, and ignores the rest of the rules. The rules are listed on the table under the UI tab by priority, starting with the highest priority rule at the top.

Policy Rule Auto-Learning

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



Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing through the Edge device within the preset period and build up a series of policy enforcement rules automatically.

All generated rules are regarded as the allow lists and added to the device rule list on the policy enforcement feature page.

Before you create the learning task, it is strongly recommended that the NTP settings are properly configured to sync the system time.

During the process of auto-learning action, the action of the default rule of policy enforcement is skipped.

Policy Rule Auto-Learning Result

IPS Profile -

Time Period -

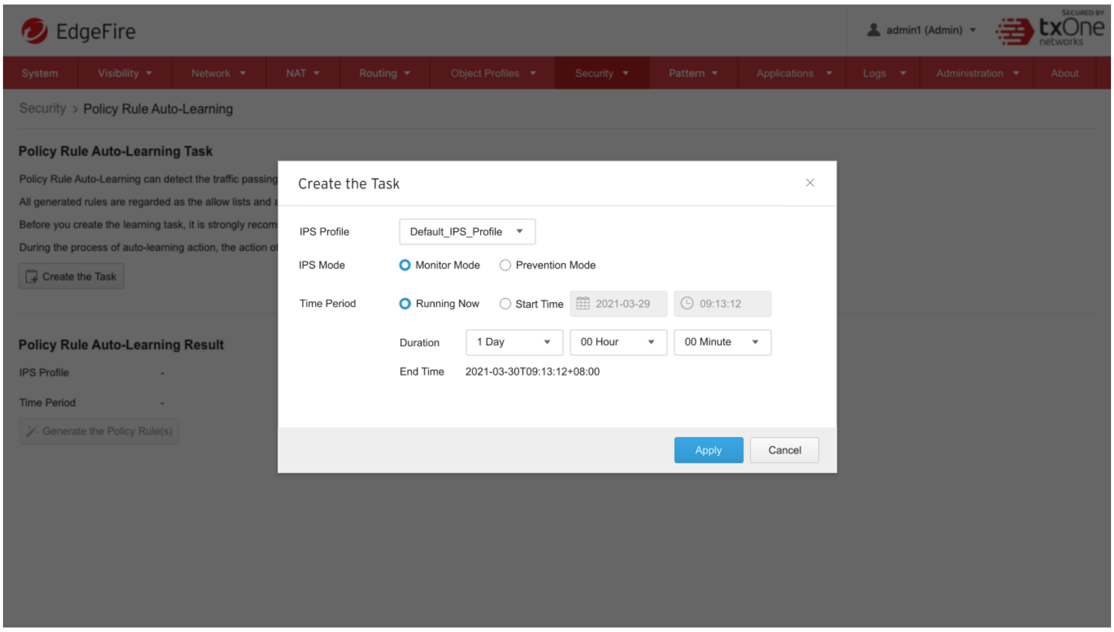
Note: Before you create the task in Policy Rule Auto-Learning, please make sure that an IPS Profile in the [Device Profiles] pane in [Object Profiles] > [IPS Profiles] is properly configured.

Configuring Policy Rule Auto-Learning

Procedure

1. Go to [Security] > [Policy Rule Auto-Learning].
2. On the [Policy Rule Auto-Learning Task] pane, you will see the [Create the Task] button.
3. Click the [Create the Task] button to create the auto-learning task.
4. Select the IPS Profile to apply to the learning task.
5. Select the IPS mode ([Monitor Mode], or [Prevention Mode]) to apply to the learning task.

6. Select the time period ([Running Now], or [Start Time]) to determine when the learning task starts auto-learning.
7. Click [Apply] to create the task.



Security > Policy Rule Auto-Learning

Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing

All generated rules are regarded as the allow lists and a

Before you create the learning task, it is strongly recom

During the process of auto-learning action, the action of

Policy Rule Auto-Learning Result

IPS Profile -

Time Period -

Create the Task

IPS Profile: Default_IPS_Profile

IPS Mode: ● Monitor Mode ○ Prevention Mode

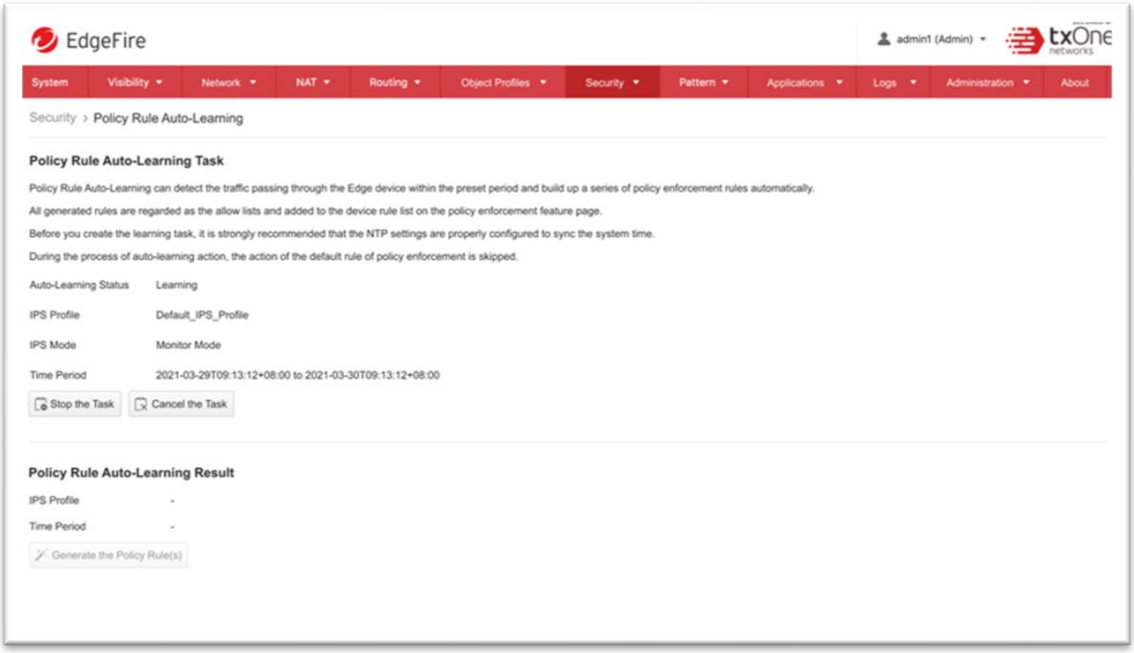
Time Period: ● Running Now ○ Start Time 2021-03-29 09:13:12

Duration: 1 Day 00 Hour 00 Minute

End Time: 2021-03-30T09:13:12+08:00

Note: When a learning task is running, the configuration file cannot be uploaded to EdgeFire™ to restore settings.

Stopping Policy Rule Auto-Learning



Security > Policy Rule Auto-Learning

Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing through the Edge device within the preset period and build up a series of policy enforcement rules automatically.

All generated rules are regarded as the allow lists and added to the device rule list on the policy enforcement feature page.

Before you create the learning task, it is strongly recommended that the NTP settings are properly configured to sync the system time.

During the process of auto-learning action, the action of the default rule of policy enforcement is skipped.

Auto-Learning Status: Learning

IPS Profile: Default_IPS_Profile

IPS Mode: Monitor Mode

Time Period: 2021-03-29T09:13:12+08:00 to 2021-03-30T09:13:12+08:00

Policy Rule Auto-Learning Result

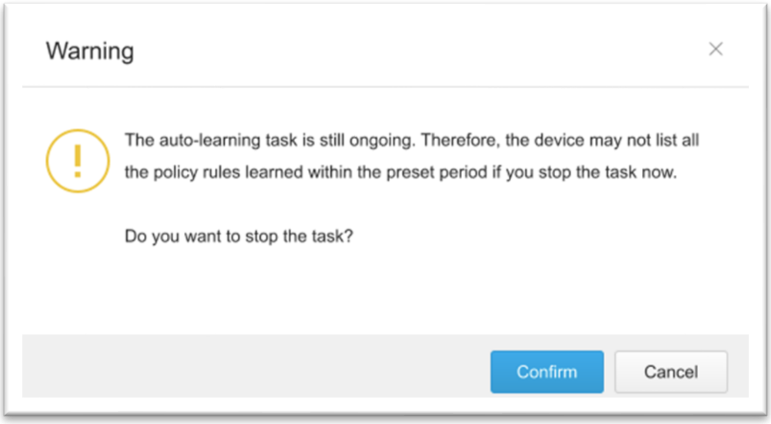
IPS Profile -

Time Period -

Procedure

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

2. On the [Policy Rule Auto-Learning Task] pane, you will see the [Stop the Task] and [Cancel the Task] buttons.
3. Click the [Stop the Task] button to stop the auto-learning task.
4. A warning message will show up for confirmation.



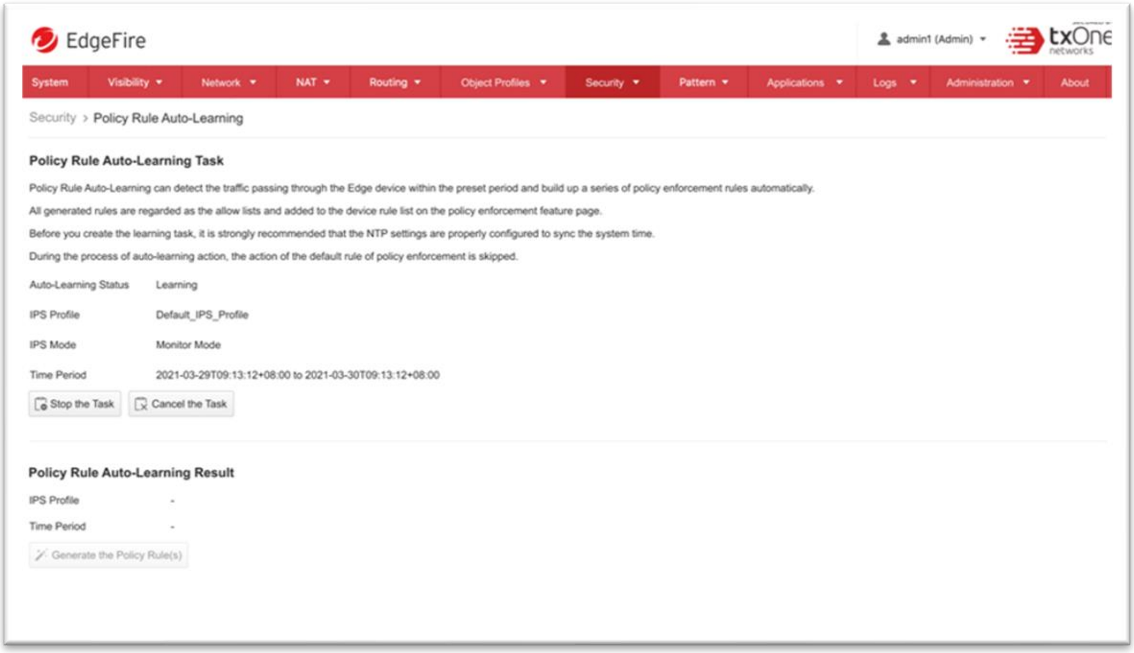
Warning

The auto-learning task is still ongoing. Therefore, the device may not list all the policy rules learned within the preset period if you stop the task now.

Do you want to stop the task?

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

Canceling Policy Rule Auto-Learning



Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing through the Edge device within the preset period and build up a series of policy enforcement rules automatically.

All generated rules are regarded as the allow lists and added to the device rule list on the policy enforcement feature page.

Before you create the learning task, it is strongly recommended that the NTP settings are properly configured to sync the system time.

During the process of auto-learning action, the action of the default rule of policy enforcement is skipped.

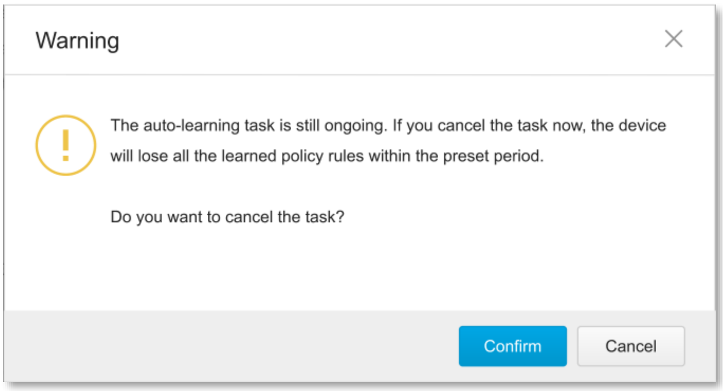
Auto-Learning Status	Learning
IPS Profile	Default_IPS_Profile
IPS Mode	Monitor Mode
Time Period	2021-03-29T09:13:12+08:00 to 2021-03-30T09:13:12+08:00

Policy Rule Auto-Learning Result

IPS Profile	-
Time Period	-

Procedure

1. When the learning task is in progress, go to [Security] > [Policy Rule Auto-Learning].
2. On the [Policy Rule Auto-Learning Task] pane, you will see the [Stop the Task] and [Cancel the Task] buttons.
3. Click the [Cancel the Task] button to cancel the auto-learning task.
4. A warning message will show up for confirmation.



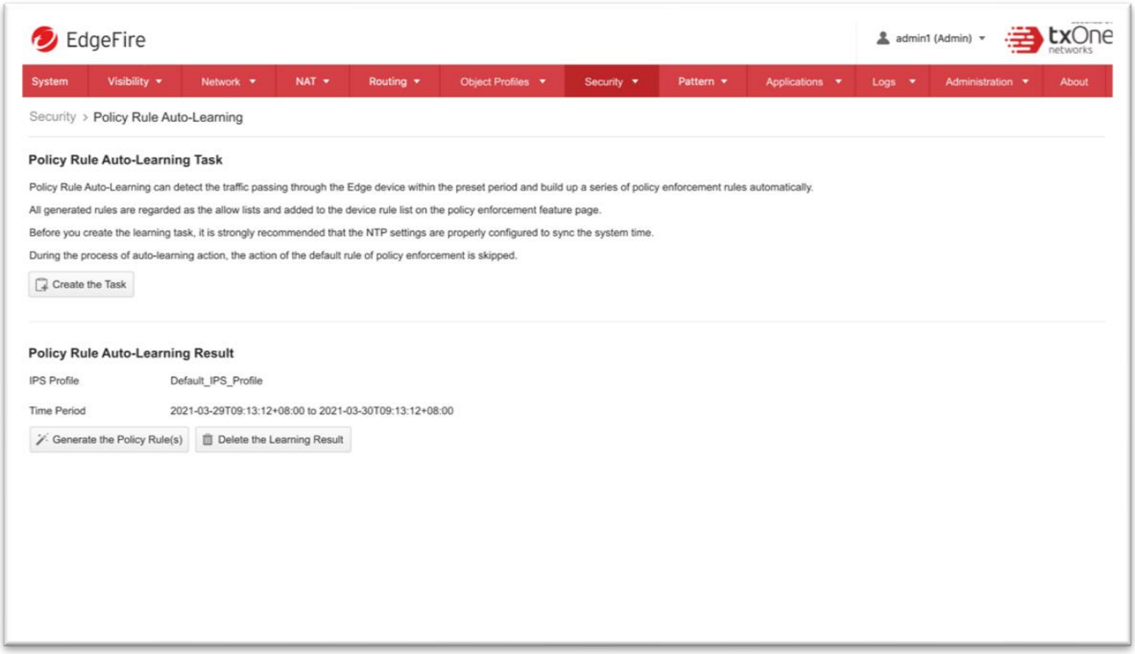
Warning

The auto-learning task is still ongoing. If you cancel the task now, the device will lose all the learned policy rules within the preset period.

Do you want to cancel the task?

5. Click [Confirm] to cancel the task. All the learned policy rules within the preset period will be discarded.

Generating the Learning Results



Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing through the Edge device within the preset period and build up a series of policy enforcement rules automatically.

All generated rules are regarded as the allow lists and added to the device rule list on the policy enforcement feature page.

Before you create the learning task, it is strongly recommended that the NTP settings are properly configured to sync the system time.

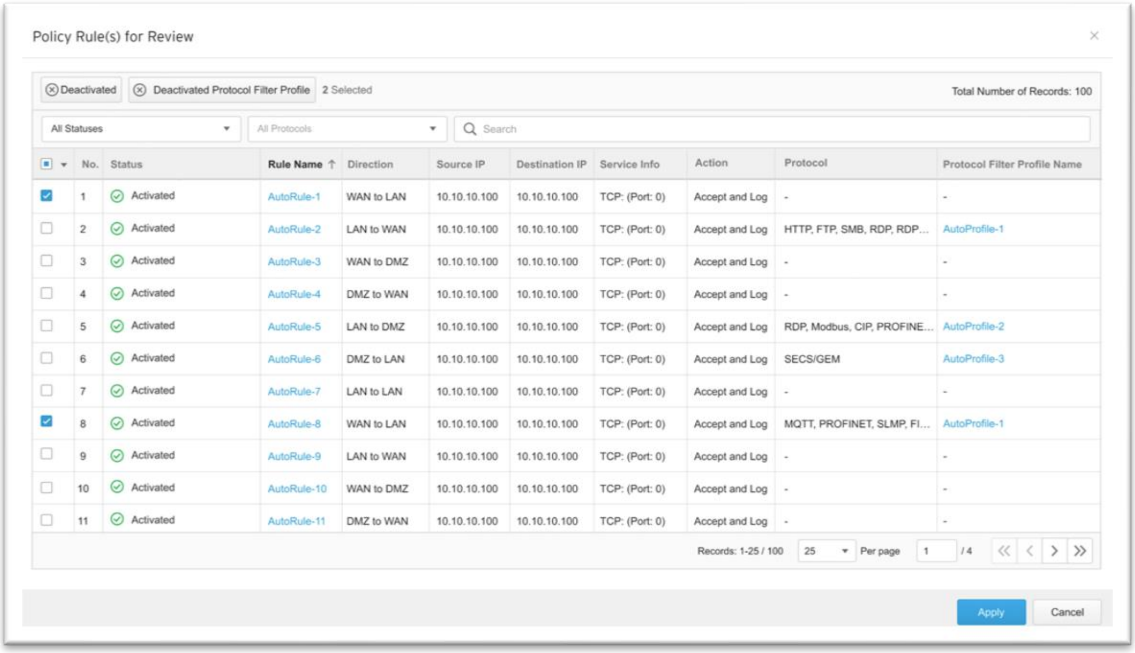
During the process of auto-learning action, the action of the default rule of policy enforcement is skipped.

Policy Rule Auto-Learning Result

IPS Profile	Default_IPS_Profile
Time Period	2021-03-29T09:13:12+08:00 to 2021-03-30T09:13:12+08:00

Procedure

1. After the learning task process is completed, or stopped, go to [Security] > [Policy Rule Auto-Learning].
2. On the [Policy Rule Auto-Learning Result] pane, you will see the [Generate Policy Rule] and [Delete the Learning Result] buttons.
3. Click the [Generate Policy Rules] button to list the policy rule list for review.



Policy Rule(s) for Review

2 Selected

Total Number of Records: 100

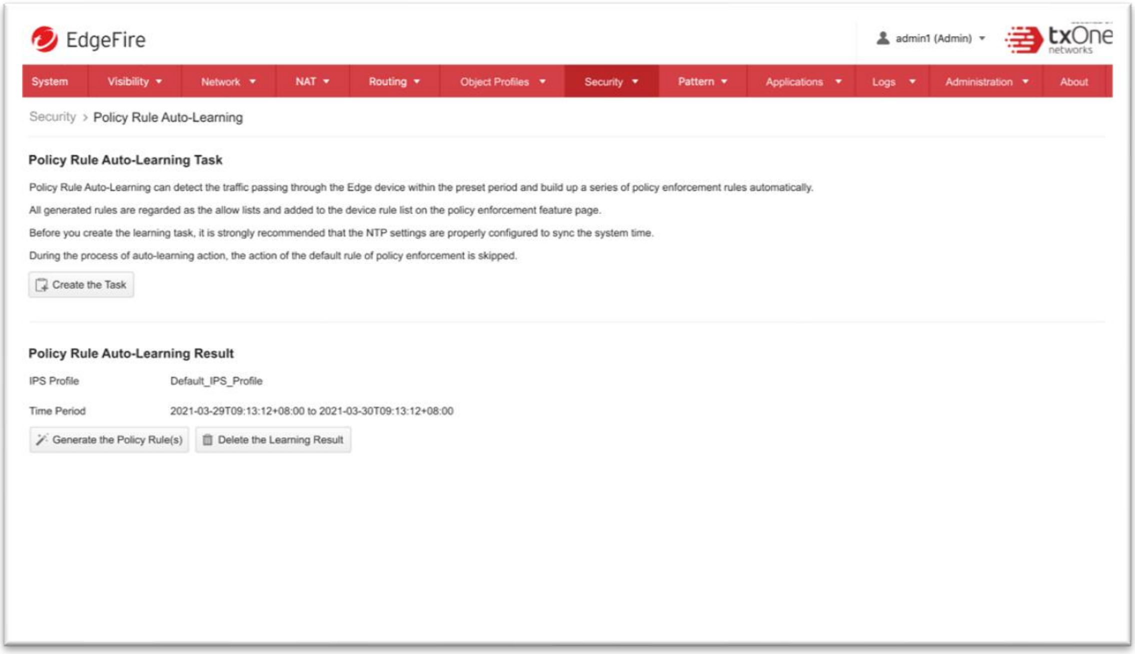
■ ▾	No.	Status	Rule Name ↑	Direction	Source IP	Destination IP	Service Info	Action	Protocol	Protocol Filter Profile Name
☑	1	✓ Activated	AutoRule-1	WAN to LAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☐	2	✓ Activated	AutoRule-2	LAN to WAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	HTTP, FTP, SMB, RDP, RDP...	AutoProfile-1
☐	3	✓ Activated	AutoRule-3	WAN to DMZ	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☐	4	✓ Activated	AutoRule-4	DMZ to WAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☐	5	✓ Activated	AutoRule-5	LAN to DMZ	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	RDP, Modbus, CIP, PROFINE...	AutoProfile-2
☐	6	✓ Activated	AutoRule-6	DMZ to LAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	SECS/GEM	AutoProfile-3
☐	7	✓ Activated	AutoRule-7	LAN to LAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☑	8	✓ Activated	AutoRule-8	WAN to LAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	MQTT, PROFINET, SLMP, FI...	AutoProfile-1
☐	9	✓ Activated	AutoRule-9	LAN to WAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☐	10	✓ Activated	AutoRule-10	WAN to DMZ	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-
☐	11	✓ Activated	AutoRule-11	DMZ to WAN	10.10.10.100	10.10.10.100	TCP: (Port: 0)	Accept and Log	-	-

Records: 1-25 / 100 25 ▾ Per page 1 / 4

4. You can activate or deactivate policy rule(s) by clicking the checkbox on the left of the window before you apply to generate the policy rule(s) as a trust list.
5. Click [Apply] and the policy rule list will be generated and moved to the device rule list in policy enforcement page.

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

Deleting the Learning Results



Policy Rule Auto-Learning Task

Policy Rule Auto-Learning can detect the traffic passing through the Edge device within the preset period and build up a series of policy enforcement rules automatically.

All generated rules are regarded as the allow lists and added to the device rule list on the policy enforcement feature page.

Before you create the learning task, it is strongly recommended that the NTP settings are properly configured to sync the system time.

During the process of auto-learning action, the action of the default rule of policy enforcement is skipped.

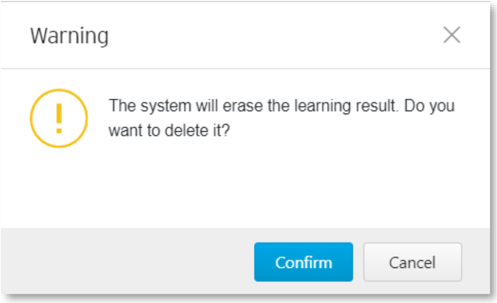
Policy Rule Auto-Learning Result

IPS Profile Default_IPS_Profile

Time Period 2021-03-29T09:13:12+08:00 to 2021-03-30T09:13:12+08:00

Procedure

1. After the learning task is completed, go to [Security] > [Policy Rule Auto-Learning].
2. At the [Policy Rule Auto-Learning Result] plane you will see the [Generate Policy Rule] and [Delete the Learning Result] button.
3. Click the [Delete the Learning Result] button.
4. A warning message will show up for confirmation.



The system will erase the learning result. Do you want to delete it?

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

Suspicious Objects

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

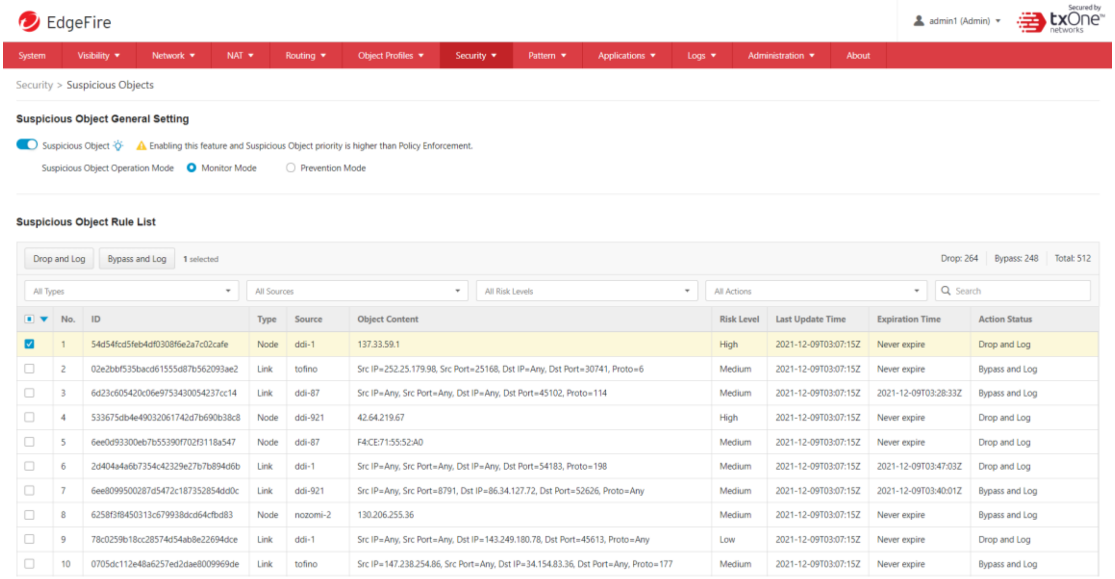
Note: Before you enable Suspicious Objects feature, please note that the [ODC Settings] pane in [Administration] > [Sync Settings], is properly configured and ODC is connected with the 3rd party API from the source of the suspicious object.

Configuring Suspicious Objects

Procedure

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

- In the [Suspicious Objects] tab, you will see the [Suspicious Object General Settings] pane.
- Use the toggle to enable or disable the suspicious object feature.
- Select a mode ([Monitor Mode], or [Prevention Mode]) for the feature.
- If you want to change the action of the specific suspicious object at the [Suspicious Object Rule List] table, select the specific suspicious object and choose the action [Drop and Log] or [Bypass and Log] when the pattern is matched.



Security > Suspicious Objects

Suspicious Object General Setting

Suspicious Object: on

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

Suspicious Object Operation Mode ● Monitor Mode ○ Prevention Mode

Suspicious Object Rule List

1 selected

Drop: 264 | Bypass: 248 | Total: 512

☐	No.	ID	Type	Source	Object Content	Risk Level	Last Update Time	Expiration Time	Action Status
☑	1	54d54fcd5feb4df0308f6e2a7c02cafe	Node	ddi-1	137.33.59.1	High	2021-12-09T03:07:15Z	Never expire	Drop and Log
☐	2	02e2bbf535bacd61555d87b562093ae2	Link	tofino	Src IP=252.25.179.98, Src Port=25168, Dst IP=Any, Dst Port=30741, Proto=6	Medium	2021-12-09T03:07:15Z	Never expire	Bypass and Log
☐	3	6d23c605420c06e9753430054237cc14	Link	ddi-87	Src IP=Any, Src Port=Any, Dst IP=Any, Dst Port=45102, Proto=114	Medium	2021-12-09T03:07:15Z	2021-12-09T03:28:33Z	Bypass and Log
☐	4	533675db4e49032061742d7b690b38c8	Node	ddi-921	42.64.219.67	High	2021-12-09T03:07:15Z	Never expire	Drop and Log
☐	5	6ee0d93300eb7b55390f702f3118a547	Node	ddi-87	F4:CE:71:55:52:A0	Medium	2021-12-09T03:07:15Z	Never expire	Drop and Log
☐	6	2d404a4a6b7354c42329e27b7b894d6b	Link	ddi-1	Src IP=Any, Src Port=Any, Dst IP=Any, Dst Port=54183, Proto=198	Medium	2021-12-09T03:07:15Z	2021-12-09T03:47:03Z	Drop and Log
☐	7	6ee8099500287d5472c187352854dd0c	Link	ddi-921	Src IP=Any, Src Port=8791, Dst IP=86.34.127.72, Dst Port=52626, Proto=Any	Medium	2021-12-09T03:07:15Z	2021-12-09T03:40:01Z	Bypass and Log
☐	8	6258f3f8450313c679938dcd64cfbd83	Node	nozomi-2	130.206.255.36	Medium	2021-12-09T03:07:15Z	Never expire	Bypass and Log
☐	9	78c0259b18cc28574d54ab8e22694dce	Link	ddi-1	Src IP=Any, Src Port=Any, Dst IP=143.249.180.78, Dst Port=45613, Proto=Any	Low	2021-12-09T03:07:15Z	Never expire	Drop and Log
☐	10	0705dc112e48a6257ed2dae8009969de	Link	tofino	Src IP=147.238.254.86, Src Port=Any, Dst IP=34.154.83.36, Dst Port=Any, Proto=177	Medium	2021-12-09T03:07:15Z	Never expire	Bypass and Log

The following table summarizes the settings:

Mode (Suspicious Objects)	Action Performed
Monitor Mode	▪ Detects network node(s) or network link(s), but does not block the traffic related to the network node(s) or network link(s). ▪ Generates logs.
Prevention Mode	▪ Blocks network node(s) or network link(s). ▪ Generates logs.

Note: The suspicious object rule list is of higher priority than the device rule and master rule lists.

The Pattern Tab

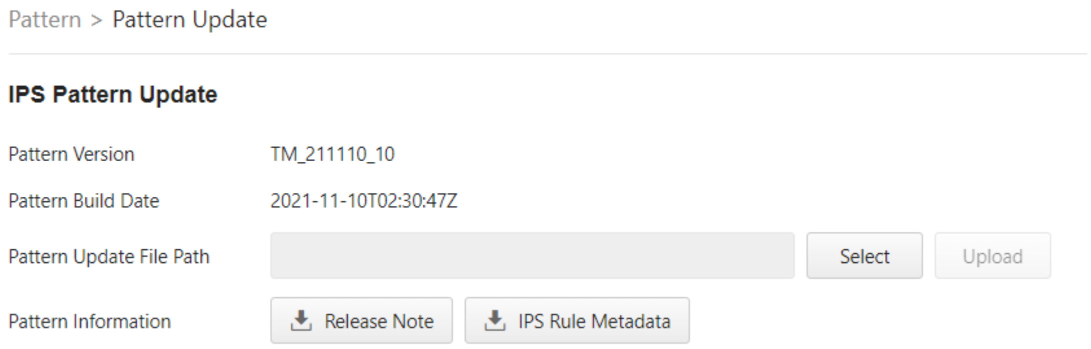
This chapter describes how to view the pattern information and how to import a DPI (Deep Packet Inspection) pattern to the EdgeFire™ device.

The DPI pattern, prepared by Trend Micro, contains signatures to enable the intrusion prevention features on the device. The intrusion prevention features detect and prevent 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. In the [Pattern Update] tab you will see the following information.
3. The [IPS Pattern Update] pane shows the current [IPS Pattern Version] and [IPS Pattern Build Date].



Pattern > Pattern Update

IPS Pattern Update

Pattern Version TM_211110_10

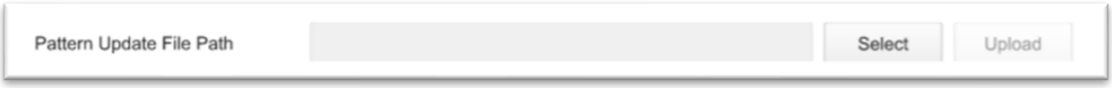
Pattern Build Date 2021-11-10T02:30:47Z

Pattern Update File Path

Manually Updating the Pattern

Procedure

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



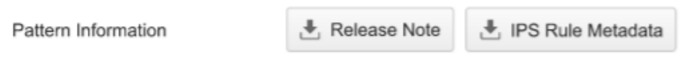
Pattern Update File Path

3. Click [Select].
4. Manually select the pattern to be deployed to the device.
5. Click [Upload] and then [Confirm].

Downloading Release Notes/IPS Rule Metadata

Procedure

1. Go to [Pattern] > [Pattern Update].
2. Click the [Download Release Notes] button to view the detailed release information.
3. Click the [Download IPS Rule Metadata] button to view the IPS Rule Metadata.



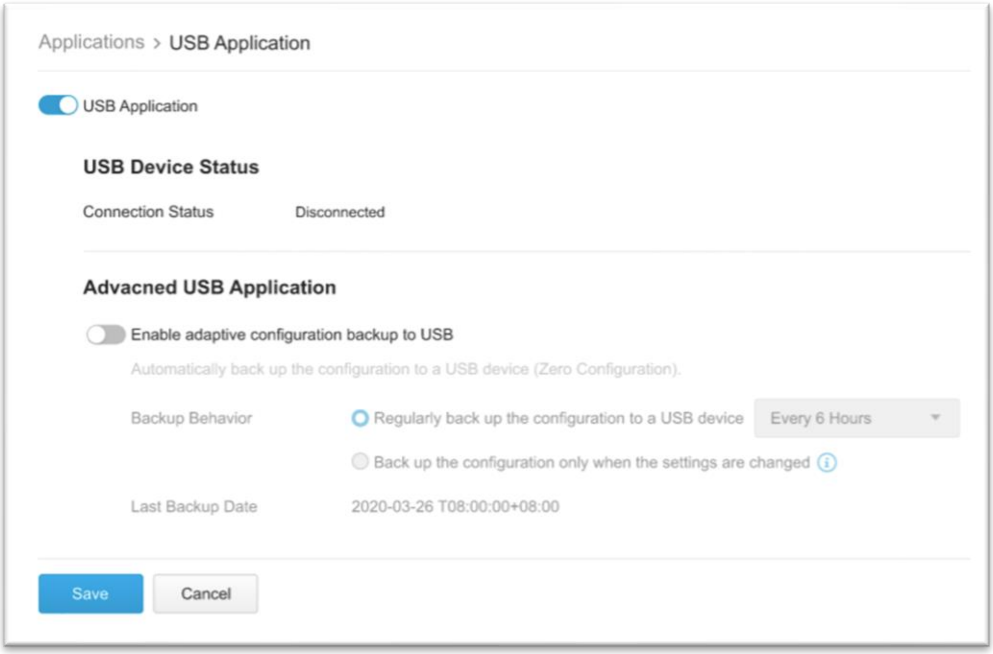
The Application Tab

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

USB Application

Procedure

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



Applications > USB Application

USB Application

USB Device Status

Connection Status Disconnected

Advacned USB Application

Enable adaptive configuration backup to USB

Automatically back up the configuration to a USB device (Zero Configuration).

Backup Behavior ○ Regularly back up the configuration to a USB device Every 6 Hours

○ Back up the configuration only when the settings are changed

Last Backup Date 2020-03-26 T08:00:00+08:00

3. Use the toggle to enable USB Application usage by enabling the USB port.
4. Once the USB Application is enabled and a USB device is plugged in, you can see its connection status.

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

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

Advanced USB Application

1. Click [Enable] to enable adaptive configuration backup for a USB-based device.
2. Back up behavior can be configured as follows:
   - Regularly backup configurations to a USB device – 5 different time periods are supported.
   - Back up configurations to a USB device only when the settings are changed.

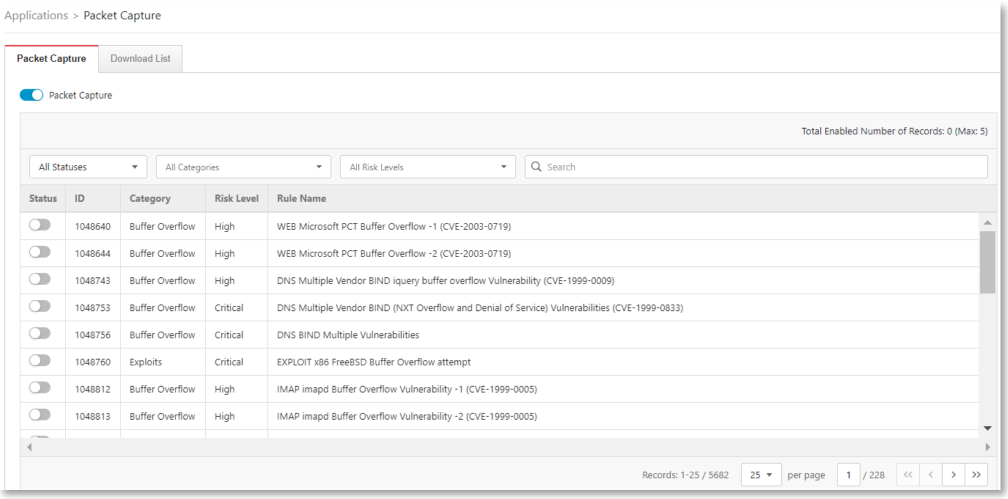
Packet Capture

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

Enabling Packet Capture

Procedure

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



Total Enabled Number of Records: 0 (Max: 5)

Status	ID	Category	Risk Level	Rule Name
○	1048640	Buffer Overflow	High	WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719)
○	1048644	Buffer Overflow	High	WEB Microsoft PCT Buffer Overflow -2 (CVE-2003-0719)
○	1048743	Buffer Overflow	High	DNS Multiple Vendor BIND iquery buffer overflow Vulnerability (CVE-1999-0009)
○	1048753	Buffer Overflow	Critical	DNS Multiple Vendor BIND (NXT Overflow and Denial of Service) Vulnerabilities (CVE-1999-0833)
○	1048756	Buffer Overflow	Critical	DNS BIND Multiple Vulnerabilities
○	1048760	Exploits	Critical	EXPLOIT x86 FreeBSD Buffer Overflow attempt
○	1048812	Buffer Overflow	High	IMAP imapd Buffer Overflow Vulnerability -1 (CVE-1999-0005)
○	1048813	Buffer Overflow	High	IMAP imapd Buffer Overflow Vulnerability -2 (CVE-1999-0005)

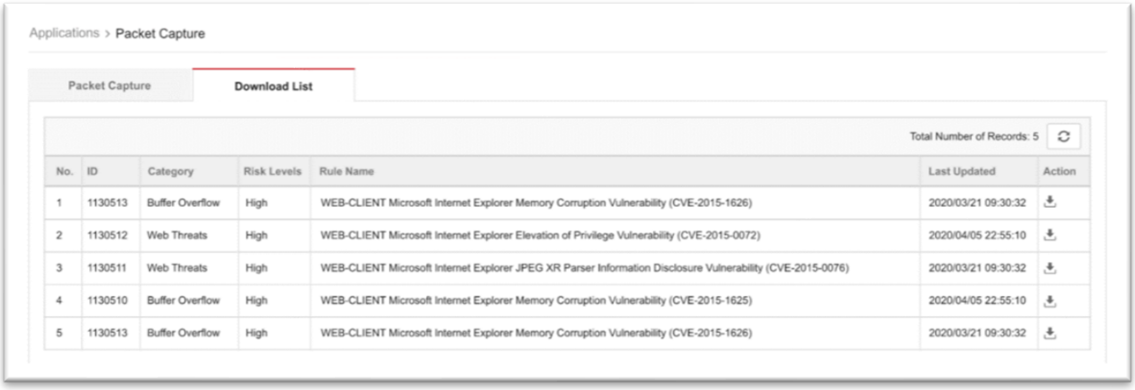
3. You can see the entire IPS rule list and select a rule to “Enable” for IPS rule capture.
4. Up to 5 IPS rules can be selected for packet capture.

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

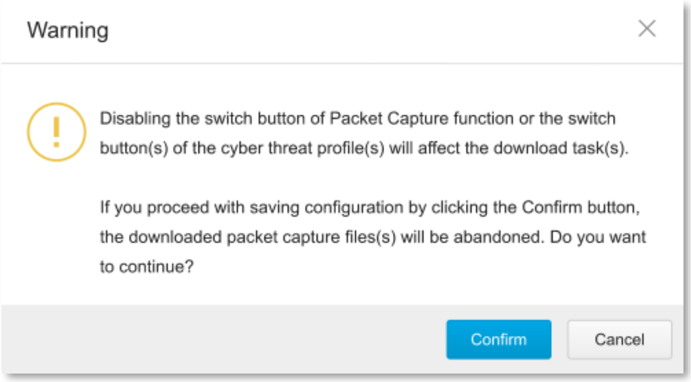
Procedure

1. Go to [Application] > [Packet Capture]
2. Click [Download List] to show a list of IPS rules.



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

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



Disabling the switch button of Packet Capture function or the switch button(s) of the cyber threat profile(s) will affect the download task(s).

If you proceed with saving configuration by clicking the Confirm button, the downloaded packet capture files(s) will be abandoned. Do you want to continue?

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

The Logs Tab

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

Note: For a list of all possible log messages and types, please refer to the document, "EdgeIPS™ / EdgeFire™ / ODC - Log Description".

You can view the following logs on EdgeFire™:

- **Cyber security logs**
- **Policy enforcement logs**
- **Protocol filter logs**
- **File filter logs**
- **Suspicious object logs**
- **Asset detection logs**
- **System logs**

Viewing Cyber Security Logs

The cyber security logs cover logs detected by denial-of service attacks.

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the rule
Profile Name	The name of the profile
Event ID	The ID of the matched signature.
TID	MITRE ID 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.
Direction	The direction flow of the connection.
Interface	The network interface which receives the connection.
Attacker	The IP address of host device which initiates the cyber attack
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The ‘source port’ of the packet, if the protocol is TCP/UDP. The ‘ICMP type’ of the packet, if the protocol is ICMP.
Destination MAC Address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The ‘destination port’ of the packet, if the protocol is TCP/UDP. The ‘ICMP code’ of the packet, if the protocol is ICMP.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.

Field	Description
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 [Advanced Filter] being enabled, i.e., the [Action] of the policy enforcement rule is either to allow or to deny.

Procedure

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

   The following table describes the log table.

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

Viewing Protocol Filter Logs

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

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule that was used to generate the log.
Profile Name	The name of the protocol filter profile that was used to generate the log.
Direction	The direction flow of the connection.
Interface	The network interface which receives the connection
Source MAC Address	The source MAC address of the connection.

Field	Description
Source IP Address	The source IP address of the connection.
Source Port	If the protocol is TCP/UDP, it indicates the source port. If the protocol is ICMP, it indicates the ICMP type.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	If the protocol is TCP/UDP, it indicates the destination port. If the protocol is ICMP, it indicates the ICMP code.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No.	The command or the function number that triggered the log.
Extra Information	Extra information provided with the log.
Action	The action performed based on the policy settings.
Count	The number of detected network packets.

Viewing File Filter Logs

The file filter logs refer to logs detected by the [File Filter] feature. 'File filter' is advanced configurations when you configure the [Policy Enforcement] settings.

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
Rule Name	The name of the policy enforcement rule set and the matched policy rule that was used to generate the log.
Profile Name	The name of the file filter profile that was used to generate the log.
Direction	Interface Direction
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	If the protocol is TCP/UDP, it indicates the source port.
Destination MAC address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Port	If the protocol is TCP/UDP, it indicates the destination port.
VLAN ID	The VLAN ID of the packet.
Protocol	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Extra Information	Extra information provided with the file filter log.
Action	The action performed based on the policy settings.

Viewing Suspicious Object Logs

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

Procedure

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

   The following table describes the log table.

Field	Description
Time	The time the log entry was created.
ID	The hash ID of the matched suspicious object.
Type	The suspicious object type, which is node type or link type.
Source	The source of suspicious object
Risk Level	The threat level of suspicious object
Expiration Time	The Expiration Time of suspicious object. When the expiration time reaches, the suspicious object will be deleted.
Direction	Interface direction
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 log table.

Field	Description
Time	The time the log entry was created.
Event Type	The log event description.
Interface	The network interface which receives the asset information.
Asset MAC Address	The MAC address of the asset.
Asset IP Address	The source IP address of the asset.

Viewing System Logs

You can view details about system events on the device.

Procedure

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

   The following table describes the log table.

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 table.

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 log in with the default "audit" account.

The Administration Tab

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

Account Management

Note: Log onto the management console using the default administrator account ("admin") to access the Account Management 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 outlines the tasks available on the [Account Management] tab.

Task	Description
Add Account(s)	Click Add to create a new user account. For more information, see *Adding a User Account on page107*.
Delete Existing Account(s)	Select the existing user account(s) and click Delete.
Edit Existing Account(s)	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 logs)	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 for the device.

Built-in 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: When you first set up the device, ensure that the passwords of the built-in accounts are changed.

Adding a User Account

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

Procedure

1. Go to [Administration] > [Account Management].
2. Click [Add].
   The Add User Account 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.
Role	Select a user role for this account. For more information, see User Roles *on page106*.
Authentication Source	Type the authentication source for this account.
Local Password	Type the account password.
Confirm Local password	Type the account password again to confirm.
Description	Add a description for this account

4. Click [Confirm].

Changing Your Password

Procedure

1. On the management console banner, click your account name.
2. Type your new password in [Local Password] field.
3. Retype your new password in [Confirm Local Password] field.
4. Click [Confirm].

Configuring Password Policy Settings

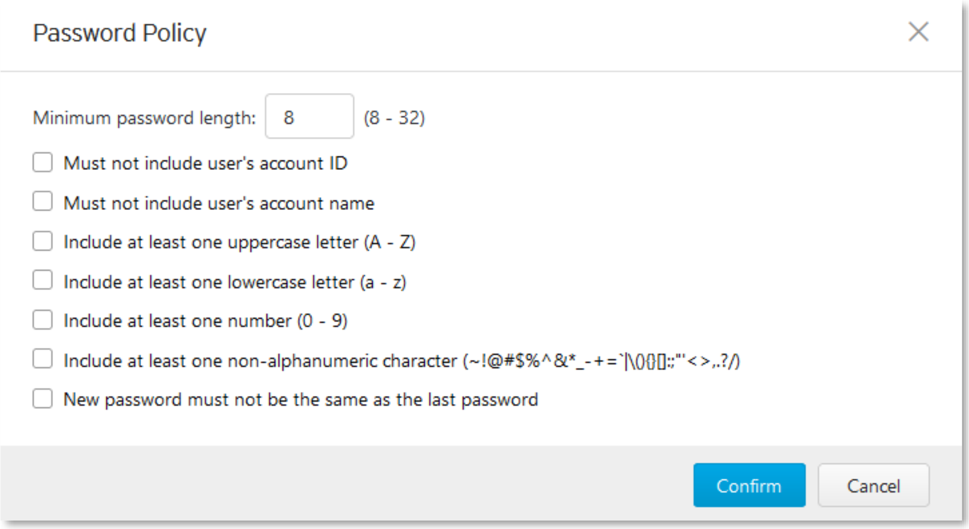
EdgeFire™ provides the following password policy settings to enhance web console access security:

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

> **Note:** When strong passwords are required and 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] window will appear.



Password Policy

Minimum password length: 8 (8 - 32)

□ Must not include user's account ID

□ Must not include user's account 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.

Auth Service

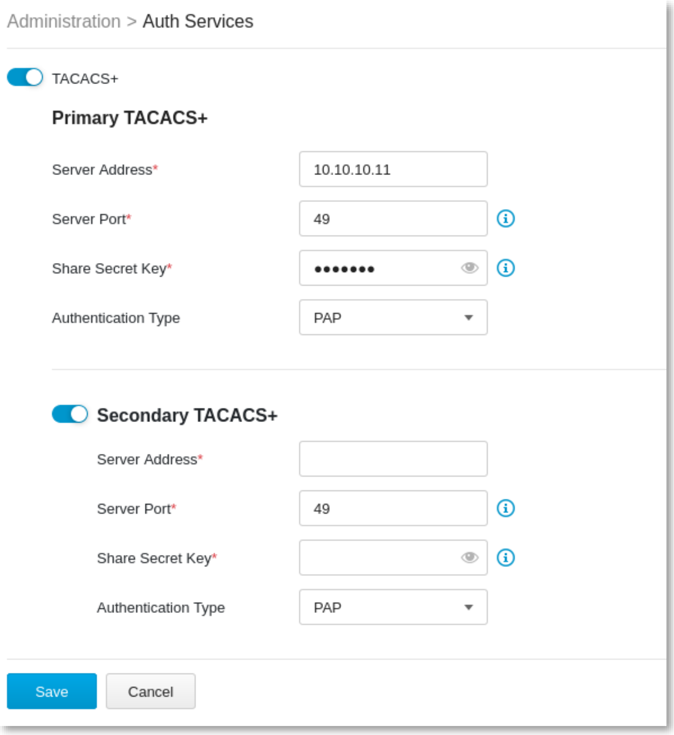
Use the [Auth Service] tab to configure the TACACS+ of the device.

Configuring TACACS+

Procedure

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

2. In the [TACACS] pane, configure the Primary and Secondary TACACS+ Servers for the device.



Administration > Auth Services

TACACS+

Primary TACACS+

Server Address*: 10.10.10.11

Server Port*: 49

Share Secret Key*: •••••••

Authentication Type: PAP

Secondary TACACS+

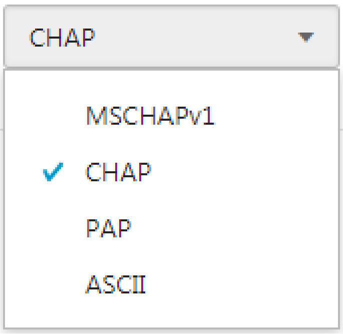
Server Address*:

Server Port*: 49

Share Secret Key*:

Authentication Type: PAP

3. Enable Primary TACACS+ and configure settings.
   - Configure the server address.
   - Configure the server port (Default port: 49).
   - Configure the shared secret key (MAX: 64 characters).
   - Select the authentication type from the list as follows:



   - Enable Secondary TACACS+ Server if you need.

System Management

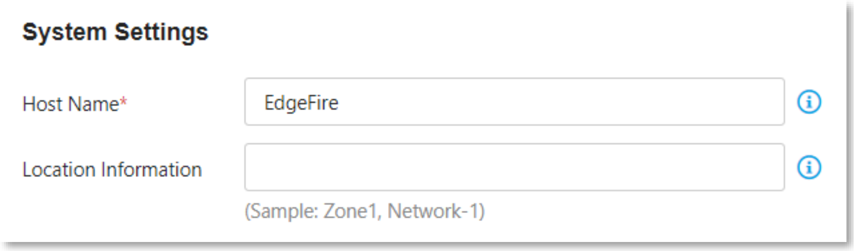
Use the [System Management] tab to do the following:

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

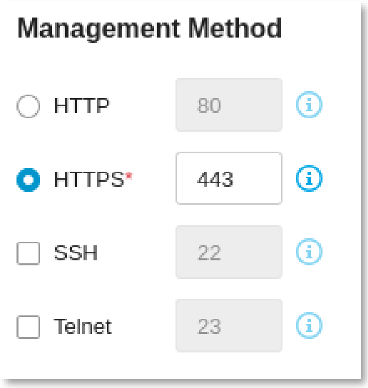
Host Name*	EdgeFire
Location Information	
	(Sample: Zone1, Network-1)

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.



Management Method

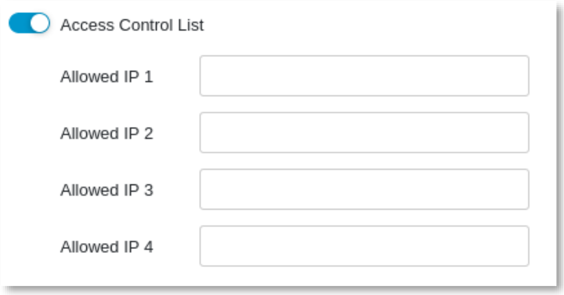
○ HTTP	80
● HTTPS*	443
□ SSH	22
□ Telnet	23

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

Configuring Access Control List from Management Clients

Procedure

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



Access Control List

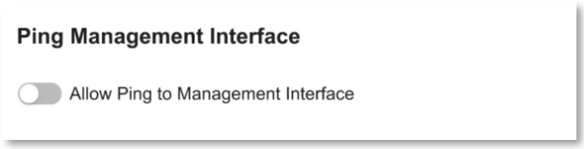
Allowed IP 1

Allowed IP 2

Allowed IP 3

Allowed IP 4

6. Check if pinging the management interface are allowed.



Ping Management Interface

Allow Ping to Management Interface

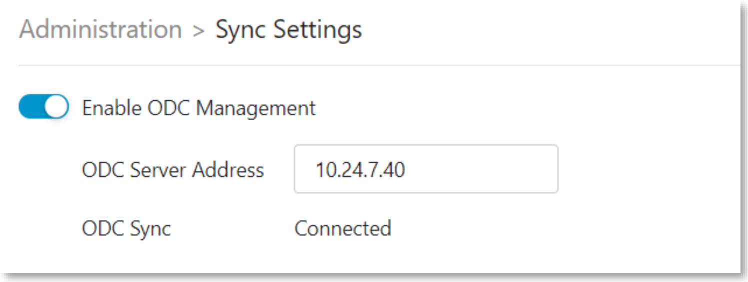
The Sync Settings Tab

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

Enabling Management by ODC

Procedure

1. Go to [Administration] > [Sync Settings].
   - Use the toggle to enable management by ODC.
   - Input the IP address of the ODC server.



Administration > Sync Settings

Enable ODC Management

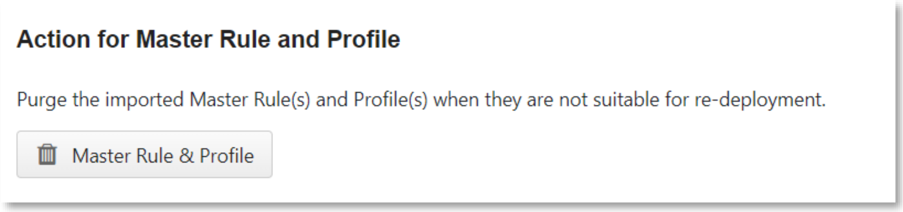
ODC Server Address 10.24.7.40

ODC Sync Connected

Action for Master Rule and Profile

Procedure

1. Go to [Administration] > [Sync Settings].
2. Click the [Master Rule & Profile] button to delete Object Profiles and Policy Enforcement rules synced from ODC



Action for Master Rule and Profile

Purge the imported Master Rule(s) and Profile(s) when they are not suitable for re-deployment.

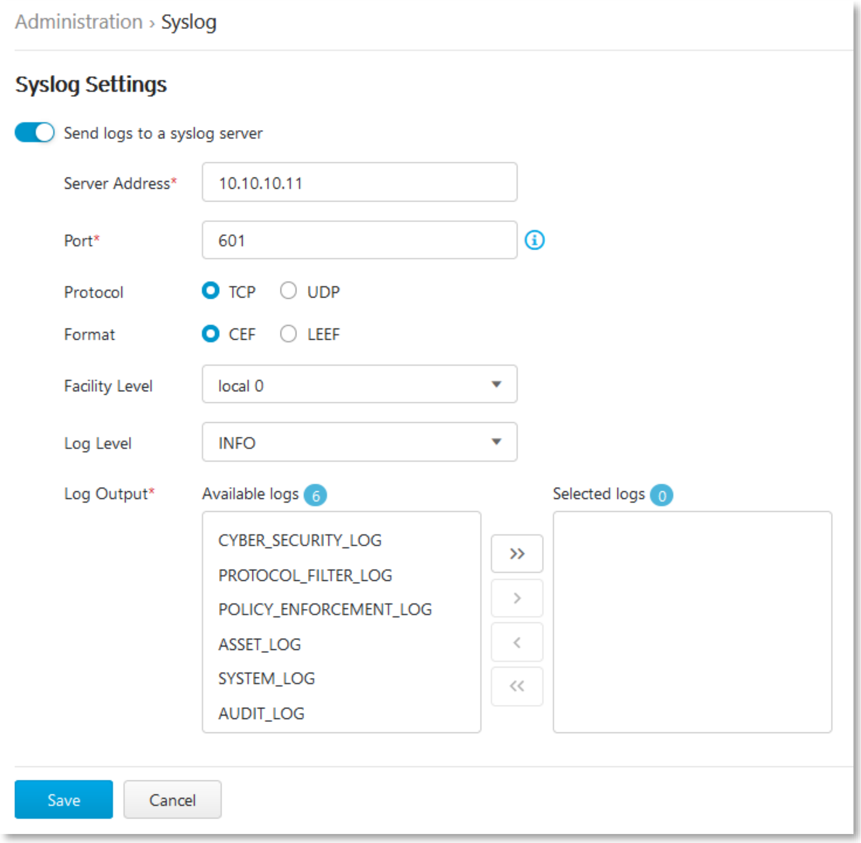
Configuring Syslog Settings

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

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

Procedure

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



Administration › Syslog

Syslog Settings

● Send logs to a syslog server

Server Address* 10.10.10.11

Port* 601

Protocol ● TCP ○ UDP

Format ● CEF ○ LEEF

Facility Level local 0

Log Level INFO

Log Output*

Available logs 6

CYBER_SECURITY_LOG
PROTOCOL_FILTER_LOG
POLICY_ENFORCEMENT_LOG
ASSET_LOG
SYSTEM_LOG
AUDIT_LOG

Selected logs 0

2. Select [Send logs to a syslog server] to set the 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. The ODC system only sends logs with the selected severity level or higher to the syslog servers. For more information, see *Syslog Severity Level Mapping Table on page 114*.

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.

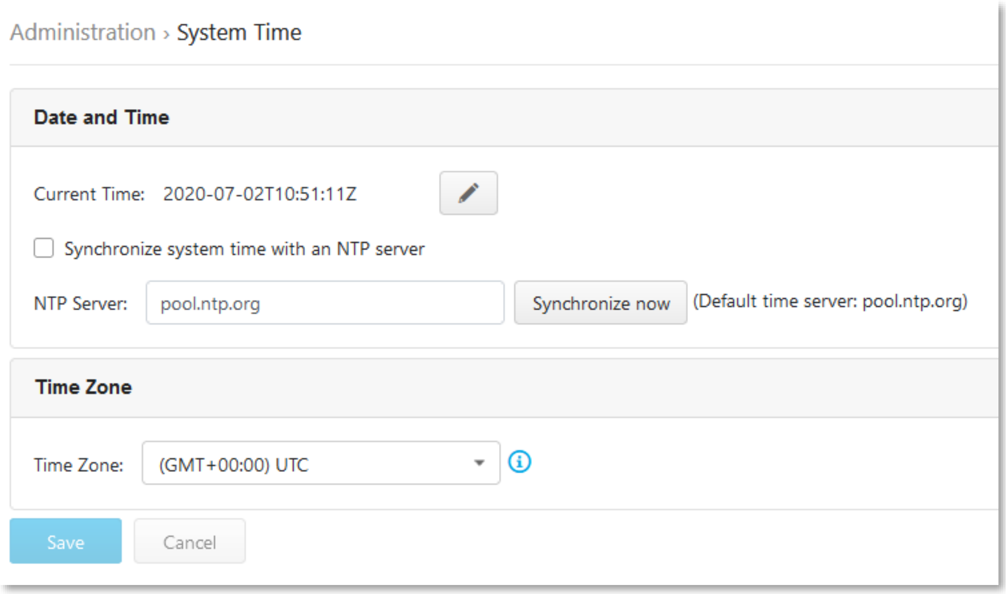
Policy Enforcement / Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
		0 - Emergency
	Critical	1 - Alert
	High	2 - Critical
		3 - Error
Deny	Medium	4 - Warning
		5 - Notice
Allow		6 - Information
		7 - Debug

Configuring System Time

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

Procedure

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



Administration › System Time

Date and Time

Current Time: 2020-07-02T10:51:11Z

□ Synchronize system time with an NTP server

NTP Server: pool.ntp.org (Default time server: pool.ntp.org)

Time Zone

Time Zone: (GMT+00:00) UTC

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

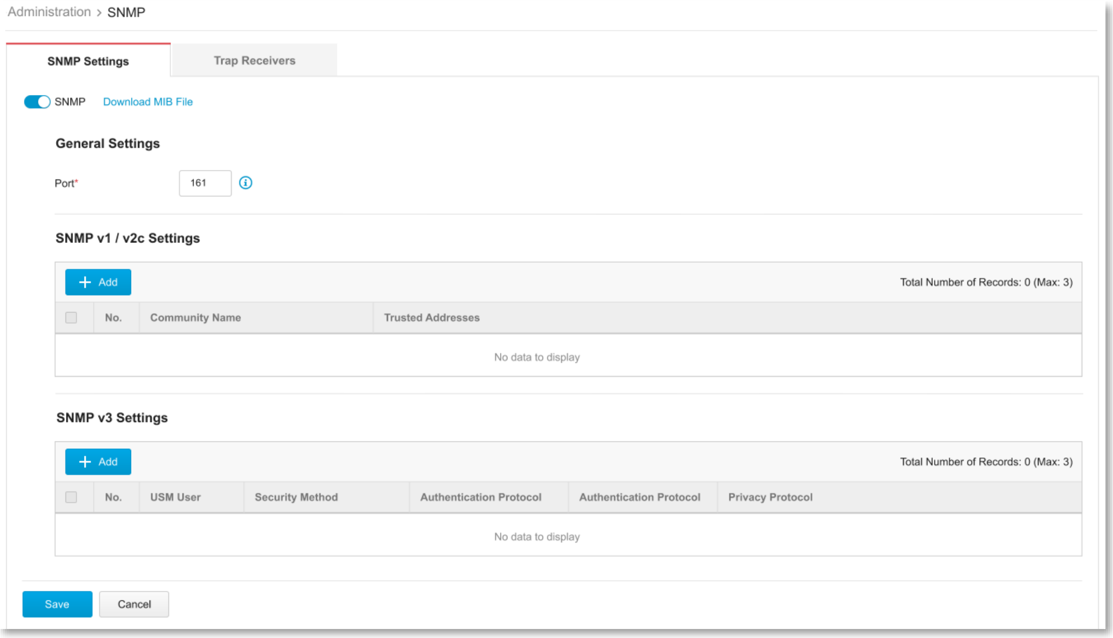
The SNMP Tab

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

Procedure

1. Go to [Administration] > [SNMP]
2. Click [Enable] to enable SNMP functionality.
3. Under General settings, you can change the SNMP port. The default setting is Port 161.

4. You can click the "Download MIB file" link to download the EdgeFire™'s MIB file.



Administration › SNMP

SNMP Settings | Trap Receivers

SNMP   Download MIB File

General Settings

Port* 161

SNMP v1 / v2c Settings

Total Number of Records: 0 (Max: 3)

□	No.	Community Name	Trusted Addresses
		No data to display	

SNMP v3 Settings

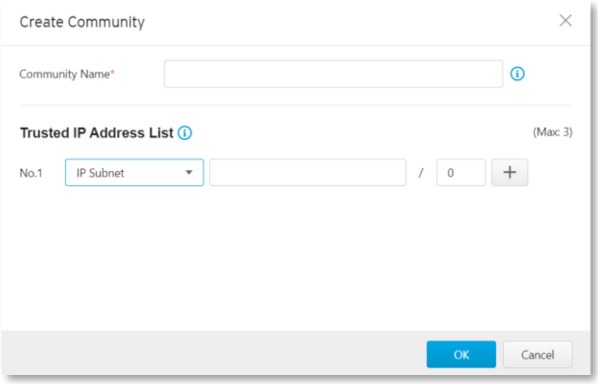
Total Number of Records: 0 (Max: 3)

□	No.	USM User	Security Method	Authentication Protocol	Authentication Protocol	Privacy Protocol
			No data to display			

Configuring SNMP v1/v2c

Procedure

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



Create Community

Community Name*

Trusted IP Address List (Max: 3)

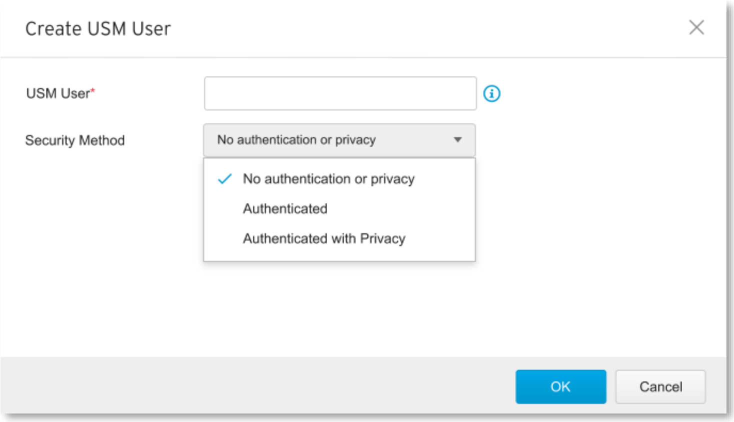
No.1   IP Subnet ▾   /   0   +

- 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 SNMP v3 settings.



Create USM User

USM User*

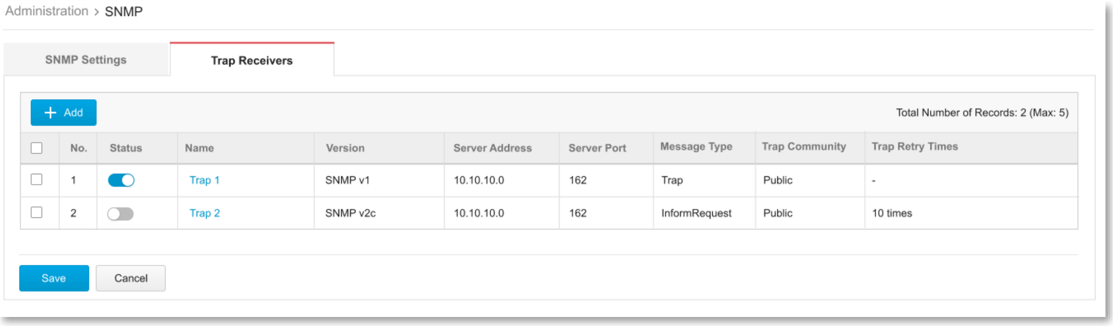
Security Method: No authentication or privacy

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

Configuring SNMP Trap Receivers

Procedure

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



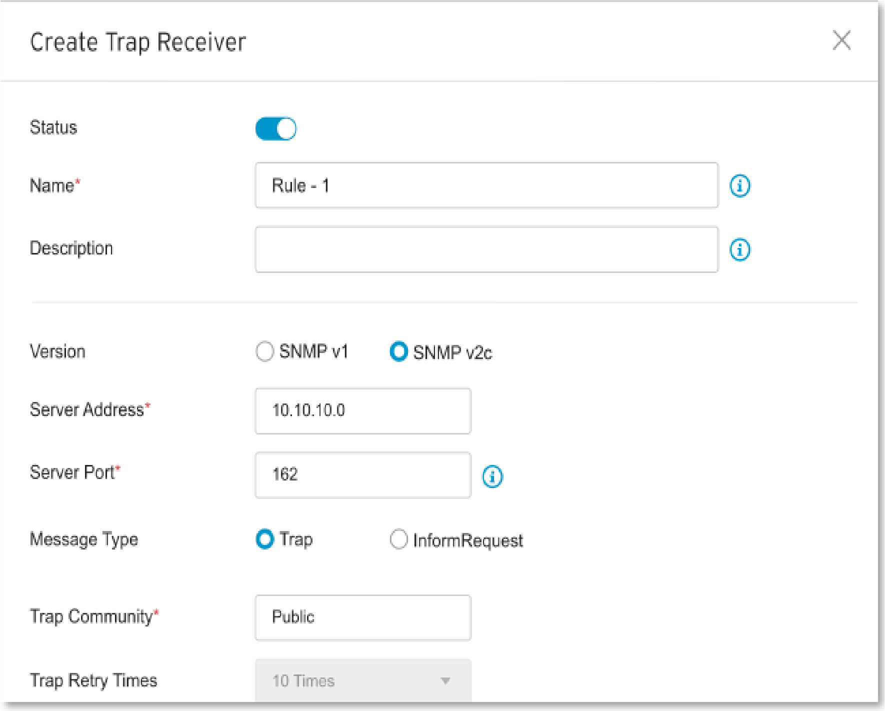
Administration › SNMP

Total Number of Records: 2 (Max: 5)

□	No.	Status	Name	Version	Server Address	Server Port	Message Type	Trap Community	Trap Retry Times
□	1	●	Trap 1	SNMP v1	10.10.10.0	162	Trap	Public	-
□	2	○	Trap 2	SNMP v2c	10.10.10.0	162	InformRequest	Public	10 times

3. Click [Add] to create a new Trap Receiver.
   - Use the toggle of [Status] to enable a Trap Receiver.
   - Enter [Name] for a Trap Receiver.
   - Add [Description] if necessary.
   - Select SNMP version: SNMP v1 or SNMP v2c
   - Enter [Server Address].
   - Enter [Server Port]. The default server port is 162.
   - Select message type: “Trap” or “informRequest”.
   - Enter [Trap Community]. The default name is PUBLIC.

- Set [Trap Retry Times] to an amount of retries, ranging from 1-10 times.



Create Trap Receiver

Status: on

Name*: Rule - 1

Description:

Version: ○ SNMP v1 ● SNMP v2c

Server Address*: 10.10.10.0

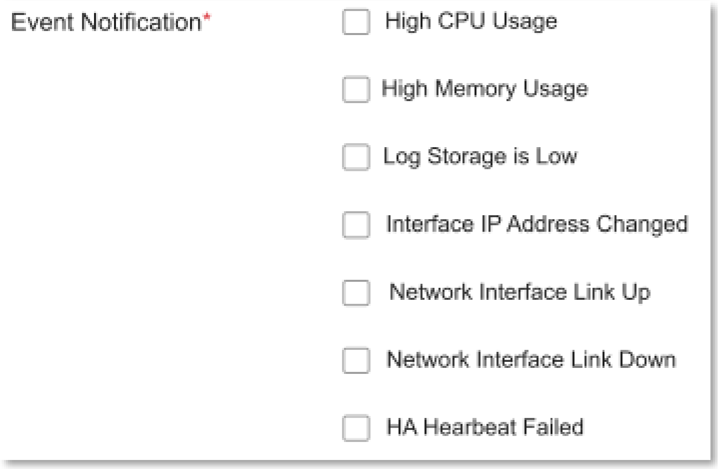
Server Port*: 162

Message Type: ● Trap ○ InformRequest

Trap Community*: Public

Trap Retry Times: 10 Times

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



Event Notification*

□ High CPU Usage

□ High Memory Usage

□ Log Storage is Low

□ Interface IP Address Changed

□ Network Interface Link Up

□ Network Interface Link Down

□ HA Hearbeat Failed

The Back Up / Restore Tab

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

We recommend the following:

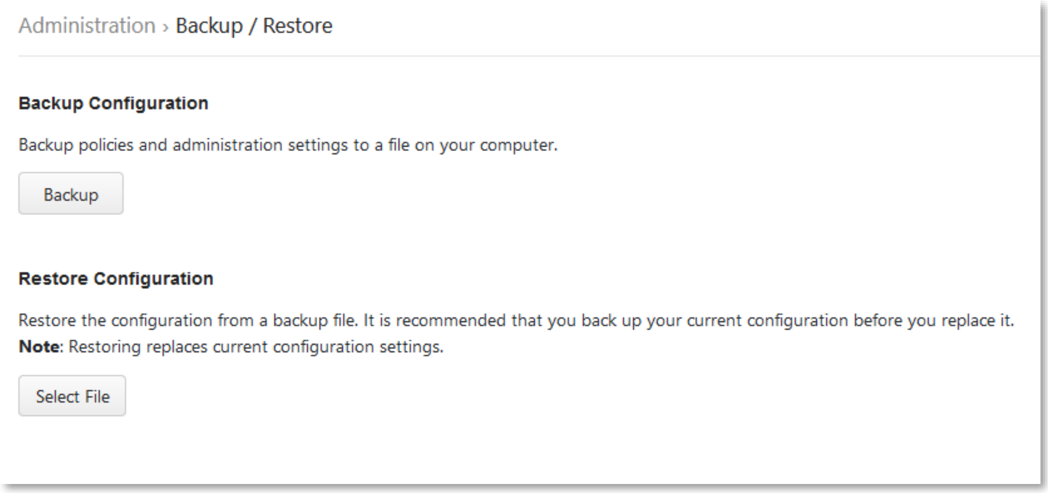
- Backing up the current configuration before each import operation.
- Performing the operation when the EdgeFire™ is idle. Importing and exporting configuration settings affects the performance of EdgeFire™.

Backing Up a Configuration

Procedure

1. Go to [Administration] > [Back Up / Restore].

   The [Back Up / Restore] tab will appear.



Administration › Backup / Restore

Backup Configuration

Backup 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 to restore the configurations of the EdgeFire™.

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:

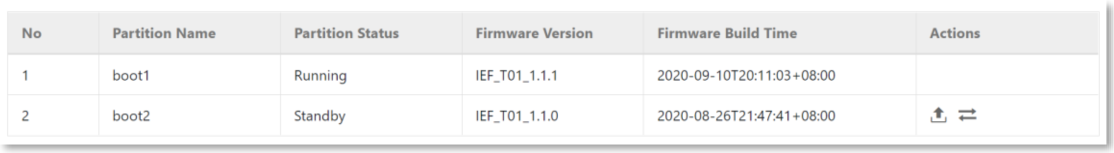
- View the firmware information of the device
- Upgrade the firmware of the device
- Boot into standby partition and firmware

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 Date].

Note: All Edge Series devices 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.



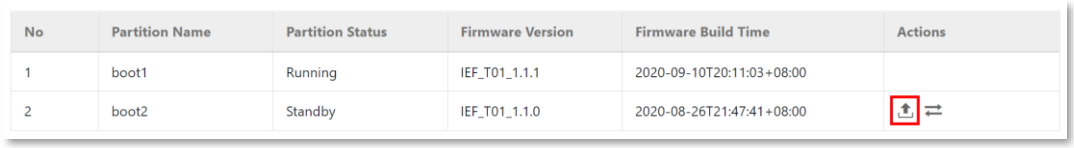
No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IEF_T01_1.1.1	2020-09-10T20:11:03+08:00	
2	boot2	Standby	IEF_T01_1.1.0	2020-08-26T21:47:41+08:00	⇧ ⇄

Updating Firmware

Procedure

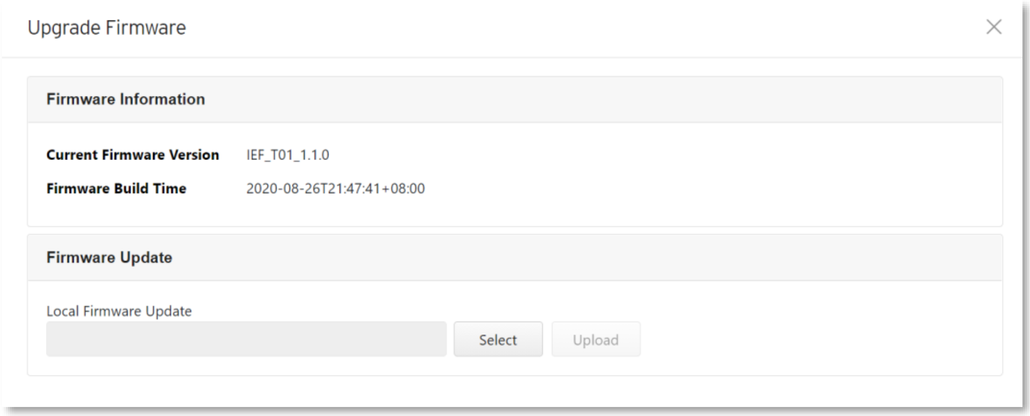
1. Go to [Administration] > [Firmware Management].

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.



No	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	boot1	Running	IEF_T01_1.1.1	2020-09-10T20:11:03+08:00	
2	boot2	Standby	IEF_T01_1.1.0	2020-08-26T21:47:41+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 [Standby Partition].



Upgrade Firmware

Firmware Information

Current Firmware Version IEF_T01_1.1.0

Firmware Build Time 2020-08-26T21:47:41+08:00

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.

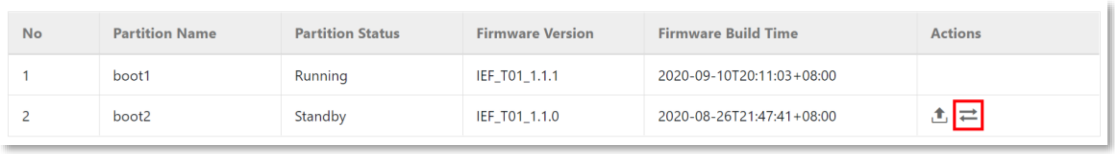
Note: Various versions of the firmware can be downloaded at the Trend Micro Download Center at https://www.trendmicro.com/en_us/business/products/downloads.html

Rebooting and Applying Firmware

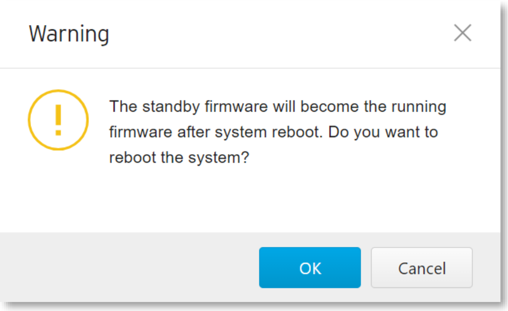
To boot into an upgraded firmware or to revert to a previous firmware, a user may need to boot into the [Standby] partition and load the firmware from it.

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	IEF_T01_1.1.1	2020-09-10T20:11:03+08:00	
2	boot2	Standby	IEF_T01_1.1.0	2020-08-26T21:47:41+08:00	⇧ ⇄



Warning

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

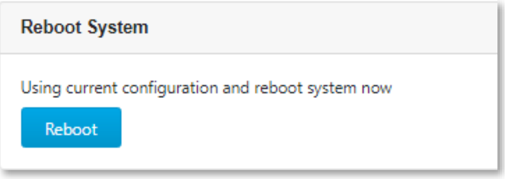
3. Click [OK] to proceed with rebooting into the [Standby] partition and making it the [Running] partition.

Reboot System

Use the [Reboot System] tab to reboot 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 EdgeFire™ 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
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

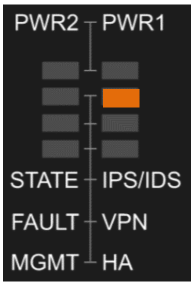
1. On-demand configuration for disk backup
2. Load pattern from disk
3. Load configuration from disk
4. Load firmware from disk

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

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

To perform any of these actions:

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



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

The functionality of the reset button will also change until the USB device is unplugged. The reset button will at this time not serve the as the reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken when a USB device is plugged in.

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

Possible Actions to Toggle Through

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

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

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

3. 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

	IPS/IDS LED	Amber – Blinking (Once every 0.5 sec)

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

Error Indication (on any error while action was being processed)	LED	COLOUR/STATE
	FAULT LED	Red – Steady

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

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

On-demand Configuration backup

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

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

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

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

Load Pattern from Disk

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

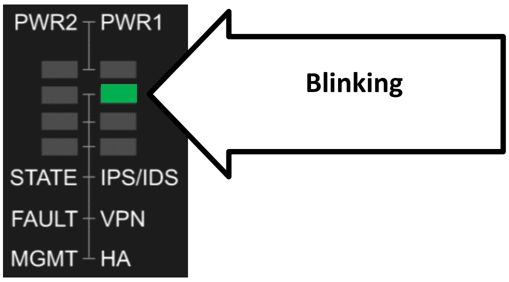
1. Save the pattern file in a USB disk device under path "**/TXone/pattern/**". Assuming a pattern file has the name pattern.acf, its file path on the USB disk device would be "**/TXone/pattern/pattern.acf**".

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

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

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

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



5. The "Load Pattern" action must now be confirmed by holding down the reset button for more than 3 seconds.
6. After confirmation, the selected action will be attempted. If successful, the USB app will return to the "Default Action" state. If any errors occur, the FAULT LED will turn red.

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

Load Configuration from Disk

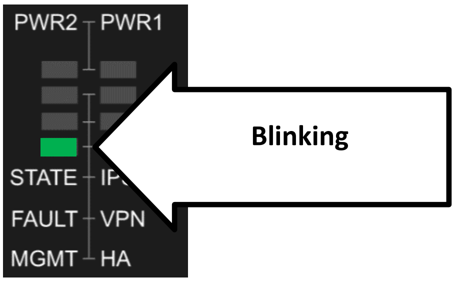
A configuration file may be easily and quickly loaded via a USB disk device. This functionality allows for a floor operator to update/restore the configuration on the physical floor of the ICS environment without the need of a client computer to log into the device.

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

Note: Saving config files under other paths or incorrect folder names will cause the file to not be detected during the pattern load process. Folder names are case-insensitive.

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

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



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

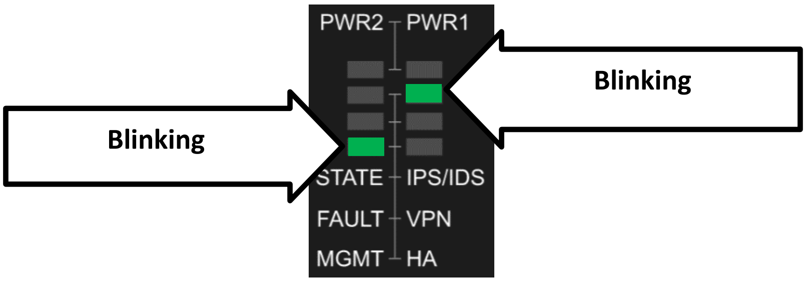
Load Firmware from Disk

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

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

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

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



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

Note: Latest versions of the firmware files can be downloaded from 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	Comment 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