EdgeIPS Pro 732

Administrator's Guide

Version 2.2

September 25, 2025

Copyright © 2025 TXOne Networks Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of TXOne Networks Incorporated.

TXOne Networks 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 at https://my.txone.com.

TXOne Networks is a registered trademark of TXOne Networks Incorporated. All other product names may be trademarks or registered trademarks of their owners.

In order to protect the value of TXOne Networks' logos and marks, it is very important that they be used appropriately and only by TXOne Networks and Partners with a current and valid partnership agreement.

The following marks are owned exclusively by TXOne Networks and may be registered in the U.S. or other countries. TXOne Networks reserves the right in its sole discretion to add additional marks to or remove marks from this list at any time and the failure of a TXOne trademark or logo to appear on this list shall not be construed as a waiver of any of TXOne Networks' rights in such trademark or logo.

- EdgeIPS
- EdgeIPS Pro
- EdgeIPS LE
- EdgeFire
- EdgeOne
- OT Defense Console

Trademark ownership is attributed in two ways, with the use of a trademark symbol (such as ™ or ®) after the trademark, and with a trademark legend, usually found at the end of a document in legible text following the copyright notice. Whenever you use one of TXOne trademarks, you must also include a proper trademark attribution statement somewhere on the same document or webpage, such as the following: "The TXOne Networks® and EdgeIPS™ trademarks are owned by TXOne Networks, Inc. and is used with permission." Remember, mere inclusion of a trademark symbol and legend does not entitle you to use a TXOne trademark.

Data Security Warning

Before removing and disposing of this product, ensure all data and configurations stored on the device are erased. You can do this by:

- manually resetting the product to factory settings, or
- handing the product to the TXOne support team, who will help you clear all stored data and configurations.

TXOne Support Team Contact Information

- Email: support@txone.com
- Website: https://www.txone.com/
- Call Center: https://help.txone.com/
- Phone:
  - US: +1 3465867975
  - Netherland: +31 402310122
  - Taiwan: +886 27727512

Table of Contents

1 About EdgeIPS Pro 732 5
1.1 Introduction to EdgeIPS Pro 732 5
1.2 Main Functions of EdgeIPS Pro 732 6

2 Getting Started 9
2.1 Getting Started Task List 9
2.2 Opening the Management Console 10

3 Visibility 13
3.1 Dashboard 13
3.1.1 System Dashboard 13
3.2 OT Visibility 18
3.2.1 Asset View 18

4 Device 31
4.1 Network & Ports 31
4.1.1 Network Settings 31
4.1.2 HA Settings 34
4.1.3 Port Mirroring 36
4.1.4 Port Settings 38

5 Objects & Profiles 40
5.1 IP/MAC/Service Objects 41
5.1.1 IP Objects 41
5.1.2 MAC Objects 42
5.1.3 Service Objects 43
5.2 Security Profiles 45
5.2.1 Protocol Filter Profiles 45
5.2.2 IPS Profiles 82
5.2.3 File Filter Profiles 85
5.2.4 Domain Name Profiles 90
5.2.5 Antivirus Profiles 91
5.3 Edge DPI Engine 96
5.3.1 Protocol Service Port Profiles 97

6 Security 99
6.1 General Settings 99
6.1.1 Deny Action Setting 99
6.2 Security Policies 99
6.2.1 L2 Policy Enforcement 100
6.2.2 Policy Enforcement 106
6.2.3 Policy Rule Auto-Learning 113
6.2.4 Port Security 122
6.2.5 Domain Name Filter Rules 128
6.2.6 Suspicious Objects 136
6.3 CPSDR Policies 137
6.3.1 CPSDR Rules 137
6.3.2 CPSDR Allow Lists & Alert Lists 140

7 Patterns 143
7.1 Pattern Updates 143
7.1.1 Security Patterns 143
7.1.2 CPSDR Patterns 145

8 Applications 147
8.1 Backup Storage 147
8.1.1 USB Disk Storage 147
8.2 Cyber Forensic Tools 149
8.2.1 IPS Event Packet Capture 149
8.2.2 Captured Packet Downloads 151
8.2.3 Pcap File Server Settings 151
8.3 Diagnostics 154
8.3.1 Hardware Diagnostics 154

9 QoS 158
9.1 Quality of Service 158
9.1.1 Bandwidth Management 158

10 Logs 160
10.1 Security Logs 160
10.1.1 Cyber Security Logs 160
10.1.2 Policy Enforcement Logs 163
10.1.3 Protocol Filter Logs 164
10.1.4 Domain Name Filter Logs 165
10.1.5 File Filter & Antivirus Logs 166
10.1.6 Suspicious Object Logs 168
10.1.7 CPSDR Logs 169
10.2 System Logs 170
10.2.1 Asset Detection Logs 171
10.2.2 System Event Logs 171
10.2.3 Audit Logs 172

11 Admin 173
11.1 Accounts 173
11.1.1 Account Management 173
11.1.2 Logout Timer 180
11.1.3 Auth Services 181
11.2 Notifications 184
11.2.1 SNMP 184
11.2.2 Syslog 189
11.3 Licensing & Updates 192
11.3.1 License Management 192
11.3.2 Firmware Updates & Management 198
11.4 System 200
11.4.1 System Management 200
11.4.2 Edge Device Security 204
11.4.3 EdgeOne Connection Settings 205
11.4.4 Language Package 207
11.4.5 API Management 208
11.4.6 SSL Certificate 211
11.4.7 Backup/Restore 214
11.4.8 System Time 216
11.4.9 System Reboot 217

12 Extended Functions via Supported USB Device 219
12.1 Backing Up Configuration 219
12.2 Loading Pattern from USB Device 221
12.3 Loading Configuration from USB Device 223
12.4 Loading Firmware from USB Device 225

13 Technical Support 228
13.1 Troubleshooting Resources 228
13.1.1 Help Center 228
13.1.2 Threat Encyclopedia 228
13.2 Contacting TXOne 228
13.2.1 Expediting Support Call 229
13.3 Other Resources 229
13.3.1 MyTXOne Portal 229
13.3.2 Documentation Feedback 229

14 Appendix A: Terms and Acronyms 230

1 About EdgeIPS Pro 732

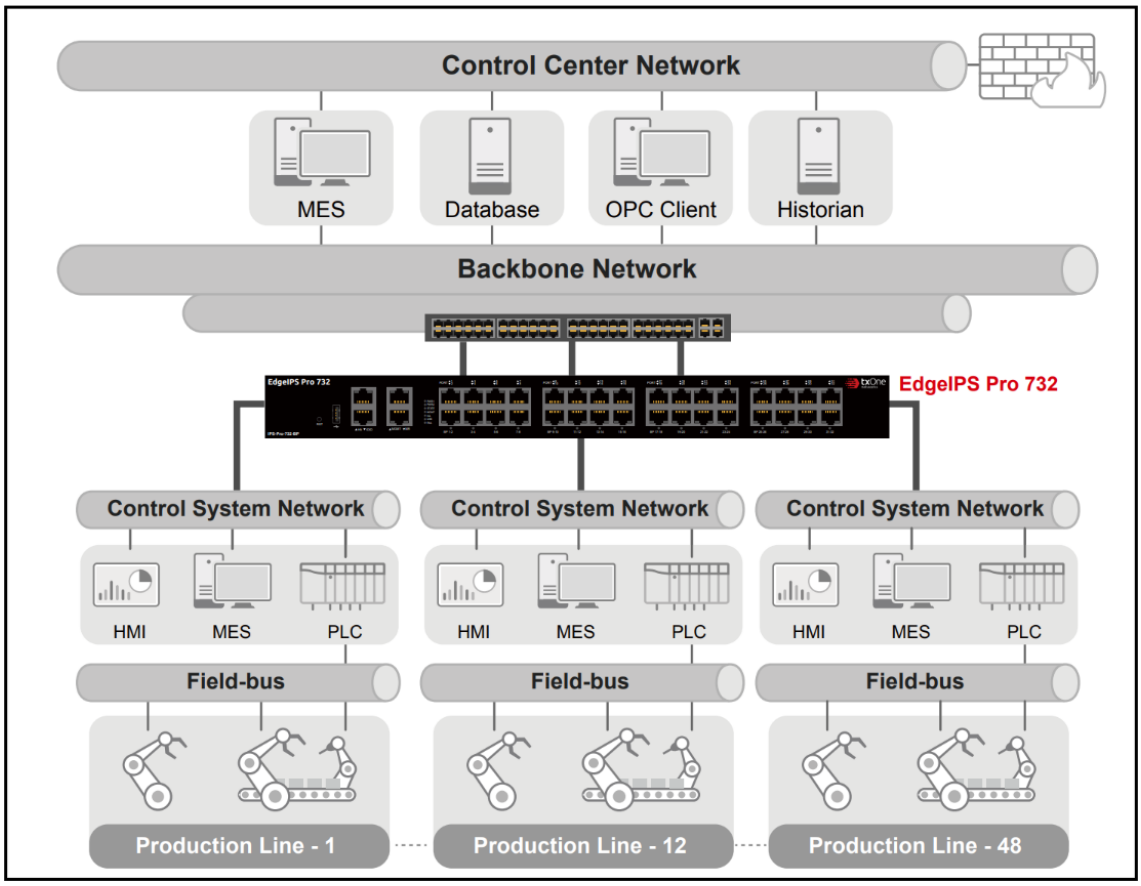
1.1 Introduction to EdgeIPS Pro 732

EdgeIPS Pro 732 is a purpose-built appliance, set up for friendly, rack-mounted deployment and equipped with in-depth OT protocol filtering to enable administrators to easily manage micro-segmentation for a complex environment. Created using the solid ICS security building block EdgeIPS, it is built from the ground up to isolate and protect multi-segment networks. This security solution is designed specifically to fit transparently into the IT/OT convergence network environment.

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

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

- Threat detection and interception, with safeguards against the spread of worms
- Protection against Advanced Persistent Threats (APTs) and Denial of Service (DoS) attacks that target vulnerable legacy devices
- Virtual patch protection against OT device exploits
- High availability with fail-safe multi-segmenting
- Flexible Universal Bypass and Logical Port Pair (LAG) modes for enhanced data transmission reliability and efficiency



1.2 Main Functions of EdgeIPS Pro 732

EdgeIPS Pro 732 is a transparent network security appliance. The main functions of this Edge series device are as follows:

Multi-Segmenting with Integrated Security

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

High Port Density and Flexible Deployment

The device comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant visibility of your shadow OT environment. Besides, it supports up to 16 segments and can flexibly switch between 'Monitor' and 'Prevention' modes. 'Monitor' mode will log traffic without interfering, while 'Prevention' mode will filter traffic based on policies you create. These modes work together to preserve your productivity while maximizing security.

Universal Bypass and Logical Port Pair (LAG) Pair Modes

The device's pair modes, Universal Bypass and Logical Port Pair (LAG), are designed specifically to enhance the efficiency and reliability of the data transmission within your production networks. When the device is in Universal Bypass mode, two port pairs are combined to ensure uninterrupted uplink transmission. In case of any uplink disconnection on the original uplink port, communications traffic can be rapidly directed to the spare port without disrupting the operation. When the device is in Logical Port Pair (LAG) mode, two or four port pairs are combined to increase the data transmission bandwidth for faster transfer speeds and enhanced network performance.

Extensive Support for Industrial Protocols

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

Policy Enforcement for Mission-Critical Machines

The device's core technology TXODI (One-pass Deep Packet Inspection for Industrial) allows administrators to maintain a Policy Enforcement database. By analyzing Layer 2 to Layer 7 network traffic between mission-critical production machines, Policy Enforcement executes filtering of control commands within the protocols and blocks traffic that is not defined in the policy rules. This feature can help prevent unexpected operational traffic, block unknown network attacks, and block other activities that match defined policy rules.

Intelligence Learning and Rule Generation for Daily Network Traffic

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

Improve Shadow OT Visibility by Integrating IT and OT Networks

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

Intrusion Prevention and Intrusion Detection

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

Cyber-Physical System Detection and Response

The device is equipped with TXOne's pioneering CPSDR (Cyber-Physical System Detection and Response) technology, designed to identify and predict anomalous network behaviors early on. With the CPSDR, your OT network can proactively stay a step ahead of cyber risks, blocking potential threats before they materialize.

Antivirus Protection

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

Top Threat Intelligence and Analytics

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

Easily Centralized Management with Convenient, Consolidated Overview

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

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

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

2 Getting Started

This chapter guides you on how to get started with EdgeIPS Pro 732 and configure the initial settings.

> For an overview of the physical hardware and characteristics, or a more condensed manual to help with initial setup of the device, please refer to the document ***EdgeIPS Pro 732 - Quick Setup Guide***.

2.1 Getting Started Task List

This task list provides a high-level overview of all procedures required to get EdgeIPS Pro 732 up and running as quickly as possible. Each step links to more detailed instructions found later in the document.

Procedure

1. Open the management console.

> For more information, see Opening the Management Console.

2. Change the administrator account ID and password.

> For more information, see *Changing Your Account ID/Password*.

3. Configure the system time.

> For more information, see Configuring System Time.

4. (Optional) Configure the Syslog settings.

> For more information, see Configuring Syslog Settings.

5. Configure objects and profiles.

> For more information, see Objects & Profiles.

6. Configure security policies.

> For more information, see Security Policies.

7. Configure the device name and location.

> For more information, see *Configuring Device Name and Location*.

8. (Optional) Configure the device access control list.

> For more information, see Configuring Access Control List.

9. (Optional) Configure management protocols and ports.

> For more information, see Configuring Management Protocols and Ports.

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

> For more information, see Updating IPS and Antivirus Patterns.

11. (Optional) Enable EdgeOne Management settings.

> For more information, see Enabling EdgeOne Management.

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

For more information, see Device.

13. (Optional) Configure password policy.

For more information, see Configuring Password Policy.

2.2 Opening the Management Console

We provide a built-in management console that you can use to configure and manage this Edge series device. View the management console using a web browser.

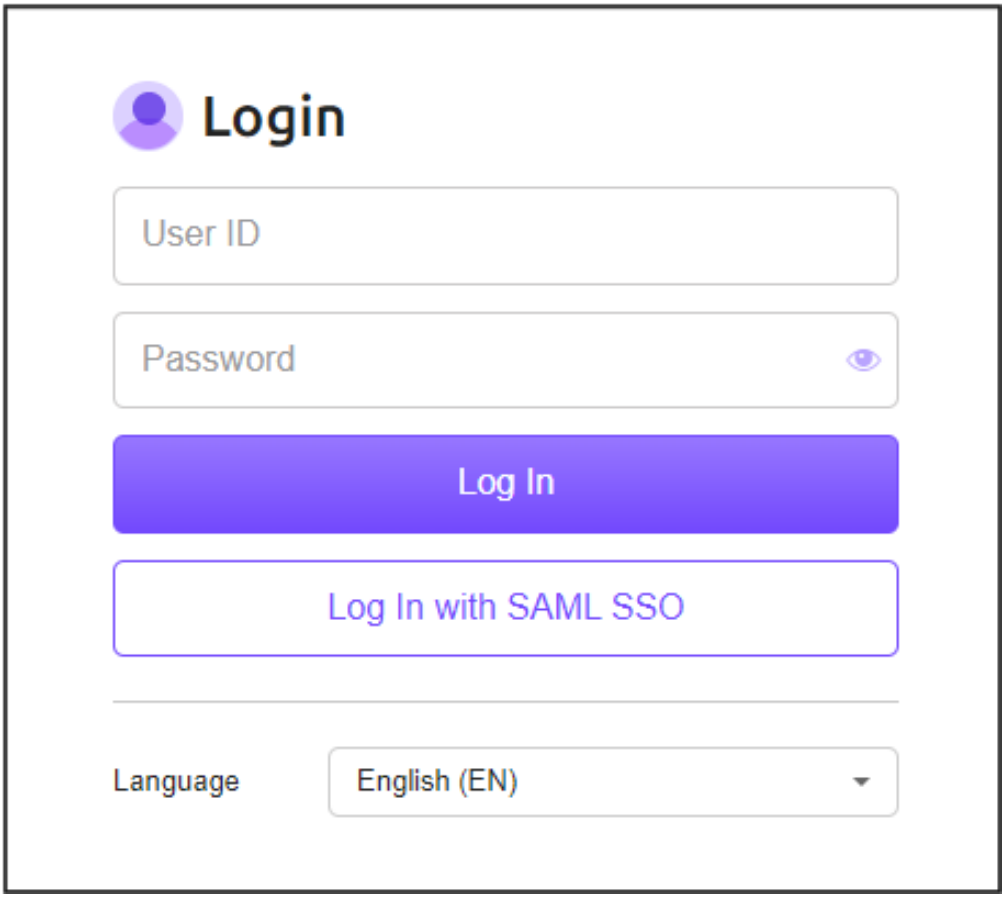
View the management console using Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; Edge version 15 or later.

Procedure

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

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

The login page will appear.



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

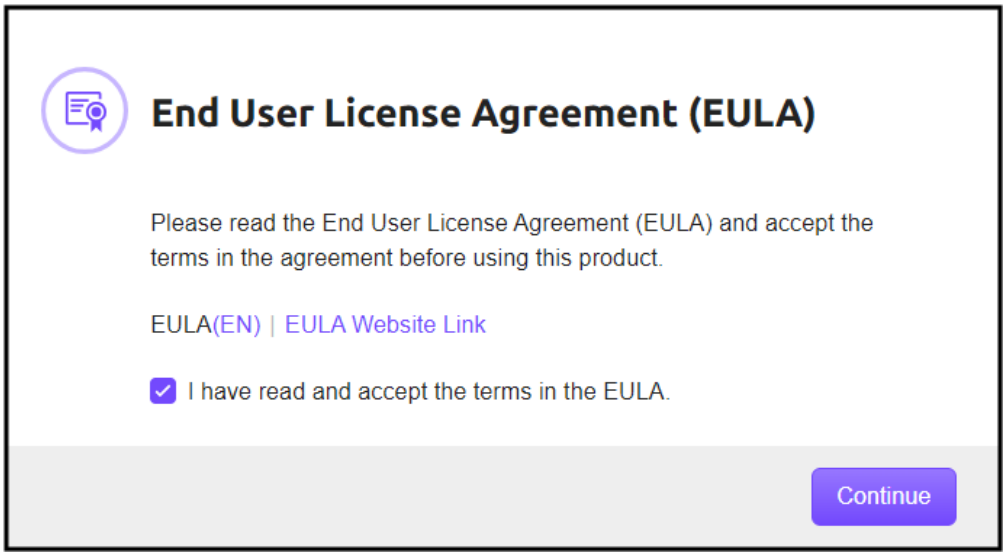
	2. TXOne products use an automatically generated self-signed SSL certificate to encrypt communications to and from the client accessing the device. Given that the certificate is self-signed, most browsers will not trust the certificate and will give a warning that the certificate being used is not signed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

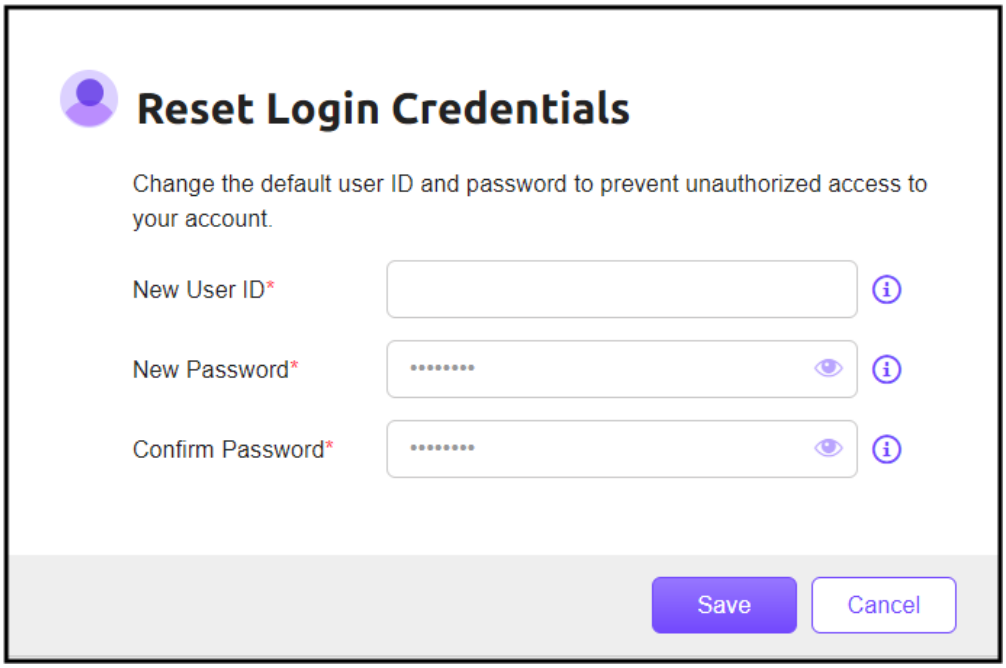
2. Input your login credentials (user ID and password). Use the default administrator credentials when logging in for the first time.

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

3. Click [Log In].

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





⚠️	1. You must change the default login name and password at your first login before you can access the management console.

	2. New login name cannot be "root", "admin", "administrator" or "auditor" (case-insensitive). 3. For enhanced security, consider using a strong password with at least 12 characters that consists of both uppercase and lowercase letters, numbers, and symbols. Avoid using common words or personal information.

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

3 Visibility

This chapter describes the visibility-related features designed to provide comprehensive insights into your OT network.

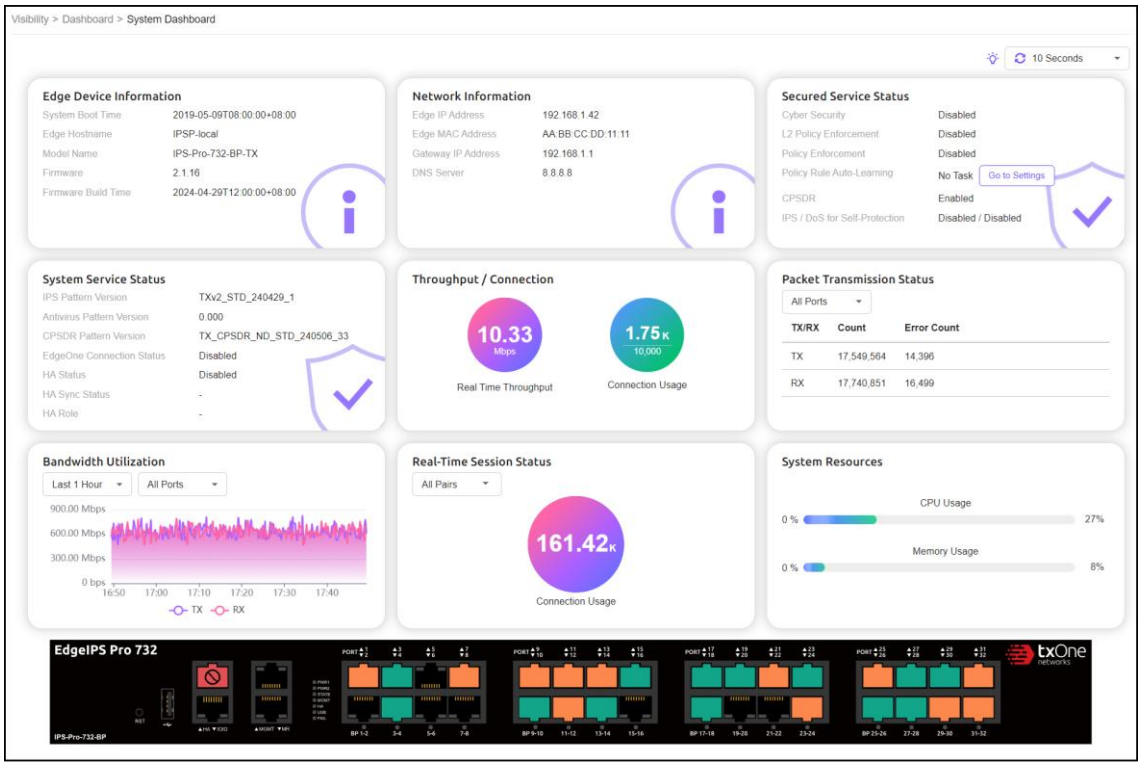
3.1 Dashboard

Monitor and analyze your assets, devices, network status, and threat detection.

- System Dashboard

3.1.1 System Dashboard

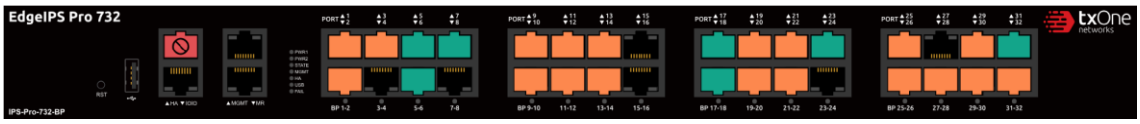
Monitor the EdgeIPS Pro 732 device information, network information, secured service status, system service status, throughput/connection, bandwidth utilization, real-time session status, packet transmission status, and system resources on the system dashboard.



3.1.1.1 Viewing System Dashboard

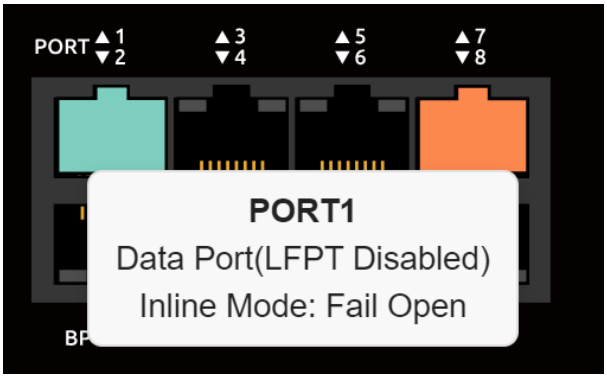
Device Panel

At the bottom of the page, you may view the device panel and the status of each port.



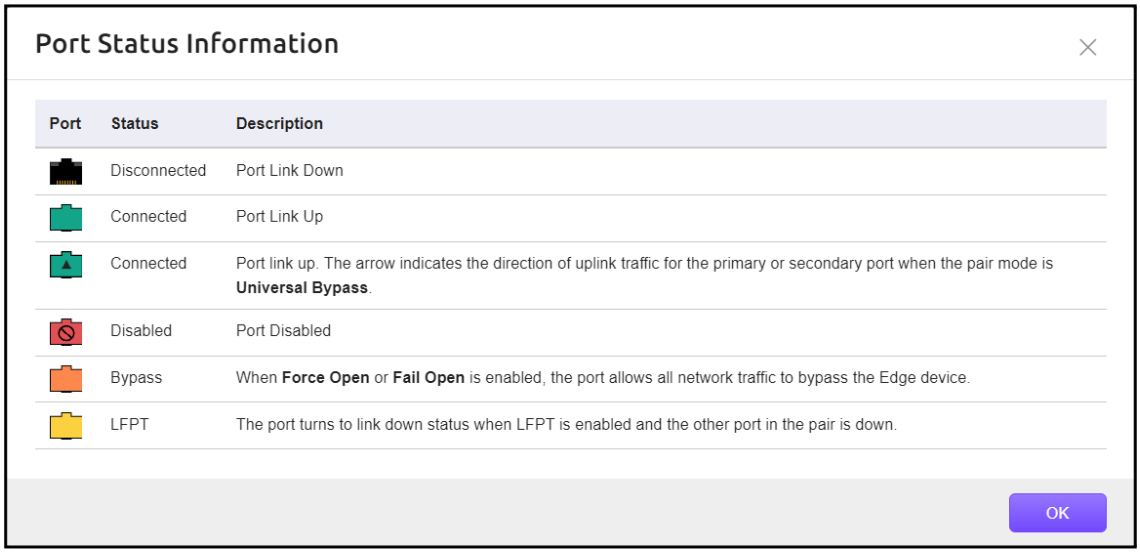
> The panel view on the page shows a graphical depiction of the connected ports on the device.

Hover your mouse over a port on the device panel to view details of the port.



Port Status Information

In the upper right corner, you may view the port status information by clicking the button.



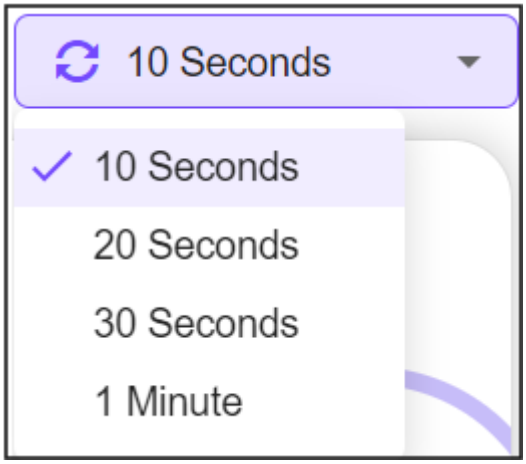
Port Status Information

Port	Status	Description
	Disconnected	Port Link Down
	Connected	Port Link Up
	Connected	Port link up. The arrow indicates the direction of uplink traffic for the primary or secondary port when the pair mode is **Universal Bypass**.
	Disabled	Port Disabled
	Bypass	When **Force Open** or **Fail Open** is enabled, the port allows all network traffic to bypass the Edge device.
	LFPT	The port turns to link down status when LFPT is enabled and the other port in the pair is down.

OK

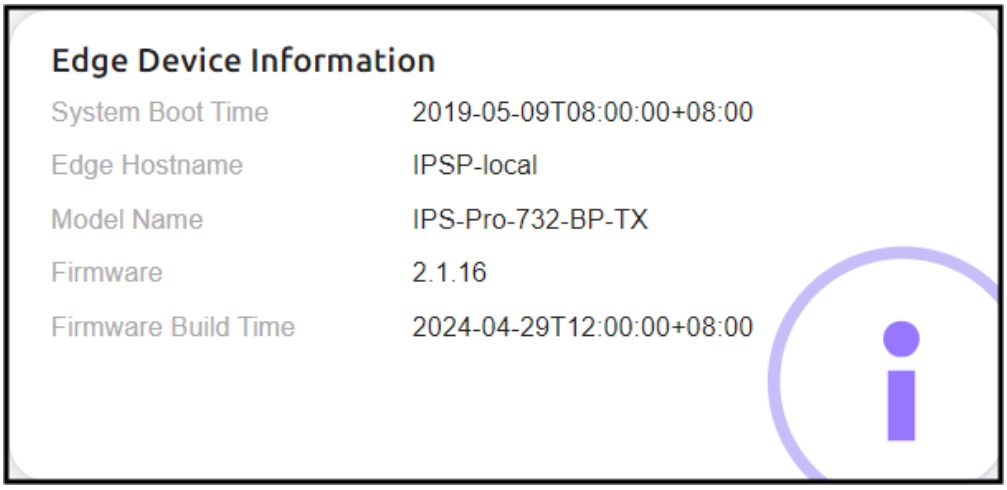
Refresh Interval Settings

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



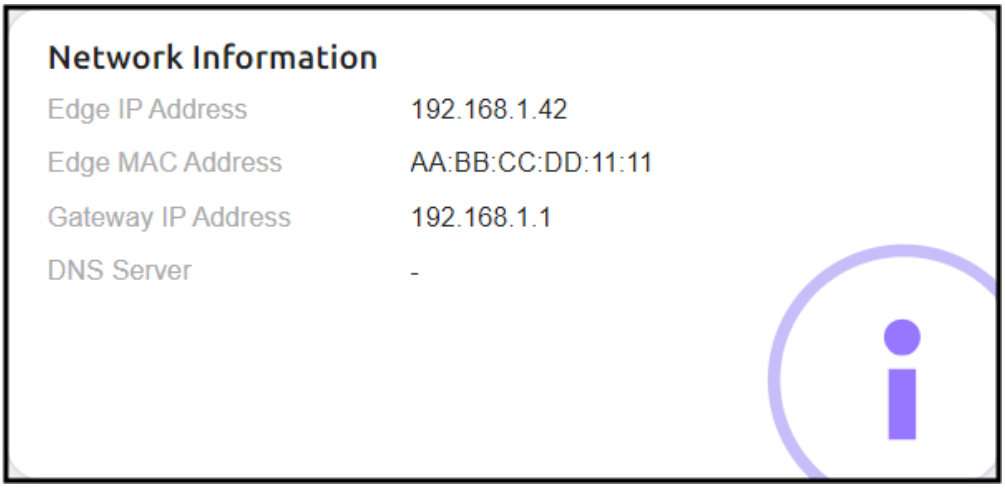
Edge Device Information

This widget shows the system boot time, Edge hostname, model name, firmware version, and firmware build time.



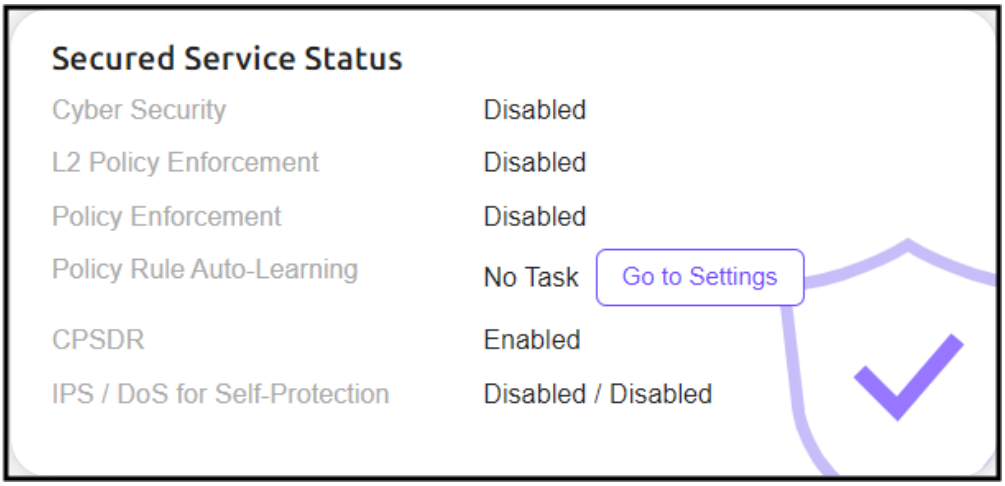
Network Information

This widget shows the the Edge IP address, Edge MAC address, gateway IP address, and DNS server.



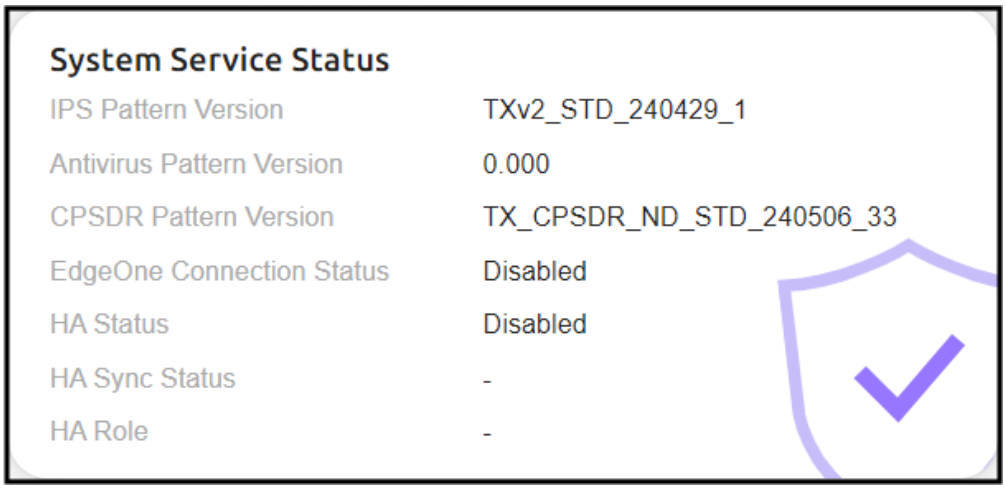
Secured Service Status

The widget shows the statuses of Cyber Security, L2 Policy Enforcement, Policy Enforcement, Policy Rule Auto-Learning, CPSDR, and IPS/DoS for Self-Protection.



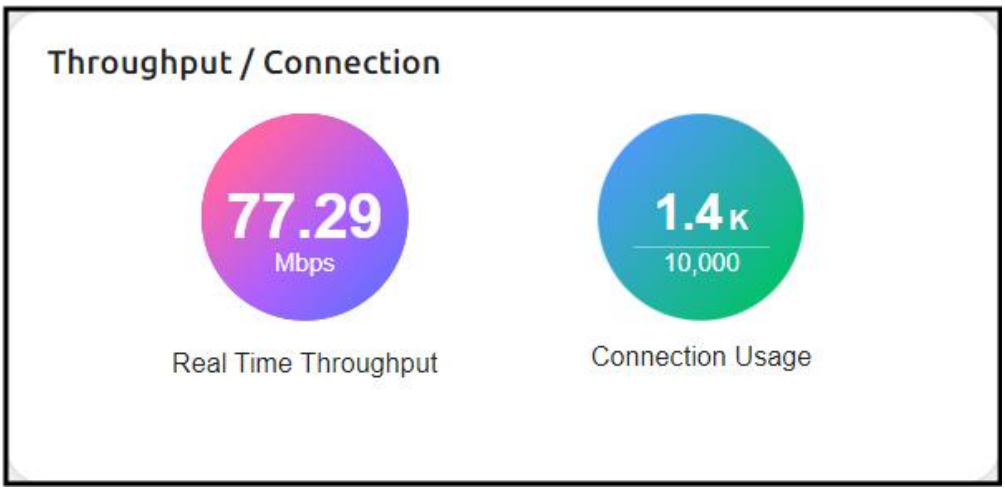
System Service Status

This widget shows the versions of IPS, antivirus, and CPSDR patterns in use, EdgeOne connection status, HA status, HA sync status (when HA is enabled), and its HA role (when HA is enabled).



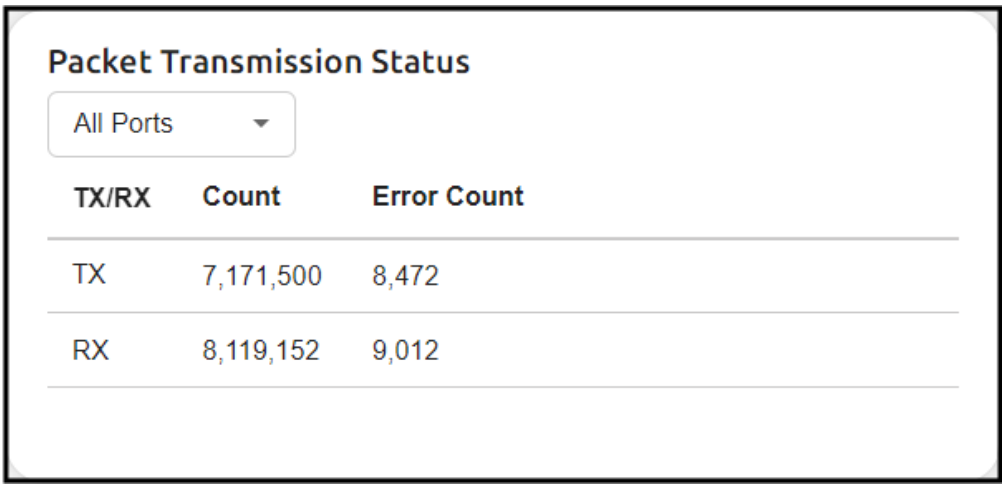
Throughput / Connection

The widget shows the current network throughput and the current network connection usage on the device.



Packet Transmission Status

This widget shows the packet count number on each interface and error count information.

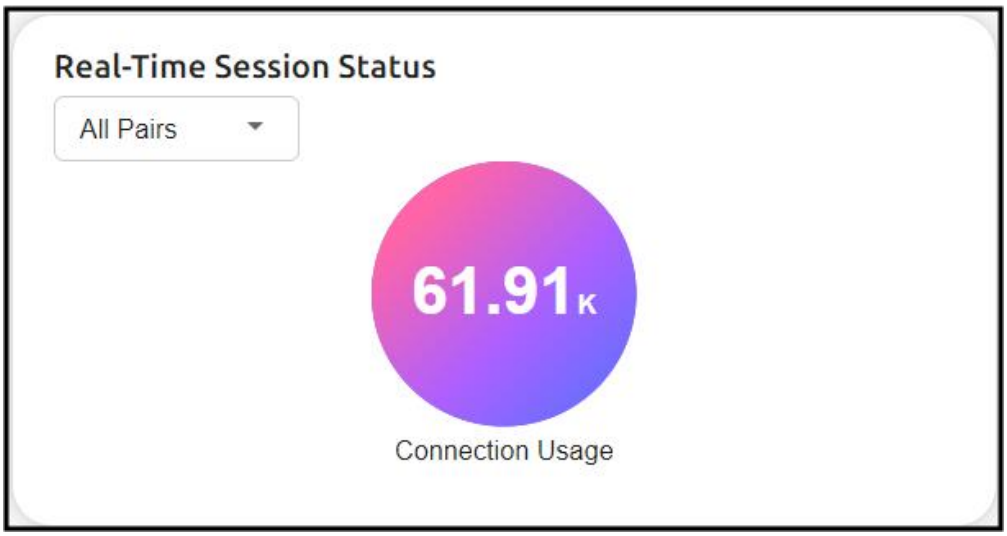


Bandwidth Utilization

This widget shows TX and RX bandwidth utilization based on the specified time interval.

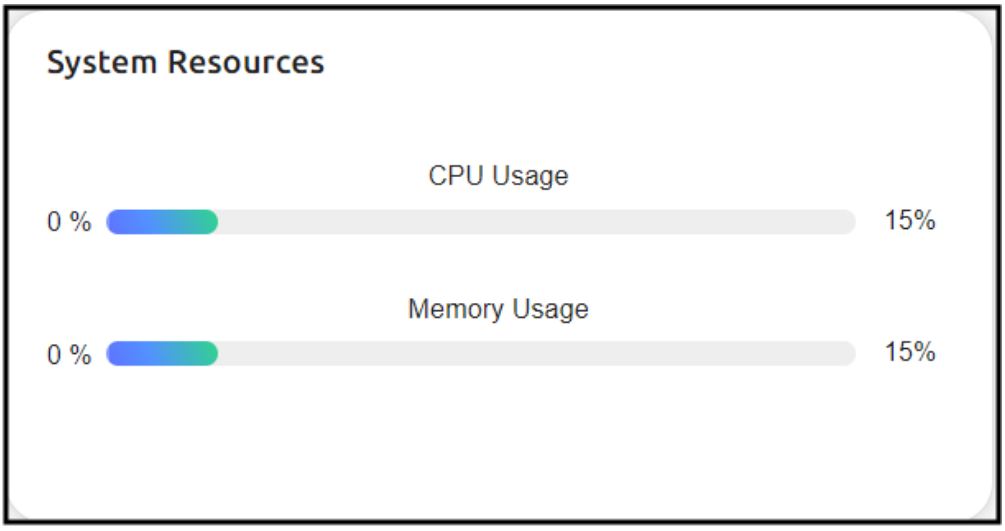
Real-Time Session Status

This widget shows how many sessions are currently in use.



System Resources

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



Item	Description
CPU Usage	Percentage of real-time CPU utilization
Memory Usage	Percentage of real-time memory utilization

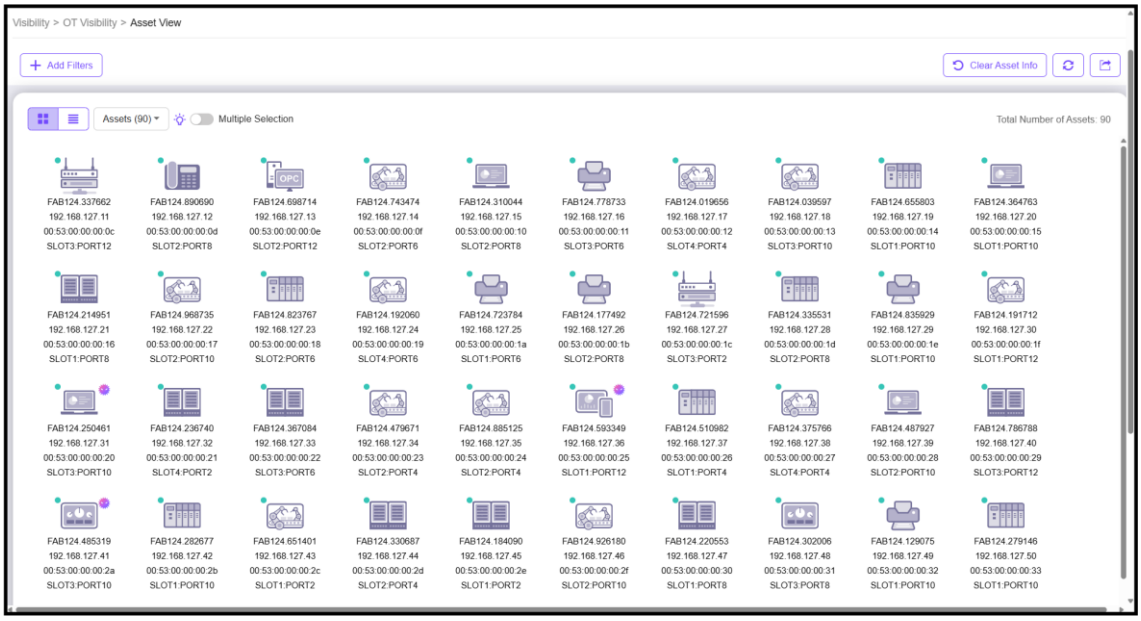
3.2 OT Visibility

Gain a comprehensive view of your OT networks from various aspects.

- Asset View

3.2.1 Asset View

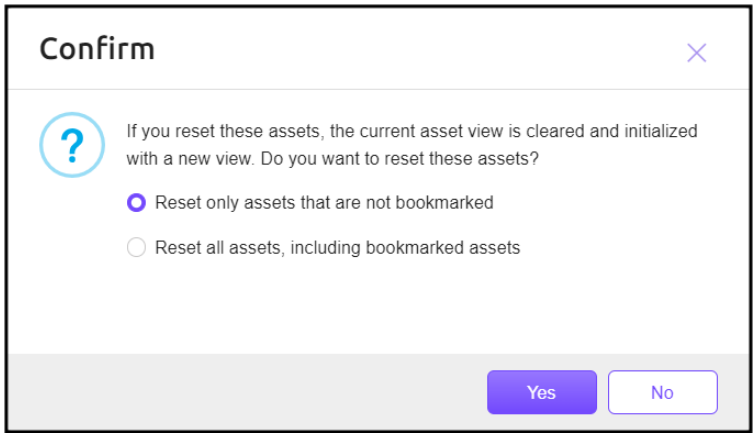
The [Asset View] page gives you an overview of your managed assets. The page provides you with timely and accurate information on the assets that are managed by your Edge series device.

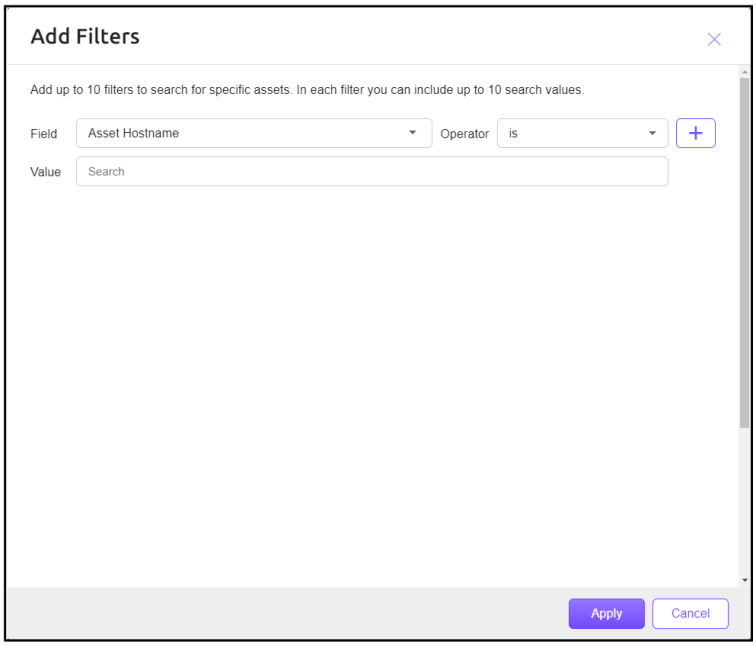


The assets listed on this page are automatically detected by the Edge series devices.

1. The term **asset** in this chapter refers to a device or host that is protected by an Edge device.
2. Starting from firmware v2.2, the identification of newly supported asset types can be enabled via IPS patterns. Even if the Edge firmware is not updated, the forward compatibility of asset type identification ensures that these asset types still appear in the asset view.

The following table lists the actions that you can perform on the [Asset View] page.

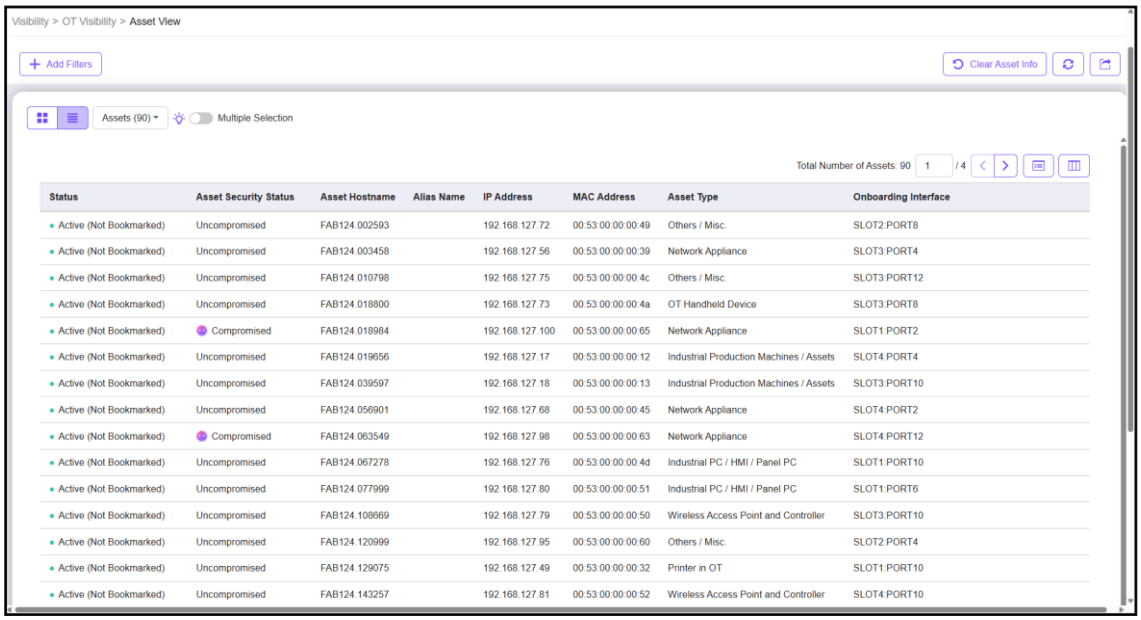
Task	Procedure
To clear the current asset information and initialize the page with a new asset view (only available for an admin role)	1. Click the [Clear Asset Info] button in the upper right corner. A confirmation window will appear.  2. Select an appropriate option and click [Yes].
To refresh the displayed information	1. Click the refresh button in the upper right corner.
To export asset information to a CSV file	1. Click the export button in the upper right corner.

Task	Procedure
To search for specific assets	1. Click [Add Filters] in the upper left corner. The [Add Filters] window will appear.  2. Create up to 10 search filters. In each filter you can include up to 10 search values. 3. Click [Apply].
To switch between the grid view and table view modes	1. Click the grid/table view buttons .
To select multiple assets	1. Enable the [Multiple Selection] toggle. 2. Click on the assets you want to select. To select all assets, click the [Select All] checkbox.
To copy an asset hostname, IP address, or MAC address	1. Select a specific asset. 2. Click the copy button . 3. Select an action, [Copy Asset Hostname], [Copy IP Address], or [Copy MAC Address], from the pop-up menu.
To use an asset's IP or MAC address for object creation	1. Select a specific asset. 2. Click the create profile button . 3. Select an action, [Create IP Object] or [Create MAC Object], from the pop-up menu.
To bookmark or unbookmark an asset	1. Select one or multiple assets. 2. Click the [Bookmark Asset] or [Unbookmark Asset] button.

Task	Procedure
	1. When an inactive asset is bookmarked, its cached information remains accessible in the Edge device GUI until the device is reset to its default settings. 2. The maximum number of detected assets is fixed for the Edge device. When an asset is bookmarked, it occupies a portion of the quota for detecting newly onboarded assets. This means that when the number of bookmarked assets is equal to the maximum number of detected assets, the Edge device will no longer be able to detect new assets.
To edit the alias name, comment, asset type, or OT layer of an asset	1. Select a bookmarked asset. 2. Click the edit asset information button .

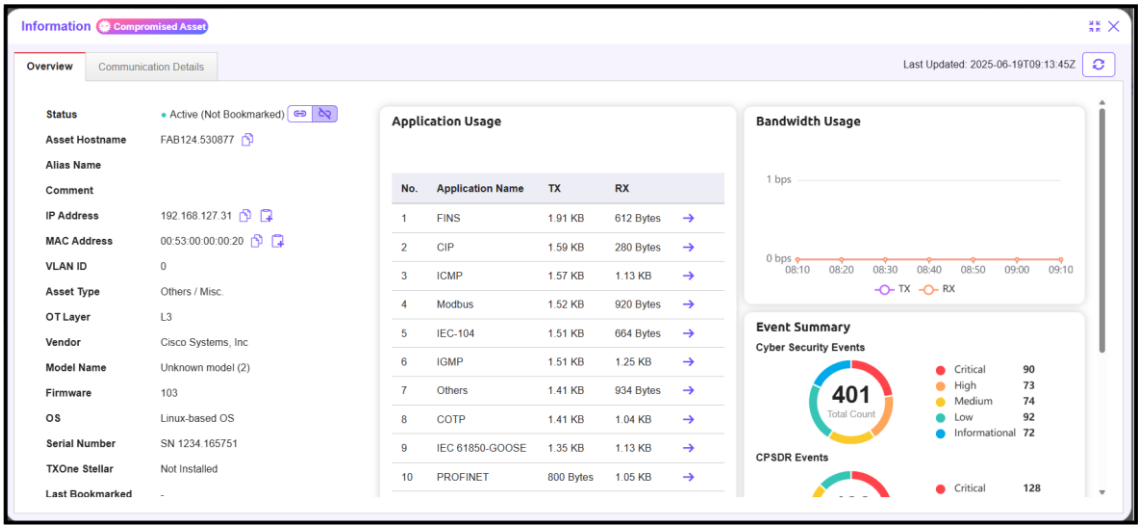
3.2.1.1 Viewing in Table View Mode

Under the [Table View] display mode, you can view detailed information on all assets managed by this Edge device.



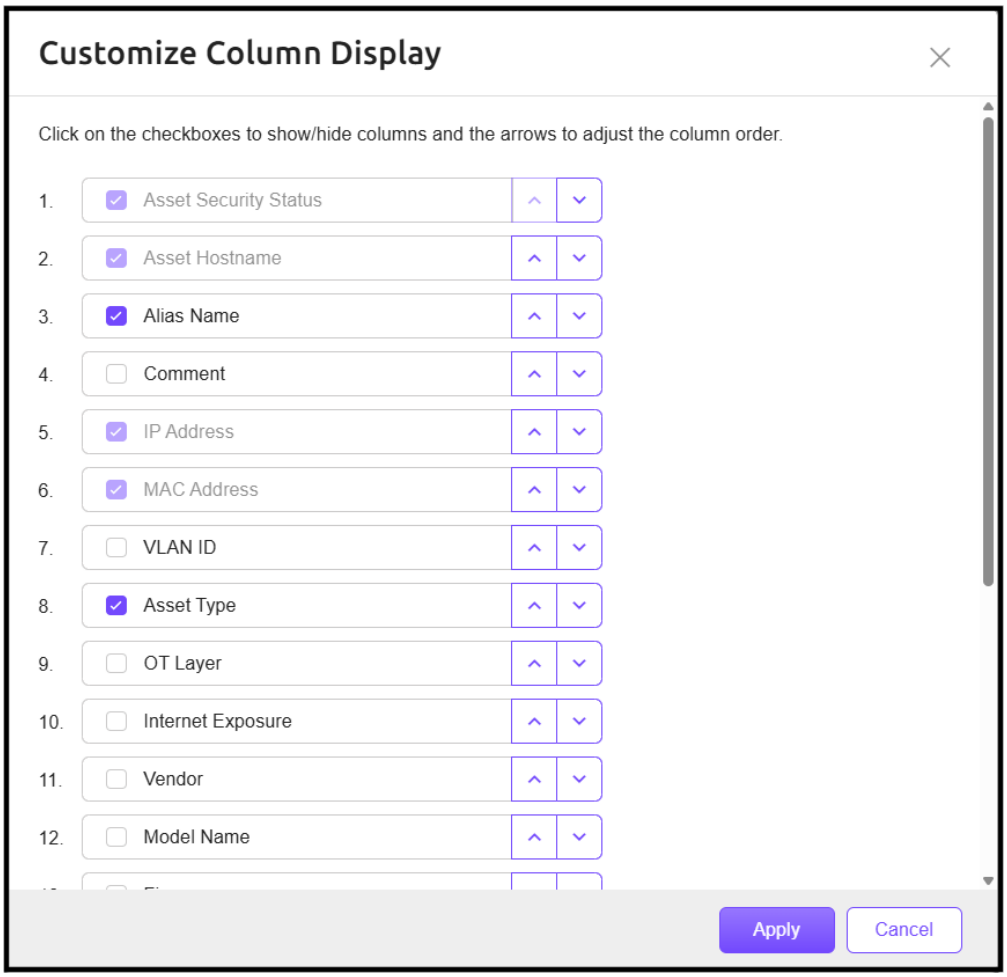
Status	Asset Security Status	Asset Hostname	Alias Name	IP Address	MAC Address	Asset Type	Onboarding Interface
Active (Not Bookmarked)	Uncompromised	FAB124.002593		192.168.127.72	00:53:00:00:00:49	Others / Misc.	SLOT2:PORT8
Active (Not Bookmarked)	Uncompromised	FAB124.003458		192.168.127.56	00:53:00:00:00:39	Network Appliance	SLOT3:PORT4
Active (Not Bookmarked)	Uncompromised	FAB124.010798		192.168.127.75	00:53:00:00:00:4c	Others / Misc.	SLOT3:PORT12
Active (Not Bookmarked)	Uncompromised	FAB124.018800		192.168.127.73	00:53:00:00:00:4a	OT Handheld Device	SLOT3:PORT8
Active (Not Bookmarked)	Compromised	FAB124.018984		192.168.127.100	00:53:00:00:00:65	Network Appliance	SLOT1:PORT2
Active (Not Bookmarked)	Uncompromised	FAB124.019656		192.168.127.17	00:53:00:00:00:12	Industrial Production Machines / Assets	SLOT4:PORT4
Active (Not Bookmarked)	Uncompromised	FAB124.039597		192.168.127.18	00:53:00:00:00:13	Industrial Production Machines / Assets	SLOT3:PORT10
Active (Not Bookmarked)	Uncompromised	FAB124.056901		192.168.127.68	00:53:00:00:00:45	Network Appliance	SLOT4:PORT2
Active (Not Bookmarked)	Compromised	FAB124.063549		192.168.127.98	00:53:00:00:00:63	Network Appliance	SLOT4:PORT12
Active (Not Bookmarked)	Uncompromised	FAB124.067278		192.168.127.76	00:53:00:00:00:4d	Industrial PC / HMI / Panel PC	SLOT1:PORT10
Active (Not Bookmarked)	Uncompromised	FAB124.077999		192.168.127.80	00:53:00:00:00:51	Industrial PC / HMI / Panel PC	SLOT1:PORT6
Active (Not Bookmarked)	Uncompromised	FAB124.108669		192.168.127.79	00:53:00:00:00:50	Wireless Access Point and Controller	SLOT3:PORT10
Active (Not Bookmarked)	Uncompromised	FAB124.120999		192.168.127.95	00:53:00:00:00:60	Others / Misc.	SLOT2:PORT4
Active (Not Bookmarked)	Uncompromised	FAB124.129075		192.168.127.49	00:53:00:00:00:32	Printer in OT	SLOT1:PORT10
Active (Not Bookmarked)	Uncompromised	FAB124.143257		192.168.127.81	00:53:00:00:00:52	Wireless Access Point and Controller	SLOT4:PORT10

Click on a row and the expand button to view general asset information, application usage, bandwidth usage, event summary, and communication details.



For more information about the information under the [Overview] and [Communication Details] tabs, see Viewing in Grid View Mode.

Click the button to show/hide certain type of information and adjust the column order.

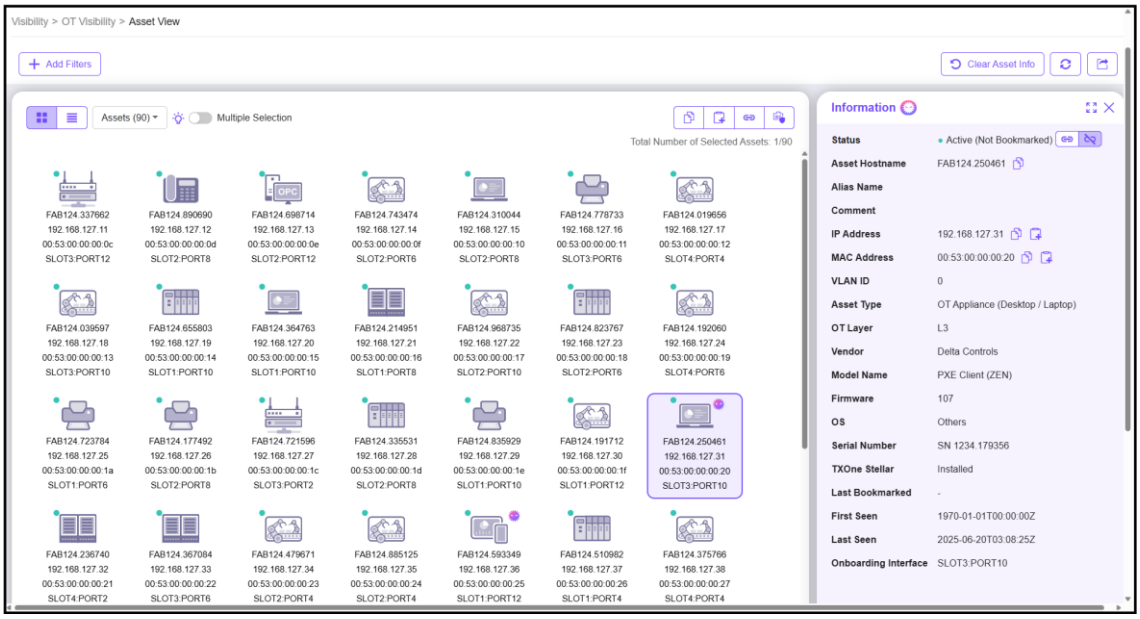


The [Asset Security Status], [Asset Hostname], [IP Address], [MAC Address], and [Onboarding Interface] columns cannot be hidden.

Click the button to adjust the number of rows in the table.

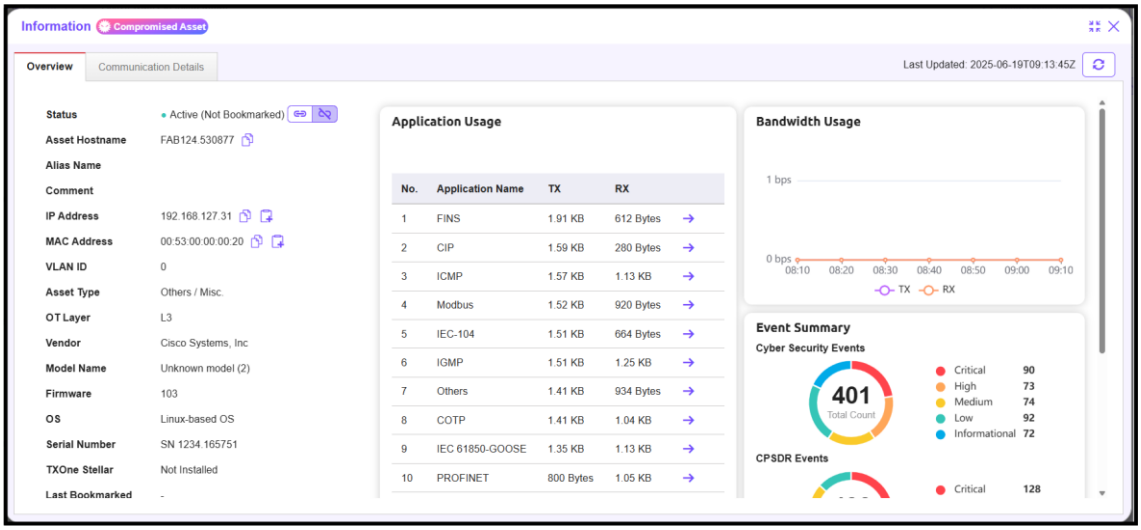
3.2.1.2 Viewing in Grid View Mode

Under the [Grid View] display mode, select a specific asset and click the expand button to view general asset information, application usage, bandwidth usage, event summary, and communication details.



Information > Overview

On the [Information] window, switch to the [Overview] tab to view the general asset information, application usage, bandwidth usage, and event summary. If the selected asset is impacted by high- or critical-severity IPS, CPSDR, or antivirus events within the last 24 hours, the [Information] window will be labeled [Compromised Asset]. If the asset has communicated with a public IP address within the last 24 hours, the window will be labeled [Internet Exposed].



Item	Description
Status	The current status of the asset. Click the buttons to bookmark or unbookmark an asset.

Item	Description
	• **Active (Not Bookmarked)**: An asset is marked as active when it has network traffic passing through it within the last hour. If the asset does not have network traffic for more than an hour and is not bookmarked, the system automatically removes it from the page. • **Active (Bookmarked)**: An asset is marked as active when it has network traffic passing through it within the last hour. If the asset does not have network traffic for more than an hour and is bookmarked, it continues to be displayed on this page. • **Inactive (Bookmarked)**: An asset is marked as inactive when no network traffic is detected within the last hour. However, if the asset is bookmarked, its cached information remains accessible on this page, despite its inactivity.
Asset Hostname	The hostname of the asset. Click the button to copy the asset hostname.
Alias Name	User-defined name of the asset. Click the button to edit the alias name. You can only edit the alias name of a bookmarked asset.
Comment	User-defined comment for the asset. Click the button to edit the comment. You can only edit the comment for a bookmarked asset.
IP Address	The IP address of the asset. Click the button to copy the IP address, or the UNKNOWN_ATTACHMENT button to create an IP object. For more information about creating an IP object, see Configuring IP Objects.
MAC Address	The MAC address of the asset. Click the button to copy the MAC address, or the UNKNOWN_ATTACHMENT button to create a MAC object. For more information about creating a MAC object, see Configuring MAC Objects.
VLAN ID	The VLAN ID of the asset.
Asset Type	The type of the asset. Click the button to edit the asset type. You can only edit the type of a bookmarked asset.

Item	Description
OT Layer	The OT layer in which the asset is located. Click the button to edit the OT layer. You can only edit the OT layer of a bookmarked asset.
Vendor	The vendor of the asset.
Model Name	The model name of the asset.
Firmware	The firmware version of the asset.
OS	The operating system of the asset.
Serial Number	The serial number of the asset.
TXOne Stellar	The TXOne Stellar installation status of the asset.
Last Bookmarked	The date and time when the asset was last bookmarked.
First Seen	The date and time when the asset was first seen.
Last Seen	The date and time when the asset was last seen.
Onboarding Interface	The Edge device interface to which the asset is onboarded.

Information > Overview > Application Usage

In the [Application Usage] pane, you can view the statistics of the network traffic passing from/to a specific asset based on different applications.

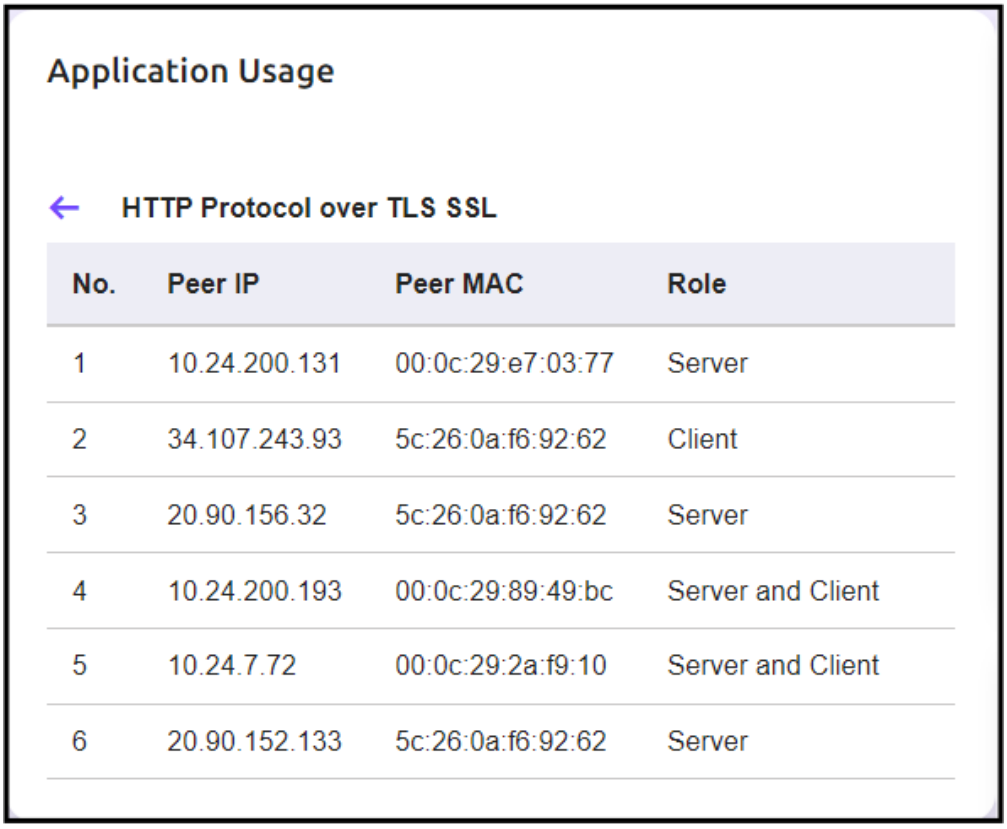
Application Usage

No.	Application Name	TX	RX	
1	SSL/TLS	315.32 MB	486.69 MB	→
2	HTTP Protocol ov...	21.08 MB	41.25 MB	→
3	MS Remote Deskt...	15.52 MB	25.50 MB	→
4	Others	6.34 MB	8.84 MB	→
5	Microsoft.com	1.58 MB	3.29 MB	→
6	FTP Applications	1.56 MB	11.62 MB	→
7	Windows Update	768.28 KB	5.90 MB	→
8	SMB2	449.97 KB	323.36 KB	→
9	HTTP	130.90 KB	6.09 MB	→
10	IGMP	84.84 KB	0 Bytes	→
11	Microsoft Office	39.61 KB	144.40 KB	→
12	Google APIs(SSL)	20.87 KB	106.56 KB	→
13	Lets Encrypt	14.78 KB	51.71 KB	→
14	QUIC	14.21 KB	28.89 KB	→
15	Microsoft Live.com	6.38 KB	16.42 KB	→
16	Web File Transfer	5.56 KB	70.30 KB	→

Item	Description
No.	The ordinal number of the application traffic.
Application Name	The application type of the traffic.
TX	The amount of traffic transmitted for this application.

Item	Description
RX	The amount of traffic received for this application.

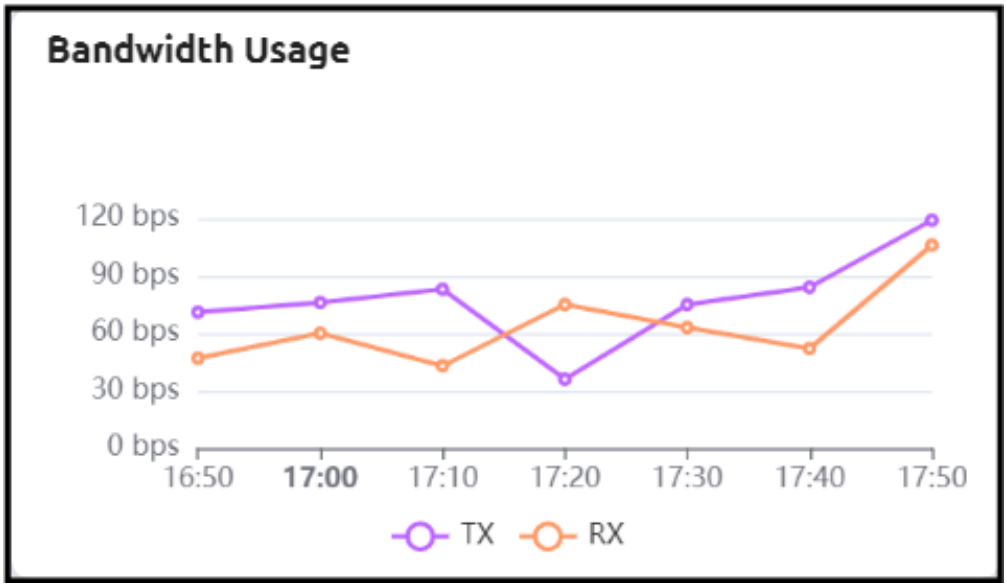
Click the arrow next to a specific application to view its peer IP, peer MAC, and role.



Item	Description
Peer IP	The IP address of the network element on the other end of the connection.
Peer MAC	The MAC address of the network element on the other end of the connection.
Role	• **Server**: The network element on the other end of the connection transmits network packets to the asset. • **Client**: The network element on the other end of the connection receives network packets from the asset.

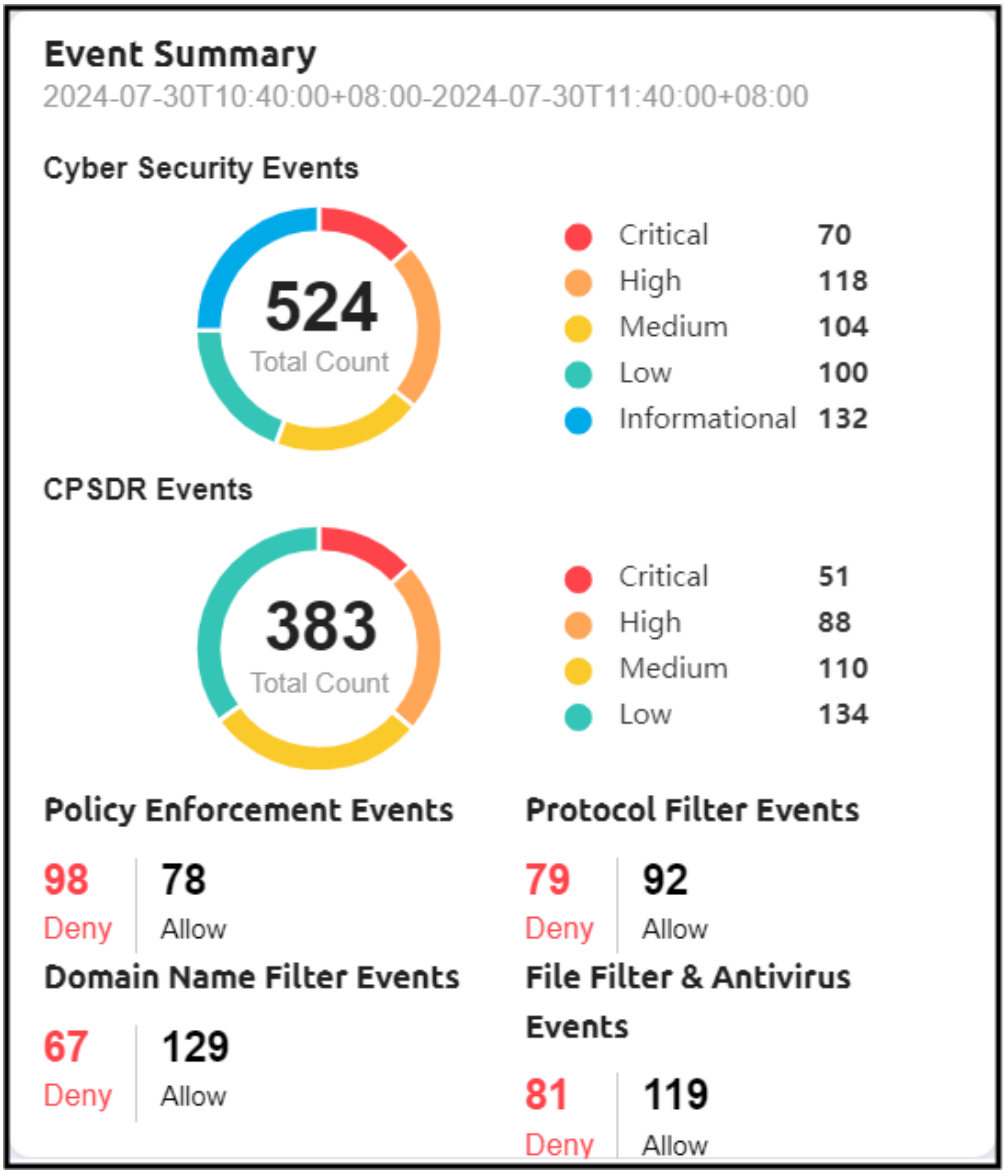
Information > Overview > Bandwidth Usage

In the [Bandwidth Usage] pane, you can monitor the bandwidth usage of a specific asset.



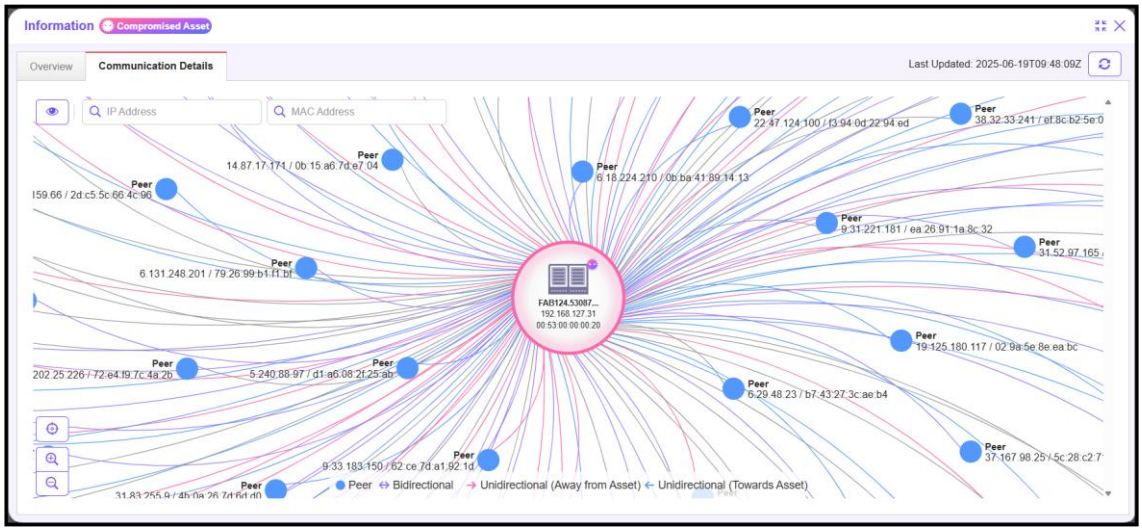
Information > Overview > Event Summary

In the [Event Summary] pane, you can monitor the counts of various types of security events, including Cyber Security, CPSDR, Policy Enforcement, Protocol Filter, Domain Name Filter, and File Filter & Antivirus events. To view detailed log information for each event type, click the number of events.



Information > Communication Details

On the [Information] window, switch to the [Communication Details] tab to view a visualized network graph showing which devices are communicating with this asset.



Task	Description
To configure display options	Click [Configure Display Options] , then check or uncheck the display options.
To search for a specific peer device by IP address	Input the IP address of the target device in the [IP Address] field.
To search for a specific peer device by MAC address	Input the MAC address of the target device in the [MAC Address] field.
To reset and center the communication graph on the asset	Click the [Recenter] button in the bottom-left corner of the communication graph.
To zoom in on the communication graph	Click the [Zoom In] button in the bottom-left corner of the communication graph.
To zoom out of the communication graph	Click the [Zoom Out] button in the bottom-left corner of the communication graph.

4 Device

This chapter describes how to configure network-related features and port settings under the [Device] tab.

4.1 Network & Ports

Configure device network and port settings.

- Network Settings
- HA Settings
- Port Mirroring
- Port Settings

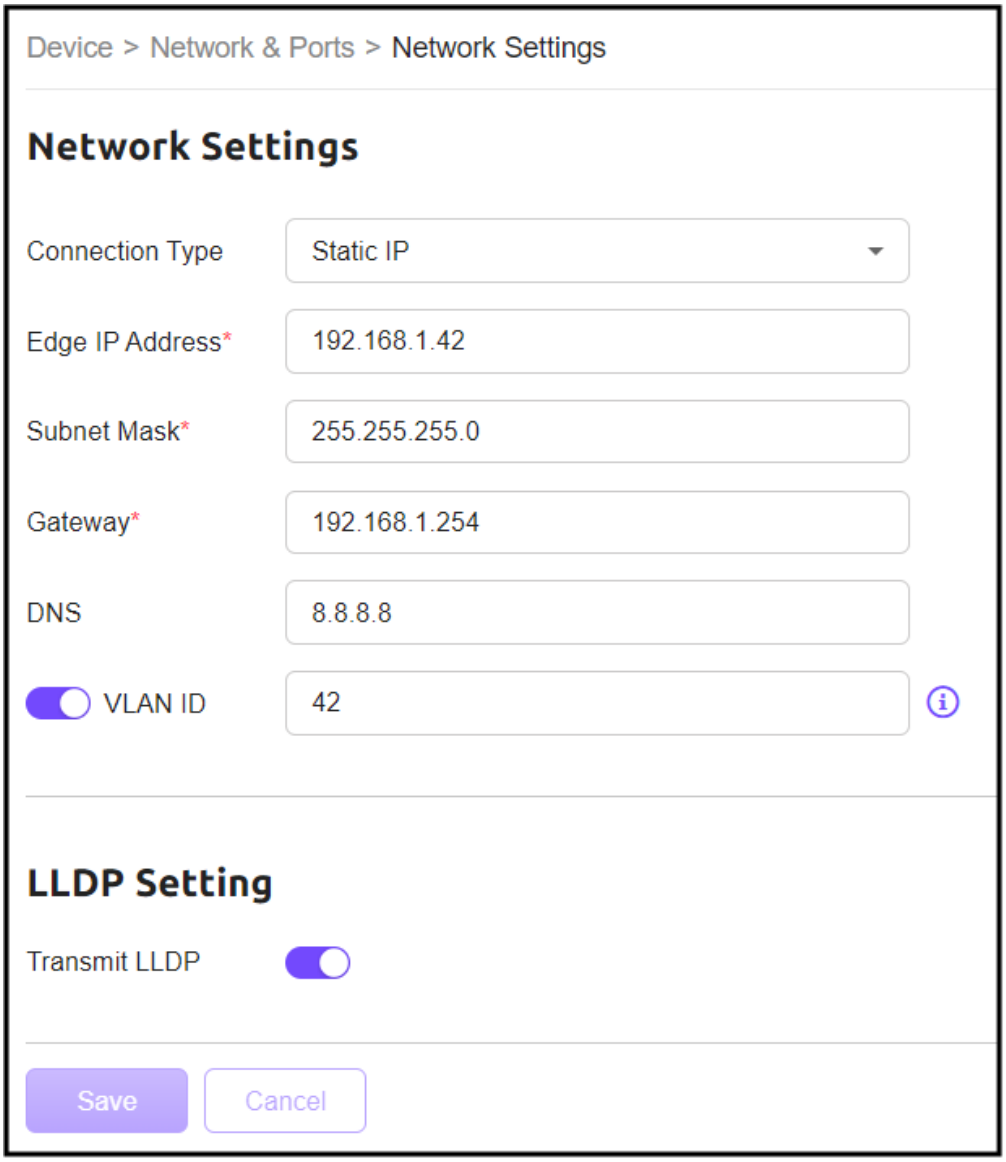
4.1.1 Network Settings

The [Network Settings] page contains setting items for IP address, netmask, gateway, DNS, VLAN ID, and transmission of LLDP of the device.

4.1.1.1 Configuring Network and LLDP Settings

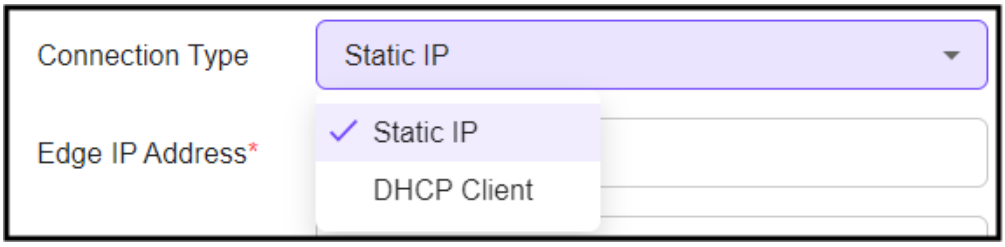
Procedure

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

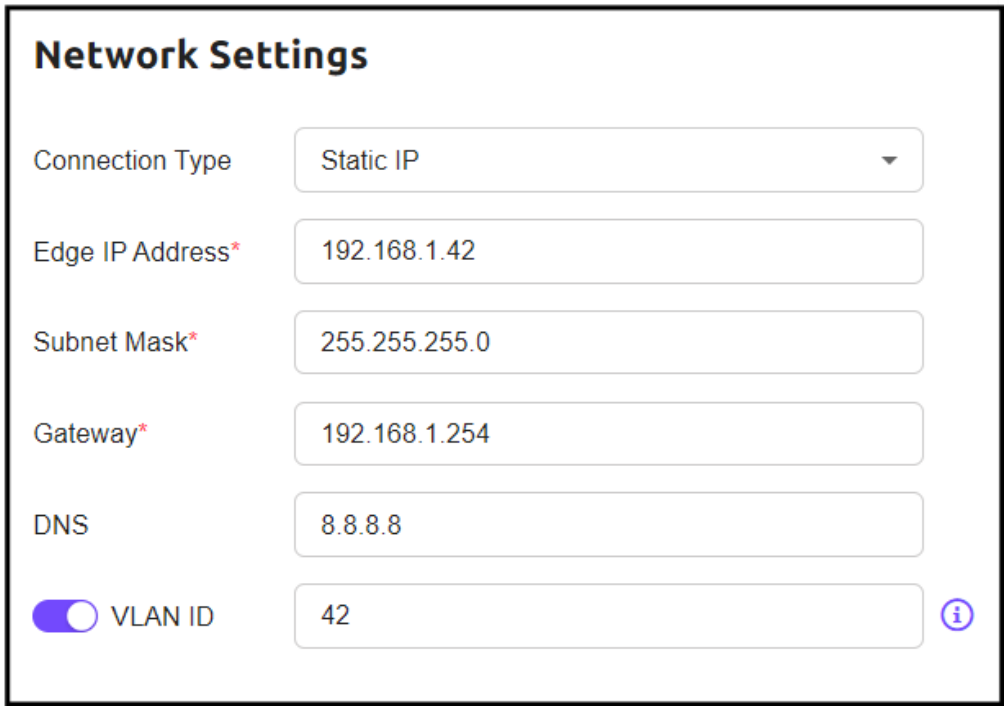


2. Configure the following settings.

- Network Settings: Select either **Static IP** or **DHCP Client** for the Connection Type.



• **Static IP**: This device uses a static IP address for this interface. If this option is selected, provide the following information.



Item	Description
Connection Type	Static IP
Edge IP Address	Input an IP Address of the device.
Subnet Mask	Input a subnet mask of the device.
Gateway	Input an IP address of the gateway that will send packets to a different network.
DNS	(Optional) Input a DNS address of the device.
VLAN ID	(Optional) Enable this function by clicking the toggle. If enabled, input a VLAN ID for the device to allow packets with the specified VLAN tag to access the management interface.

• **DHCP Client**: The interface functions as a DHCP client and automatically get an IP address from a DHCP server. If this option is selected, provide the following information.

Item	Description
Connection Type	DHCP Client
VLAN ID	(Optional) Enable this function by clicking the toggle. If enabled, input a VLAN ID for the device to allow packets with the specified VLAN tag to access the management interface.

- LLDP Setting

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

3. Click [Save].

4.1.2 HA Settings

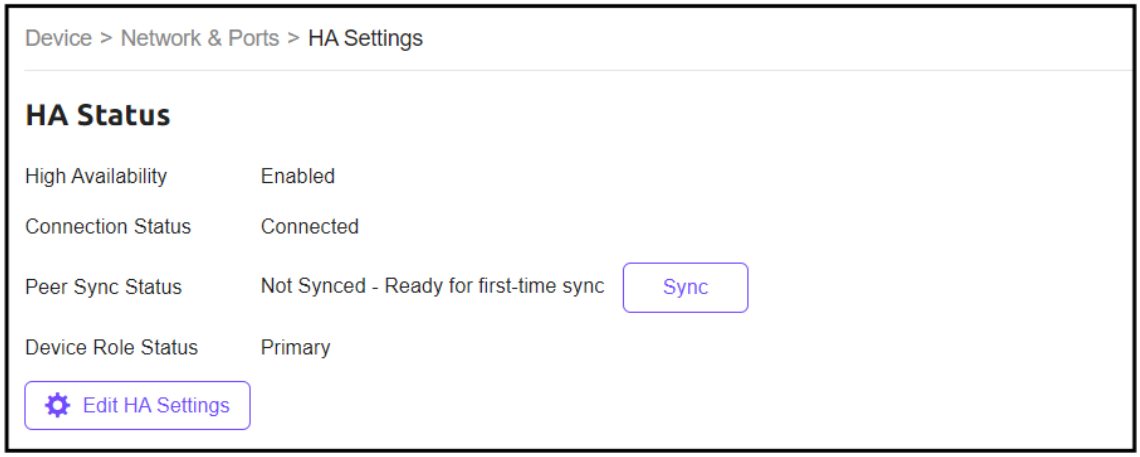
Using a single device for network security and traffic flow can create a single point of failure. This Edge series device provides a High Availability (HA) feature that enables redundancy by way of the ability to add and synchronize configurations with a secondary backup device. This eliminates the single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

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

4.1.2.1 Configuring HA Settings

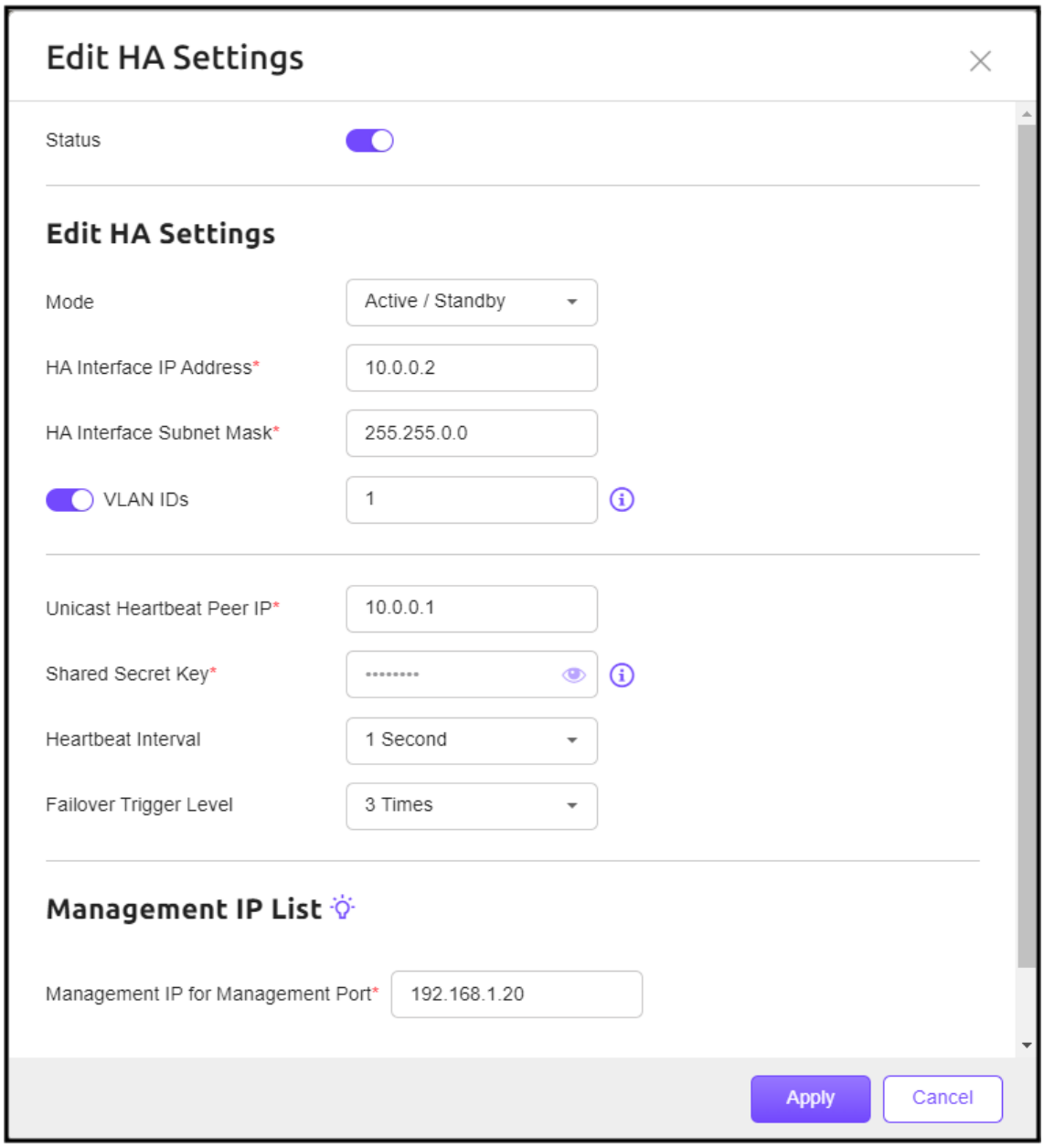
Procedure

1. Go to [Device] > [Network & Ports] > [HA Settings].



Item	Description
High Availability	The status of HA, either **Enabled** or **Disabled**. If High Availability is enabled, the following status information will be shown.
Connection Status	The status of connection, either **Connected** or **Disconnected**.
Peer Sync Status	The status of peer synchronization, either **Synced** or **Not Synced**.
Device Role Status	The status of device role, either **Primary** or **Secondary**.

2. Click the [Edit HA Settings] button. The [Edit HA Settings] window will appear.



3. Configure the following HA settings and management IP.

Item	Description
Status	The HA sync status between two Edge devices in the same HA group. This also displays the sync progress. Enable the HA function by clicking the toggle.

- HA Settings

Item	Description
Mode	Select either **Active/Active** or **Active/Standby** for the HA mode. • **Active/Active**: Both devices in the HA group are fully active and online. Traffic may flow via either device. If a single connection's traffic is split across the two devices, it may cause the packet classifier to not be able to classify the traffic and thus not be able to apply any filtering/security policies. A single connection's complete session must pass through a single device. In this mode,

Item	Description
	the switching/flow of traffic between devices is handled by an external/upper layer that is outside the devices. • **Active/Standby**: Only one device in 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	Input an IP Address of the HA interface that sends/receives HA heartbeats and data messages to/from its peer.
HA Interface Subnet Mask	Input a subnet mask of the HA interface.
VLAN ID	(Optional) Enable this function by clicking the toggle. If enabled, input a VLAN ID of the device to allow packets with the specified VLAN tag to access the HA interface.
Unicast Heartbeat Peer IP	Input an IP address of the HA peer.
Shared Secret key	Input a shared secret key to allow for two HA peers to authenticate and communicate with each other.
Heartbeat Interval	Select an interval between sent heartbeats ranging from 1 to 10 seconds (default: 1).
Failover Trigger Level	Select a maximum number of consecutive missed heartbeats before secondary to primary switch is triggered ranging from 1 to 10 times (default: 3).

- Management IP List

Item	Description
Management IP for Management Port	When HA is enabled and the configuration is synced up, the IP settings for all the interfaces will be synced to the active device. To access the management interface of the active device or the standby device, create at least a management IP to bridge to a designated management interface.

4. Click [Save].

4.1.3 Port Mirroring

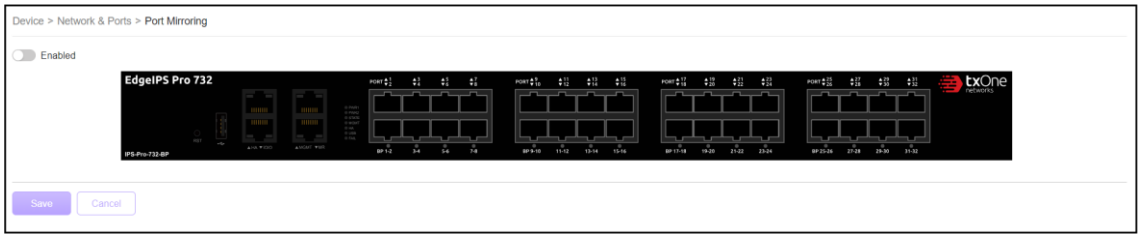
To monitor the network, all the traffic from any of the protected segments will be mirrored to the reserved port, i.e., the Mirror Port.

📝	Instead of pair-based, the Port Mirroring feature is port-based.

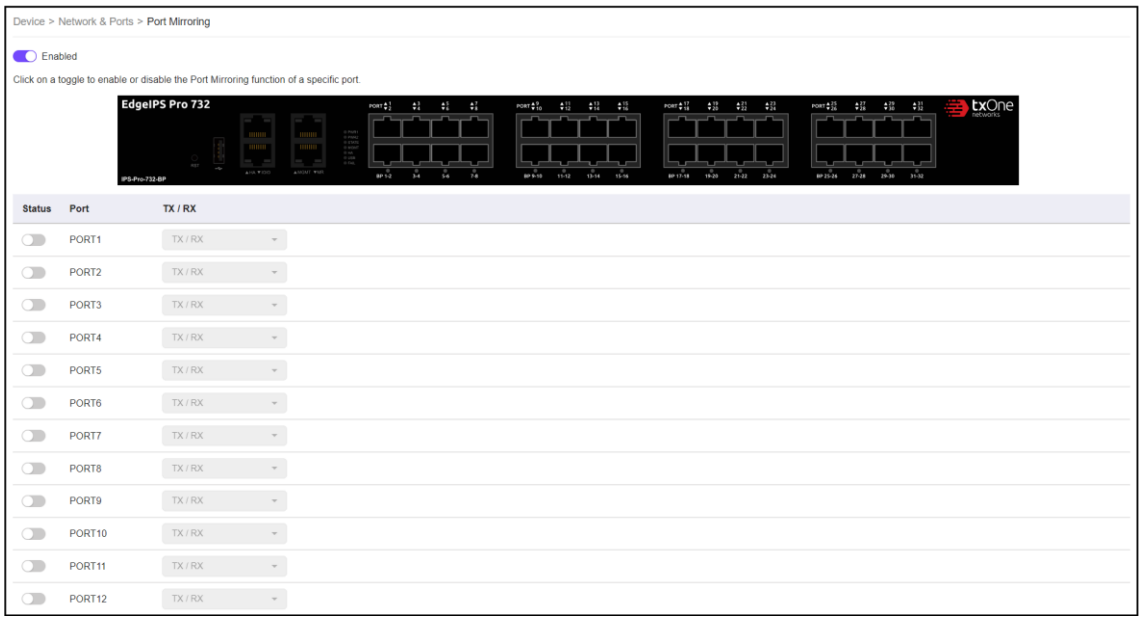
4.1.3.1 Configuring Port Mirroring Settings

Procedure

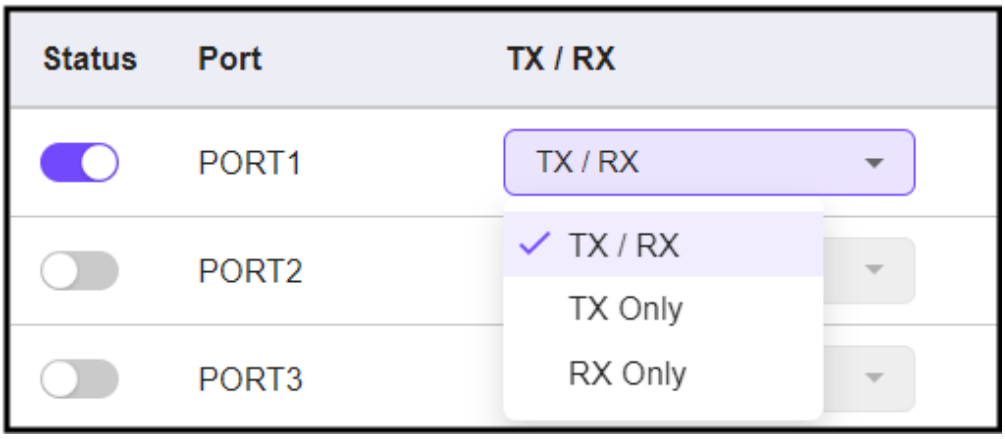
1. Go to [Device] > [Network & Ports] > [Port Mirroring].



2. Enable the Port Mirroring function by clicking the toggle. You will then be able to configure the port mirroring settings on this page.



3. Click a port on the front panel to configure the following port mirror settings.



Item	Description
Status	The connection status of the mirror port. Enable or disable the port by clicking the toggle.
TX/RX	Select a mirror traffic direction, **TX Only**, **RX Only** or **TX/RX** for the port.

4. Click [Save].

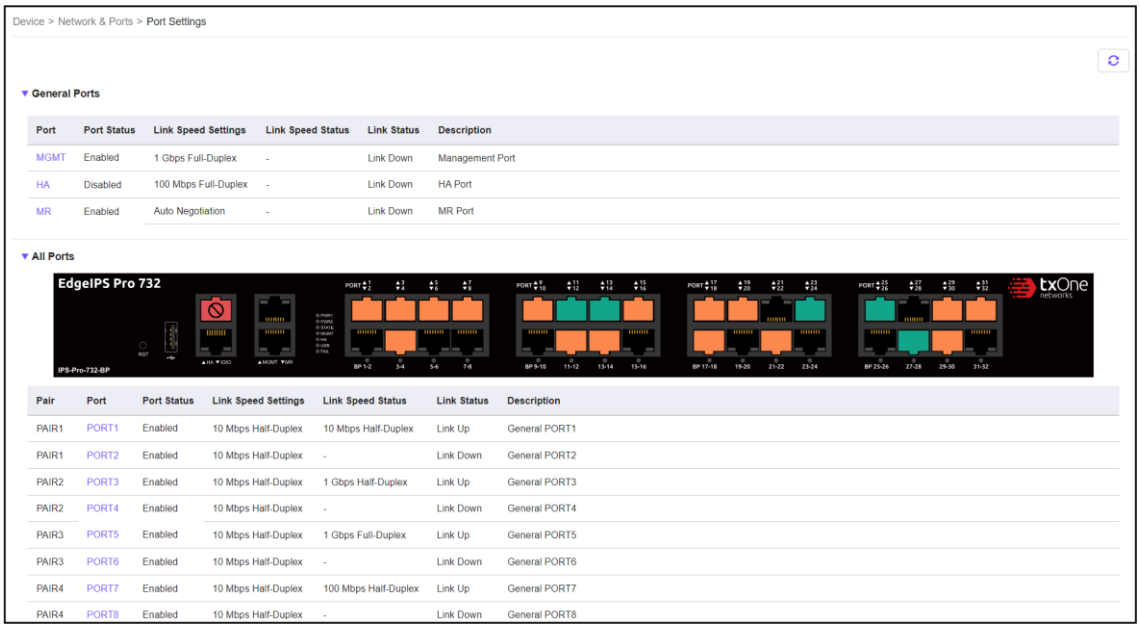
4.1.4 Port Settings

The [Port Settings] page contains setting items for port connection statuses and port link speeds.

4.1.4.1 Configuring Port Settings

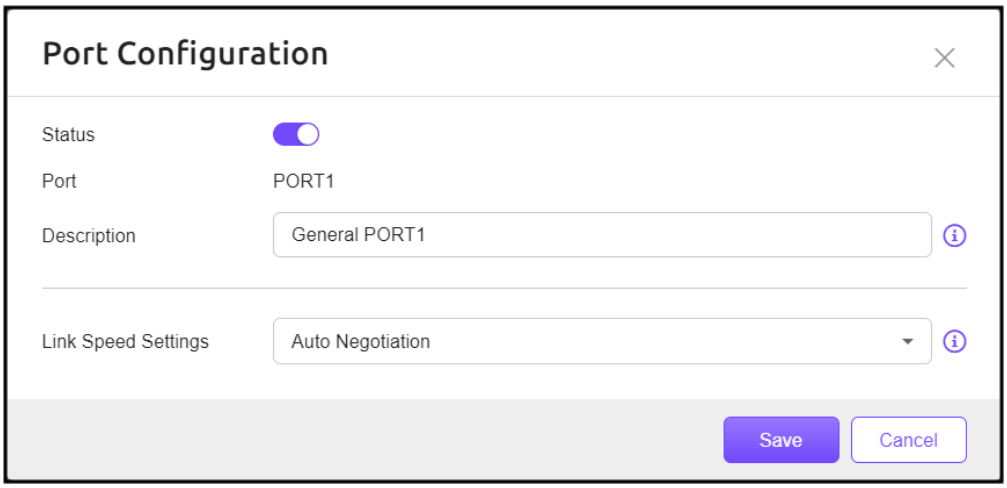
Procedure

1. Go to [Device] > [Network & Ports] > [Port Settings].



> The panel view on the page shows a graphical depiction of the connected ports on the device.

2. Click a port in the [Port] column. The [Port Configuration] window will appear.



3. Configure the following port settings.

Item	Description
Status	The connection status of the port. Enable or disable the port by clicking the toggle. ⚠ The MGMT port cannot be disabled.

Item		Description
Description		(Optional) Type a description for the port.
Link Speed Settings	For MGMT port and MR port	Select a speed and negotiation method, **Auto Negotiation**,**100 Mbps Full-Duplex**, **1 Gbps Full-Duplex** or **10 Gbps Full-Duplex** for the port. Select [Auto Negotiation] if you would like the interface to automatically negotiate with the highest speed that both sides can work with. Otherwise, the link speed would be set to the configured speed value based on your selection.
	For HA port	Select a speed and negotiation method, **Auto Negotiation**, **10 Mbps Half-Duplex**, **10 Mbps Full-Duplex**, **100 Mbps Half-Duplex** or **100 Mbps Full-Duplex** for the port.
	For all port pairs	Select a speed and negotiation method, **Auto Negotiation**, **10 Mbps Half-Duplex**, **10 Mbps Full-Duplex**, **100 Mbps Half-Duplex**, **100 Mbps Full-Duplex** or **1 Gbps Full-Duplex** for the port.

4. Click [Save].

The MGMT port is an out-of-band management port that serves as an independent interface on an Edge series device when it's configured in Inline mode. The MGMT port is logically separate from the data ports. Traffic passing through these two types of ports is isolated and does not interchange (except for transferring management data stored in an Edge series device).

- MGMT Port: This port connects the Edge series device to EdgeOne for device management.
- Data Ports: These ports connect the Edge series device to target assets for asset protection.

5 Objects & Profiles

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

Each type of object and profile (except for MAC objects) has the following types of sub-profile lists for this device:

- **Device Objects/Profiles**: Contains objects and profiles created and configured by users with Edge device local account privileges to be applied to policy rules.
- **EdgeOne Objects/Profiles**: Contains objects and profiles synced from EdgeOne. Users with EdgeOne local account privileges can apply them to policy rules. Users with only Edge device local account privileges can only view and copy objects/profiles from the [EdgeOne Profiles] list to the [Device Profiles] list.

📝	MAC objects can only be configured on the Edge device management console.

You can perform the following tasks when you view a profile list.

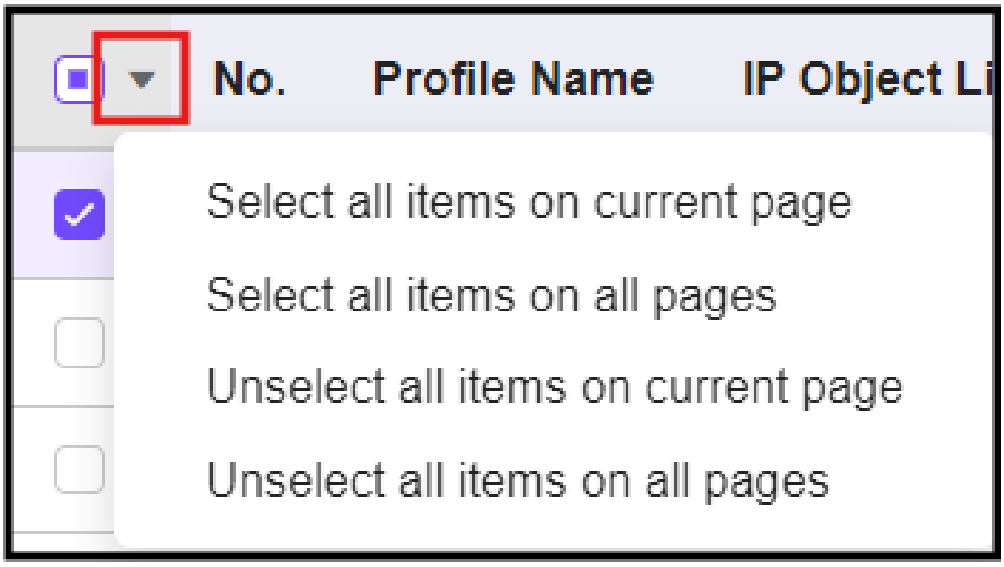
- **Device Objects/Profiles**:

Task	Description
Create object/profile	Click [Create] to create a new object/profile.
Edit object/profile	Click a(n) object/profile name to edit the settings.
Delete object/profile	Select one or multiple objects/profiles and click [Delete] to delete them.
Duplicate object/profile	Select a(n) object/profile and click [duplicate] to duplicate it.

- **EdgeOne Objects/Profiles**:

Task	Description
Copy object/profile to [Device Objects/Profiles]	Select one or multiple objects/profiles and click [Copy EdgeOne Profiles to Device Profiles] to copy the objects/profiles on the [EdgeOne Objects/Profiles] list and paste them to the [Device Objects/Profiles] list.

On the table header row, click the down arrow icon next to the checkbox, and a drop-down menu for selecting objects/profiles will be shown.



5.1 IP/MAC/Service Objects

Create and manage groups of MAC/IP addresses and service objects shared among multiple Policy Enforcement rules.

- IP Objects
- MAC Objects
- Service Objects

5.1.1 IP Objects

IP objects contain IP addresses which you can apply to policy rules. The types of IP addresses you can assign are:

- **Single IP address**

For example: 192.168.1.1

- **IP range**

For example: from 192.168.1.1 to 192.168.1.20

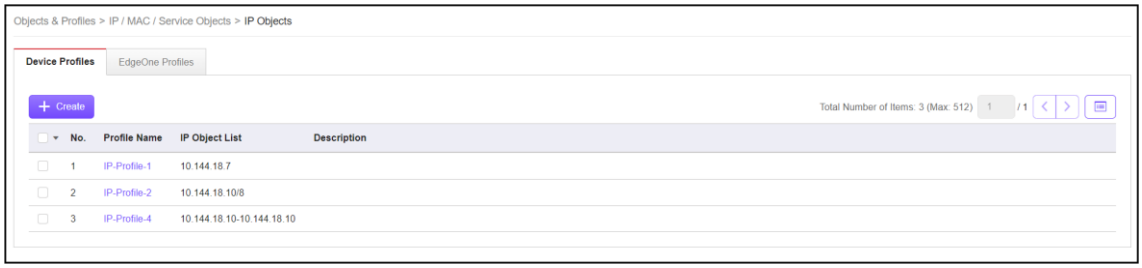
- **IP subnet**

For example: 192.168.1.0/24

5.1.1.1 Configuring IP Objects

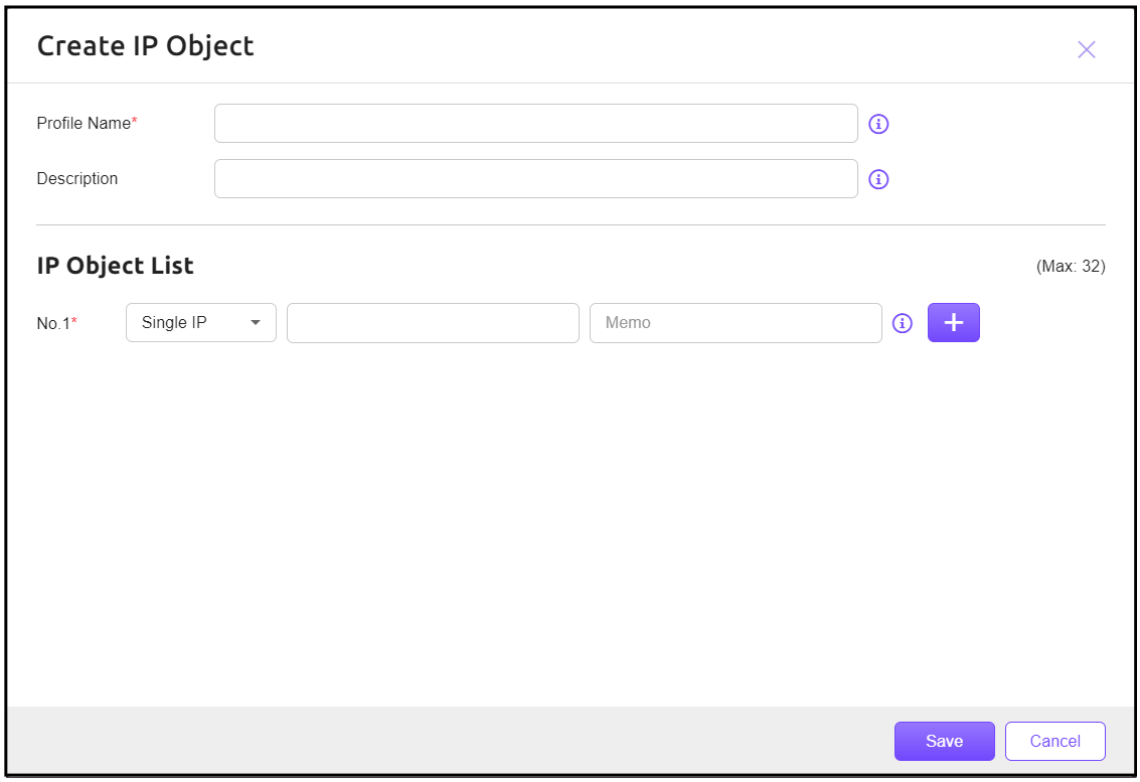
Procedure

1. Go to [Objects & Profiles] > [IP/MAC/Service Objects] > [IP Objects].



2. Do one of the following.

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



3. Configure the following IP object settings.

Item	Description
Profile Name	Type a profile name for this IP object.
Description	(Optional) Type a description.
IP Object List	Specify an IP address, an IP range, or an IP subnet. If needed, fill out the [Memo] field. Click the [Add Entry] button + to add another entry, or the [Remove Entry] button − to remove an entry.

4. Click [Save].

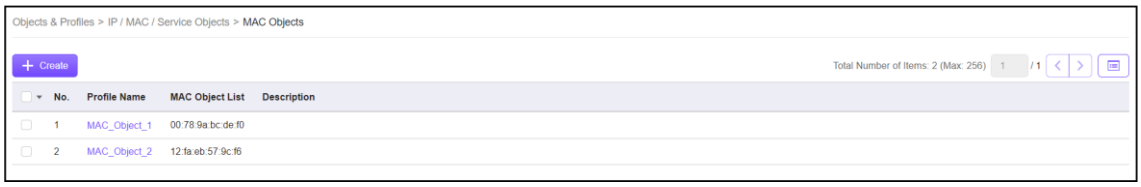
5.1.2 MAC Objects

MAC objects contain MAC addresses which you can apply to policy rules.

5.1.2.1 Configuring MAC Objects

Procedure

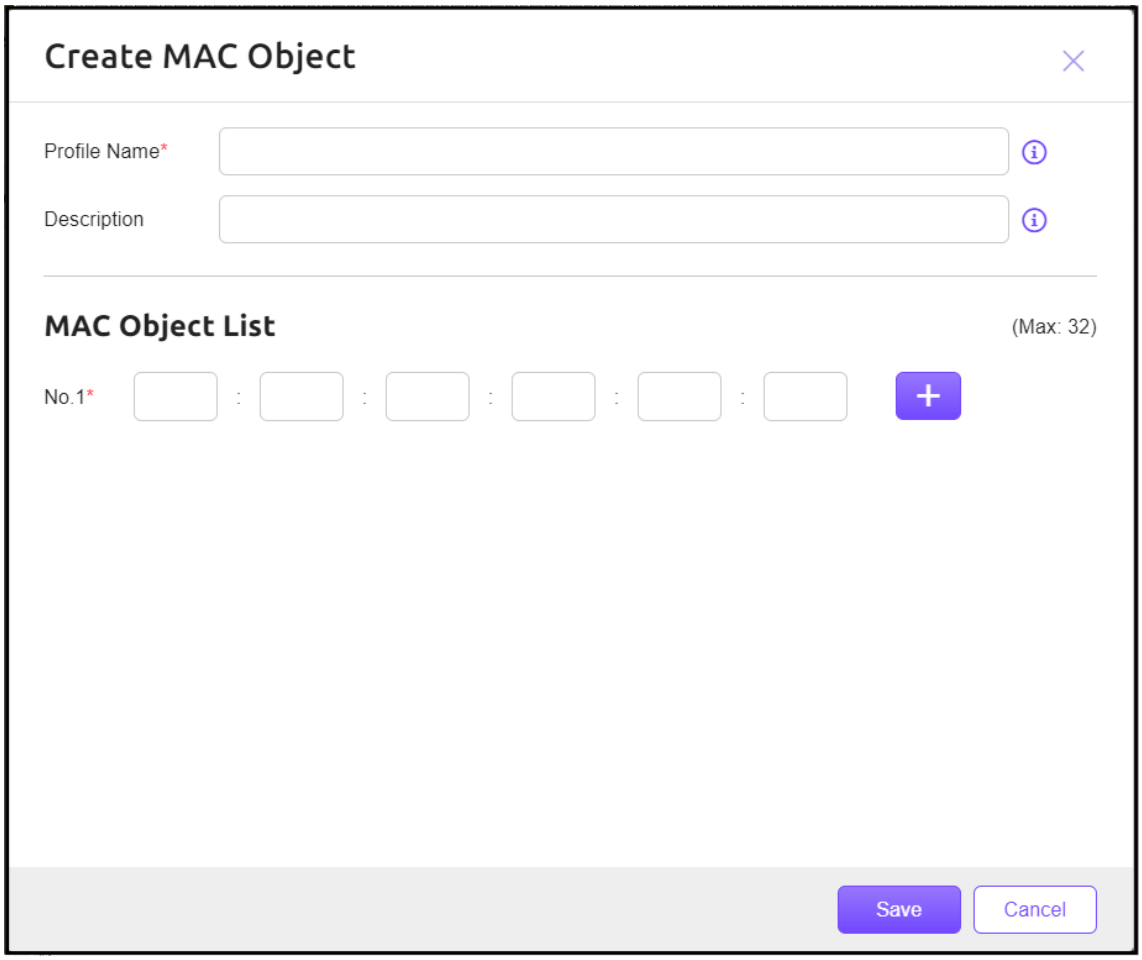
1. Go to [Objects & Profiles] > [IP/MAC/Service Objects] > [MAC Objects].



2. Do one of the following.

- Click [Create] to create an object. The [Create MAC Object] window will appear.

- Click a profile name to edit settings. The [Edit MAC Object] window will appear.



3. Configure the following MAC object settings.

Item	Description
Profile Name	Type a profile name for this MAC object.
Description	(Optional) Type a description.
MAC Object List	Specify a MAC address. Click the [Add Entry] button + to add another entry, or the [Remove Entry] button − to remove an entry.

4. Click [Save].

5.1.3 Service Objects

Service objects contain service definitions, including TCP port ranges, UDP port ranges, ICMP, and custom protocol numbers, which you can apply to policy rules.

- **TCP protocol port range**

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

- **UDP protocol port range**

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

- **ICMP protocol type and code**

For example: ICMP type 8 code 0

- **Custom protocol with specified protocol number**

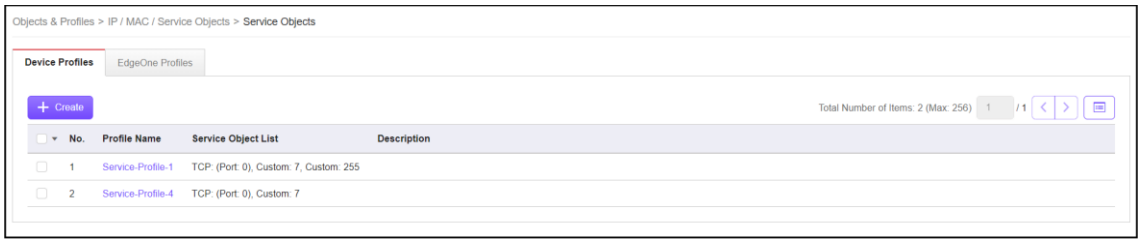
For example: protocol number 6 and service ports ranging from 100 to 120

> The term "protocol number" refers to the protocol number defined in the Internet protocol suite.

5.1.3.1 Configuring Service Objects

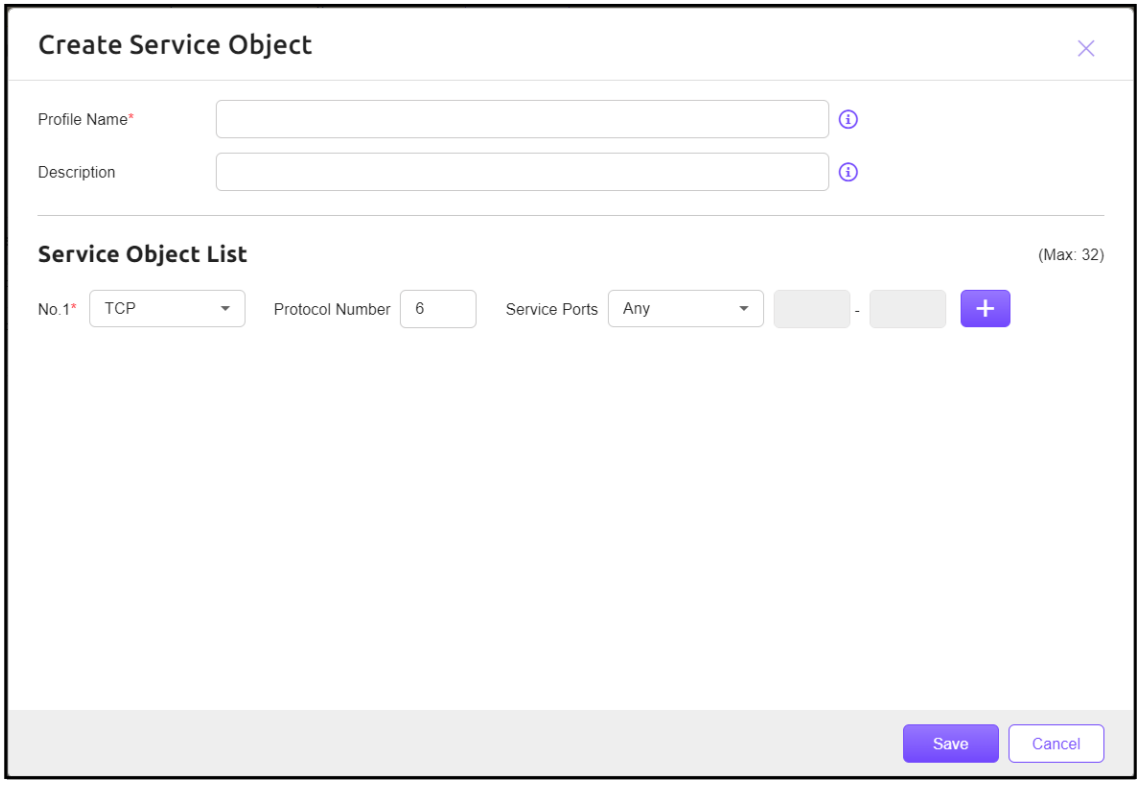
Procedure

1. Go to [Objects & Profiles] > [IP/MAC/Service Objects] > [Service Objects].



2. Do one of the following:

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



3. Configure the following service object settings.

Item	Description
Profile Name	Type a profile name for this service object.
Description	(Optional) Type a description.
Service Object List	Provide one of the following definitions. • **TCP** protocol number and its port range

Item	Description
	• **UDP** protocol number and its port range • **ICMP** protocol number and its type and code • **Custom** protocol with specified protocol number and port range Click the [Add Entry] button + to add another entry, or the [Remove Entry] button − to remove an entry.

4. Click [Save].

5.2 Security Profiles

Create and manage security profiles to control communications across your network.

- Protocol Filter Profiles
- IPS Profiles
- File Filter Profiles
- Domain Name Profiles
- Antivirus Profiles

5.2.1 Protocol Filter Profiles

Protocol Filter profiles contain sophisticated and advanced ICS (Industrial Control System) protocol settings which you can apply to policy rules. The types of ICS protocols you can include in a Protocol Filter profile are:

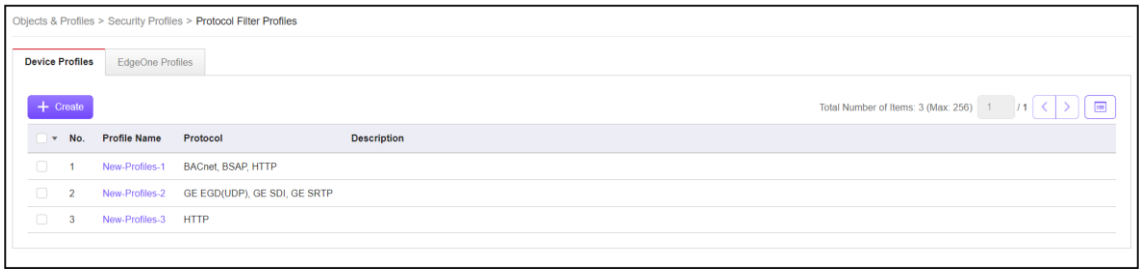
Factory Automation	• CIP • CODESYS • FINS • GE CMP • GE SRTP • MELSOFT • Modbus • OPC CLASSIC • OPC UA • PROFINET • S7COMM • S7COMM_PLUS • SECS/GEM	• SLMP • TOYOPUC • TSAA • BSAP • CC-Link IE Field Basic • Emerson DeltaV • Emerson ROC • EtherCAT • FANUC FOCAS • FL-net • GE EGD (HTTP) • GE EGD (UDP)	• GE SDI • GE iFIX • HART-IP • ION • Panasonic MEWTOCOL • PTP • ROS SimpleMessage • TriStation • Valmet DNA
Building Automation	• BACnet • CN/IP	• KNX • LonWorks/LonTalk	• Niagara Fox

General OT Protocol	• CoAP • Ether-S-Bus • EtherSIO	• MDLC • Moxa Protocol • PCWorx	• RTPS/DDS • Wonderware SuiteLink
HealthCare	• DICOM	• HL7	
Power and Electricity	• IEC 61850-GOOSE • IEC 61850-R-GOOSE • DNP3	• ICCP TASE.2 • IEC 61850-MMS • IEC-104 • IEEE C37.118	• OCPP 1.6J • OCPP 2.0.1 • IEC 61850-R-SV • IEC 62056
Common	• SMB • DNS • FTP • HTTP • HTTPS • MQTT	• MS RPC • PAgP • RDP • SIP/RTP • SMTP • SNMP	• SSH • TELNET • TFTP • TLS • VNC • Windows Update

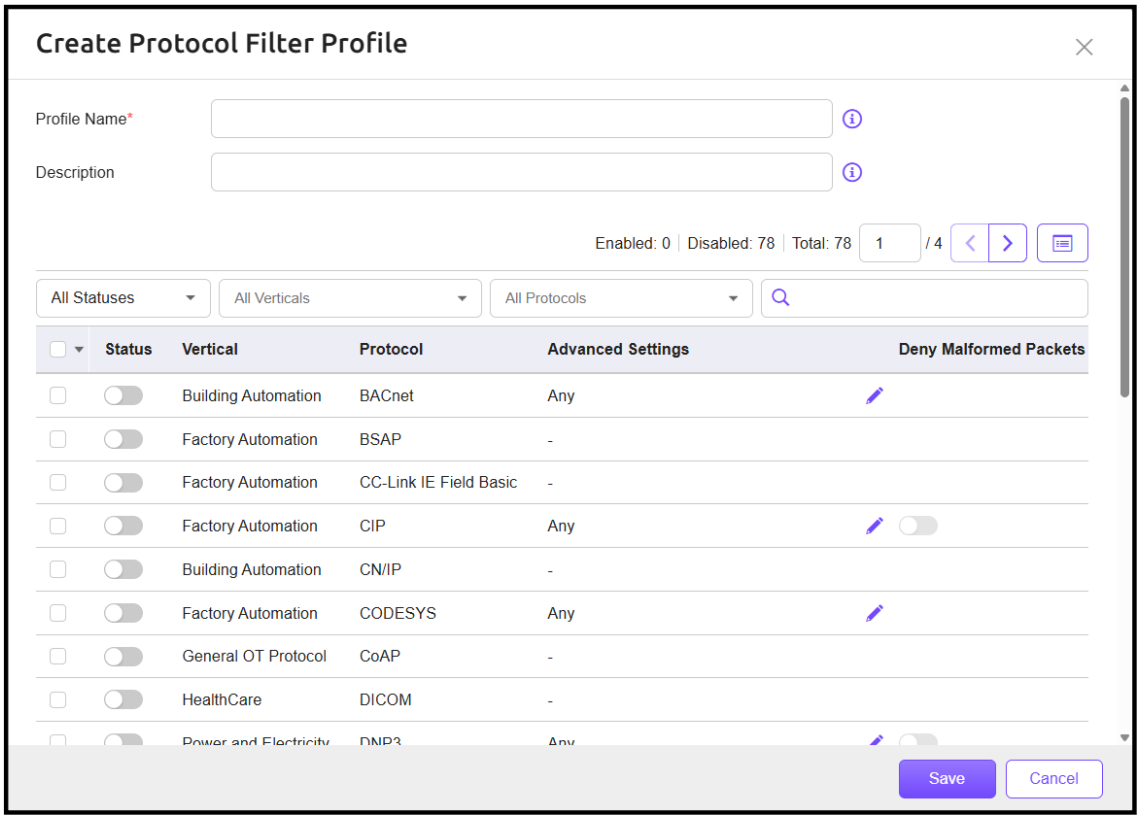
5.2.1.1 Configuring Protocol Filter Profiles

Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [Protocol Filter Profiles].



2. Do one of the following.
   - Click [Create] to create a profile. The [Create Protocol Filter Profile] window will appear.
   - Click a profile name to edit settings. The [Edit Protocol Filter Profile] window will appear.



3. Configure the following Protocol Filter profile settings.

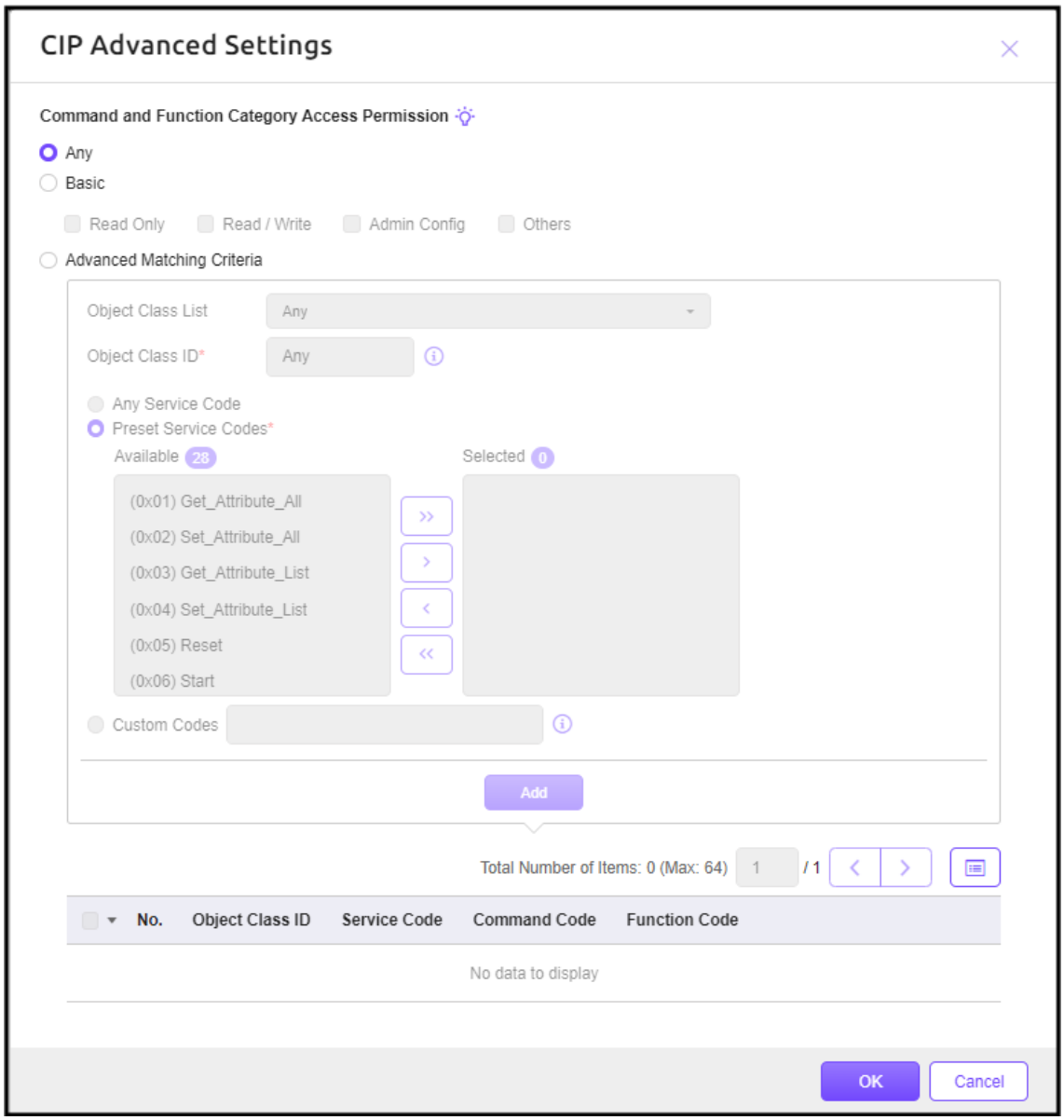
Item	Description
Profile Name	Type a profile name for this Protocol Filter profile.
Description	(Optional) Type a description.
Status	Enable the operational statuses of one or multiple protocols you want to include in this Protocol Filter profile by clicking the toggles. (Default status: Disabled) If you enable Windows Update protocol, you need to enable DNS protocol as well in order for the Windows Update protocol to function properly.
Advanced Settings	Configure advanced settings of each protocol by clicking the edit icon . For more information about configuring the advanced settings of each protocol, see: • Configuring IEC 61850-GOOSE and IEC 61850-R-GOOSE Advanced Settings • Configuring SMB Advanced Settings • Configuring BACnet Advanced Settings • Configuring CIP Advanced Settings • Configuring FINS and PROFINET Advanced Settings • Configuring MELSOFT Advanced Settings • Configuring Modbus Advanced Settings • Configuring S7COMM Advanced Settings • Configuring S7COMM_PLUS Advanced Settings

Item	Description
	• Configuring SECS/GEM Advanced Settings • Configuring SLMP Advanced Settings • Configuring TOYOPUC Advanced Settings • Configuring DNP3 Advanced Settings • Configuring ICCP TASE.2 and IEC61850-MMS Advanced Settings • Configuring IEC-104 Advanced Settings • Configuring IEEE C37.118 Advanced Settings • Configuring GE CMP Advanced Settings • Configuring GE SRTP Advanced Settings • Configuring OCPP 1.6J and OCPP 2.0.1 Advanced Settings • Configuring OPC CLASSIC Advanced Settings • Configuring OPC UA Advanced Settings
Deny Malformed Packets	(Optional) Enable the [Deny Malformed Packets] function by clicking the toggles. 1. When the [Deny Malformed Packets] function is enabled, the Edge device will strictly check the packet format of the specified ICS protocol. If the packet format is incorrect, the device will drop the packets of the ICS protocol. 2. This feature is only applicable to the following nine protocols: IEC 61850-GOOSE, IEC 61850-R-GOOSE, CIP, FINS, Modbus, TOYOPUC, IEC-104, DNP3, and ION (firmware version v2.1 or later).

4. Click [Save].

5.2.1.2 Configuring CIP Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

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

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

   a. From the [Object Class List] drop-down list, select an object class of this protocol. If you want to specify an object class by yourself, then select [Custom] and input an object class ID in the [Object Class ID] field.

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

   • **Any Service Code**: Select this option if you want any of the service codes within the function you specified to be applied.

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

   • **Preset Service Codes**: Select this option if you want to specify one or multiple service codes, then move the service codes from the [Available] field to the [Selected] field.

   • **Custom Codes**: Select this option if you want to specify one or multiple service codes by yourself, then input service codes in the [Custom Codes] field.

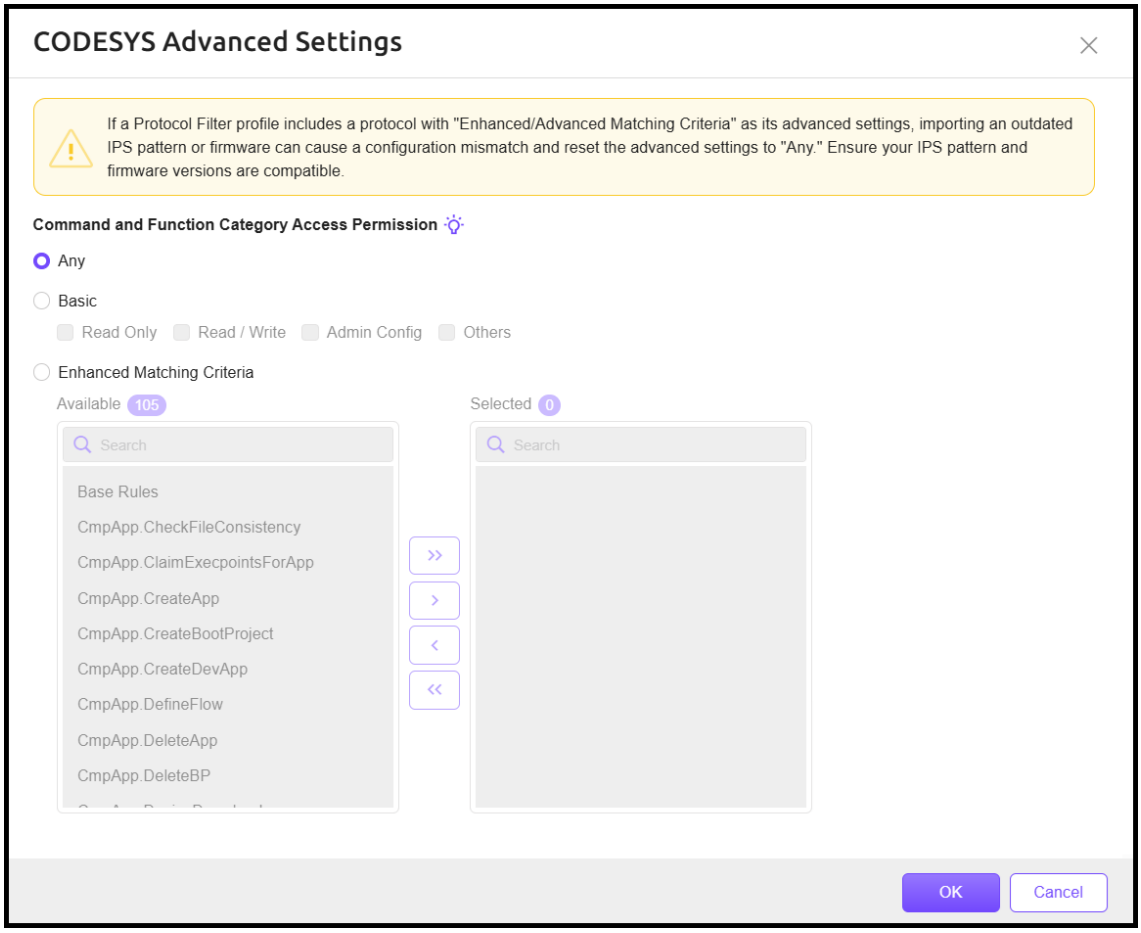
   c. Click [Add].

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

3. Click [OK].

5.2.1.3 Configuring CODESYS Advanced Settings

Through the [CODESYS Advanced Settings] window, you can further configure the command and function category access permission settings, including the enhanced matching criteria based on which the protocol will work.



After you access the [CODESYS Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Enhanced Matching Criteria**: Select this option to further configure enhanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Enhanced Matching Criteria], select one or multiple criteria in the [Available] field and move them to the [Selected] field.

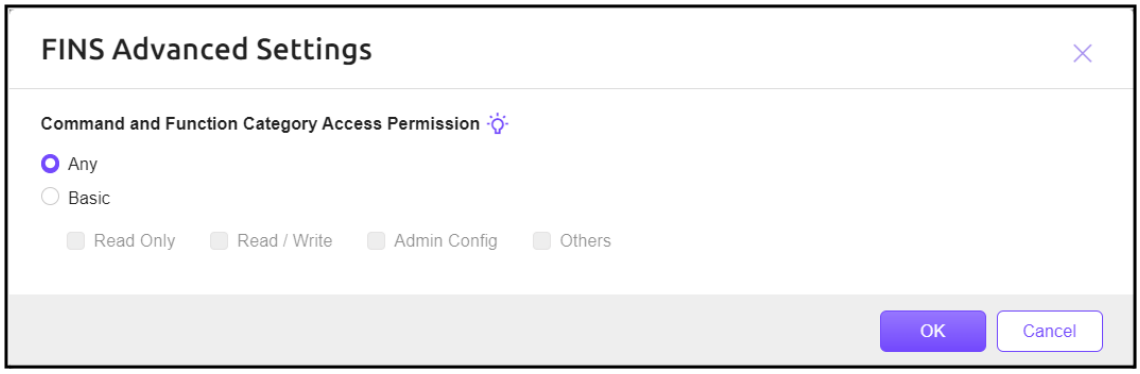
3. Click [OK].

> ⚠ If a Protocol Filter profile includes a protocol with "Enhanced/Advanced Matching Criteria" as its advanced settings, importing an outdated IPS pattern or firmware can cause a configuration mismatch and reset the advanced settings to "Any." Ensure your IPS pattern and firmware versions are compatible.

5.2.1.4 Configuring FINS and PROFINET Advanced Settings

Through the [FINS/PROFINET Advanced Settings] window, you can further specify the command and function category access permission based on which the protocol will work.

In this section, we will demonstrate how to configure the FINS advanced settings. Please take the same approach when configuring the PROFINET advanced settings.



After you access the [FINS Advanced Settings] window, follow the procedure below.

Procedure

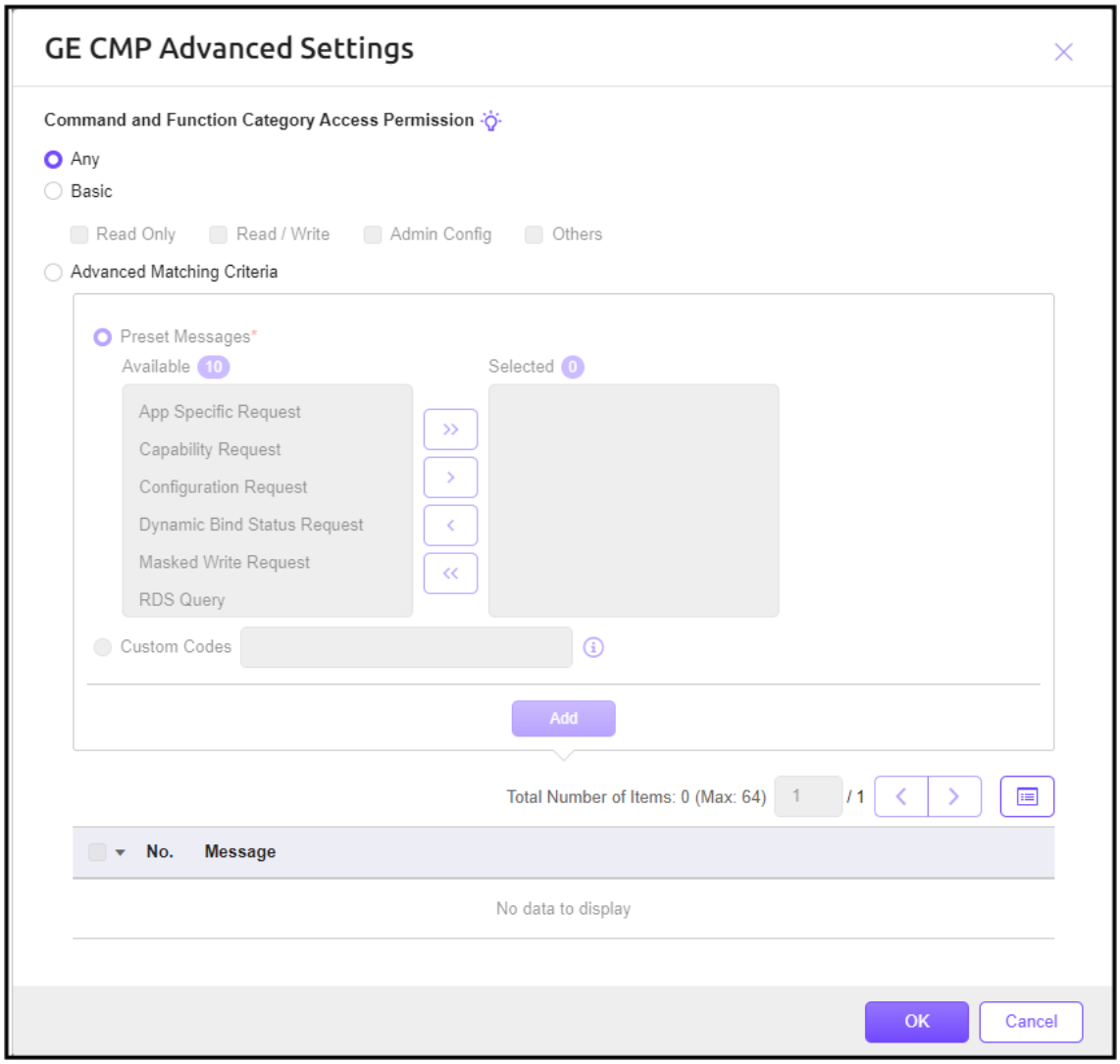
1. Configure [Command and Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

2. Click [OK].

5.2.1.5 Configuring GE CMP Advanced Settings

Through the [GE CMP Advanced Settings] window, you can further configure the command and function category access permission settings, including message types based on which the protocol will work.



After you access the [GE CMP Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], follow the steps below to configure the message types.

   a. Select [Preset Messages] or [Custom Codes] based on your needs.

      • **Preset Messages**: Select this option if you want to specify one or multiple types of messages, then move the message types from the [Available] field to the [Selected] field.

      • **Custom Codes**: Select this option if you want to specify one or multiple codes by yourself, then input codes in the [Custom Codes] field.

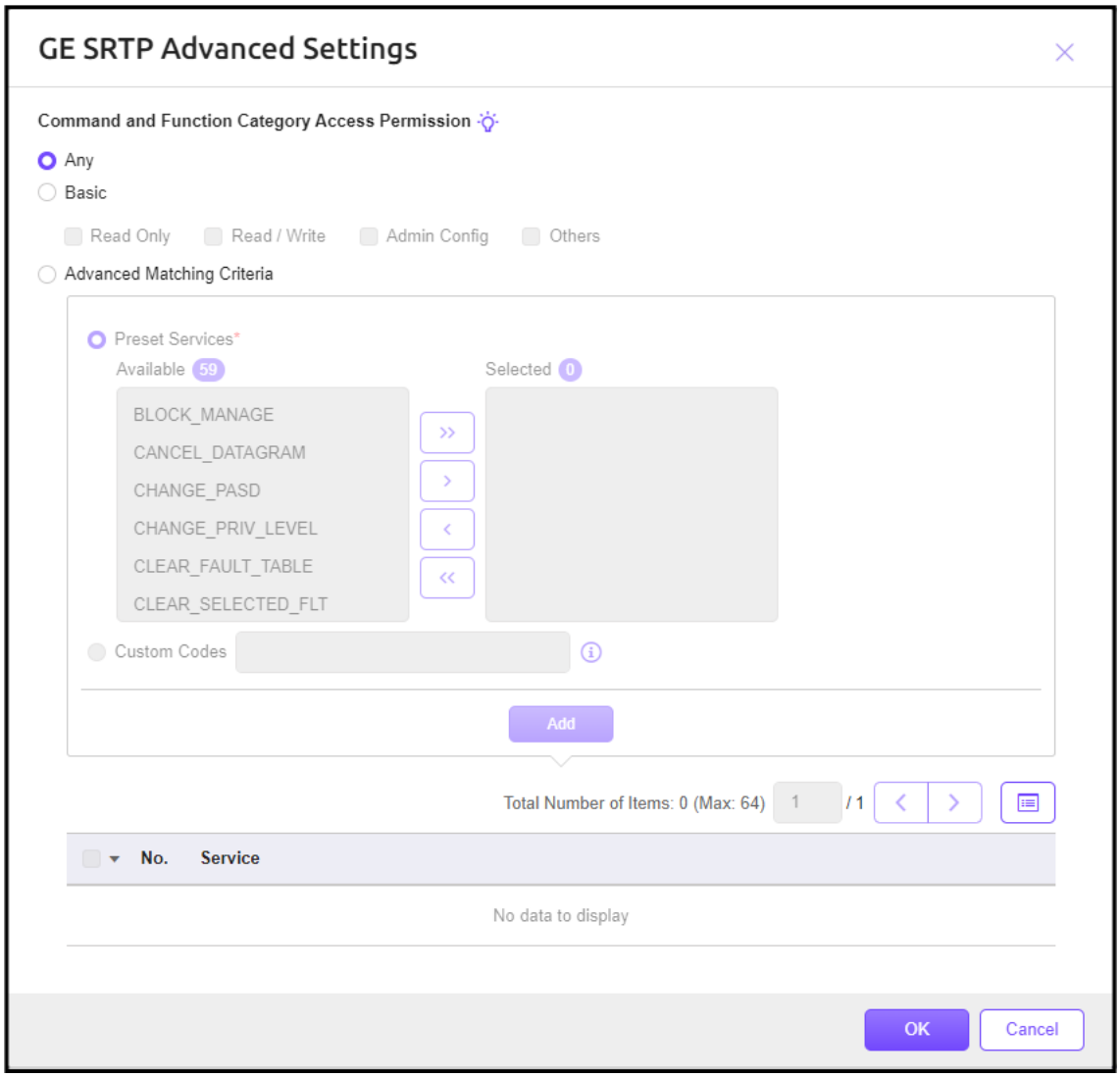
   b. Click [Add].

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

3. Click [OK].

5.2.1.6 Configuring GE SRTP Advanced Settings

Through the [GE SRTP Advanced Settings] window, you can further configure the command and function category access permission settings, including service types based on which the protocol will work.



After you access the [GE SRTP Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], follow the steps below to configure the service types.

a. Select [Preset Services] or [Custom Codes] based on your needs.

• **Preset Services**: Select this option if you want to specify one or multiple types of services, then move the service types from the [Available] field to the [Selected] field.

• **Custom Codes**: Select this option if you want to specify one or multiple codes by yourself, then input codes in the [Custom Codes] field.

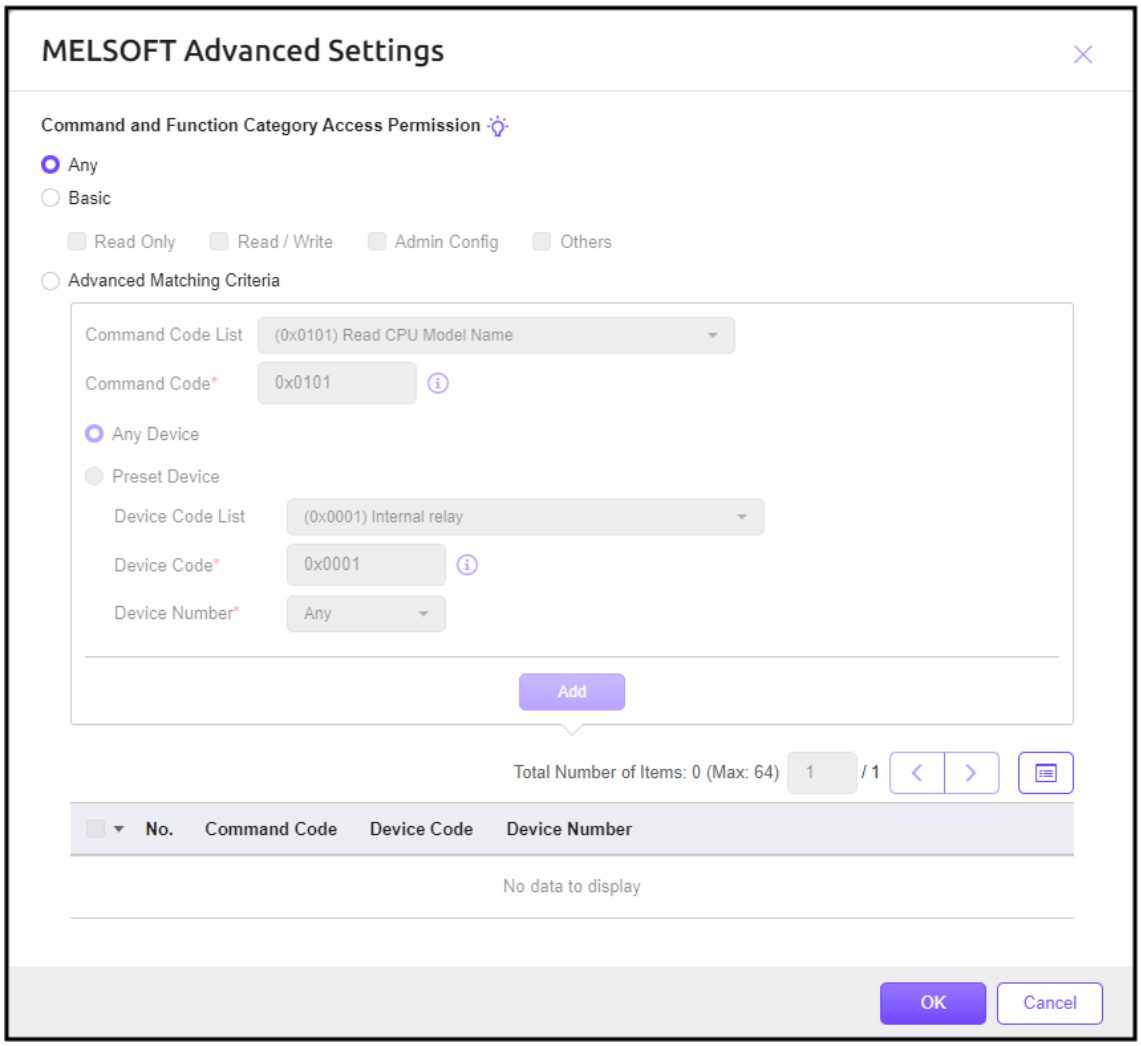
b. Click [Add].

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

3. Click [OK].

5.2.1.7 Configuring MELSOFT Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

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

a. From the [Command Code List] drop-down list, select a command code of this protocol. If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

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

- **Any Device**: Select this option if you want any of the device codes within the function you specified to be applied.
- **Preset Device**: Select this option if you want to specify a device code, then further configure the following settings.
  - From the [Device Code List] drop-down list, select a device code. If you want to specify a device code by yourself, then select [Custom] and input a device code in the [Device Code] field.
  - From the [Device Number] drop-down list, select one of the following options based on your needs.
    - **Any**: Select this option if you don't want to include a device number as a filter criterion.
    - **Single**: Select this option if you want to specify a device number.
    - **Range**: Select this option if you want to specify a range of device numbers.

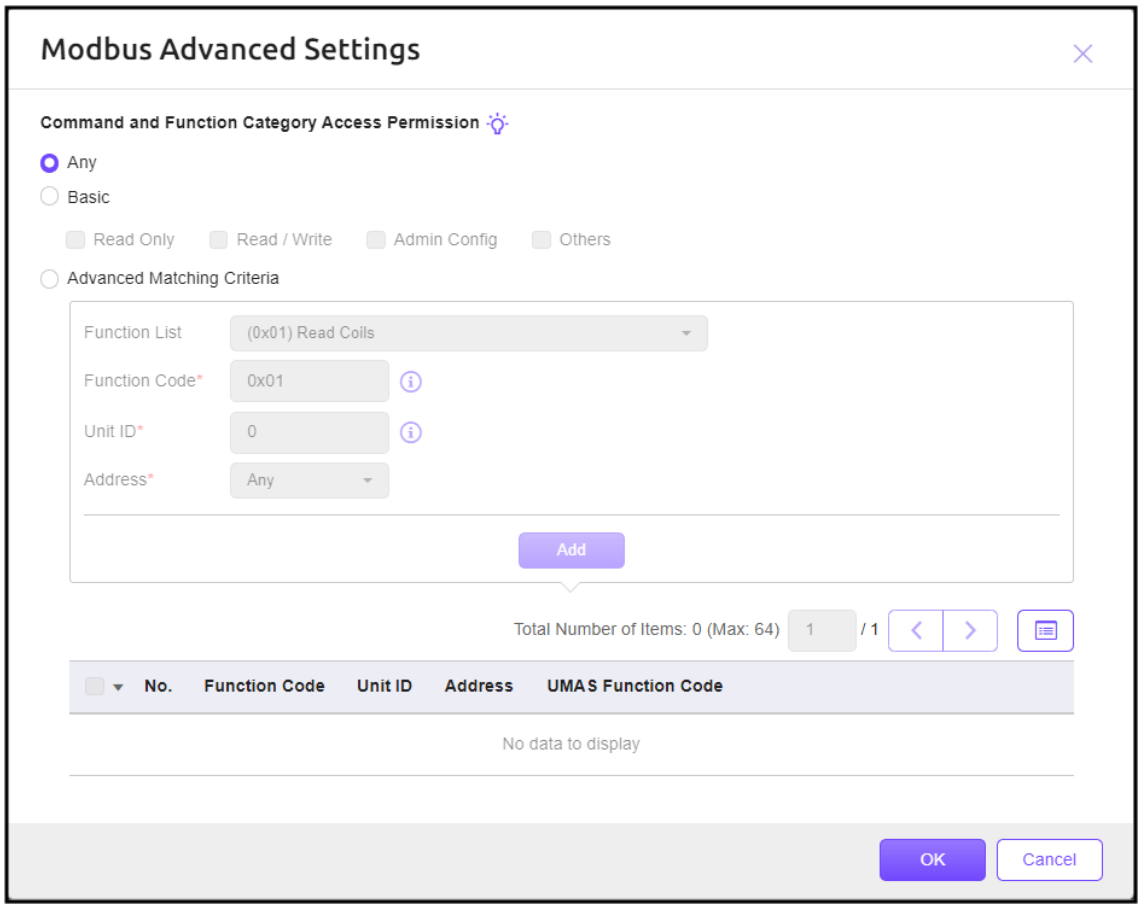
b. Click [Add].

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

3. Click [OK].

5.2.1.8 Configuring Modbus Advanced Settings

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



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

Procedure

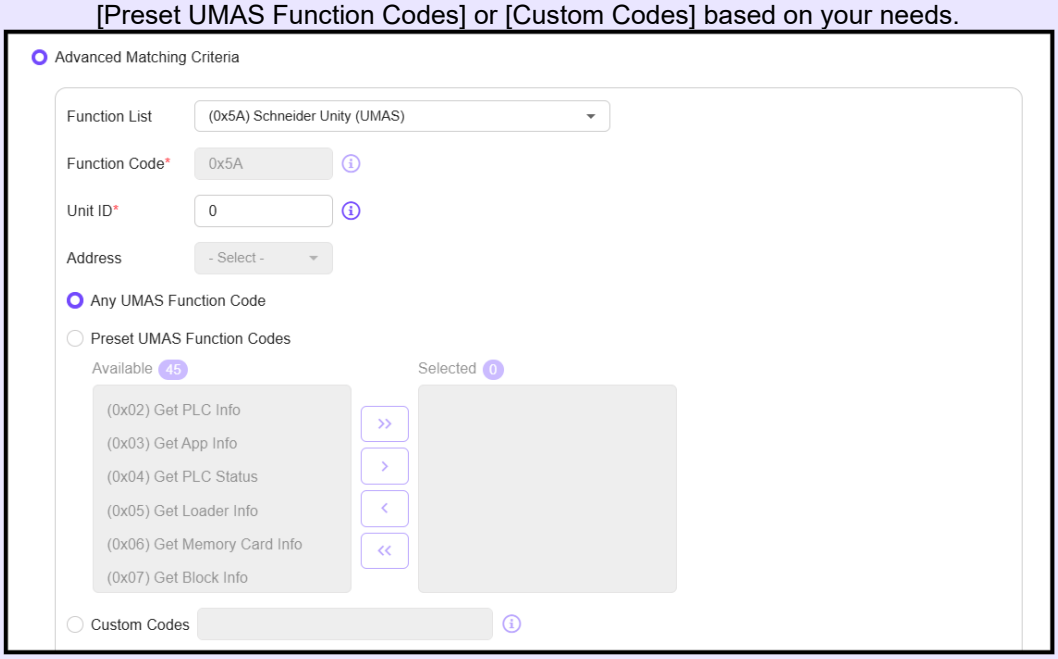
1. Configure [Command and Function Category Access Permission] by selecting one of the following options.

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

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

   a. From the [Function List] drop-down list, select a function of this protocol. If you want to specify a function by yourself, then select [Custom] and input a function code in the [Function Code] field.

If you select [(0x5A) Schneider Unity (UMAS)], further select [Any UMAS Function Code], [Preset UMAS Function Codes] or [Custom Codes] based on your needs.



- **Any UMAS Function Code**: Select this option if you want any of the UMAS function codes to be applied.
- **Preset UMAS Function Codes**: Select this option if you want to specify one or multiple UMAS function codes, and then move the UMAS function codes from the [Available] to the [Selected] field.
- **Custom Codes**: Select this option if you want to specify one or multiple UMAS codes by yourself, and then input UMAS codes in the [Custom Codes] field.

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

c. For some function codes, select **Any**, **Single** or **Range** from the [Address] drop-down list. If you select Single or Range, further specify an address or range of addresses based on which the function will operate.

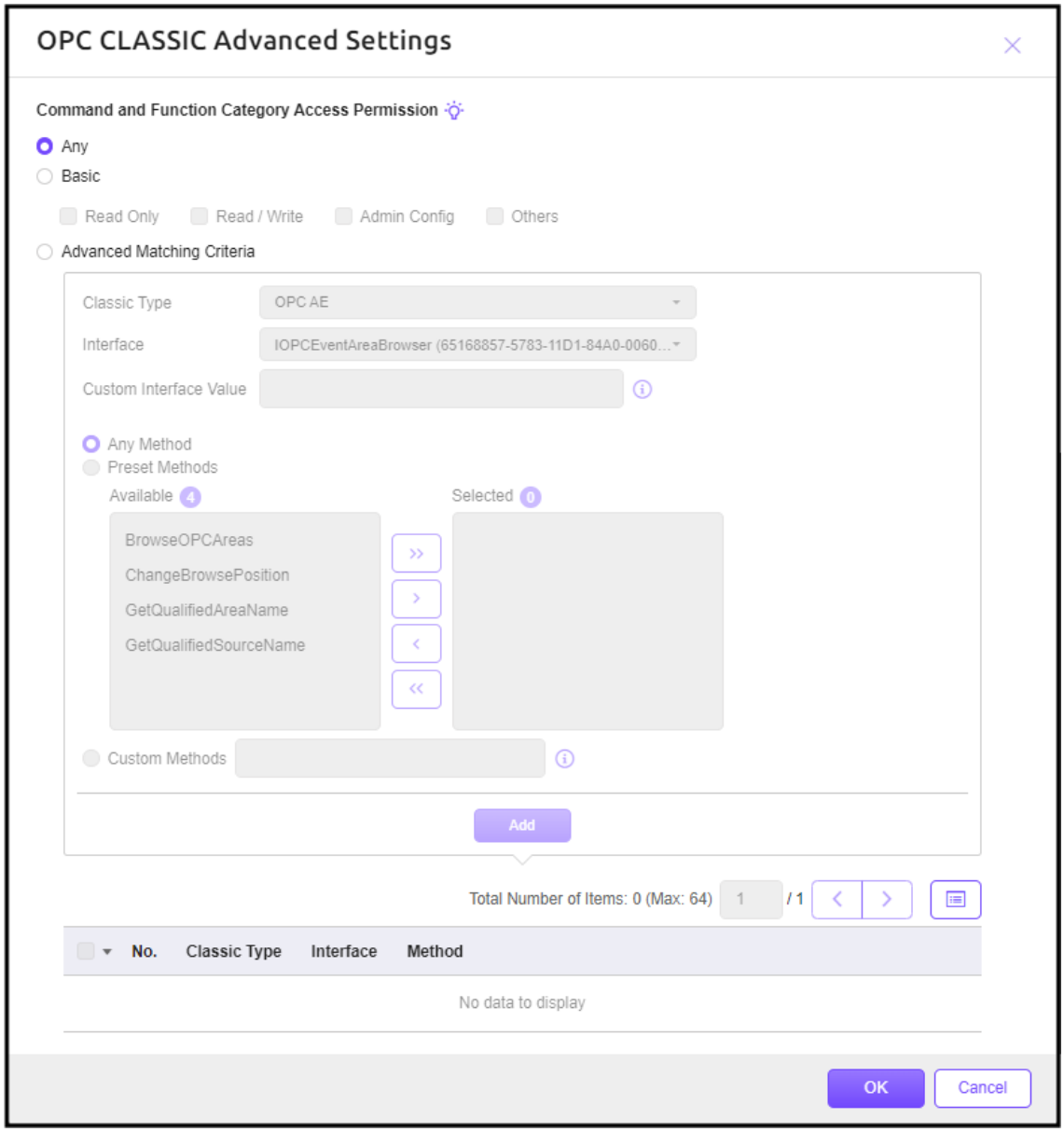
d. Click [Add].

e. (Optional) Repeat the above steps to add more protocol definition entries.

3. Click [OK].

5.2.1.9 Configuring OPC CLASSIC Advanced Settings

Through the [OPC CLASSIC Advanced Settings] window, you can further configure the command and function category access permission settings, including classic types, interfaces, and method types based on which the protocol will work.



After you access the [OPC CLASSIC Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

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

2. If you select [Advanced Matching Criteria], follow the steps below to configure the classic types, interfaces, and method types.

   a. From the [Classic Type] drop-down list, select a classic type of this protocol, then select an interface from the [Interface] drop-down list for your selected classic type.

   b. If your classic type and interface are [Custom], further input a UUID (Universally Unique Identifier) in the [Custom Interface Value] field.

   c. Select [Any Method], [Preset Methods] or [Custom Methods] based on your needs.

      • **Any Method**: Select this option if you want any of the method types within the function you specified to be applied.

      • **Preset Methods**: Select this option if you want to specify one or multiple method types, then move the method types from the [Available] field to the [Selected] field.

⚠️	The [Preset Methods] option is not available if the classic type and interface are [Custom].

      • **Custom Methods**: Select this option if you want to specify one or multiple method types by yourself, then input method values in the [Custom Methods] field.

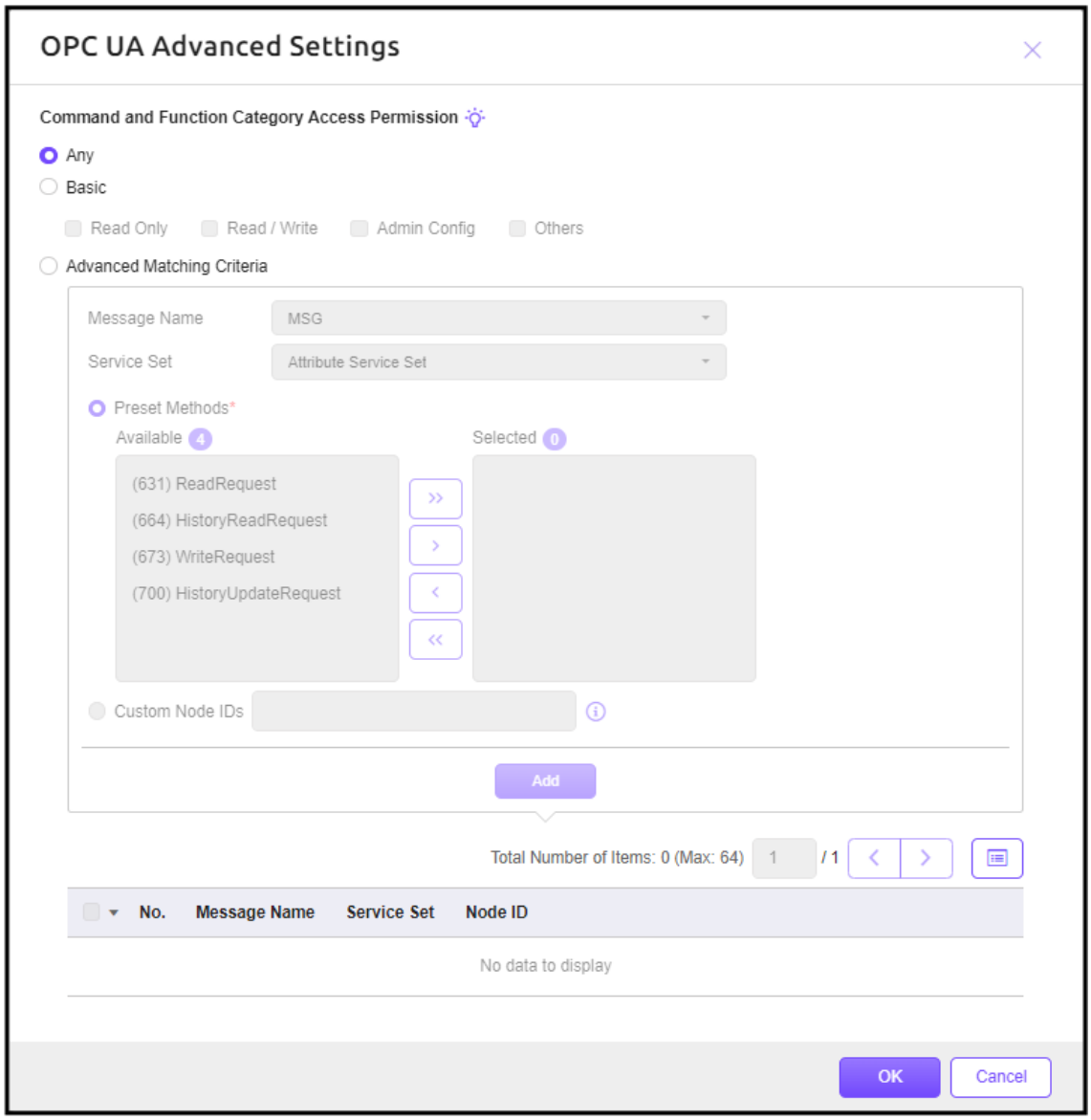
   d. Click [Add].

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

3. Click [OK].

5.2.1.10 Configuring OPC UA Advanced Settings

Through the [OPC UA Advanced Settings] window, you can further configure the command and function category access permission settings, including service sets and method types based on which the protocol will work.



After you access the [OPC UA Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

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

2. If you select [Advanced Matching Criteria], follow the steps below to configure the service sets and method types.

   a. From the [Service Set] drop-down list, select a service set of this protocol and its method types, then move the method types from the [Available] field to the [Selected] field.

   b. If your service set is [Custom], input one or multiple node IDs in the [Custom Node IDs] field.

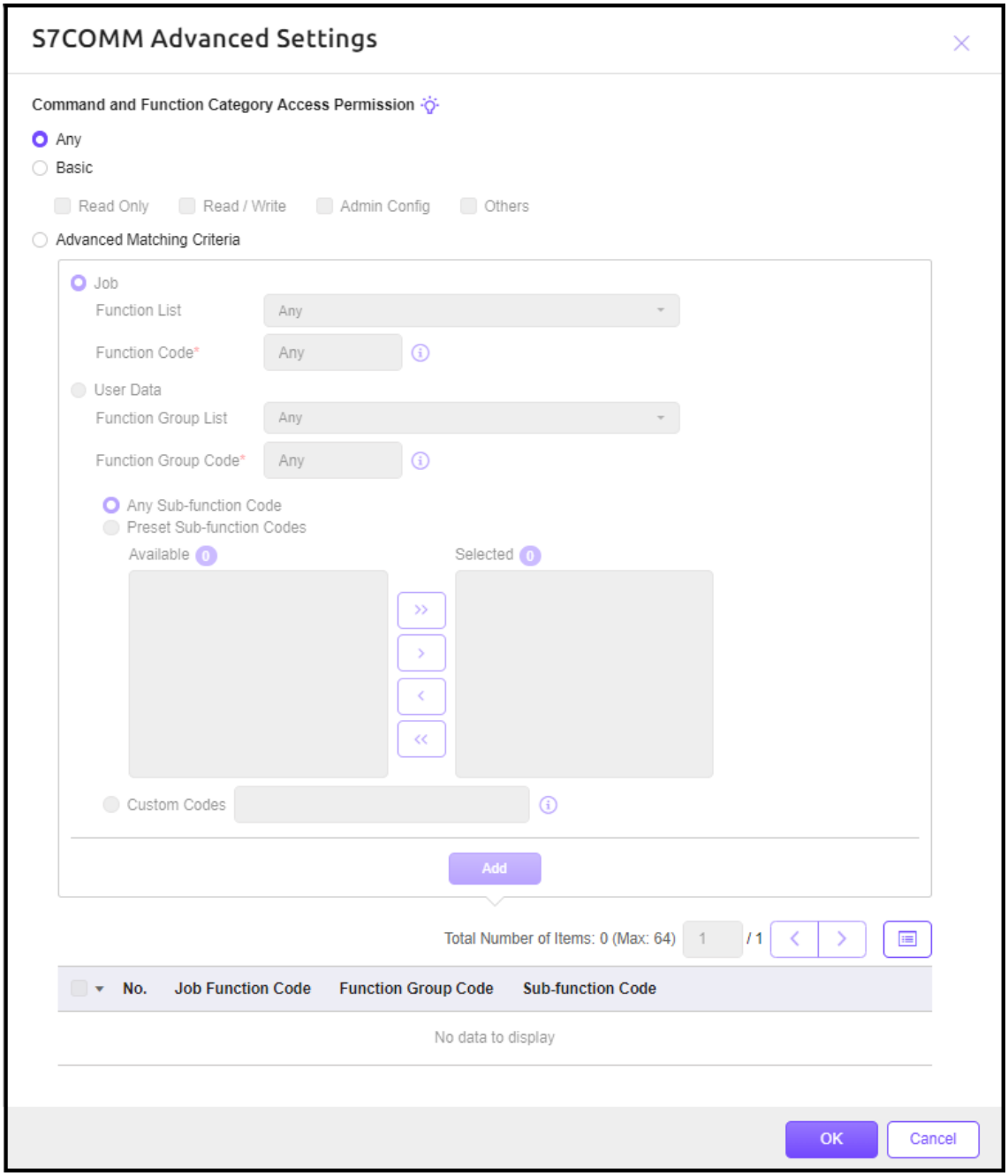
   c. Click [Add].

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

3. Click [OK].

5.2.1.11 Configuring S7COMM Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)

- **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
- **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
- **Others**: Proprietary, customized, or undocumented commands

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

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

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

• **Job**: Select this option to specify one function code from the [Function list] drop-down list. If you want to specify a function by yourself, then select [Custom] and input a function code in the [Function Code] field.

• **User Data**: Select this option to specify one function group code from the [Function Group List] drop-down list. If you want to specify a function group by yourself, then select [Custom] and input a function group code in the [Function Group Code] field.

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

• **Any Sub-function Code**: Select this option if you want any of the sub-function codes within the function group code you specified to be applied.

• **Preset Sub-function Codes**: Select this option if you want to specify one or multiple sub-function codes, and then move the sub-function codes from the [Available] field to the [Selected] field.

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

• **Custom Codes**: Select this option if you want to specify one or multiple sub-function codes by yourself, and then input sub-function codes in the [Custom Codes] field.

⚠	The [Custom Codes] option is not available if the function group is [Any].

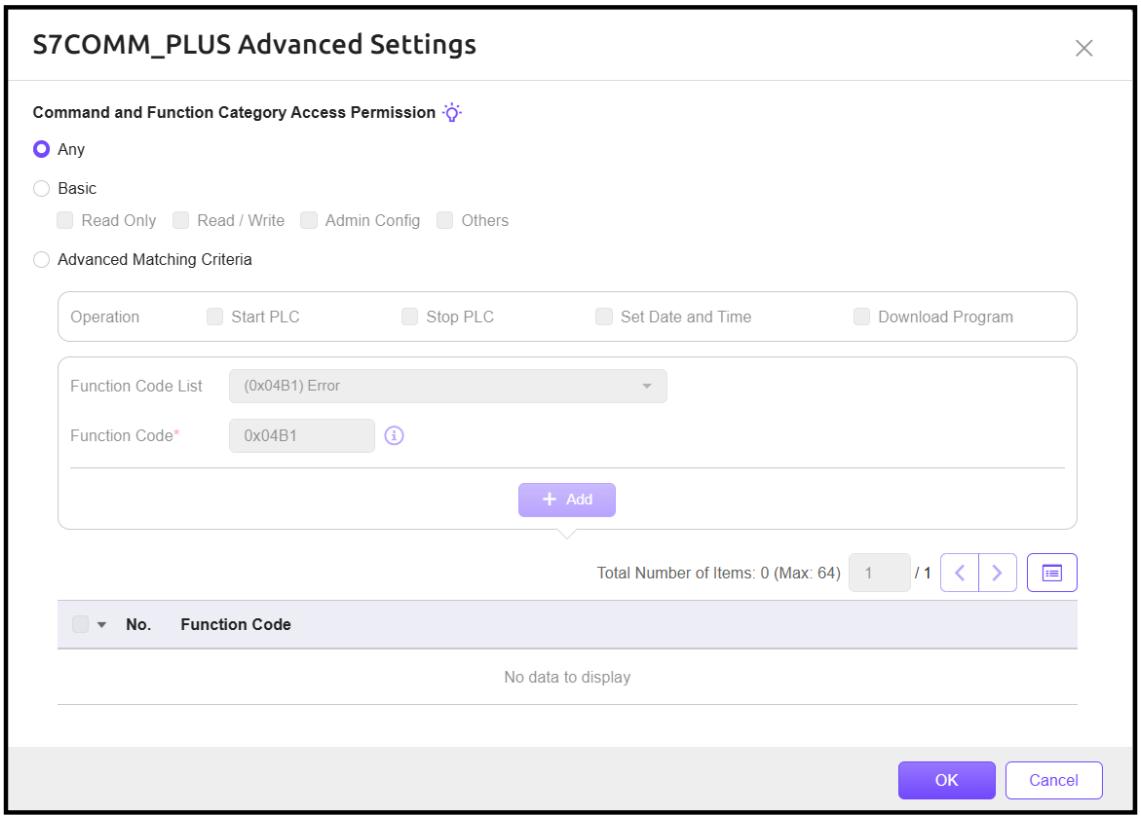
b. Click [Add].

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

3. Click [OK].

5.2.1.12 Configuring S7COMM_PLUS Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], follow the steps below to configure operations and function codes.

a. (Optional) In the [Operation] section, select one or multiple operation options.

b. From the [Function Code List] drop-down list, select a function of this protocol. If you want to specify a function by yourself, then select [Custom] and input a function code in the [Function Code] field.

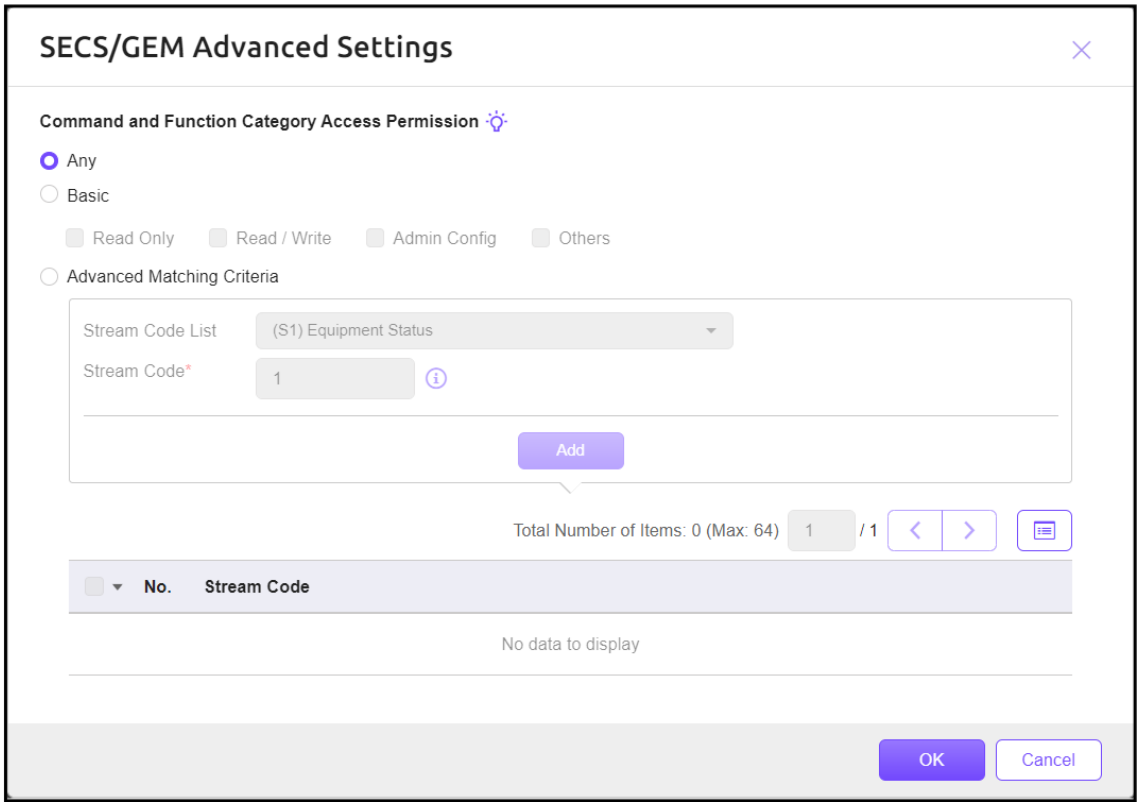
c. Click [Add].

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

3. Click [OK].

5.2.1.13 Configuring SECS/GEM Advanced Settings

Through the [SECS/GEM Advanced Settings] window, you can further configure the command and function category access permission settings, including stream codes based on which the protocol will work.



After you access the [SECS/GEM Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], follow the steps below to configure the stream codes.

a. From the [Stream Code List] drop-down list, select a function of this protocol. If you want to specify a function by yourself, then select [Custom] and input a stream code in the [Stream Code] field.

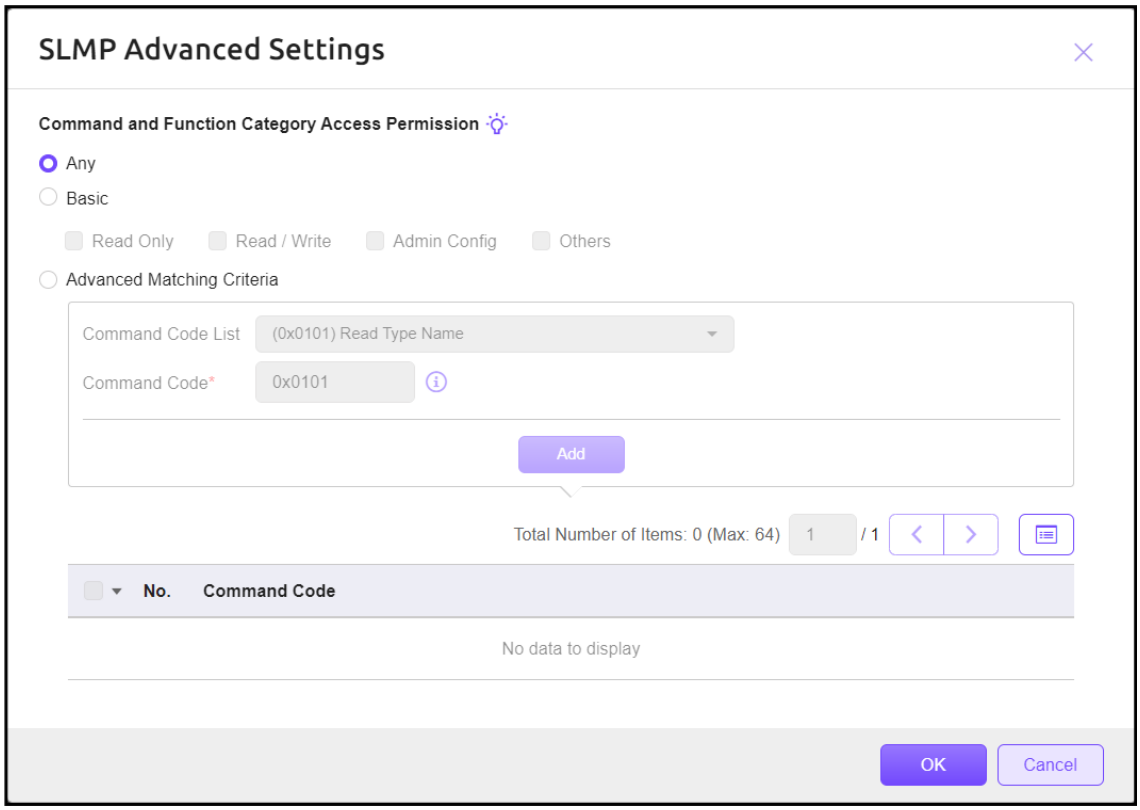
b. Click [Add].

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

3. Click [OK].

5.2.1.14 Configuring SLMP Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

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

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

   a. From the [Command Code List] drop-down list, select a command code of this protocol. If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

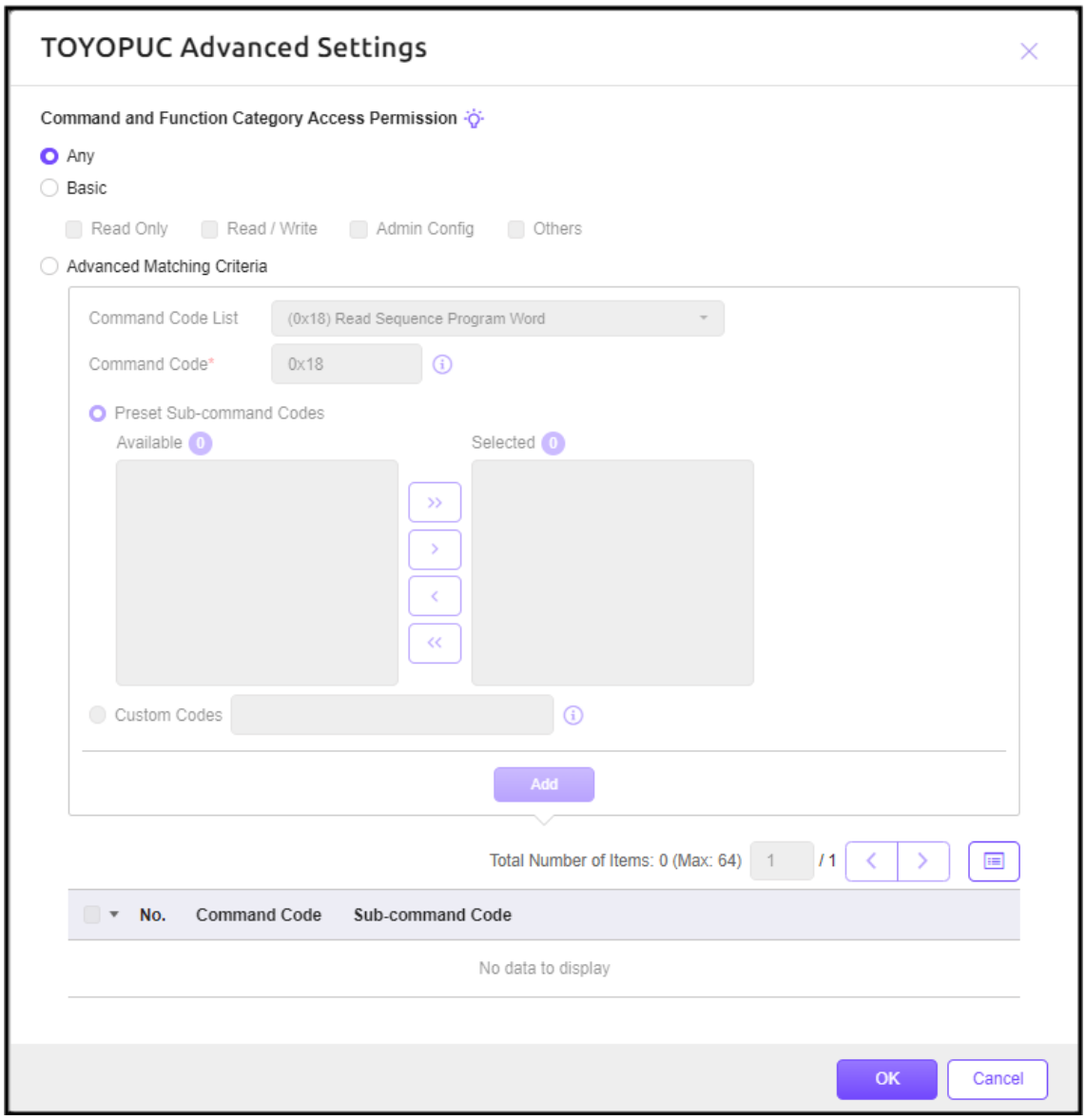
   b. Click [Add].

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

3. Click [OK].

5.2.1.15 Configuring TOYOPUC Advanced Settings

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



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

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

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

a. From the [Command Code List] drop-down list, select a command code of this protocol. If you want to specify a command code by yourself, then select [Custom] and input a command code in the [Command Code] field.

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

• **Preset Sub-command Codes**: Select this option if you want to specify one or multiple sub-command codes, and then move the sub-command codes from the [Available] field to the [Selected] field.

• **Custom Codes**: Select this option if you want to specify one or multiple sub-command codes by yourself, then input sub-command codes in the [Custom Codes] field.

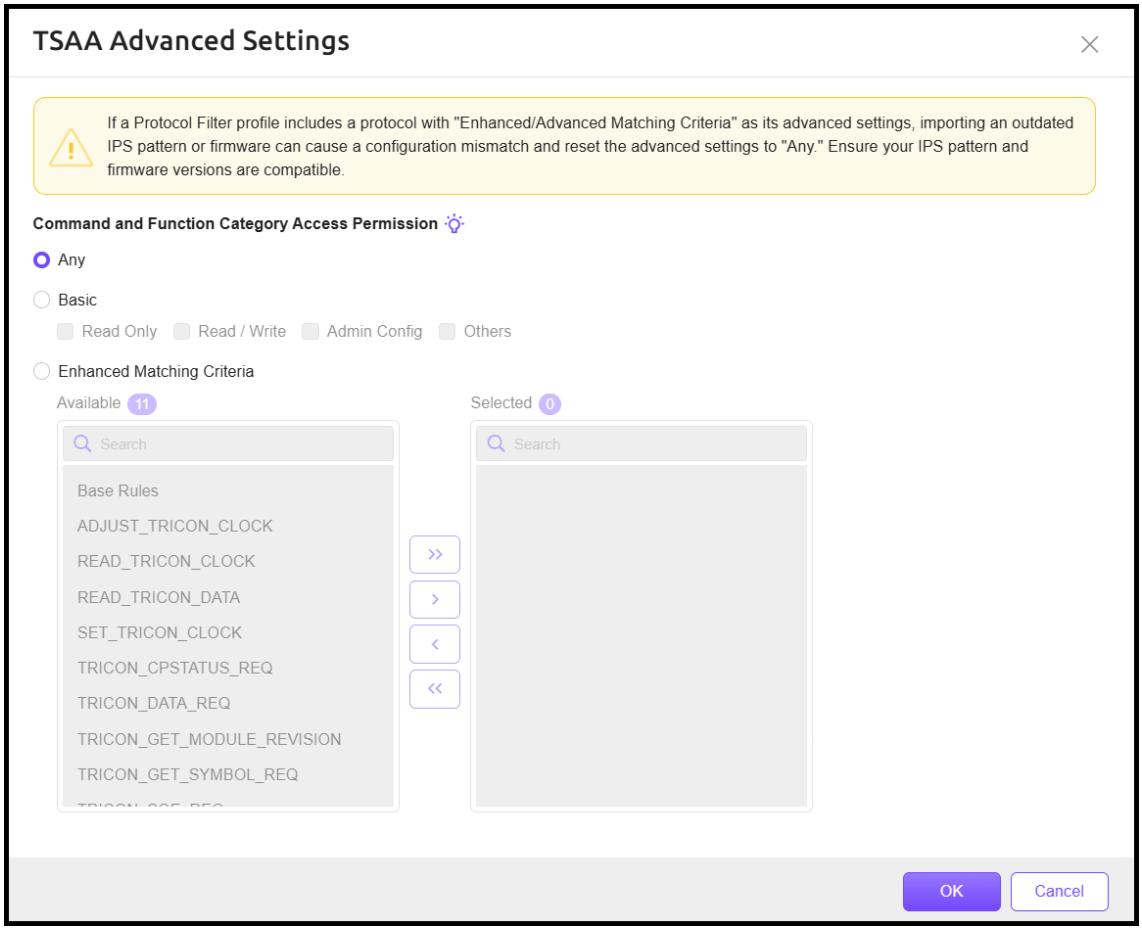
c. Click [Add].

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

3. Click [OK].

5.2.1.16 Configuring TSAA Advanced Settings

Through the [TSAA Advanced Settings] window, you can further configure the command and function category access permission settings, including the enhanced matching criteria based on which the protocol will work.



After you access the [TSAA Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Enhanced Matching Criteria**: Select this option to further configure enhanced matching criteria for the [Command and Function Category Access Permission].

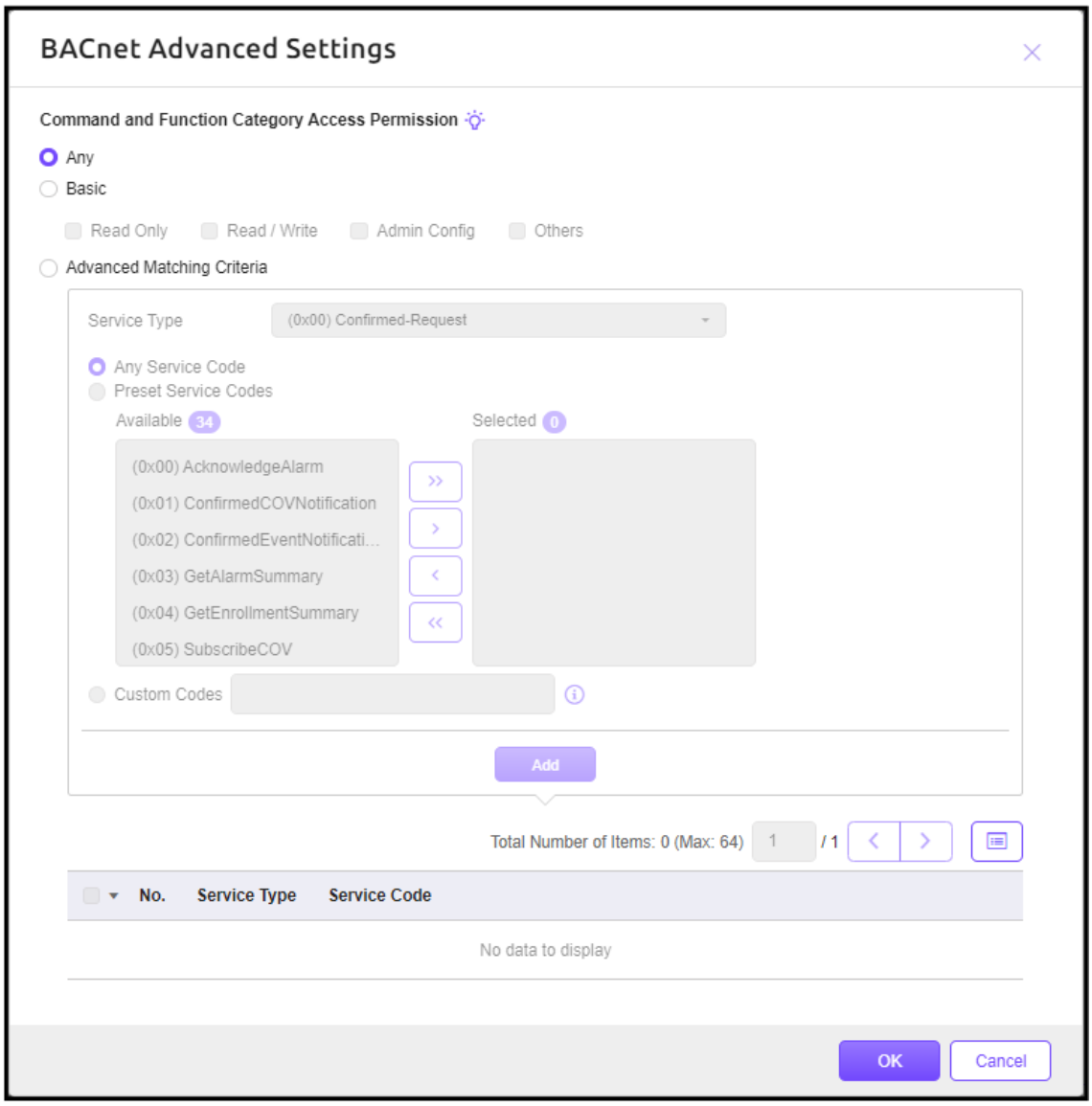
2. If you select [Enhanced Matching Criteria], select one or multiple criteria in the [Available] field and move them to the [Selected] field.

3. Click [OK].

> ⚠ If a Protocol Filter profile includes a protocol with "Enhanced/Advanced Matching Criteria" as its advanced settings, importing an outdated IPS pattern or firmware can cause a configuration mismatch and reset the advanced settings to "Any." Ensure your IPS pattern and firmware versions are compatible.

5.2.1.17 Configuring BACnet Advanced Settings

Through the [BACnet Advanced Settings] window, you can further configure the command and function category access permission settings, including service types and service codes based on which the protocol will work.



After you access the [BACnet Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:

- **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
- **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
- **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
- **Others**: Proprietary, customized, or undocumented commands

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

2. If you select [Advanced Matching Criteria], follow the steps below to configure the service types and service codes.

   a. From the [Service Type] drop-down list, select a service type of this protocol.

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

   • **Any Service Code**: Select this option if you want any of the service codes within the function you specified to be applied.

   • **Preset Service Codes**: Select this option if you want to specify one or multiple service codes, then move the service codes from the [Available] field to the [Selected] field.

   • **Custom Codes**: Select this option if you want to specify one or multiple service codes by yourself, then input service codes in the [Custom Codes] field.

   c. Click [Add].

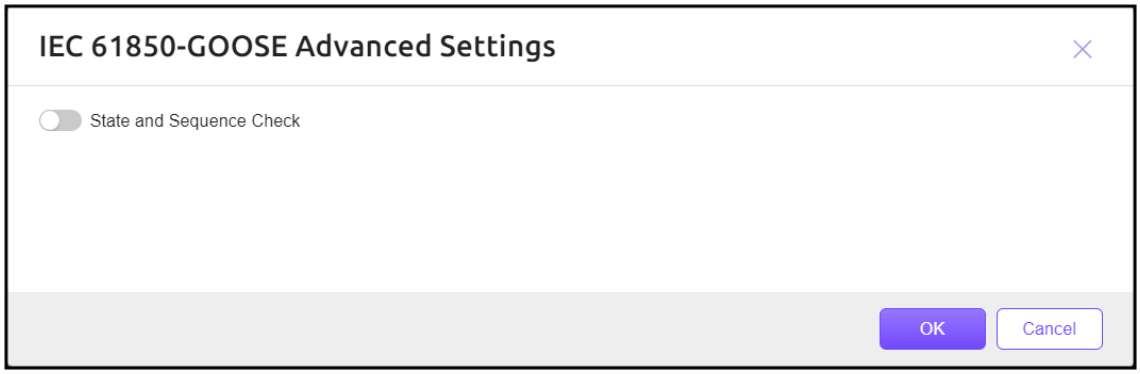
   d. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

5.2.1.18 Configuring IEC 61850-GOOSE and IEC 61850-R-GOOSE Advanced Settings

Through the [IEC 61850-GOOSE/IEC 61850-R-GOOSE Advanced Settings] window, you can further enable or disable the [State and Sequence Check] function.

In this section, we will demonstrate how to configure the IEC 61850-GOOSE advanced settings. Please take the same approach when configuring the IEC 61850-R-GOOSE advanced settings.



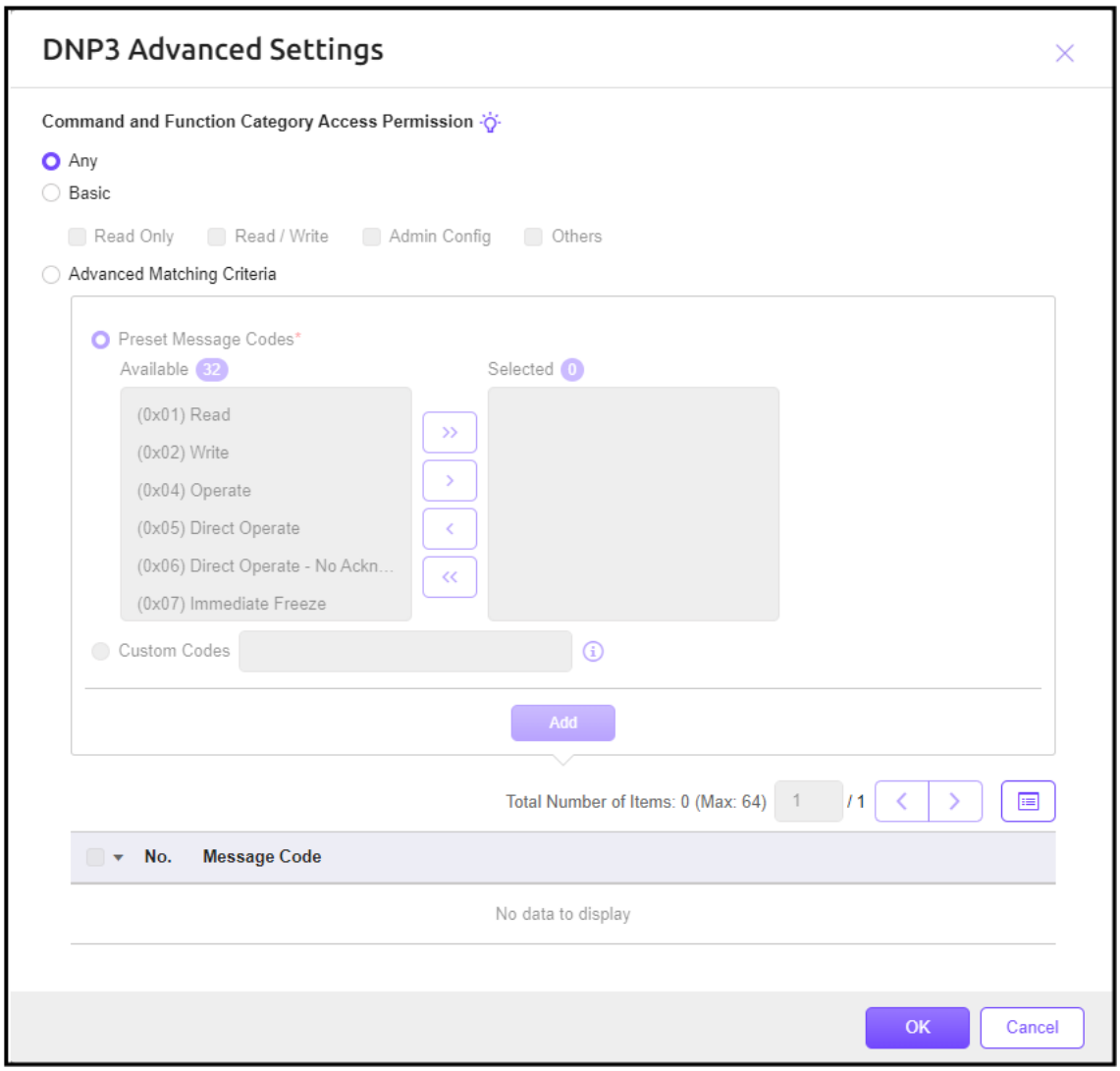
After you access the [IEC 61850-GOOSE Advanced Settings] window, follow the procedure below.

Procedure

1. Enable or disable the [State and Sequence Check] function by clicking the toggle.
2. Click [OK].

5.2.1.19 Configuring DNP3 Advanced Settings

Through the [DNP3 Advanced Settings] window, you can further configure the command and function category access permission settings, including message codes based on which the protocol will work.



After you access the [DNP3 Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system

- **Others**: Proprietary, customized, or undocumented commands

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

2. If you select [Advanced Matching Criteria], follow the steps below to configure the message codes.

a. Select [Preset Message Codes] or [Custom Codes] based on your needs.

• **Preset Message Codes**: Select this option if you want to specify one or multiple message codes, then move the message codes from the [Available] field to the [Selected] field.

• **Custom Codes**: Select this option if you want to specify one or multiple message codes by yourself, then input message codes in the [Custom Codes] field.

b. Click [Add].

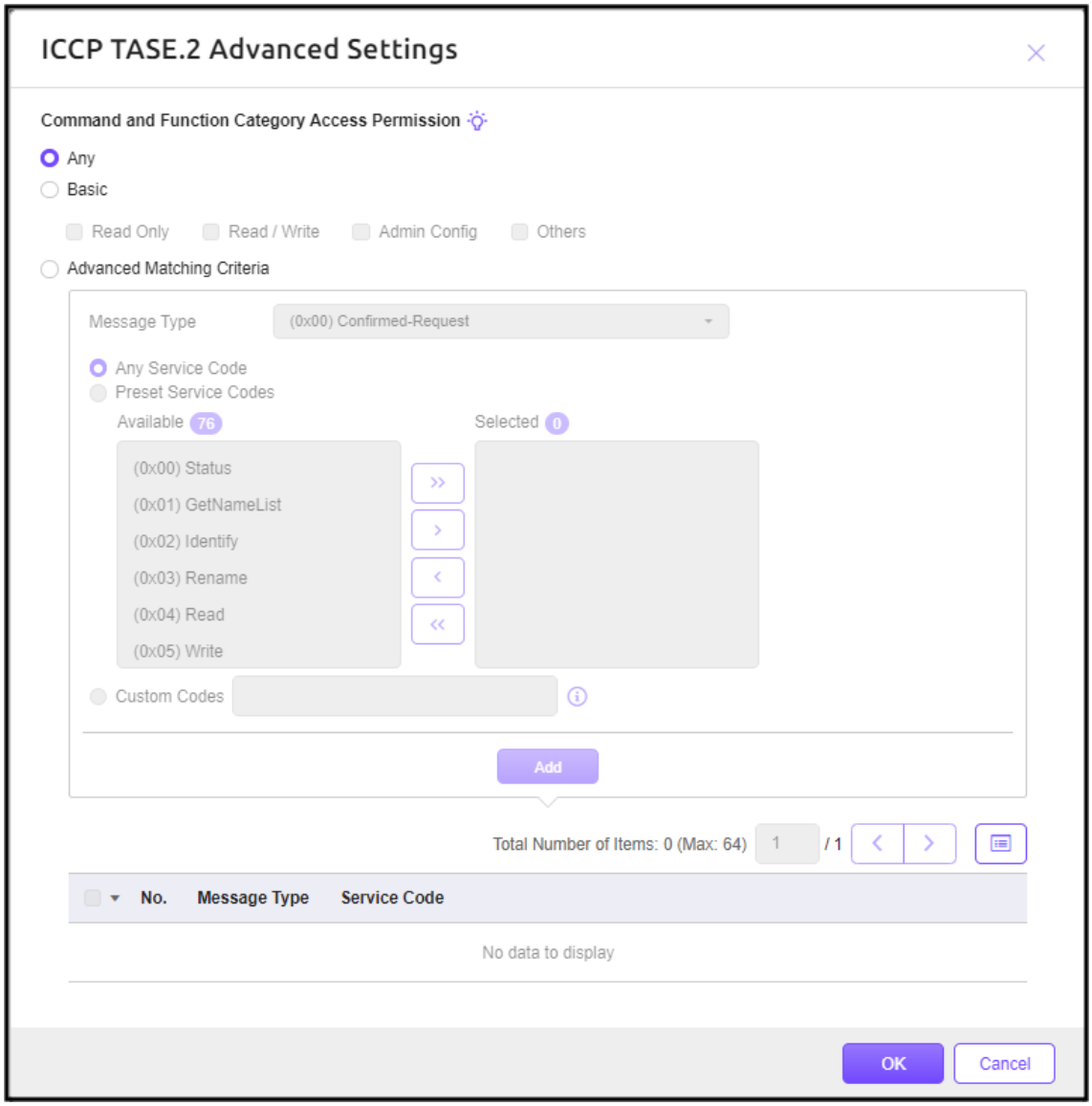
c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

5.2.1.20 Configuring ICCP TASE.2 & IEC61850-MMS Advanced Settings

Through the [ICCP TASE.2/IEC61850-MMS Advanced Settings] window, you can further configure the command and function category access permission settings, including message types and service codes based on which the protocol will work.

In this section, we will demonstrate how to configure the ICCP TASE.2 advanced settings. Please take the same approach when configuring the IEC61850-MMS advanced settings.



After you access the [ICCP TASE.2 Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands

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

2. If you select [Advanced Matching Criteria], follow the steps below to configure the message types and service codes.

   a. From the [Message Type] drop-down list, select a message type of this protocol.

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

      • **Any Service Code**: Select this option if you want any of the service codes within the function you specified to be applied.

      • **Preset Service Codes**: Select this option if you want to specify one or multiple service codes, then move the service codes from the [Available] field to the [Selected] field.

      • **Custom Codes**: Select this option if you want to specify one or multiple service codes by yourself, then input service codes in the [Custom Codes] field.

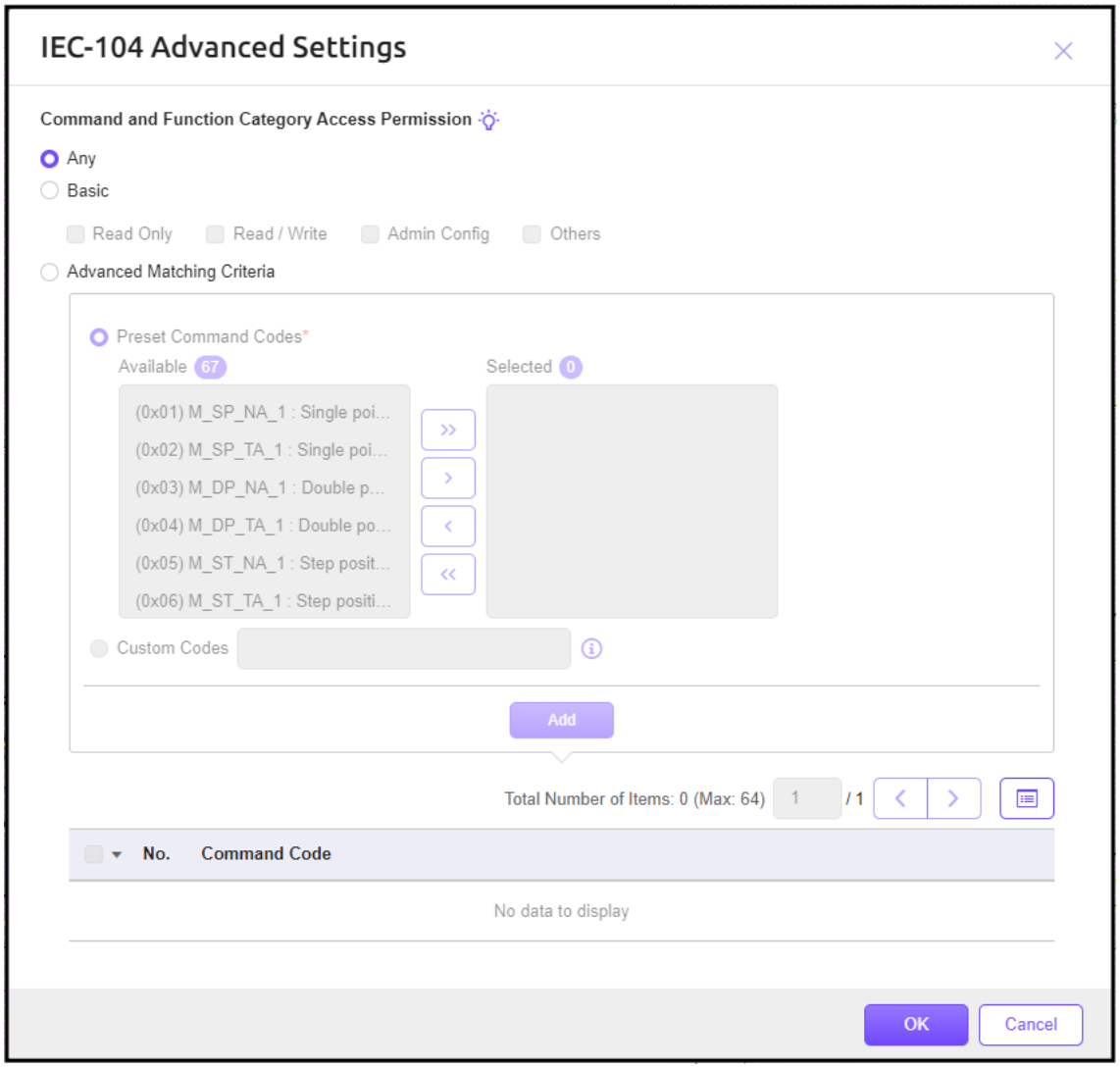
   c. Click [Add].

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

3. Click [OK].

5.2.1.21 Configuring IEC-104 Advanced Settings

Through the [IEC-104 Advanced Settings] window, you can further configure the command and function category access permission settings, including command codes based on which the protocol will work.



After you access the [IEC-104 Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

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

   a. Select [Preset Command Codes] or [Custom Codes] based on your needs.

      • **Preset Command Codes**: Select this option if you want to specify one or multiple command codes, then move the command codes from the [Available] field to the [Selected] field.

      • **Custom Codes**: Select this option if you want to specify one or multiple command codes by yourself, then input command codes in the [Custom Codes] field.

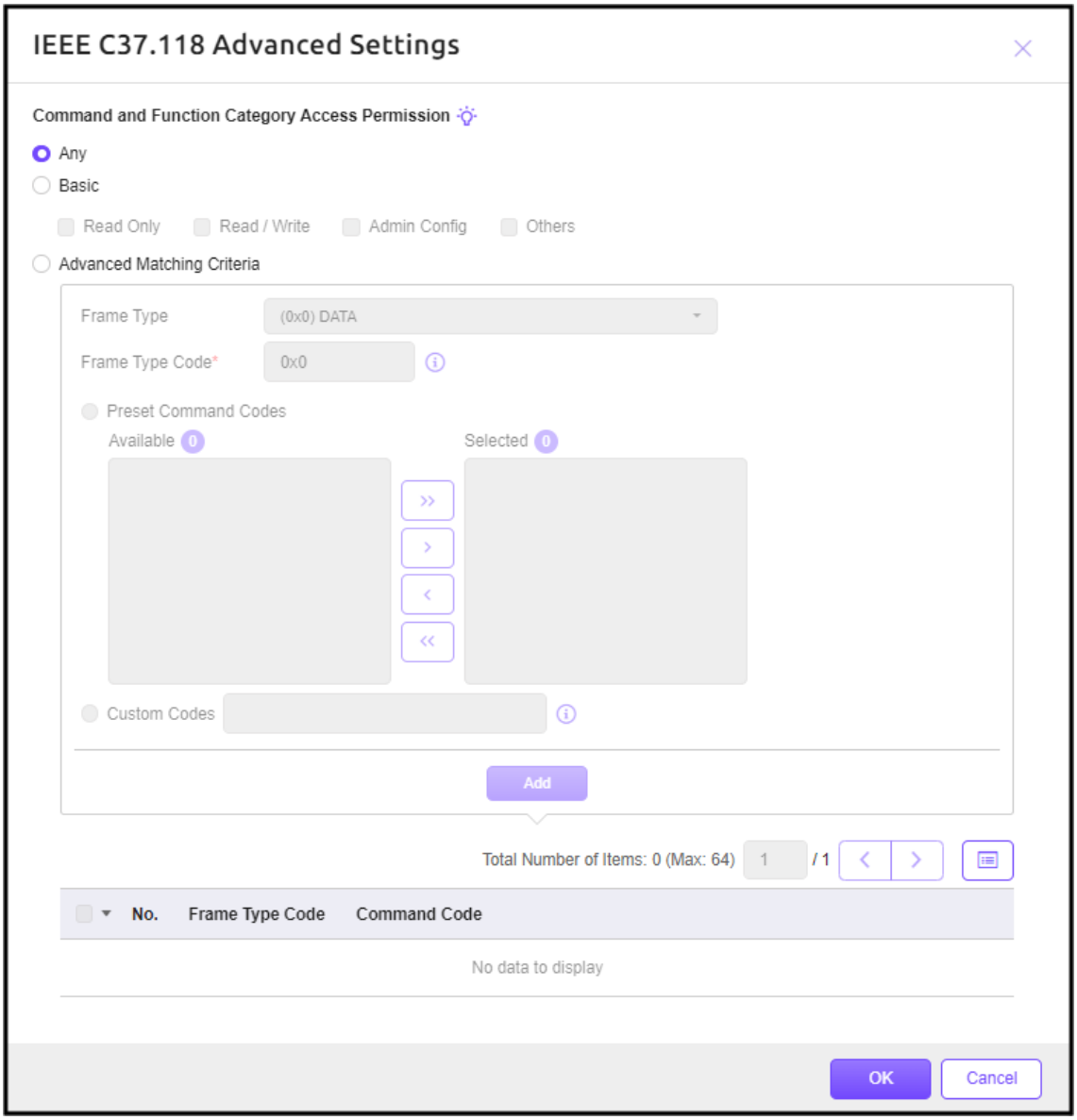
   b. Click [Add].

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

3. Click [OK].

5.2.1.22 Configuring IEEE C37.118 Advanced Settings

Through the [IEEE C37.118 Advanced Settings] window, you can further configure the command and function category access permission settings, including frame types and command codes based on which the protocol will work.



After you access the [IEEE C37.118 Advanced Settings] window, follow the procedure below.

Procedure

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

- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Basic**: Multiple selections as follows:
  - **Read Only**: Read commands between assets (such as HMI, EWS, SCADA, and PLC)
  - **Read/Write**: Read and write commands from one asset (such as HMI, EWS, and SCADA) to another (such as PLC)
  - **Admin Config**: Configuration commands, including PLC firmware updates, admin configuration commands, and other upgrades, from an asset (such as EWS) to a programmable control system
  - **Others**: Proprietary, customized, or undocumented commands
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], follow the steps below to configure the frame types and command codes.

a. From the [Frame Type] drop-down list, select a frame type of this protocol. If you want to specify a frame type by yourself, then select [Custom] and input a frame type code in the [Frame Type Code] field.

For the frame type code [(0x4) CMD], further select [Preset Command Codes] or [Custom Codes] based on your needs.

• **Preset Command Codes**: Select this option if you want to specify one or multiple command codes, then move the command codes from the [Available] field to the [Selected] field.

• **Custom Codes**: Select this option if you want to specify one or multiple command codes by yourself, then input command codes in the [Custom Codes] field.

b. Click [Add].

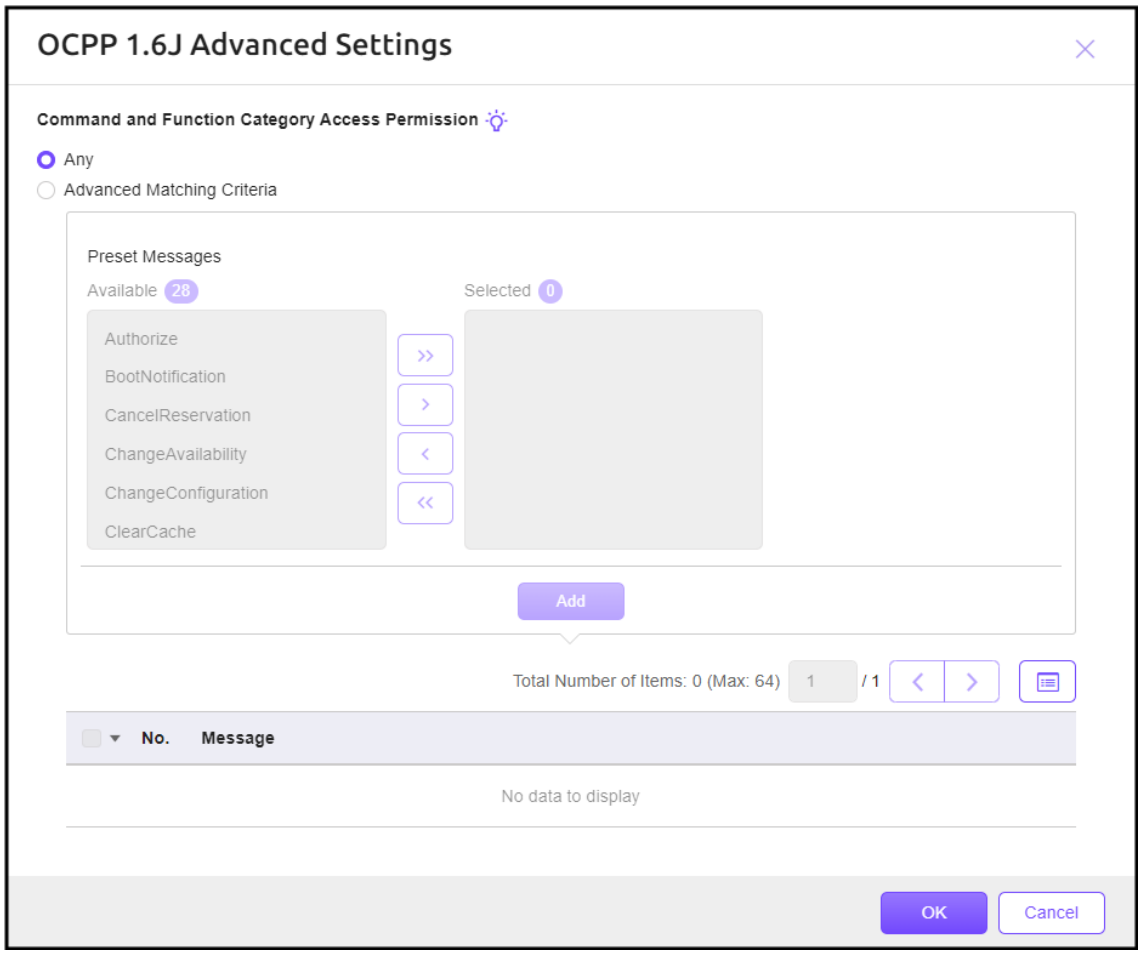
c. Repeat the above steps if you want to add more protocol definition entries.

3. Click [OK].

5.2.1.23 Configuring OCPP 1.6J and OCPP 2.0.1 Advanced Settings

Through the [OCPP 1.6J/OCPP 2.0.1 Advanced Settings] window, you can further configure the command and function category access permission settings, including message types based on which the protocol will work.

In this section, we will demonstrate how to configure the OCPP 1.6J advanced settings. Please take the same approach when configuring the OCPP 2.0.1 advanced settings.



After you access the [OCPP 1.6J Advanced Settings] window, follow the procedure below.

Procedure

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

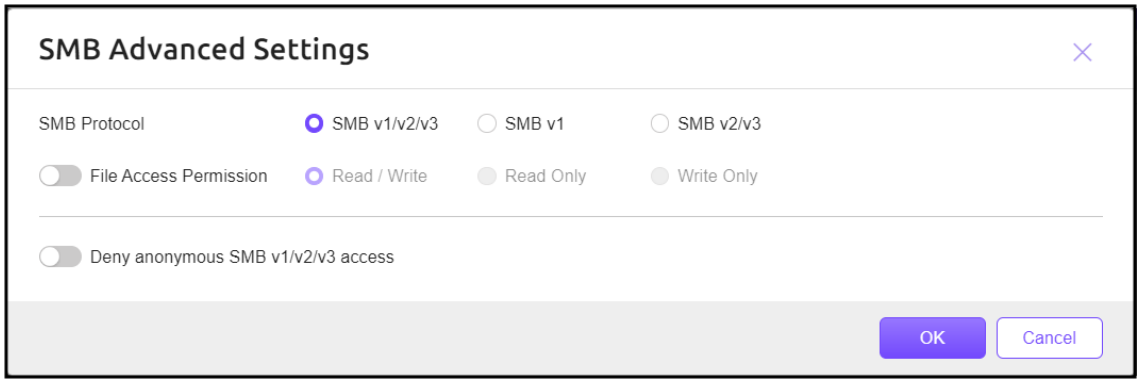
- **Any**: Select this option to choose any of the commands or function access in this protocol.
- **Advanced Matching Criteria**: Select this option to further configure advanced matching criteria for the [Command and Function Category Access Permission].

2. If you select [Advanced Matching Criteria], further select one or multiple types of messages, then move the message types from the [Available] field to the [Selected] field. Repeat this step if you want to add more protocol definition entries.

3. Click [OK].

5.2.1.24 Configuring SMB Advanced Settings

Through the [SMB Advanced Settings] window, you can further specify the SMB protocol version combination, file access permission and enable or disable the [Deny anonymous SMB v1/v2/v3 access] setting.



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

Procedure

1. Configure the following SMB advanced settings.
   - **SMB Protocol**: Select an SMB protocol version combination, **SMB v1/v2/v3**, **SMB v1** or **SMB v2/v3**.
   - **File Access Permission**: If needed, enable this function and select one of the following file access behaviors.
     - **Read / Write**: File access for reading and writing.
     - **Read Only**: File access for reading only.
     - **Write Only**: File access for writing only.
   - **Deny anonymous SMB v1/v2/v3 access**: If needed, enable this setting to deny access over SMB v1/v2/v3 for anonymous accounts.
2. Click [OK].

5.2.2 IPS Profiles

IPS profiles contain sophisticated IPS pattern rules which you can apply to policy rules for granular control. In IPS profiles, you can configure:

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

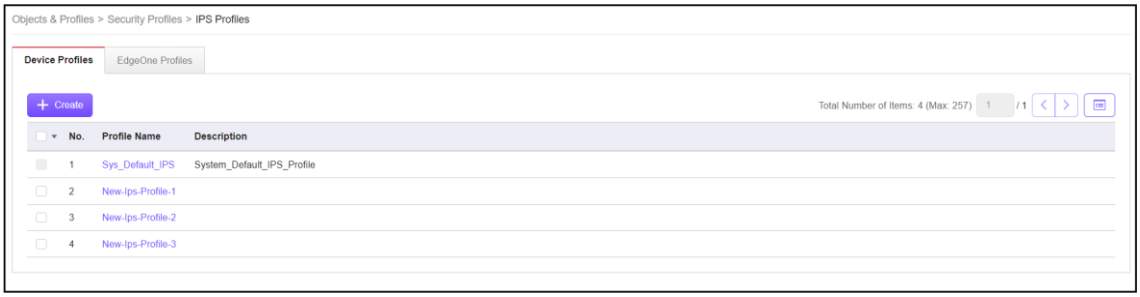
- High
- Critical

- **IPS pattern rule default actions**, including:
  - Allow and Log
  - Deny and Log

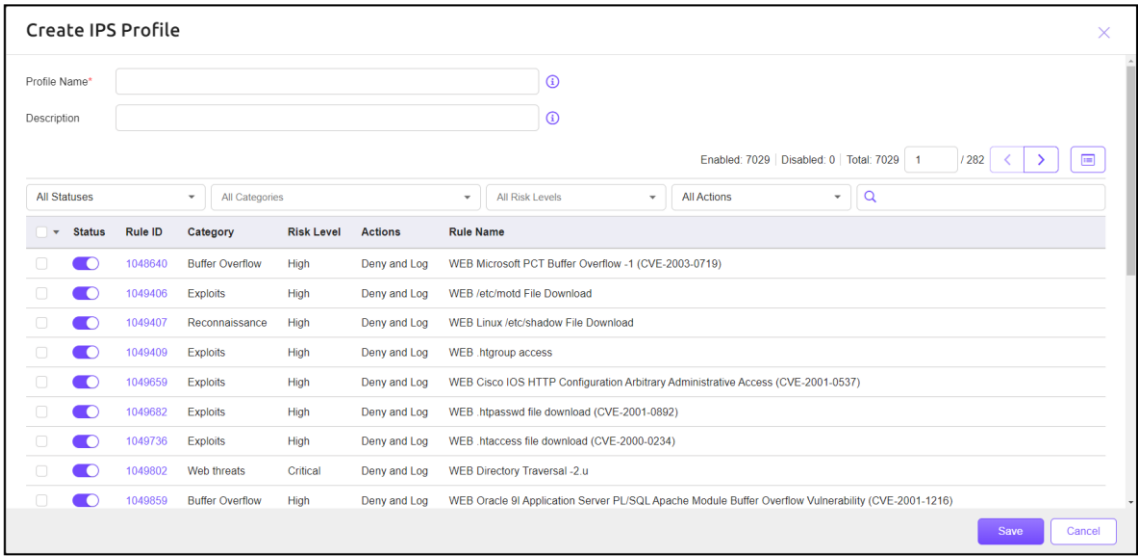
5.2.2.1 Configuring IPS Profiles

Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [IPS Profiles].

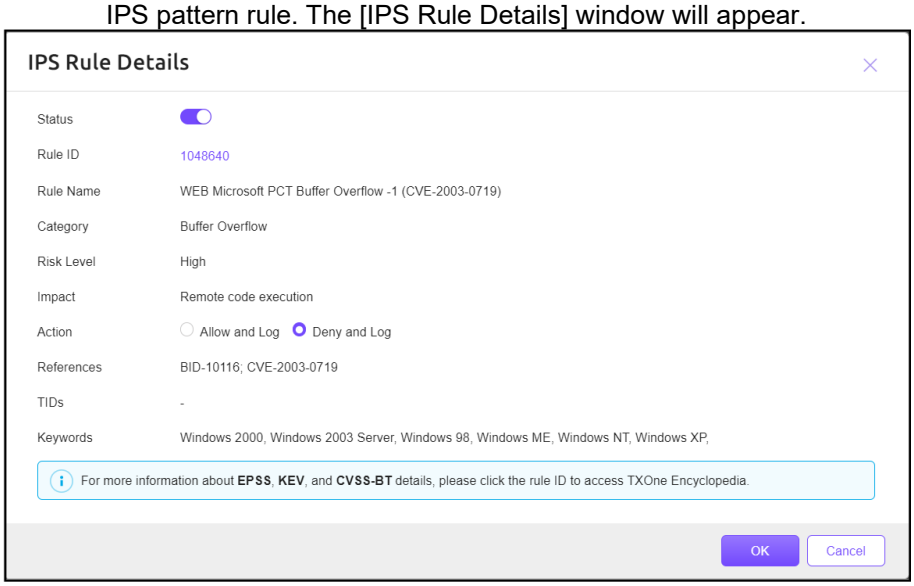
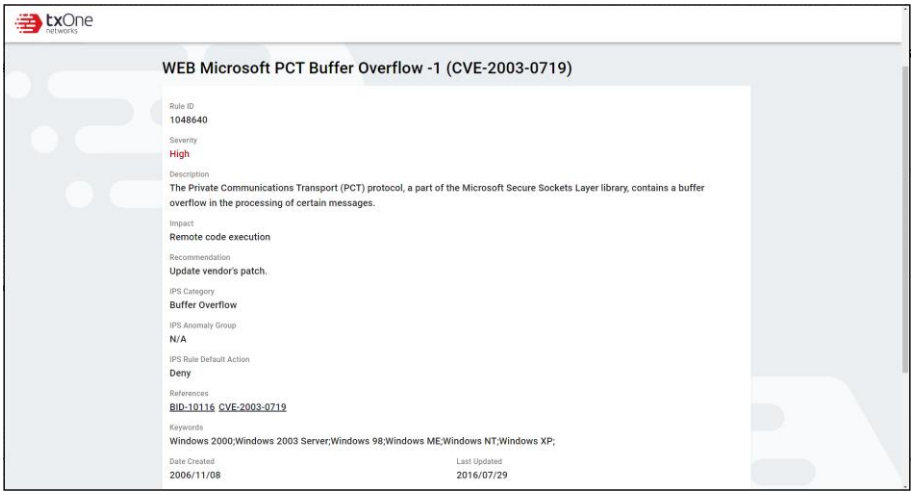


2. Do one of the following.
   - Click [Create] to create a profile. The [Create IPS Profile] window will appear.
   - Click a profile name to edit settings. The [Edit IPS Profile] window will appear.



3. Configure the following IPS profile settings.

Item	Description
Profile Name	Type a profile name for this IPS profile.
Description	(Optional) Type a description.
Status	Disable the operational statuses of one or multiple IPS pattern rules you want to exclude from this IPS profile by clicking the toggles. (Default status: Enabled)

Item	Description
Rule ID (IPS Rule Granular Control Details)	Click the rule ID in the [Rule ID] column to configure and view details of each IPS pattern rule. The [IPS Rule Details] window will appear.  • **Status**: The operational status of this single IPS pattern rule. **Use the toggle to enable/disable this rule.** • **Rule ID**: The ID number of this IPS pattern rule. You can view the threat information regarding this IPS pattern rule in detail by clicking the rule ID number, and you will then be redirected to the TXOne Threat Encyclopedia as shown below.  • **Rule Name**: The name of this IPS pattern rule regarding the cyber attack. • **Category**: The threat category of this IPS pattern rule regarding the cyber attack, including File Vulnerabilities, Buffer Overflow, DoS Attacks, Exploits, Malware Traffic, Reconnaissance, Web Threats, ICS Threats, Others and Misc. • **Risk Level**: The suggested security level regarding the cyber attack, including Information, Low, Medium, High and Critical. • **Impact**: The damage that will be caused to the target network device if the cyber attack succeeds.

Item	Description

	• **Action**: The preset action for the cyber attack. **Select either [Allow and Log] or [Deny and Log].** (Default action: Deny and Log)
	  ○ **Allow and Log**: When the attack is detected by the Edge series device, the attack will be bypassed and logged for monitoring.
	  ○ **Deny and Log**: When the attack is detected by the Edge series device, the attack will be blocked and logged for monitoring.
	• **References**: The vulnerability IDs of the cyber attack.
	• **TIDs**: MITRE TID information.
	• **Keywords**: The keywords for searching this IPS pattern rule.
	Click [OK] to save the configurations of the IPS rule details.

4. Click [Save].

📝	The built-in IPS profile [Sys_Default_IPS] is view-only and cannot be deleted or configured.

5.2.3 File Filter Profiles

File Filter profiles contain detailed access protocols as well as settings for executable file types and Active Directory (AD) GPO dispatch which you can apply to policy rules. In File Filter profiles, you can configure:

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

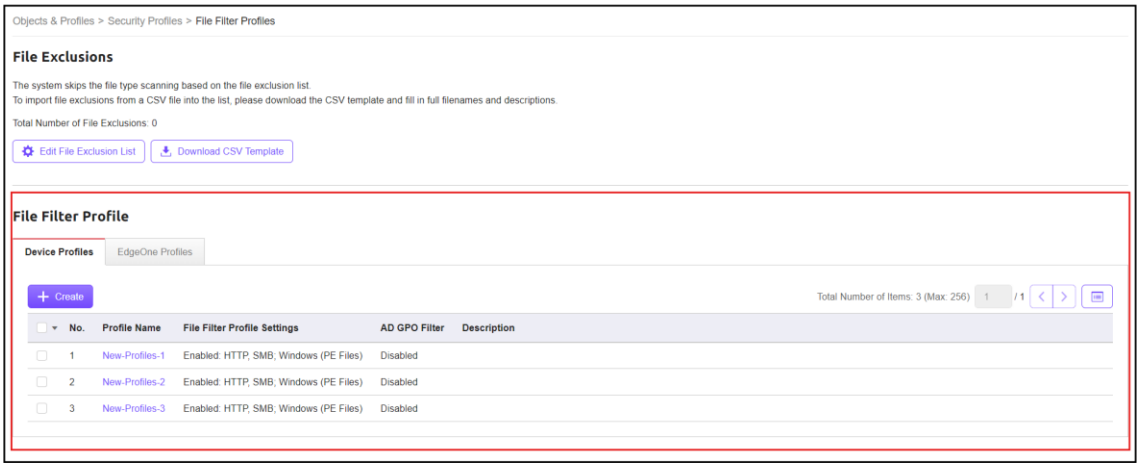
On the [File Filter Profiles] page, you can further configure the **File Exclusions** function to exclude certain files from the file filter profiles you're enabling. The Edge device skips the file type scanning based on your File Exclusion list. This can increase the flexibility of configuration and obtain real control for your OT network.

We provide two methods for configuring the File Exclusion settings, either adding file items one by one or importing an edited CSV file with multiple **filename** items.

5.2.3.1 Configuring File Filter Profiles

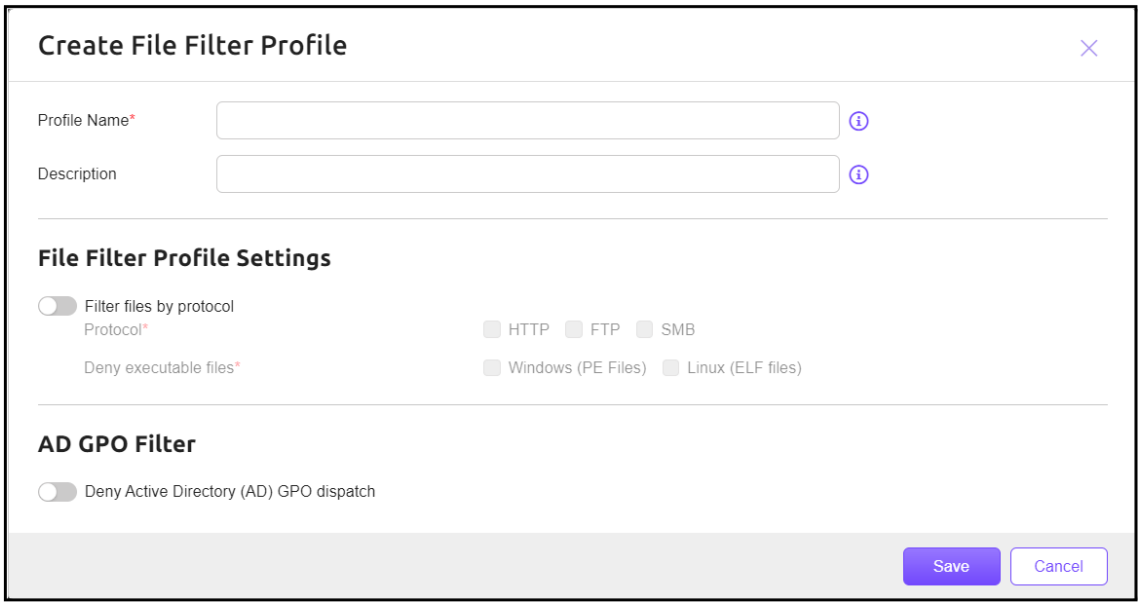
Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [File Filter Profiles].



2. Do one of the following:

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



3. Configure the following File Filter profile settings.

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

- File Filter Profile Settings

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

- AD GPO Filter

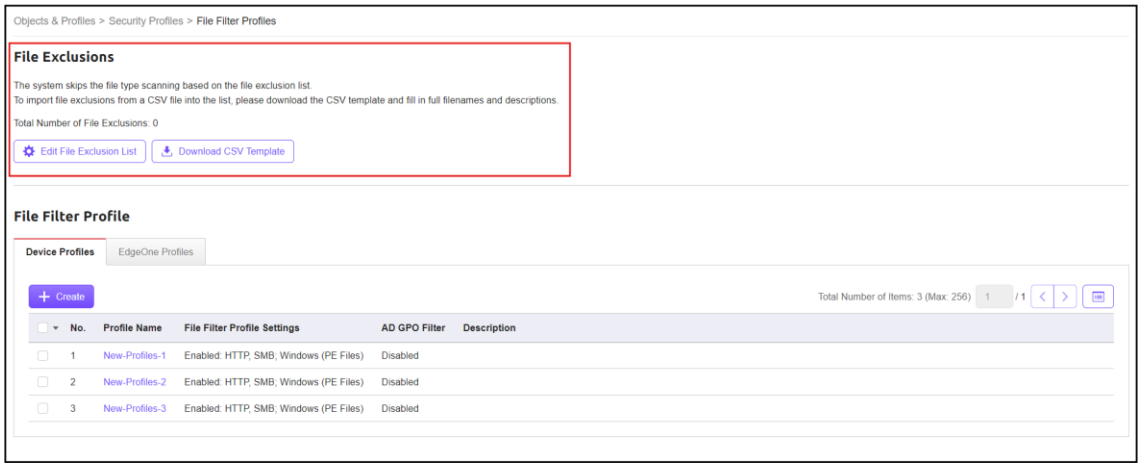
Item	Description
Deny Active Directory (AD) GPO dispatch	(Optional) Enable this function by clicking the toggle if you want to filter AD GPOs.

4. Click [Save].

5.2.3.2 Configuring File Exclusions

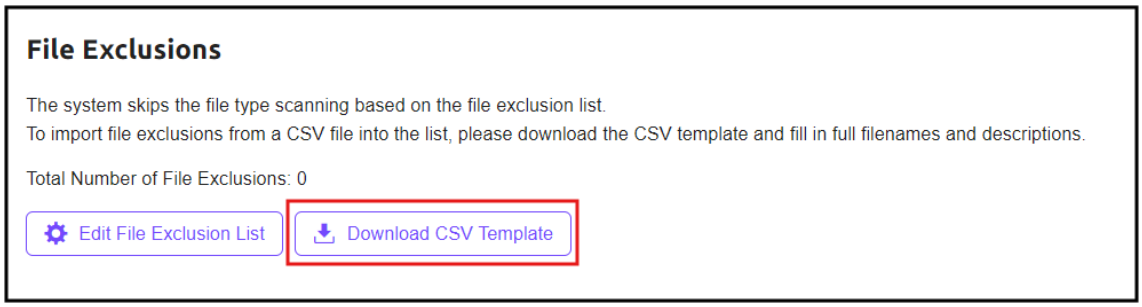
Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [File Filter Profiles].



- **Method 1 (Steps 2-5): Importing a File List Using the Built-in CSV File Template**

2. Click the [Download CSV Template] button to download the CSV template.



📝	To avoid CVS file compatibility issue, we recommend using the CSV template provided on the page for importing full filenames into the console.

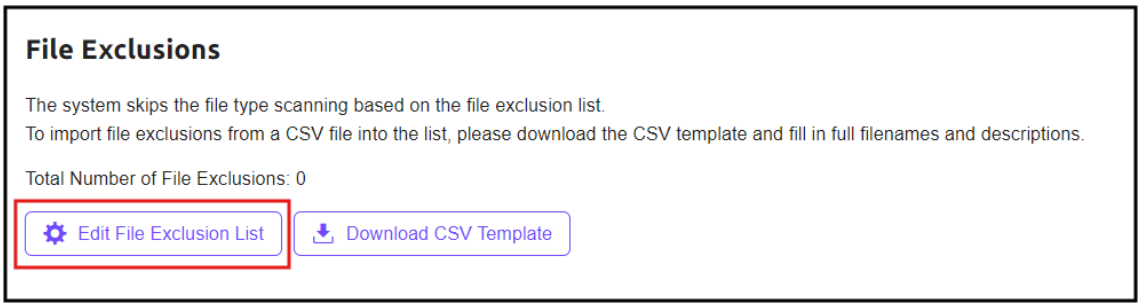
3. Open the downloaded CSV file and input the full filenames (mandatory) and descriptions (optional). For example:

Full Filename	Description
abc.exe	Windows PE File
def.bat	Windows PE File
ghi.o	Linux ELF File

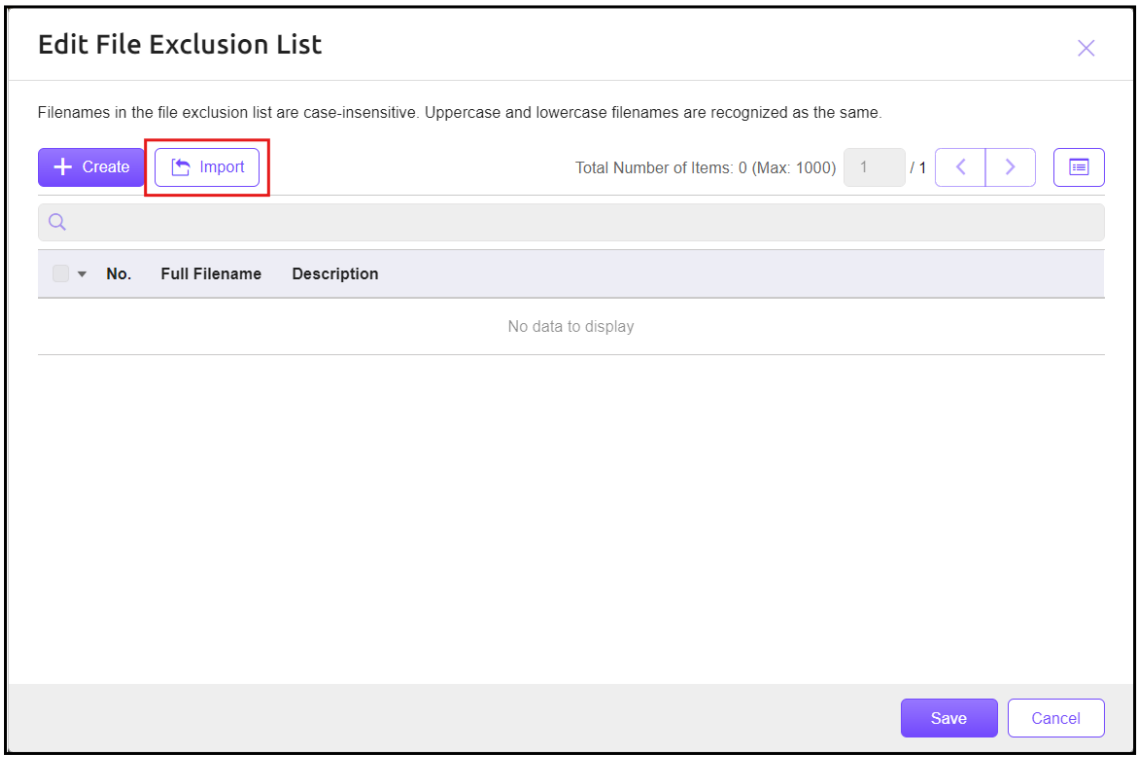
📝	1. You do not need to unzipp zip/gz file(s) for scanning each compressed file, as the system can identify zip/gz file(s) and determine whether the filename list contains the file items for exclusions. Notice that zip/gz files larger than 100MB will be ignored.

2. The filename format can be <filename>+"."+<file extension> (e.g. abc.exe), or just <filename> (e.g. abc). We recommend inputting full filenames (with file extensions).
3. The file system is not case sensitive. Filenames in uppercase or lowercase are identified as the same file. In addition, Whitespace character(s) cannot be included in the beginning and the end of a filename. Special characters (<, >, :, “, /, \, |, and ?) are not allowed.
4. Filenames that start or end with whitespace characters or contain only one asterisk (*) are not valid. To use wildcard search in a file exclusion list, you can insert an asterisk at any point within the filename.
5. The maximum full filename length (<filename>+"."+<file extension>) is 128 characters (UTF-8, English characters). If user inputs any non-English characters, the full filename length will be shortened to 32 characters.

4. Click the [Edit File Exclusion List] button to edit a File Exclusion list.

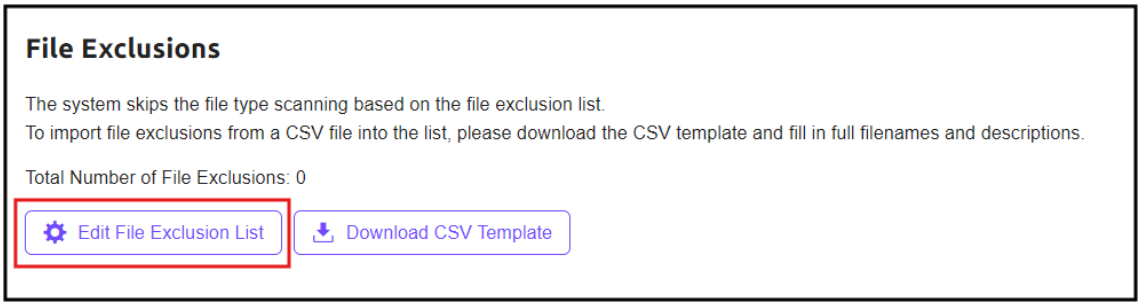


5. Click the [Import] button to import file exclusion items from your CSV file.

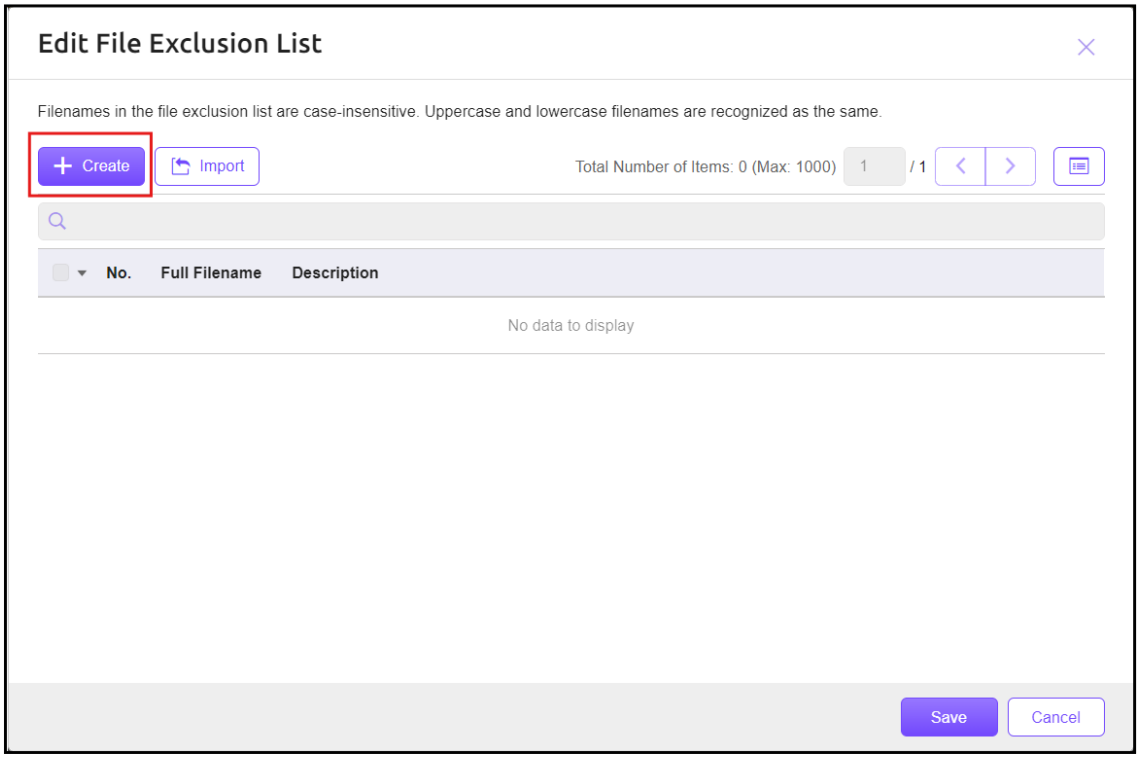


- **Method 2 (Steps 2-5): Manually Adding Full Filenames to the File Exclusion List**

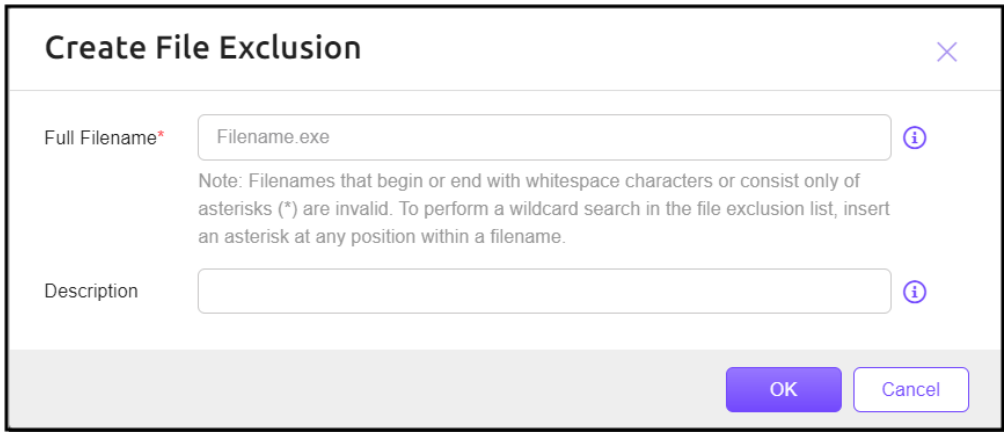
2. Click the [Edit File Exclusion List] button to edit a File Exclusion list.



3. Click the [Create] button to access the [Create File Exclusion] window.



4. Input a full filename. The description is optional.



5. Click [OK]. Repeat the above steps 3-4 if you want to add multiple file exclusion items.

6. After you have completed the file exclusion settings by either of the methods, click [Save].

7. Use the search bar to search for the information you need if necessary.

5.2.4 Domain Name Profiles

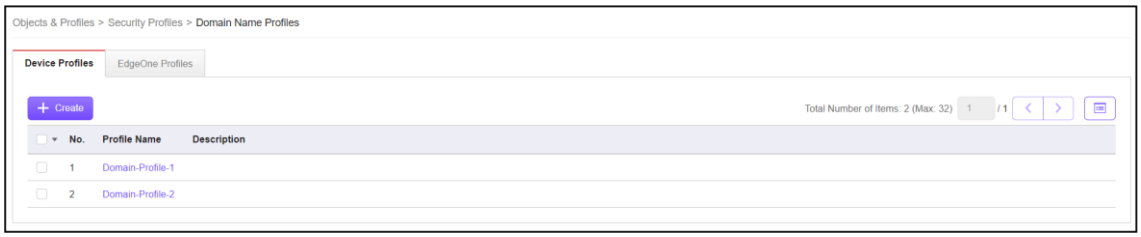
Domain Name profiles contain lists of domain names and their types (domains or subdomains) which you can apply to Domain Name Filter rules.

> For more information about the filtering mechanisms of Domain Name Filter rules, see Domain Name Filter Rules.

5.2.4.1 Configuring Domain Name Profiles

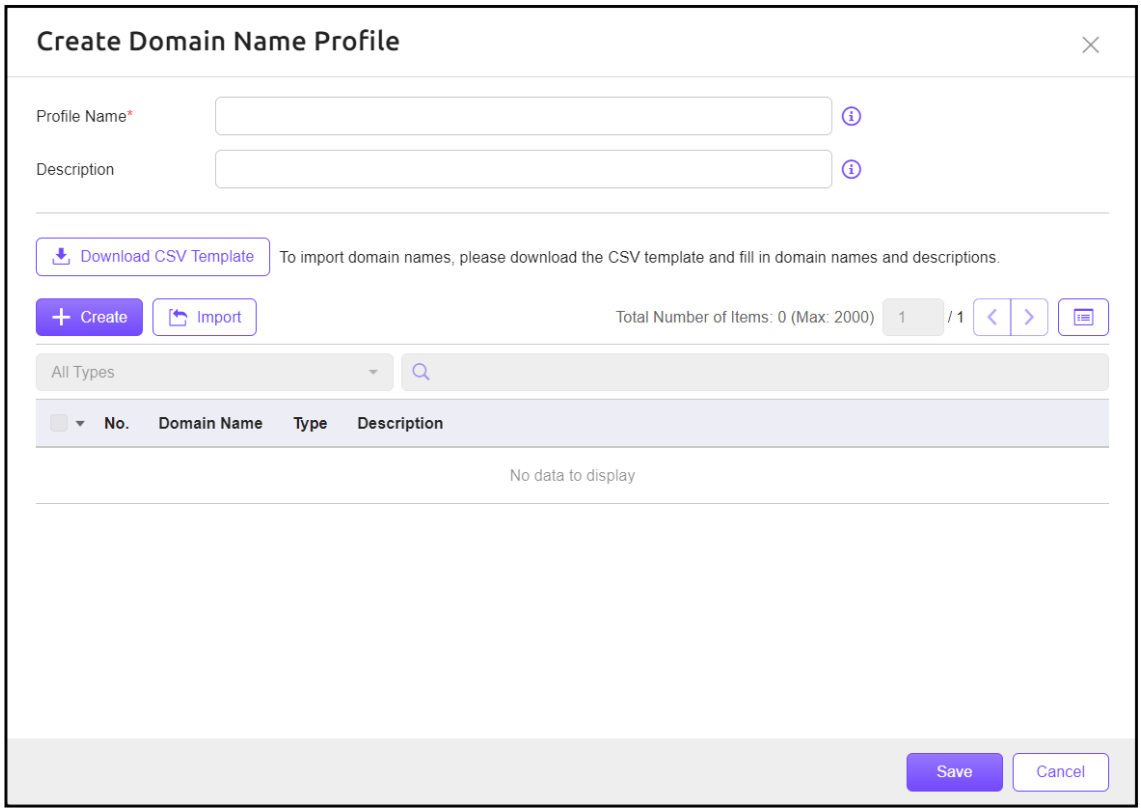
Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [Domain Name Profiles].



2. Do one of the following:

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



3. Configure the following Domain Name profile settings.

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

- **Method 1 (Steps 4-6): Importing a Domain Name List Using the Built-in CSV File Template**

4. Click the [Download CSV Template] button to download the CSV template.

5. Open the downloaded CSV file and input the domain names (mandatory), their types (mandatory), and descriptions (optional). For example:

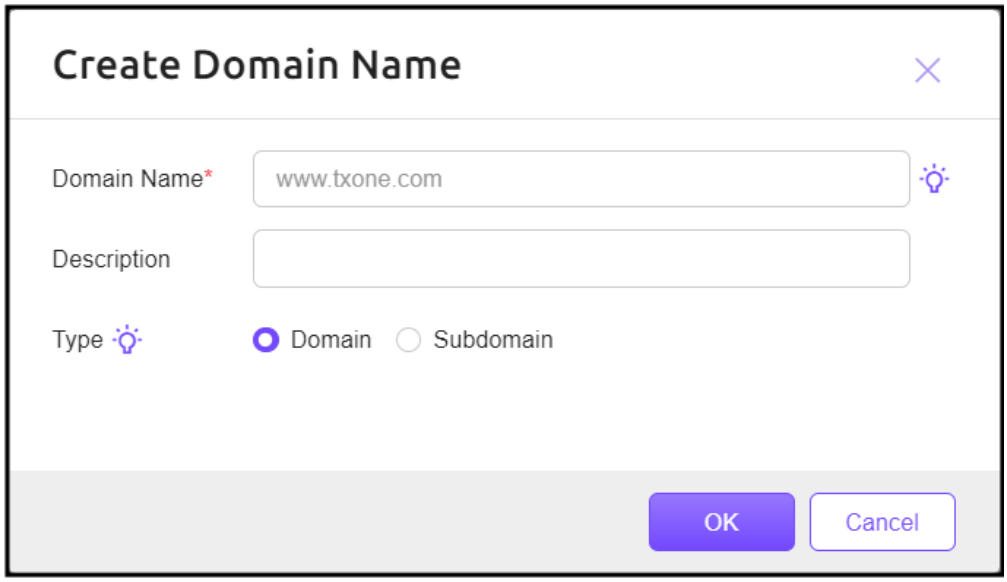
Domain Name	Type	Description
myhost.abc.com	domain	Domain 1
www.def.com	subdomain	Domain 2

When inputting the domain name types, please input either "domain" or "subdomain" with all the letters in lowercase.

6. Click the [Import] button to import the edited CSV file.

- **Method 2 (Steps 4-6): Manually Adding Domain Names to the Domain Name List**

4. Click the [Create] button to open the [Create Domain Name] window.



5. Input a domain name and select its type, either **Domain** or **Subdomain**. The description is optional.

6. Click [OK]. Repeat the above steps 3-4 if you want to add multiple domain names.

7. After you have completed the Domain Name profile settings by either of the methods, click [Save].

8. Use the search bar to search for the information you need if necessary.

5.2.5 Antivirus Profiles

EdgeIPS Pro Antivirus is a streaming-based design. You can configure Antivirus profiles to check HTTP or FTP protocols, edit advanced settings such as file size limitations and compressed file scanning, and apply these profiles to policy rules.

In an Antivirus profile, you can define the following:

- File exceptions (SHA1-based exception list)

- Protocol settings for HTTP and FTP

Advanced settings include:

- Maximum file size
- Compressed file scanning

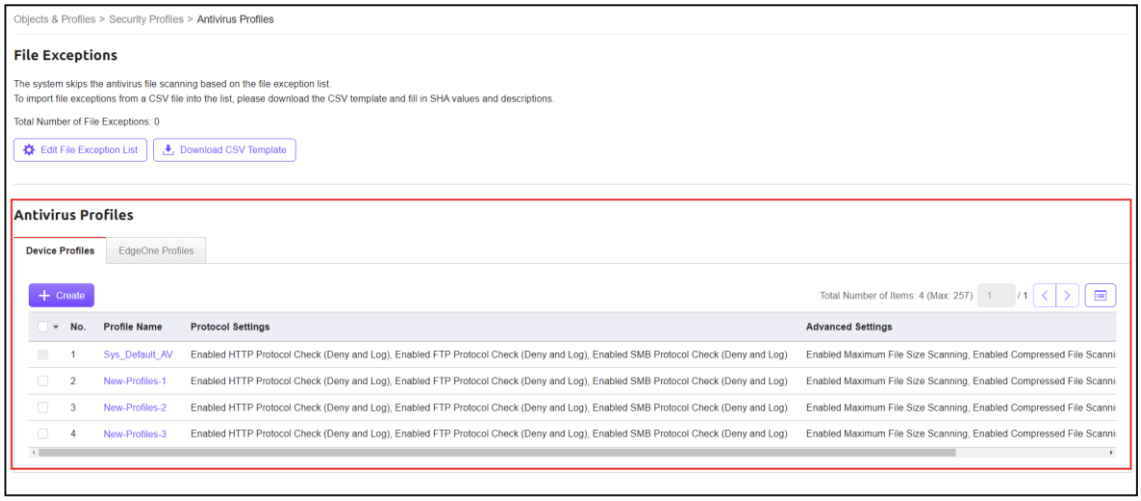
On the [Antivirus Profiles] page, you can further configure the **File Exceptions** function to except certain files from the antivirus profiles you're enabling. The Edge device skips the file scanning based on your File Exception list. This can increase the flexibility of configuration and obtain the real control for your OT network.

We provide two methods for configuring the File Exception settings, either adding file items one by one or importing an edited CSV file with multiple **SHA-1** items.

5.2.5.1 Configuring Antivirus Profiles

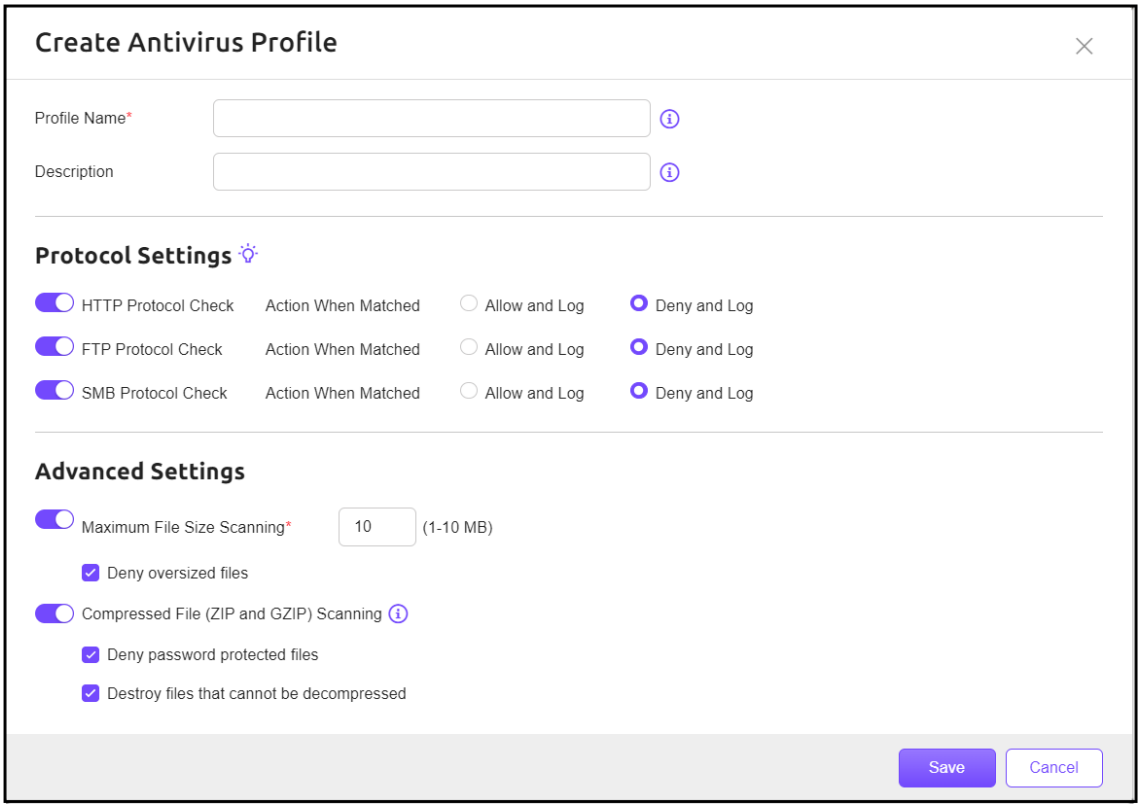
Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [Antivirus Profile].



2. Do one of the following:

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



3. Configure the following Antivirus profile settings.

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

- Protocol Settings

Item	Description
HTTP Protocol Check	Enable the protocols by clicking the toggles for examining files based on the enabled protocols. If one or multiple of the options are enabled, further select their respective actions, either **Allow and Log** or **Deny and Log**, when a match is detected.
FTP Protocol Check	
SMB Protocol Check	

- Advanced Settings

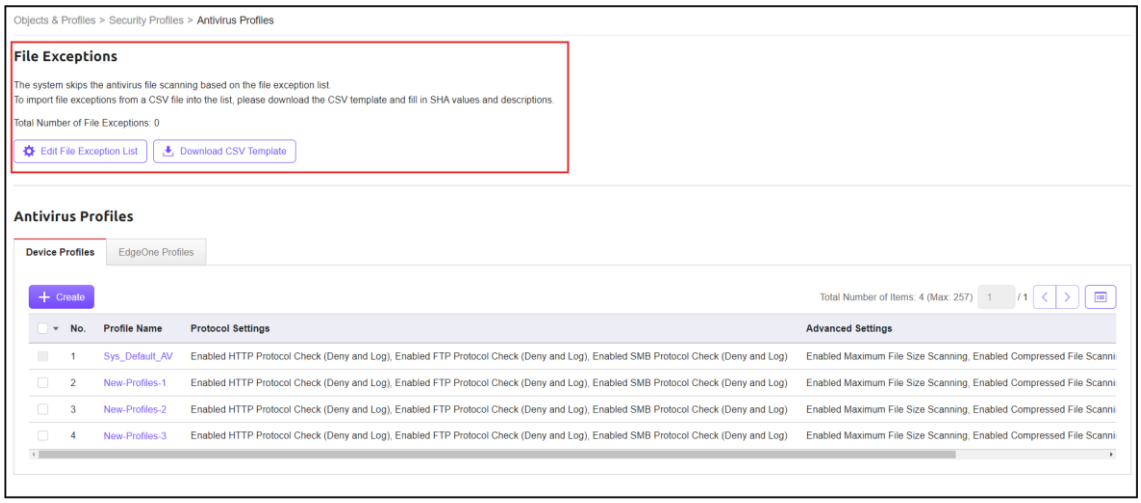
Item	Description
Maximum File Size Scanning	Enable this option by clicking the toggle. If the option is enabled, further specify the maximum value of the file size for scanning, and whether the device should deny oversize files.
Compressed File (ZIP and GZIP) Scanning	Enable this option by clicking the toggle. If the option is enabled, further specify whether the device should deny password protected files, and whether the device should destroy files that cannot be decompressed.

4. Click [Save].

5.2.5.2 Configuring File Exceptions

Procedure

1. Go to [Objects & Profiles] > [Security Profiles] > [Antivirus Profiles].



- **Method 1 (Steps 2-5): Importing a File List Using the Built-in CSV File Template**

2. Click the [Download CSV Template] button to download the CSV template.

> To avoid CSV file compatibility issue, we recommend using the CSV template provided on the page for importing SHA-1 values into the console.

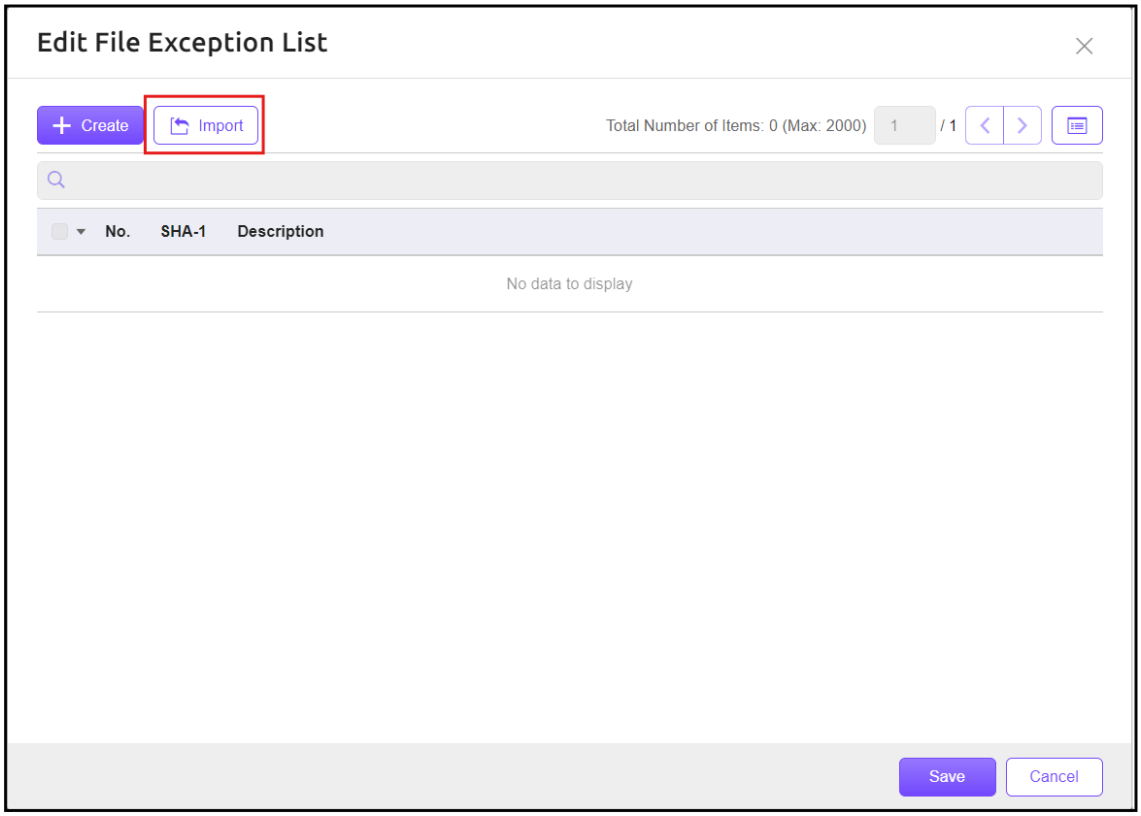
3. Open the downloaded CSV file and input the full SHA-1 values (mandatory) and descriptions (optional). For example:

SHA Type	Value	Description
SHA-1	9365e80854461496b6803cec83dd9814eea71788	Windows PE File
SHA-1	1e783af70e201a6dab6a3a7b64821fc4563d200a	Windows PE File
SHA-1	b5f744020ed1abffe19dc2e66ac5a0390d9df01c	Linux ELF File

> The length of a hash value (SHA-1, hexadecimal number) should be 40 digits long.

4. Click the [Edit File Exception List] button to edit a File Exception list.

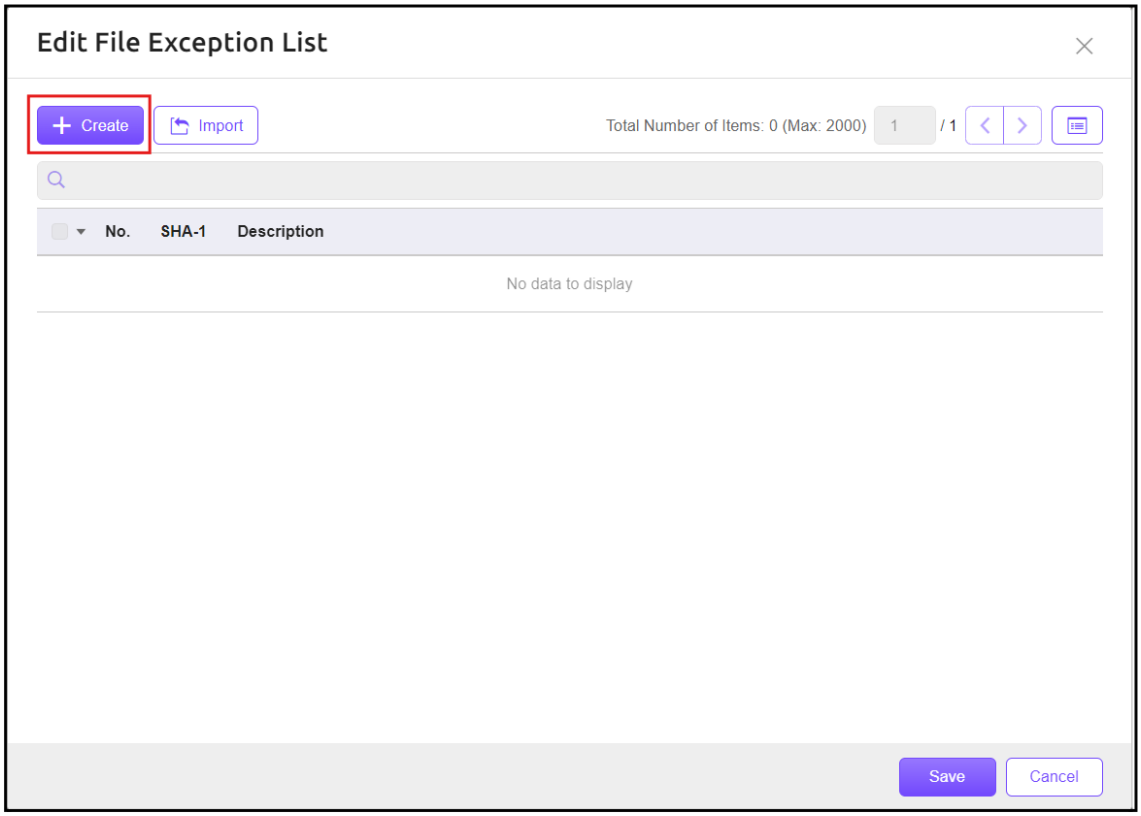
5. Click the [Import] button to import file exception items from your CSV file.



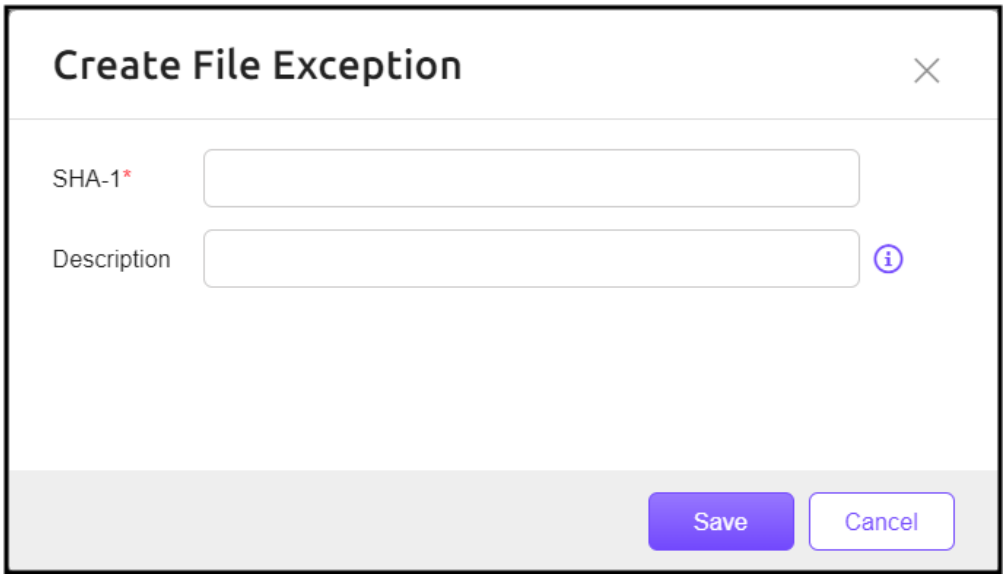
- **Method 2 (Steps 2-5): Manually Adding Full SHA-1 Values to the File Exception List**

2. Click the [Edit File Exception List] button to edit a File Exception list.

3. Click the [Create] button to access the [Create File Exception] window.



4. Input a SHA-1 value. The description is optional.



5. Click [OK]. Repeat the above steps 3-4 if you want to add multiple file exception items.

6. After you have completed the file exception settings by either of the methods, click [Save].
7. Use the search bar to search for the information you need if necessary.

5.3 Edge DPI Engine

Customize settings for the supported communication protocols used in your network.

- Protocol Service Port Profiles

5.3.1 Protocol Service Port Profiles

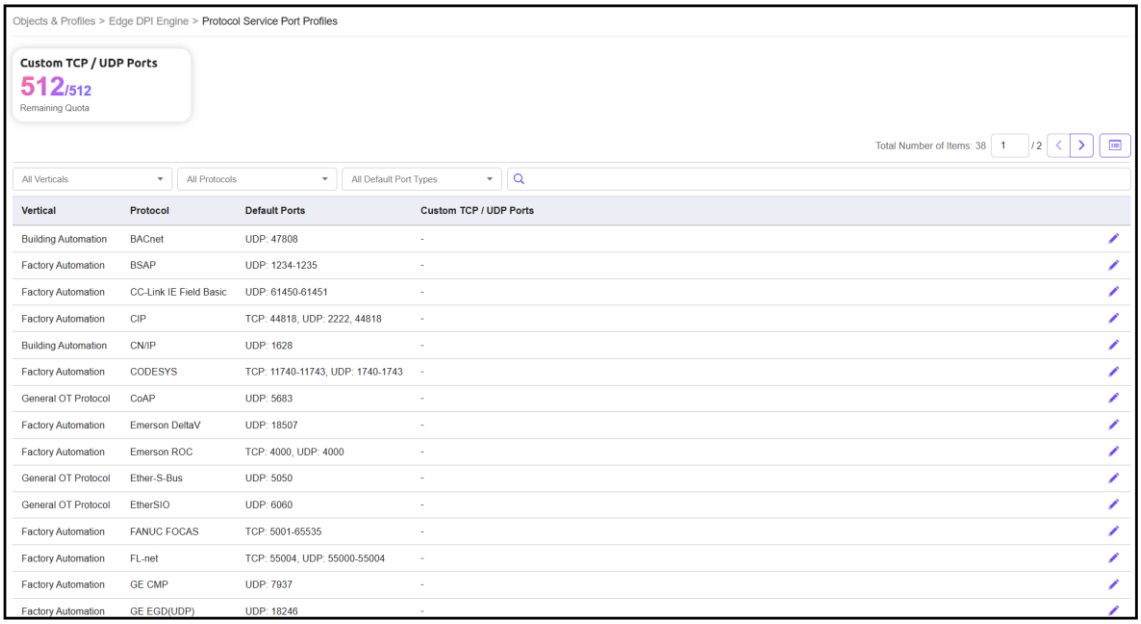
Protocol Service Port profiles contain customized ports or port ranges used by each OT protocol. By specifying which protocols use which ports, these settings improve the traffic examination accuracy of OT protocol filters, enabling the Edge device to precisely identify the protocols in use on each port.

1. The [Protocol Service Port Profiles] feature is only applicable to Edge devices running firmware version 2.2 or later.
2. You can customize ports or port ranges only for designated OT protocols. IT protocols such as SMB, HTTPS, and SSH are not supported.

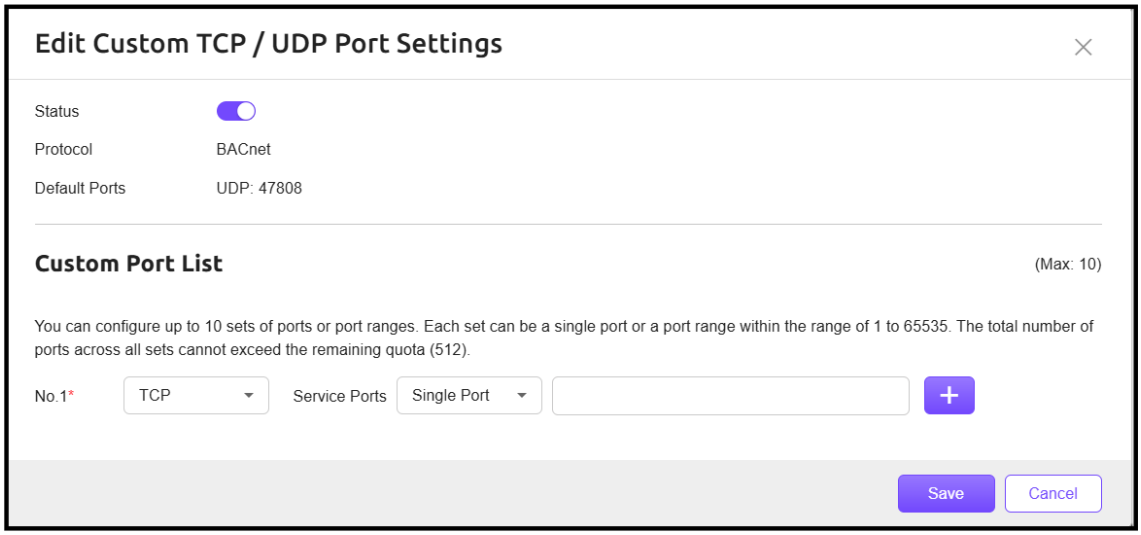
5.3.1.1 Configuring Protocol Service Port Profiles

Procedure

1. Go to [Objects & Profiles] > [Edge DPI Engine] > [Protocol Service Port Profiles].



2. Click ✎ to edit TCP/UDP ports of a protocol. The [Edit Custom TCP/UDP Port Settings] window will appear.



3. Select **TCP** or **UDP** from the drop-down list.
4. Select **Single Port** or **Port Range** from the drop-down list.

5. Input a port number or a port range within the range of 1 to 65535 in the field.

6. Click the [Add Entry] button + to add another entry, or the [Remove Entry] button − to remove an entry.

📝	You can create up to 10 sets of ports or port ranges for each protocol. The total number of ports for all protocols cannot exceed 512.

7. Click [Save].

6 Security

This chapter describes how to configure security features on your Edge device to protect your assets.

6.1 General Settings

Configure global device settings, such as the deny action setting, for all port pairs.

- Deny Action Setting

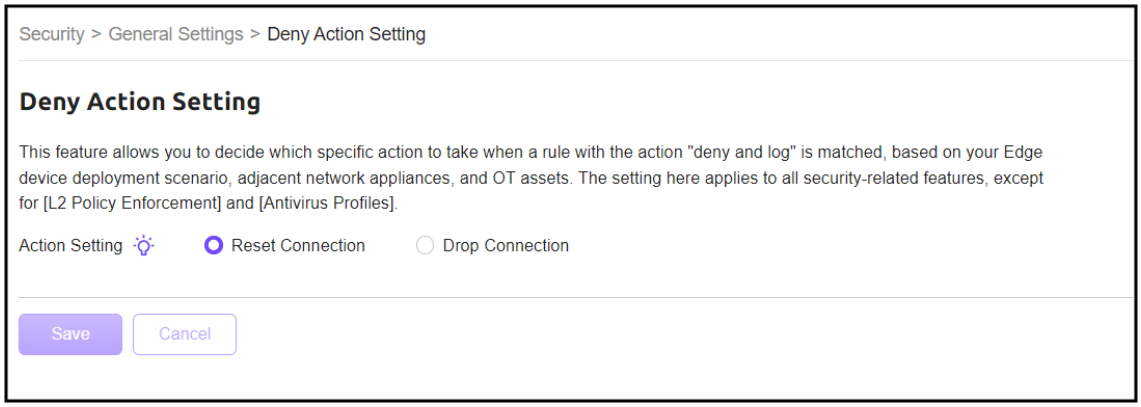
6.1.1 Deny Action Setting

On the [Deny Action Setting] page, you can decide which specific action to take when a rule with the action "deny and log" is matched, based on your Edge device deployment scenario, adjacent network appliances, and OT assets. The setting on this page applies to all security-related features across the entire console, except for [L2 Policy Enforcement] and [Antivirus Profiles].

6.1.1.1 Configuring Deny Action Setting

Procedure

1. Go to [Security] > [General Settings] > [Deny Action Setting].



2. Configure the deny action setting.

Deny Action	Description
Reset Connection	When the deny action is [Reset Connection], the Edge device sends a notification when it rejects any packets associated with an unwanted connection.
Drop Connection	When the deny action is [Drop Connection], the Edge device simply discards any packets without sending a notification.

3. Click [Save].

6.2 Security Policies

Create and manage various types of policy rules to safeguard your OT networks and assets.

- L2 Policy Enforcement
- Policy Enforcement
- Policy Rule Auto-Learning

- Port Security
- Domain Name Filter Rules
- Suspicious Objects

6.2.1 L2 Policy Enforcement

The Edge solution is an OT-native network security solution, specifically designed for legacy production tools and environments without an IP-based production network. Our solution provides L2 Policy Enforcement feature, allowing you to set up network access policies for Layer 2 network protection by defining MAC address-related configurations while still enabling security policy configurations. By applying user-defined Layer 2 access rules with various traffic filtering conditions, the system determines whether specific network activities should be allowed or blocked based on the adopted rule settings.

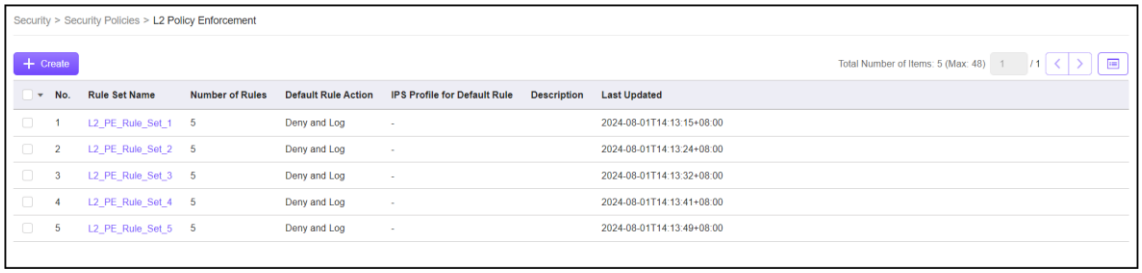
Comparing L2 and L3 Policy Enforcement Rules in Edge Device

- **L2 Policy Enforcement:** L2 policies are designed to control non-IP traffic—specifically, Ethernet frames that do not encapsulate IPv4 or IPv6 packets. These are typically used in OT environments where communication is based on MAC addresses, often due to legacy protocols. For example, blocking a specific MAC address without reference to higher-layer protocols.
- **L3 Policy Enforcement:** L3 policies apply to all IPv4 traffic, including ICMP, TCP, and UDP. Although IPv4 packets (like ping/ICMP) are carried within Ethernet frames, they are handled by L3 rules, not L2. Therefore, any enforcement for such traffic must be done via L3 policies. For more information about L3 Policy Enforcement, see Policy Enforcement.

6.2.1.1 Configuring L2 Policy Enforcement Rule Sets

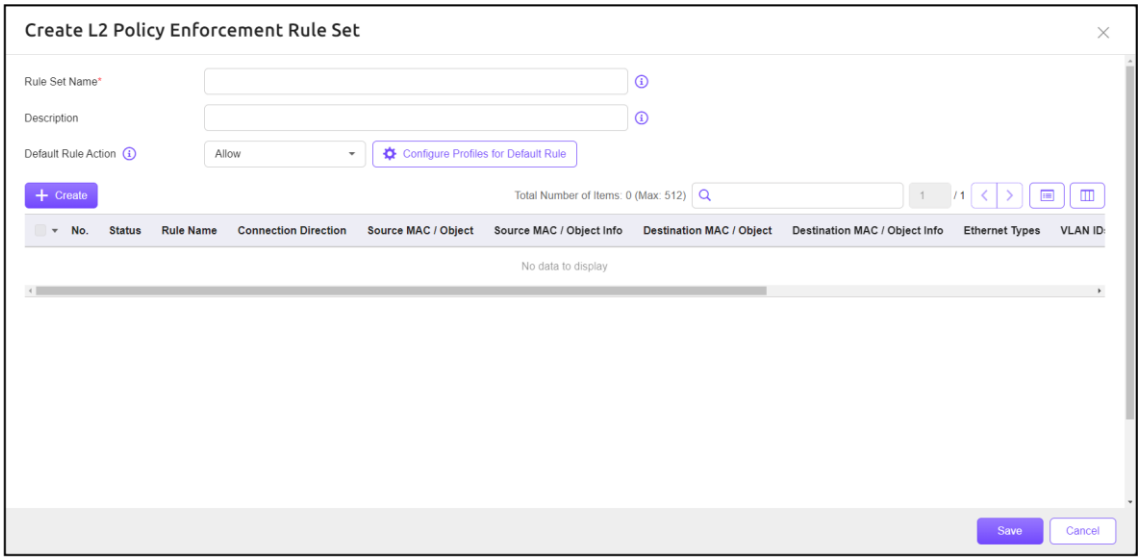
Procedure

1. Go to [Security] > [Security Policies] > [L2 Policy Enforcement].

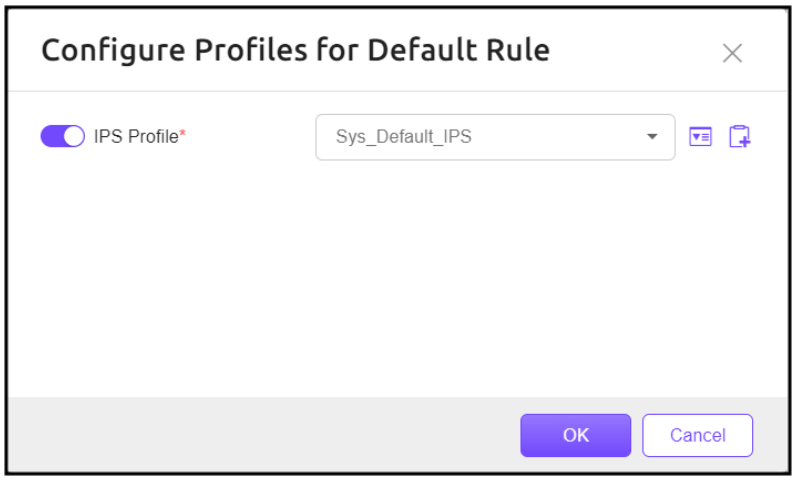


2. On the [L2 Policy Enforcement] page, do one of the following.

- Click [Create] to create a rule set and add L2 rules to this new rule set. The [Create L2 Policy Enforcement Rule Set] window will appear.
- Click the name of the rule set that you want to add L2 rules to or modify its existing rules. The [Edit L2 Policy Enforcement Rule Set] window will appear.



3. Configure the following settings.

Item	Description
Rule Set Name	Type a rule name for this L2 Policy Enforcement rule set.
Description	(Optional) Type a description.
Default Rule Action	Select a default action, **Allow**, **Allow and Log** or **Deny and Log**, for when no L2 Policy Enforcement rule is matched.
Configure Profiles for Default Rule	(Optional) If the default rule action is **Allow** or **Allow and Log**, click the [Configure Profiles for Default Rule] button to specify which IPS profile to use for traffic examintion when no L2 Policy Enforcement rule is matched.  a. Click the [IPS Profile] toggle to enable the setting. b. Select a pre-defined IPS profile from the drop-down list or use the system default IPS profile (Sys_Default_IPS). c. (Optional) To view/edit detailed IPS profile settings, click the button. d. (Optional) To create an IPS profile, click the button. e. Click [OK].

4. On the [Create/Edit L2 Policy Enforcement Rule Set] window, do one of the following.

- Click [Create] to create a new L2 Policy Enforcement rule.

- Click a rule name to edit L2 rule settings.

For more information about creating/editing L2 policy rules, see Configuring L2 Policy Enforcement Rules.

5. Click [OK] on the [Create/Edit L2 Policy Enforcement Rule] window.

6. Click [Save] on the [Create/Edit L2 Policy Enforcement Rule Set] window.

6.2.1.2 Configuring L2 Policy Enforcement Rules

Procedure

1. Configure the required objects and profiles.

- MAC Objects

For more information, see Configuring MAC Objects.

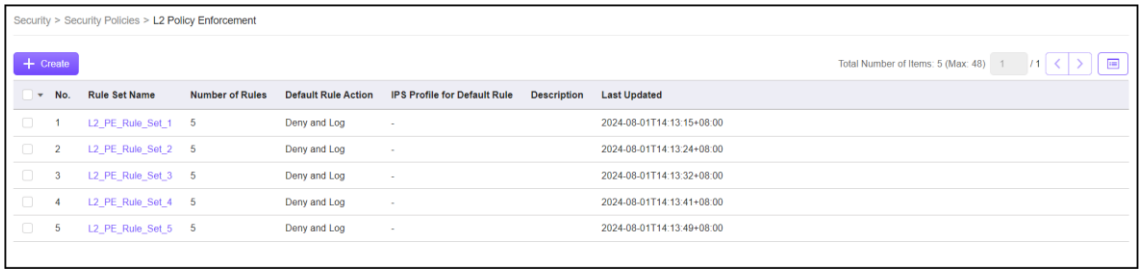
- Protocol Filter Profiles

For more information, see Configuring Protocol Filter Profiles.

- IPS Profiles

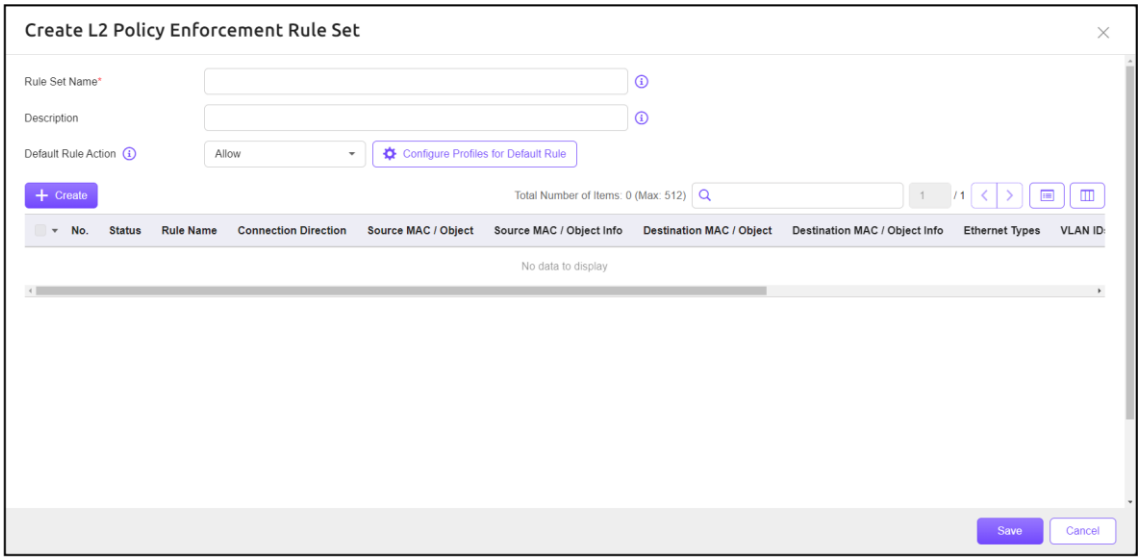
For more information, see Configuring IPS Profiles.

2. Go to [Security] > [Security Policies] > [L2 Policy Enforcement].

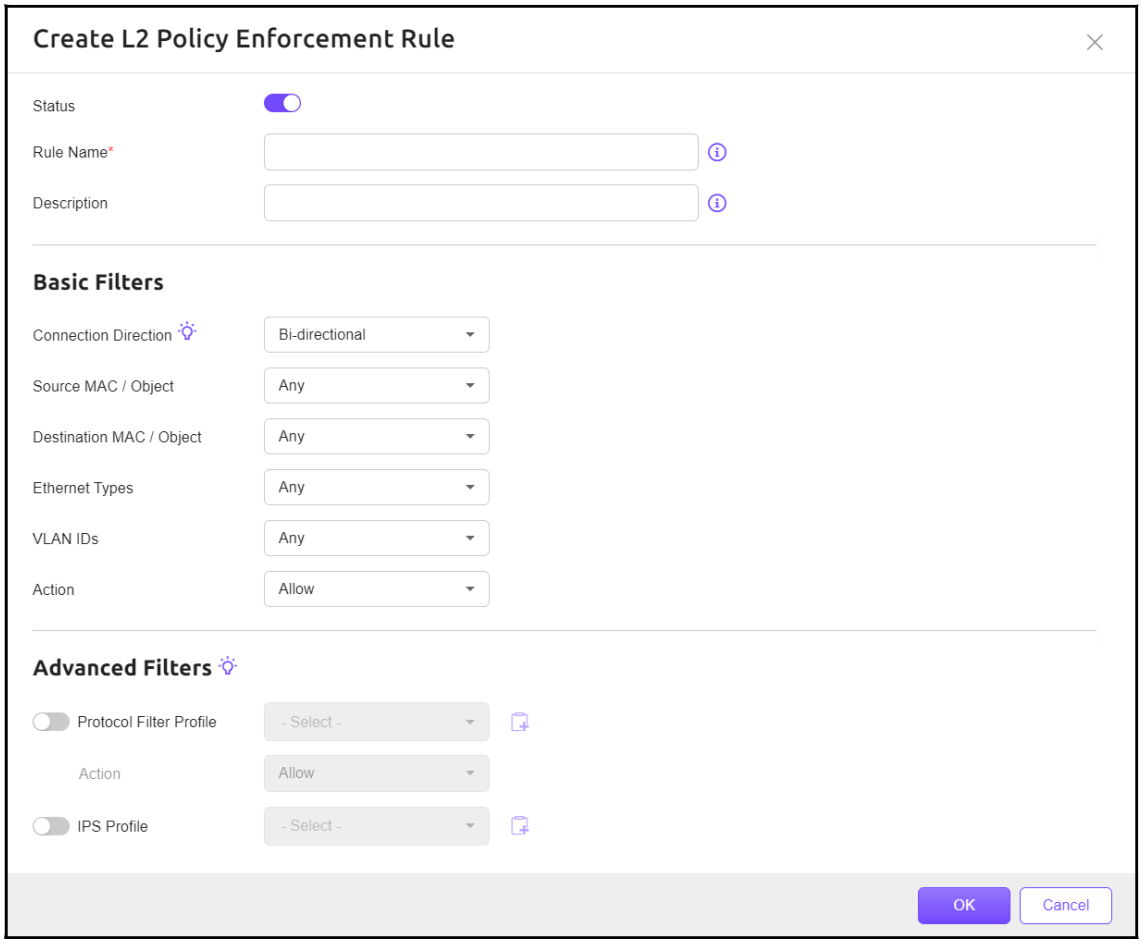


3. On the [L2 Policy Enforcement] page, do one of the following.

- Click [Create] to create a rule set and add L2 rules to this new rule set. The [Create L2 Policy Enforcement Rule Set] window will appear.
- Click the name of the rule set that you want to add L2 rules to or modify its existing rules. The [Edit L2 Policy Enforcement Rule Set] window will appear.



4. On the [Create/Edit L2 Policy Enforcement Rule Set] window, do one of the following.
   - Click [Create] to add a new L2 Policy Enforcement rule. The [Create L2 Policy Enforcement Rule] window will appear.
   - Click a rule name to edit L2 rule settings. The [Edit L2 Policy Enforcement Rule] window will appear.



5. Configure the following settings.

Item	Description
Status	Enable the operational status of this L2 Policy Enforcement rule by clicking the toggle.
Rule Name	Type a rule name for this L2 Policy Enforcement rule.
Description	(Optional) Type a description.

- Basic Filter

Item	Description
Connection Direction	Select one of the following directions: • **Bi-directional**: The Edge device doesn't consider the direction of a detected connection as a rule matching criterion in the basic filter. • **Towards Asset**: The Edge device considers the direction of a detected connection as a rule matching criterion in the basic filter. When the connection direction is set to **Towards Asset** and the detected connection is initiated from a non-asset towards an asset, this criterion is met, and the Edge device takes the specified rule action accordingly. If the detected connection does not meet this criterion, the Edge device proceeds to check the next specified criterion in the basic filter. • **Away from Asset**: The Edge device considers the direction of a detected connection as a rule matching criterion in the basic filter. When the connection direction is set to **Away from Asset** and the detected connection is initiated from an asset towards a non-asset, this criterion is met, and the Edge device takes the specified rule action accordingly. If the detected connection does not meet this criterion, the Edge device proceeds to check the next specified criterion in the basic filter.
Source MAC/Object	Select one of the following for the source MAC addresses: • Any • MAC Address • MAC Object If you select [MAC Object], you can select a MAC object that has been created beforehand on the [MAC Objects] page or click the button to create a new MAC object.
Destination MAC/Object	Select one of the following for the destination MAC addresses: • Any • MAC Address • MAC Object
Ethernet Types	Select either one of the following for the Ethernet types: • Any

Item	Description
	• Custom: Specify at least one Ethernet type. A maximum of five Ethernet types can be applied to one policy rule. For more information about Ethernet type, visit IANA (Internet Assigned Number Authority).
VLAN IDs	Select either one of the following for the VLAN IDs: • Any • Custom: Specify at least one VLAN ID for this protocol. A maximum of five VLAN IDs can be applied to one policy rule.
Action	Select one of the following actions: • **Allow**: Select this option to allow network traffic that matches this rule. • **Allow and Log**: Select this option to allow network traffic that matches this rule and output a log. • **Deny and Log**: Select this option to block network traffic that matches this rule and output a log.

- Advanced Filters: If you select [Allow] or [Allow and Log] for [Action], you can set advanced filters (Protocol Filter profile and IPS profile) to conduct further actions.

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

6. Click [OK].

7. Click [Save] on the [Create/Edit L2 Policy Enforcement Rule Set] window.

You may click the button in the upper right corner of the table to show/hide certain type of information and adjust the column order. For more information, see Viewing in Table View Mode.

6.2.1.3 Managing L2 Policy Enforcement Rule Sets and Rules

The following tables list the common tasks for managing L2 Policy Enforcement rule sets and rules.

- **Rule Sets:**

Task	Action
To create an L2 Policy Enforcement rule set	Click the [Create] button to create a new L2 Policy Enforcement rule set.
To delete an L2 Policy Enforcement rule set	Click the checkbox of a rule set and click the [Delete] button.
To duplicate an L2 Policy Enforcement rule set	Click the checkbox of a rule set and click the [Duplicate] button.
To edit an L2 Policy Enforcement rule set	Click the name of a rule set, and an [Edit L2 Policy Enforcement Rule Set] window will appear.

- **Rules:**

Task	Action
To create an L2 Policy Enforcement rule	Click the [Create] button to create a new L2 Policy Enforcement rule.
To delete an L2 Policy Enforcement rule	Click the checkbox of a rule and click the [Delete] button.
To duplicate an L2 Policy Enforcement rule	Click the checkbox of a rule and click the [Duplicate] button.
To edit an L2 Policy Enforcement rule	Click the name of a rule, and an [Edit L2 Policy Enforcement Rule] window will appear.
To change the priority of an L2 Policy Enforcement rule	Click the checkbox of a rule, click the [Change Priority] button, and specify a new priority for this rule.

When more than one L2 Policy Enforcement rule is matched, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules listed in a rule set table are ordered by priority, with the highest priority rule listed on the first row of the table.

6.2.2 Policy Enforcement

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

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

- **Device Rule Set**: Contains the policy rule sets created and configured by users with the Edge device local account privileges.
- **EdgeOne Rule Set**: Contains the policy rule sets synced from EdgeOne. Users with EdgeOne local account privileges can apply them to the devices managed by EdgeOne. Users with the Edge device local account privileges can only view these EdgeOne policy rules.

The device rules take higher priorities than the EdgeOne rules.

Comparing L2 and L3 Policy Enforcement Rules in Edge Device

- **L2 Policy Enforcement:** L2 policies are designed to control non-IP traffic—specifically, Ethernet frames that do not encapsulate IPv4 or IPv6 packets. These are typically used in OT environments where communication is based on

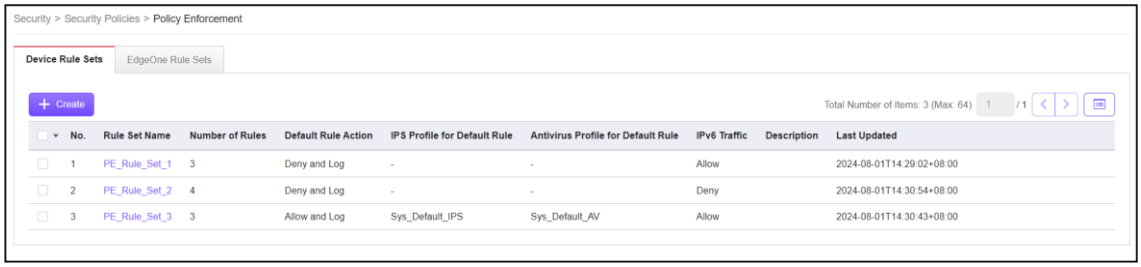
MAC addresses, often due to legacy protocols. For example, blocking a specific MAC address without reference to higher-layer protocols. For more information about L2 Policy Enforcement, see L2 Policy Enforcement.

- **L3 Policy Enforcement:** L3 policies apply to all IPv4 traffic, including ICMP, TCP, and UDP. Although IPv4 packets (like ping/ICMP) are carried within Ethernet frames, they are handled by L3 rules, not L2. Therefore, any enforcement for such traffic must be done via L3 policies.

6.2.2.1 Configuring Policy Enforcement Rule Sets

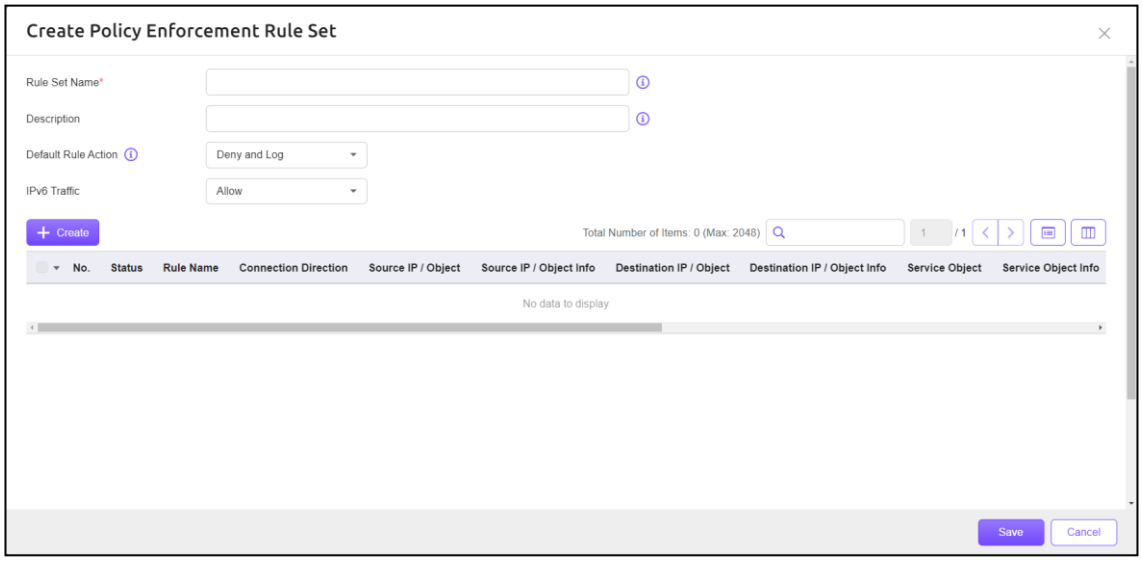
Procedure

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



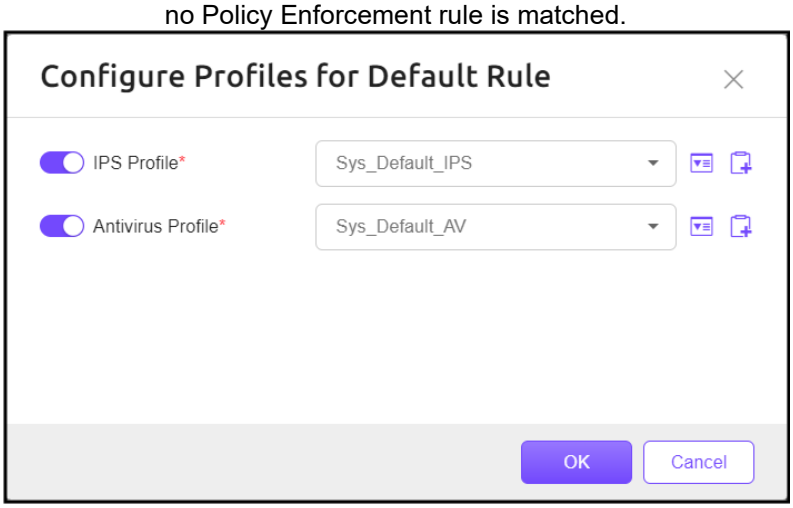
2. On the [Policy Enforcement] page, do one of the following.

- Click [Create] to create a rule set and add rules to this new rule set. The [Create Policy Enforcement Rule Set] window will appear.
- Click the name of the rule set that you want to add rules to or modify its existing rules. The [Edit Policy Enforcement Rule Set] window will appear.



3. Configure the following settings.

Item	Description
Rule Set Name	Type a rule name for this Policy Enforcement rule set.
Description	(Optional) Type a description.
Default Rule Action	Select a default action, **Allow**, **Allow and Log** or **Deny and Log**, for when no Policy Enforcement rule is matched.
Configure Profiles for Default Rule	(Optional) If the default rule action is **Allow** or **Allow and Log**, click the [Configure Profiles for Default Rule] button to specify which IPS and antivirus profiles to use for traffic examination when

Item	Description
	no Policy Enforcement rule is matched.  a. Click the [IPS Profile] and [Antivirus Profile] toggles to enable the settings. b. Select a pre-defined IPS profile and an antivirus profile from the drop-down lists or use the system default profiles (Sys_Default_IPS and Sys_Default_AV). c. (Optional) To view/edit detailed profile settings, click the button. d. (Optional) To create a profile, click the button. e. Click [OK].
IPv6 Traffic	Select an action, **Allow** or **Deny**, for the device to perform when it detects IPv6 packets.

4. On the [Create/Edit Policy Enforcement Rule Set] window, do one of the following.
   - Click [Create] to create a new Policy Enforcement rule.
   - Click a rule name to edit rule settings.

For more information about creating/editing policy rules, see Configuring Policy Enforcement Rules.

5. Click [OK] on the [Create/Edit Policy Enforcement Rule] window.
6. Click [Save] on the [Create/Edit Policy Enforcement Rule Set] window.

6.2.2.2 Configuring Policy Enforcement Rules

Procedure

1. Configure the required objects and profiles.
   - IP Objects

For more information, see Configuring IP Objects.

   - Service Objects

For more information, see Configuring Service Objects.

   - Protocol Filter Profiles

For more information, see Configuring Protocol Filter Profiles.

   - IPS Profiles

For more information, see Configuring IPS Profiles.

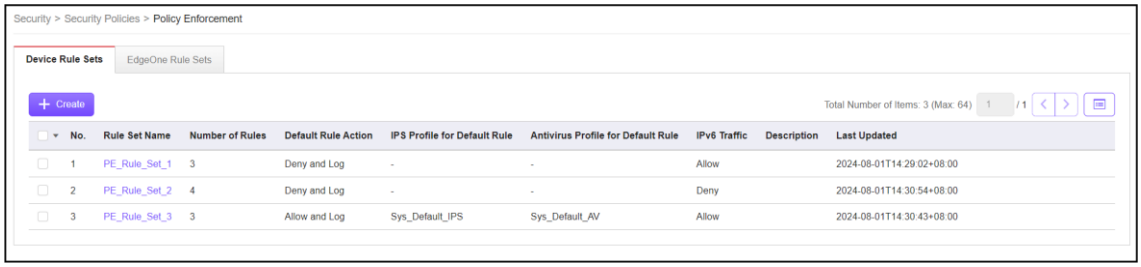
- File Filter Profiles

For more information, see Configuring File Filter Profiles.

- Antivirus Profiles

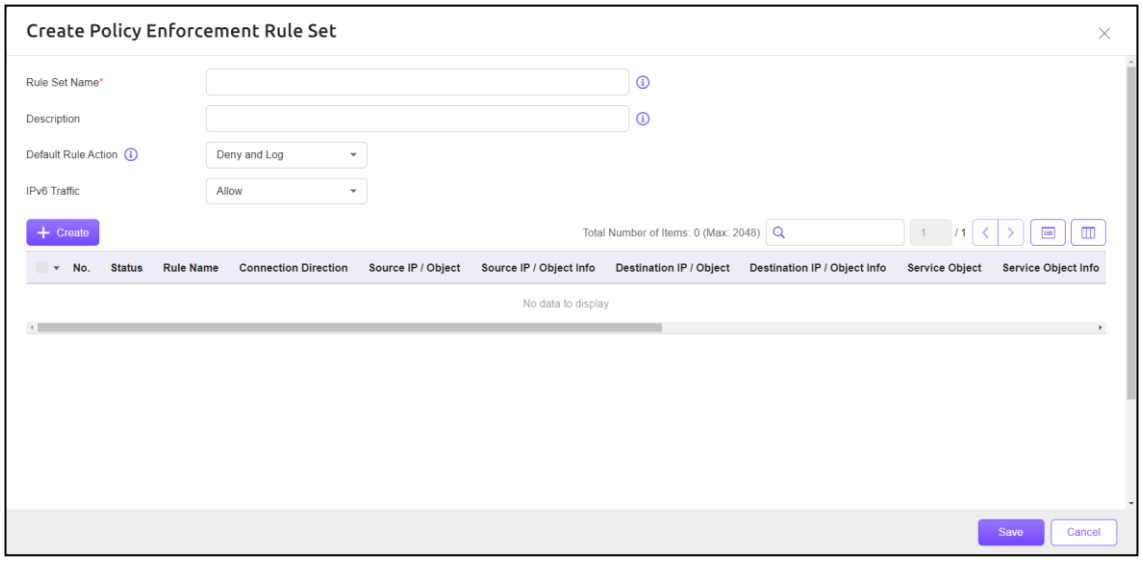
For more information, see Configuring Antivirus Profiles.

2. Go to [Security] > [Security Policies] > [Policy Enforcement].



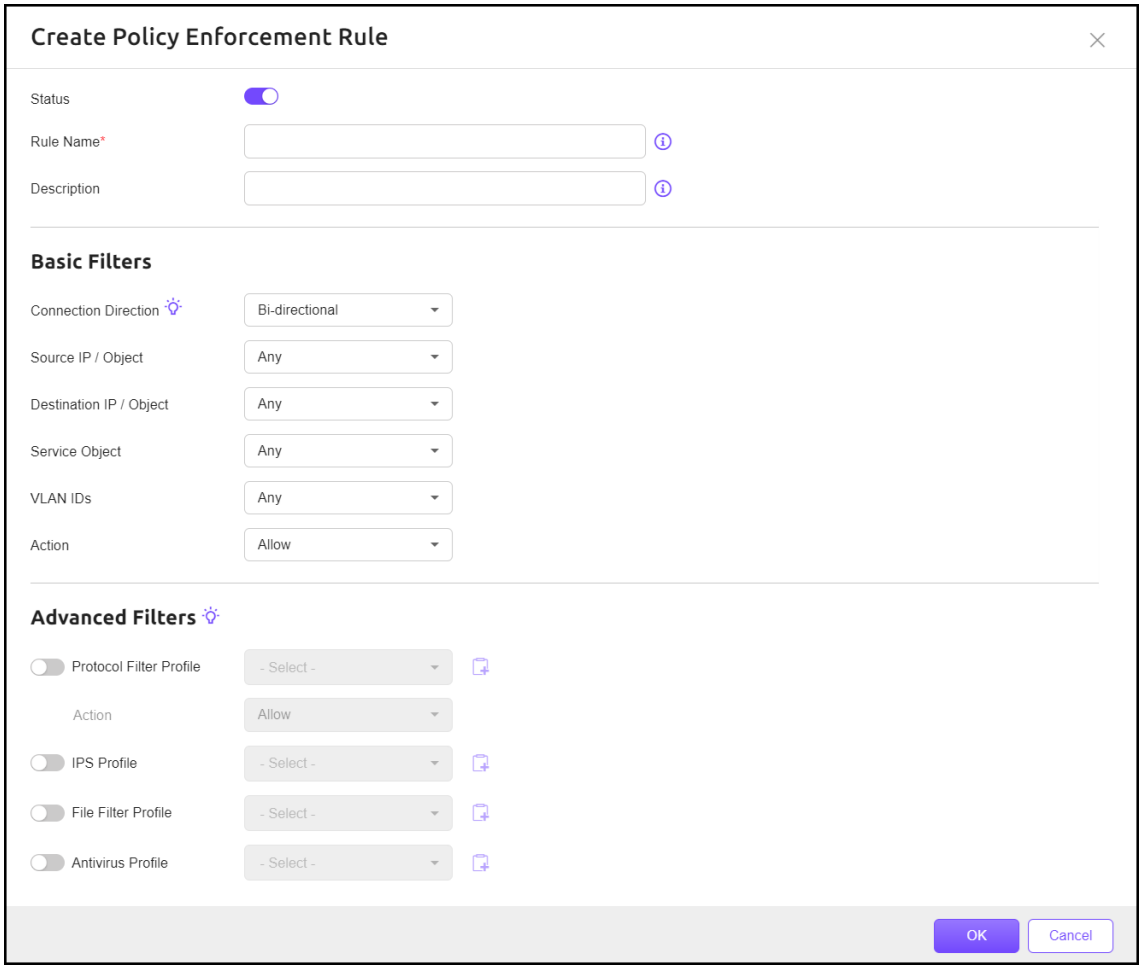
3. On the [Policy Enforcement] page, do one of the following.

- Click [Create] to create a rule set and add rules to this new rule set. The [Create Policy Enforcement Rule Set] window will appear.
- Click the name of the rule set that you want to add rules to or modify its existing rules. The [Edit Policy Enforcement Rule Set] window will appear.



4. On the [Create/Edit Policy Enforcement Rule Set] window, do one of the following.

- Click [Create] to add a new Policy Enforcement rule. The [Create Policy Enforcement Rule] window will appear.
- Click a rule name to edit rule settings. The [Edit Policy Enforcement Rule] window will appear.



5. Configure the following settings.

Item	Description
Status	Enable the operational status of this Policy Enforcement rule by clicking the toggle.
Rule Name	Type a rule name for this Policy Enforcement rule.
Description	(Optional) Type a description.

- Basic Filters

Item	Description
Connection Direction	Select one of the following directions: • **Bi-directional**: The Edge device doesn't consider the direction of a detected connection as a rule matching criterion in the basic filter. • **Towards Asset**: The Edge device considers the direction of a detected connection as a rule matching criterion in the basic filter. When the connection direction is set to **Towards Asset** and the detected connection is initiated from a non-asset towards an asset, this criterion is met, and the Edge device takes the specified rule action accordingly. If the detected connection does not meet this

Item	Description
	criterion, the Edge device proceeds to check the next specified criterion in the basic filter. • **Away from Asset**: The Edge device considers the direction of a detected connection as a rule matching criterion in the basic filter. When the connection direction is set to **Away from Asset** and the detected connection is initiated from an asset towards a non-asset, this criterion is met, and the Edge device takes the specified rule action accordingly. If the detected connection does not meet this criterion, the Edge device proceeds to check the next specified criterion in the basic filter.
Source IP/Object	Select one of the following for the source IP addresses: • Any • Single IP • IP Range • IP Subnet • IP Object If you select [IP Object], you can select an IP object that has been created beforehand on the [IP Objects] page or click the button to create a new IP object.
Destination IP/Object	Select one of the following for the destination IP addresses: • Any • Single IP • IP Range • IP Subnet • IP Object
Service Object	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 If you select [Service Object], you can select a service object that has been created beforehand on the [Service

Item	Description
	Objects] page or click the button to create a new service object.
VLAN IDs	Select either one of the following for the VLAN IDs: • Any • Custom: Specify at least one VLAN ID for this protocol. A maximum of five VLAN IDs can be applied to one policy rule.
Action	Select one of the following actions: • **Allow**: Select this option to allow network traffic that matches this rule. • **Allow and Log**: Select this option to allow network traffic that matches this rule and output a log. • **Deny and Log**: Select this option to block network traffic that matches this rule and output a log.

- Advanced Filters: If you select [Allow] or [Allow and Log] for [Action], you can set advanced filters (Protocol Filter profile, IPS profile, and File Filter profile) to conduct further actions.

Item	Description
Protocol Filter Profile	Select a Protocol Filter profile you have defined beforehand or click the button to create a new profile. From the [Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.
IPS Profile	Select an IPS profile you have defined beforehand or click the button to create a new profile.
File Filter Profile	Select a File Filter profile you have defined beforehand or click the button to create a new profile.
Antivirus Profile	Select an Antivirus profile you have defined beforehand or click the button to create a new profile.

6. Click [OK].

7. Click [Save] on the [Create/Edit Policy Enforcement Rule Set] window.

You may click the button in the upper right corner of the table to show/hide certain type of information and adjust the column order. For more information, see Viewing in Table View Mode.

6.2.2.3 Managing Policy Enforcement Rule Sets and Rules

The following tables list the common tasks for managing Policy Enforcement rule sets and rules.

- **Device Rule Sets:**

Task	Action
To create a Policy Enforcement rule set	Click the [Create] button to create a new Policy Enforcement rule set.
To delete a Policy Enforcement rule set	Click the checkbox of a rule set and click the [Delete] button.
To duplicate a Policy Enforcement rule set	Click the checkbox of a rule set and click the [Duplicate] button.
To edit a Policy Enforcement rule set	Click the name of a rule set, and an [Edit Policy Enforcement Rule Set] window will appear.

- **EdgeOne Rule Sets:**

Task	Description
N/A	The Policy Enforcement rule sets on the [EdgeOne Rule Set] list are view-only.

- **Rules:**

Task	Action
To create a Policy Enforcement rule	Click the [Create] button to create a new Policy Enforcement rule.
To delete a Policy Enforcement rule	Click the checkbox of a rule and click the [Delete] button.
To duplicate a Policy Enforcement rule	Click the checkbox of a rule and click the [Duplicate] button.
To edit a Policy Enforcement rule	Click the name of a rule, and an [Edit Policy Enforcement Rule] window will appear.
To change the priority of a Policy Enforcement rule	Click the checkbox of a rule, click the [Change Priority] button, and specify a new priority for this rule.

When more than one Policy Enforcement rule is matched, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules listed in a rule set table are ordered by priority, with the highest priority rule listed on the first row of the table.

6.2.3 Policy Rule Auto-Learning

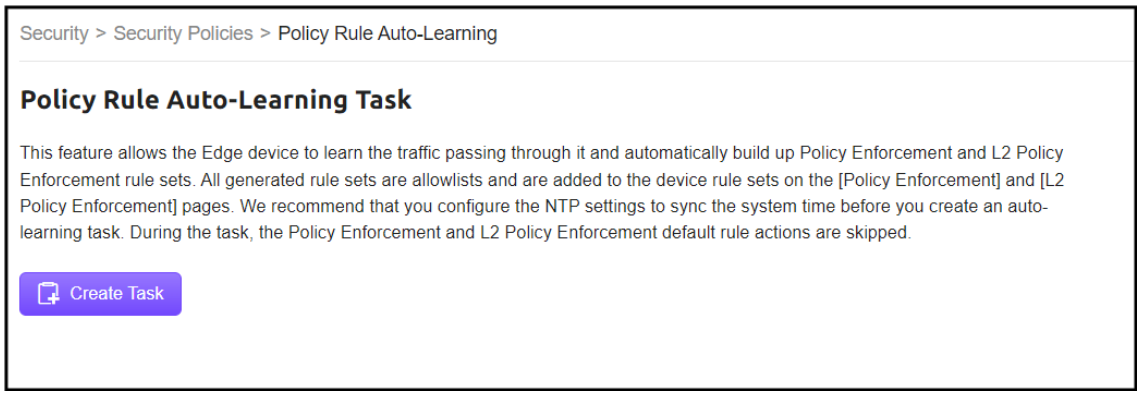
Policy Rule Auto-Learning allows you to create a learning task within a scheduled period of time to collect information about legitimate network traffic, and then use it to generate a trust list of Policy Enforcement baseline rules for your network environment.

Before you create a policy rule auto-learning task, ensure that IPS profiles are properly configured. For more information about IPS profiles, see IPS Profiles.

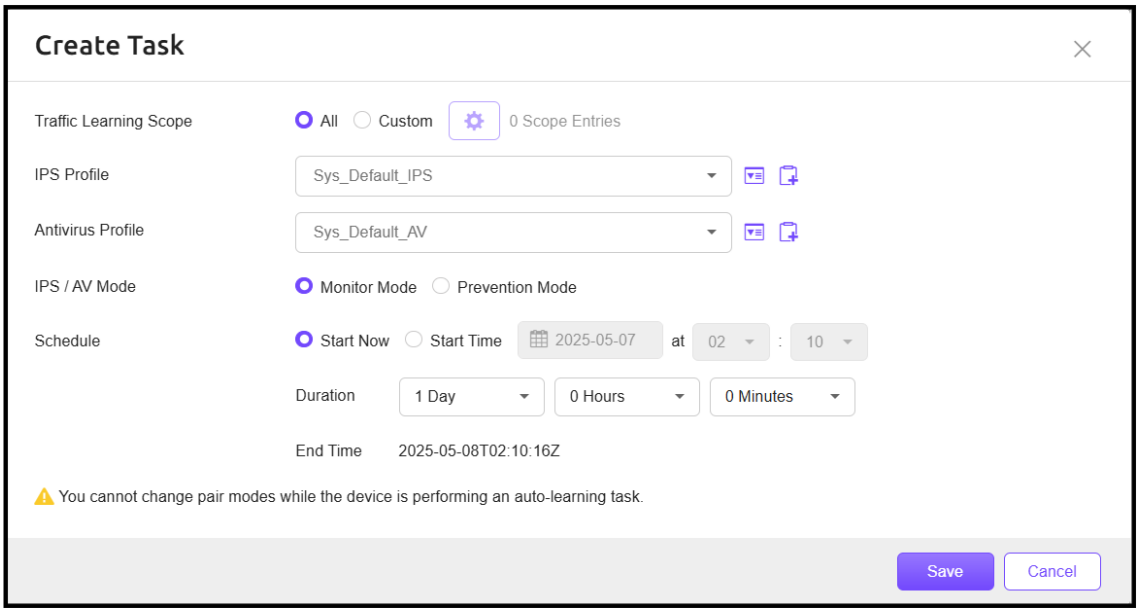
6.2.3.1 Creating Policy Rule Auto-Learning Tasks

Procedure

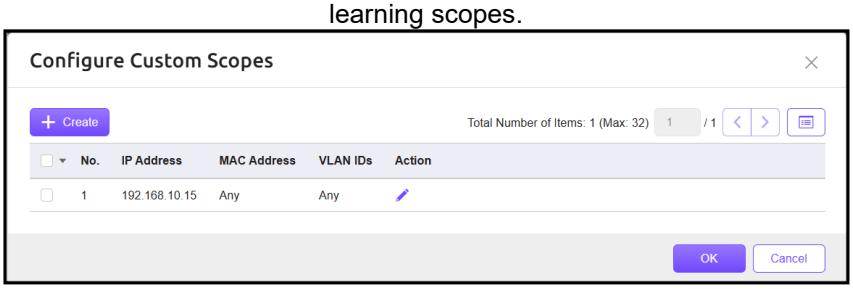
1. Go to [Security] > [Security Policies] > [Policy Rule Auto-Learning].

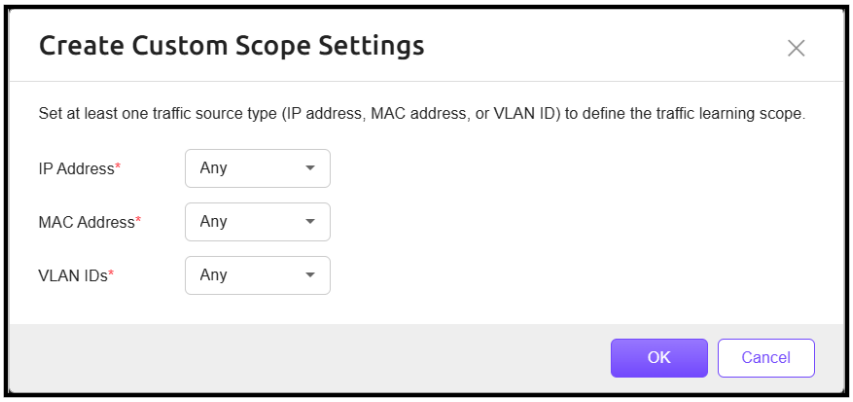


2. Click the [Create Task] button to create an auto-learning task. The [Create Task] window will appear.



3. Configure the following settings.

Item	Description
Traffic Learning Scope	Select **All** to perform the learning task based on all traffic flowing through the device, or **Custom** to define the specific types of traffic the device should use for learning. If you select **Custom**, click the button to further configure traffic learning scopes.  1. On the [Configure Custom Scopes] window, do one of the following. • Click [Create] to create a scope entry. The [Create Custom Scope Settings] window will appear. • Click to edit scope settings. The [Edit Custom Scope Settings] window will appear.

Item	Description
	 2. Set at least one traffic source type, including IP address, MAC address, and VLAN ID to define the traffic learning scope. • **IP Address**: Select one of the following for the source IP addresses: ○ Any ○ Single IP: Specify an IP address. ○ IP Range: Specify an IP range. ○ IP Subnet: Specify an IP subnet. • **MAC Address**: Select either one of the following for the source MAC addresses: ○ Any ○ Custom: Specify a MAC address. • **VLAN IDs**: Select either one of the following for the source VLAN IDs: ○ Any ○ Custom: Specify one to five VLAN IDs. 3. Click [OK] on the [Create Custom Scope Settings] or [Edit Custom Scope Settings] window, then click [OK] on the [Configure Custom Scopes] window.
IPS Profile	Select an IPS profile to apply to the learning task.
Antivirus Profile	Select an Antivirus profile to apply to the learning task.
IPS / AV Mode	Select **Monitor Mode** or **Prevention Mode** to apply to the learning task.
Schedule	Select **Start Now** to start the task once you complete the task settings, or **Start Time** and specify a specific time to schedule the task. • Duration: Specify the duration of the task. • End Time: The system will calculate the end time based on your execution time and duration.

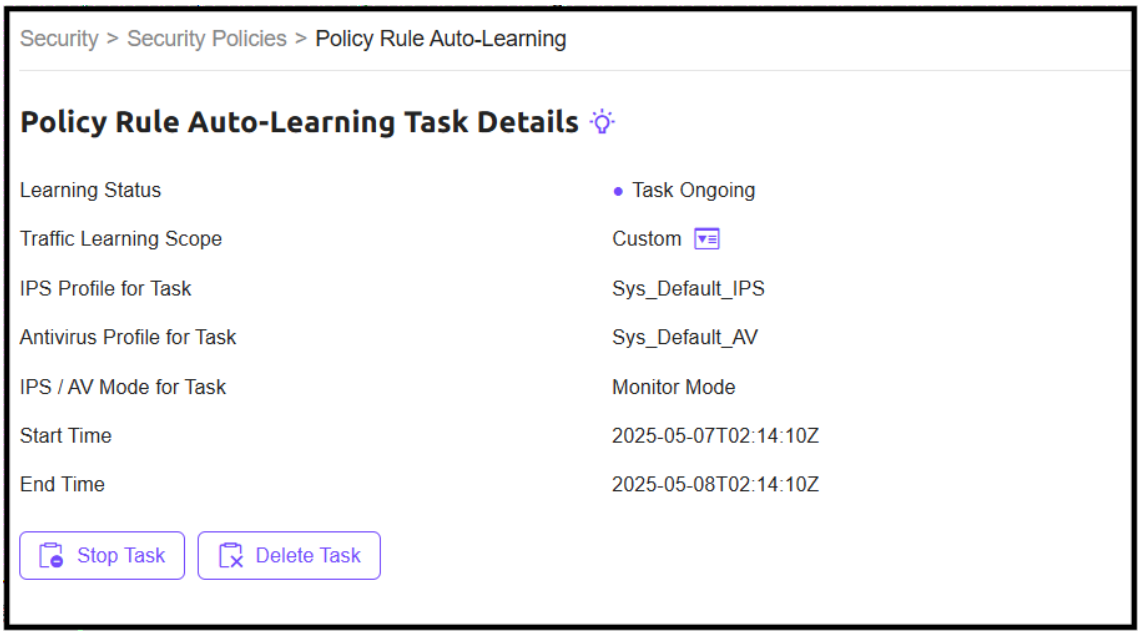
4. Click [Save] to create the task.

When a learning task is running, you cannot upload a configuration file to restore settings or change pair modes.

6.2.3.2 Stopping Policy Rule Auto-Learning Tasks

Procedure

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

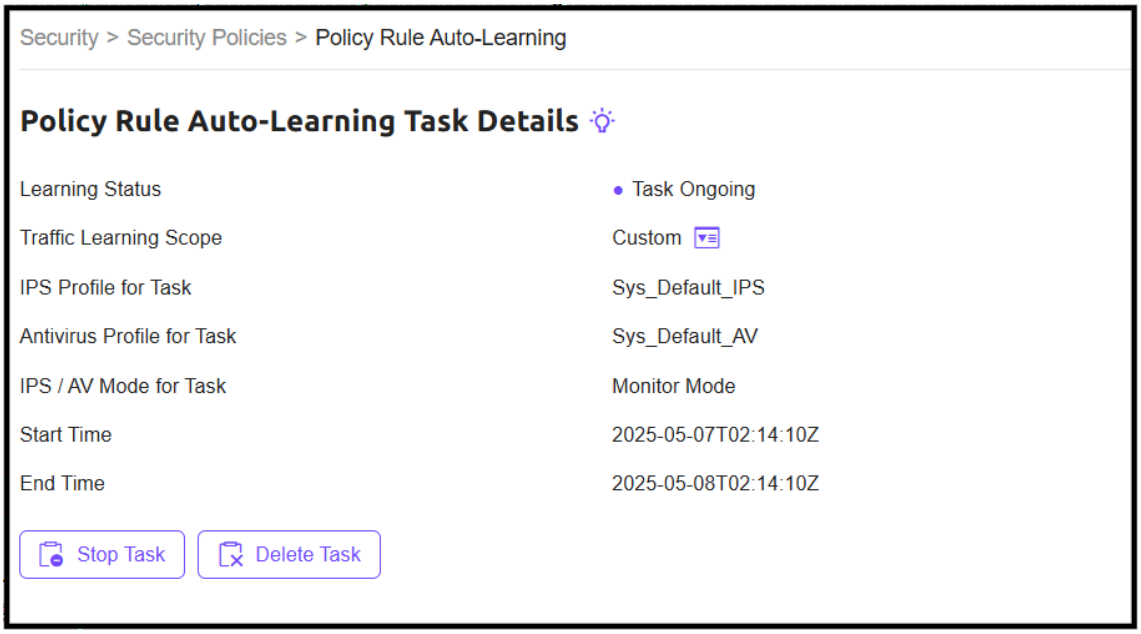


2. Click the [Stop Task] button to stop the auto-learning task. After you stop the task, a learning result will still be generated for your review.

6.2.3.3 Deleting Policy Rule Auto-Learning Tasks

Procedure

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

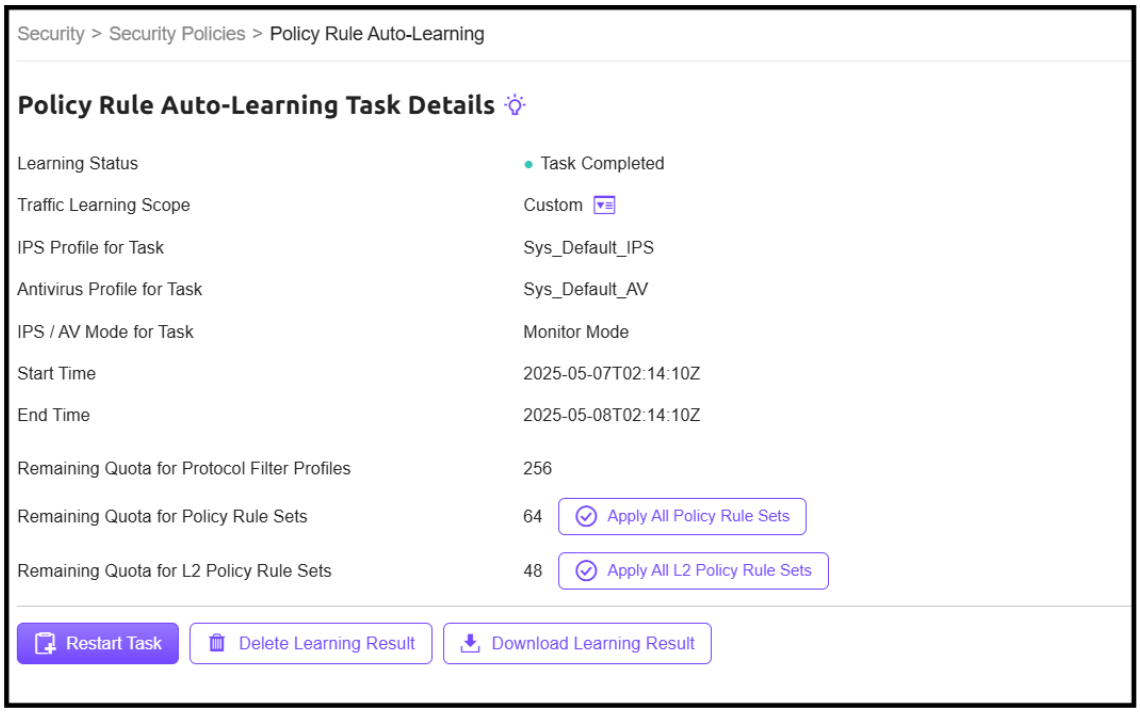


2. Click the [Delete Task] button to delete the auto-learning task. Note that if you delete the task, the learning result will be erased.

6.2.3.4 Restarting Policy Rule Auto-Learning Tasks

Procedure

1. After a learning task is completed/stopped, go to [Security] > [Security Policies] > [Policy Rule Auto-Learning].

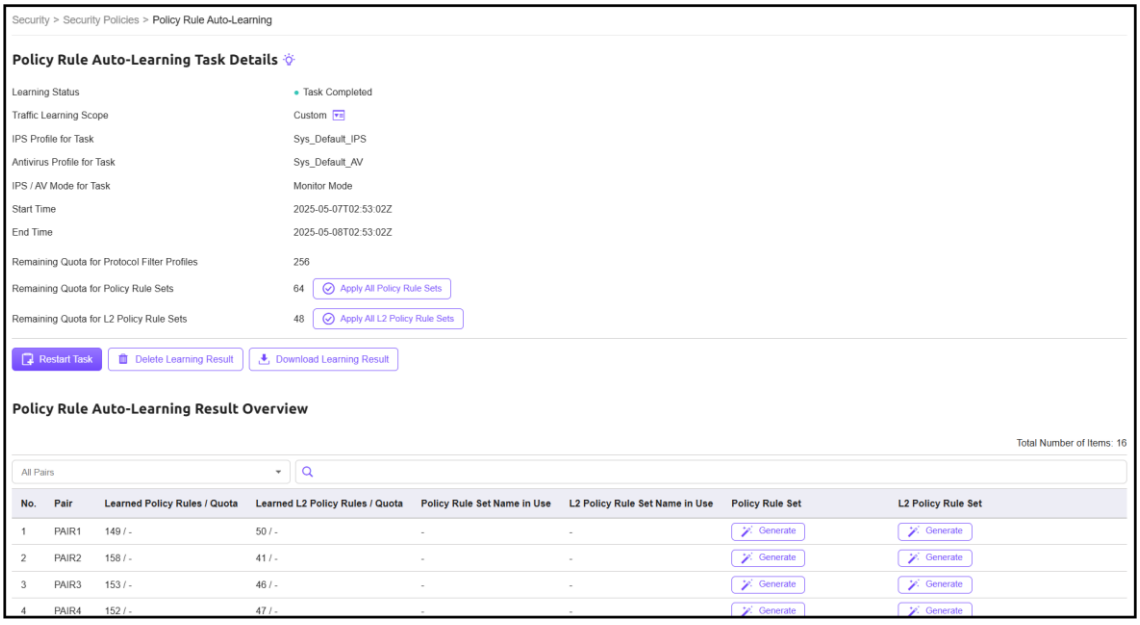


2. Click the [Restart Task] button to restart the auto-learning task. Note that if you restart the task, the previous learning result will be erased.

6.2.3.5 Generating and Applying Learned Policy Enforcement Rule Sets

Procedure

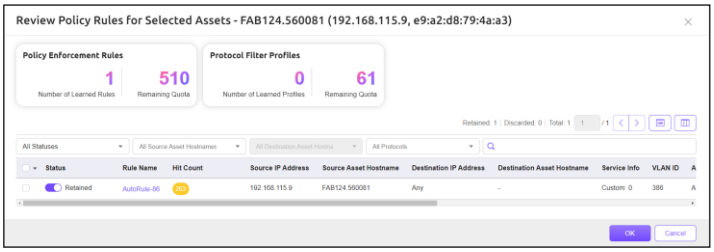
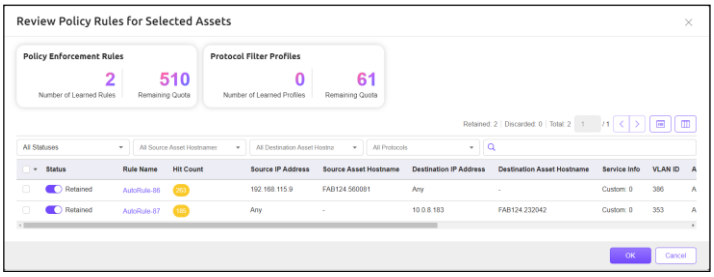
1. After a learning task is completed/stopped, go to [Security] > [Security Policies] > [Policy Rule Auto-Learning].

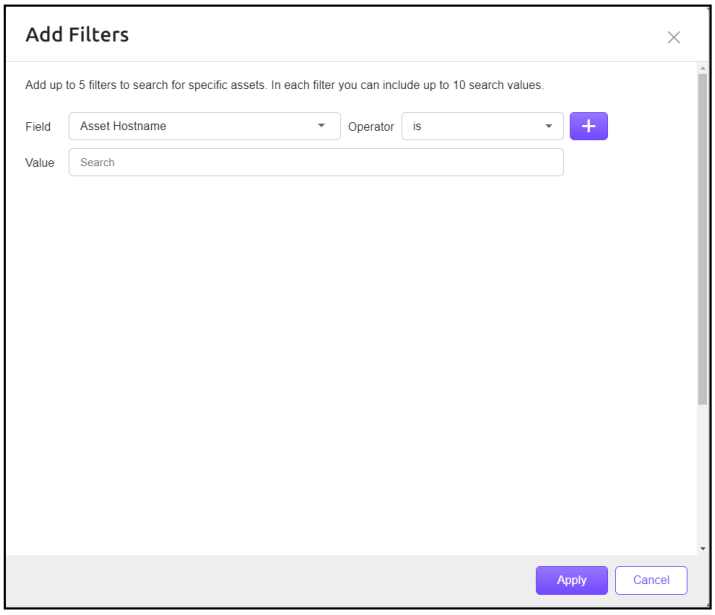


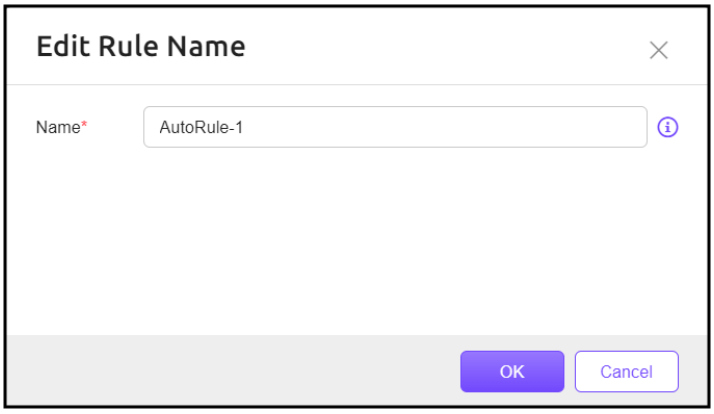
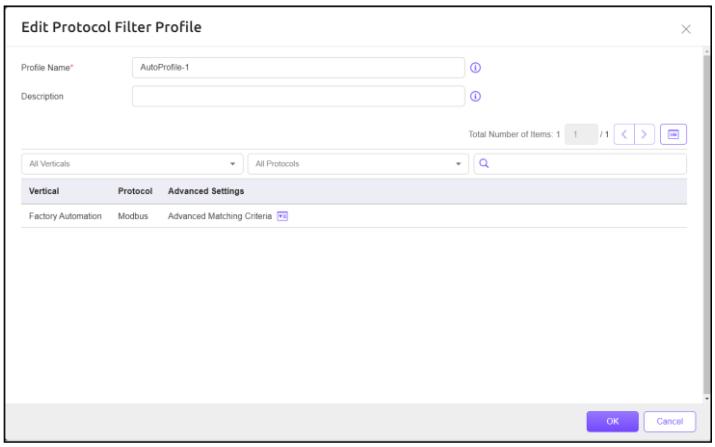
2. To apply all the learned policy rule sets to the device, click [Apply All Policy Rule Sets].

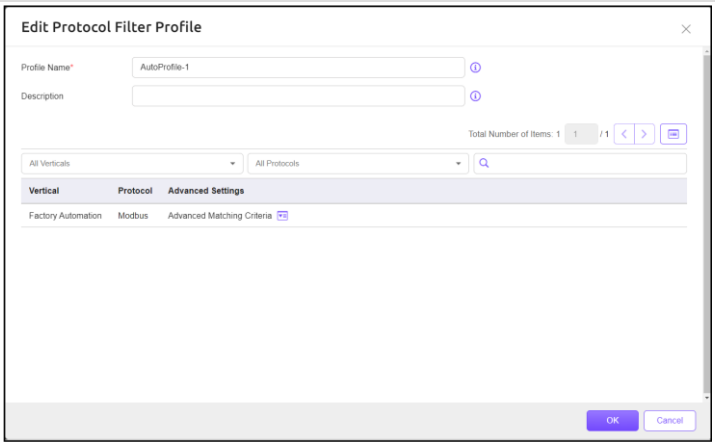
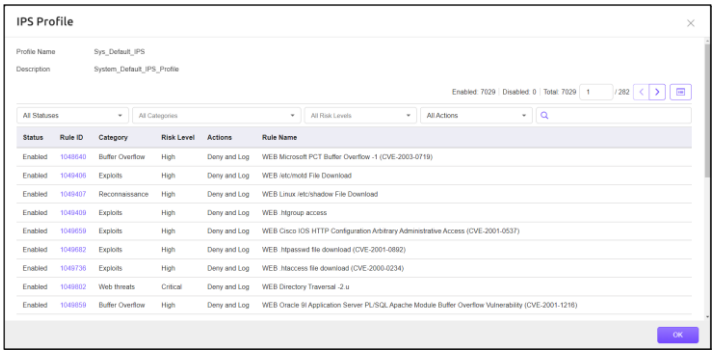
3. To review the learned policy rule sets of each interface and decide which rule sets to apply, click [Generate]. The [Review Generated Policy Rule Set] or [Review Generated L2 Policy Rule Set] window will appear.

The following table lists the tasks that you can perform on the [Review Generated Policy Rule Set] and [Review Generated L2 Policy Rule Set] windows.

Task	Procedure
To review policy rules based on network traffic from one asset	1. Go to the [Review Rules by Asset] tab. 2. Select an asset. The following window will appear.  3. All learned policy rules are retained by default. To discard unwanted rules, click the toggles in the [Status] column. 4. Click [OK]. 📝 The number of retained policy rules and Protocol Filter profiles must not exceed their respective remaining quotas.
To review policy rules based on network traffic from multiple assets	1. Go to the [Review Rules by Asset] tab. 2. Check the [Multiple Selection] checkbox. 3. Select multiple assets and click [Review Rules for Selected Assets]. The following window will appear. 

Task	Procedure
	4. All learned policy rules are retained by default. To discard unwanted rules, click the toggles in the [Status] column. 5. Click [OK]. The number of retained policy rules and Protocol Filter profiles must not exceed their respective remaining quotas.
To review all learned policy rules	1. Go to the [Review All Rules] tab. 2. All learned policy rules are retained by default. To discard unwanted rules, click the toggles in the [Status] column. The number of retained policy rules and Protocol Filter profiles must not exceed their respective remaining quotas.
To switch between the grid view and table view modes under the [Review Rules by Asset] tab	1. Click the grid/table view buttons .
To search for specific assets under the [Review Rules by Asset] tab	1. Click the button. The [Add Filters] window will appear.  2. Create up to five search filters. In each filter you can include up to 10 search values. 3. Click [Apply].
To edit a policy rule name	1. Go to the generated policy rule list under either tab. 2. Click a policy rule name in the [Rule Name] column. The [Edit Rule Name] window will appear.

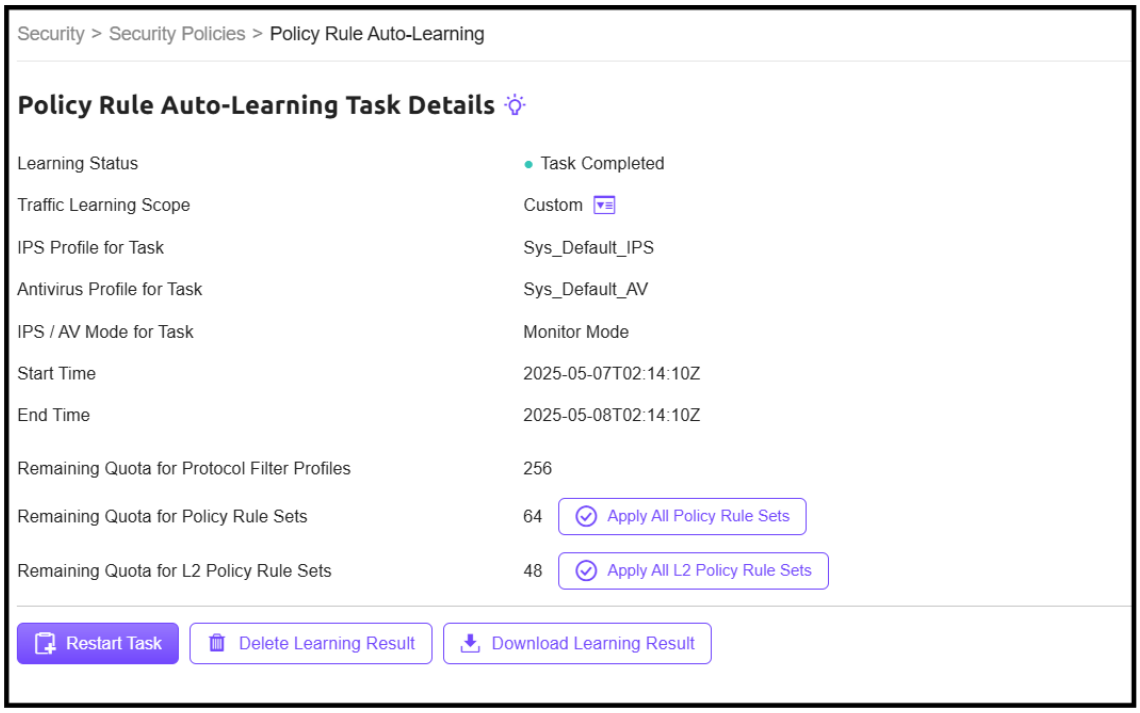
Task	Procedure
	 3. Input a new name. 4. Click [OK].
To edit a Protocol Filter profile name and description	1. Go to the generated policy rule list under either tab. 2. Click a Protocol Filter profile name in the [Protocol Filter Profile] column. The [Edit Protocol Filter Profile] window will appear.  3. Input a new name and/or descrption. 4. Click [OK].
To view details of a learned Protocol Filter profile	1. Go to the generated policy rule list under either tab. 2. Click a Protocol Filter profile name in the [Protocol Filter Profile] column. The [Edit Protocol Filter Profile] window will appear.

Task	Procedure
	 3. Click the [View Detailed Information] button .
To view details of the applied IPS profile	1. Go to the generated policy rule list under either tab. 2. Click the name of the applied IPS profile in the [IPS Profile] column. The following window will appear. 
To save a draft of the generated policy rule list	1. Click [Save as Draft]. To edit a saved draft, click [Generate] on the [Policy Rule Auto-Learning] page.
To apply retained policy rules and Protocol Filter profiles to the Edge device	1. Click [Apply to Device]. The applied policy rules and Protocol Filter profiles will be added to the [Policy Enforcement], [L2 Policy Enforcement], and [Protocol Filter Profiles] pages.

6.2.3.6 Deleting Learning Results

Procedure

1. After a learning task is completed/stopped, go to [Security] > [Security Policies] > [Policy Rule Auto-Learning].

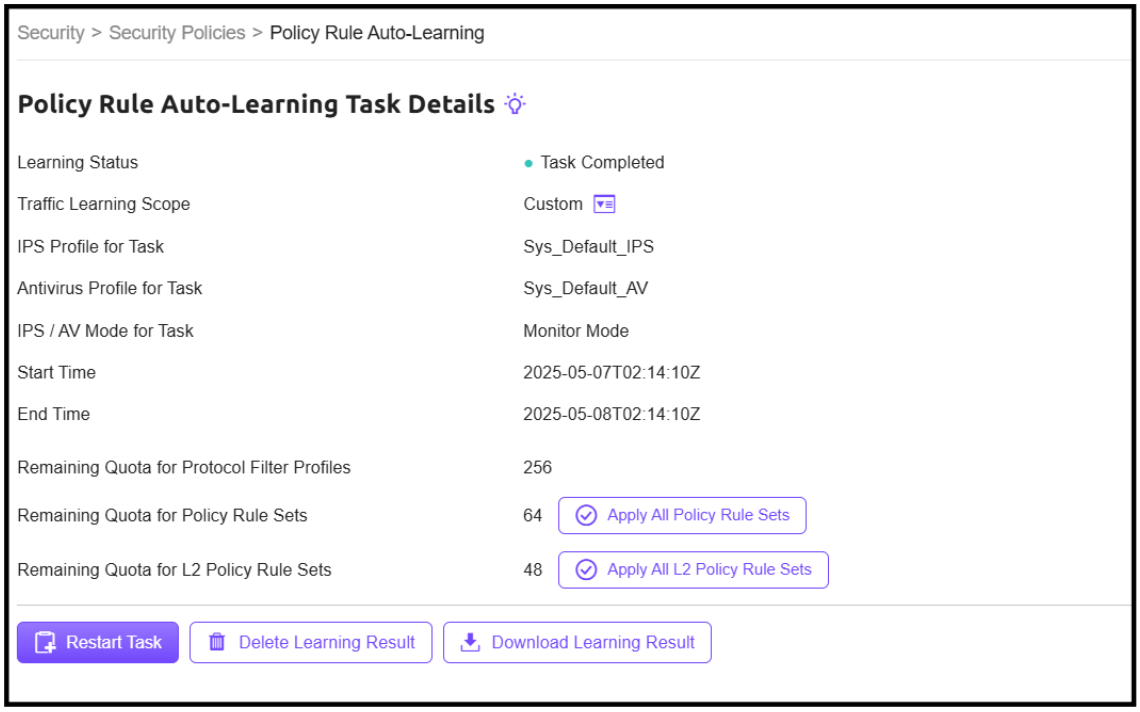


2. Click the [Delete Learning Result] button.

6.2.3.7 Downloading Learning Results

Procedure

1. After a learning task is completed/stopped, go to [Security] > [Security Policies] > [Policy Rule Auto-Learning].



2. Click the [Download Learning Result] button.

6.2.4 Port Security

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

Inline and **Offline Modes** are the security operation modes users can switch between to detect cyber threats and prevent malicious traffic from intruding into your network.

Universal Bypass and **Logical Port Pair (LAG)** are the additional pair mode options specifically designed to optimize the reliability and efficiency of data transmission within your production networks. Universal Bypass combines two port pairs to ensure seamless uplink transmission, with automatic switchover to a spare port in case of any uplink disconnection on the original port, without any disruption to the operation. Logical Port Pair (LAG) combines two or four port pairs to increase the data transmission bandwidth, resulting in faster transfer speeds and improved network performance.

Fail Open, **Fail Close**, and **Force Open** are the hardware bypass modes for different use cases. When the hardware bypass mode is Fail Open, if any hardware failure occurs, the connection will be recovered rapidly. When the hardware bypass mode is Fail Close, if any hardware failure occurs, users might not be able to access the system. When the hardware bypass mode is Force Open, the device allows packets to pass through without conducting packet scanning.

Prevention and **Monitor Modes** are the security deployment modes users can switch between to decide either to prevent or monitor cyber threats. The predefined **Policy Enforcement** and **L2 Policy Enforcement** ruleset templates are used to apply the access rules to the specified conditions per port or pair.

DoS Prevention are used to prevent the Denial of the Service attack to flood/crash the service with the traffic or the trigger, making it inaccessible for the intended users.

LFPT (Link Fault Pass Through) functions to constantly monitor the physical links to prevent data loss, lest, when one side of the link fails, the other side still continues to transmit packets and waits for a response that will never arrive. When an incident of link failure occurred on one node, the link failure signal will pass to the other node so system administrators are able to troubleshoot the problem within a short period of time, minimalizing the potentially severe impact on the service.

6.2.4.1 Configuring Port Security

Procedure

1. Configure the required settings.

- Port Settings

📖	For more information, see Configuring Port Settings.

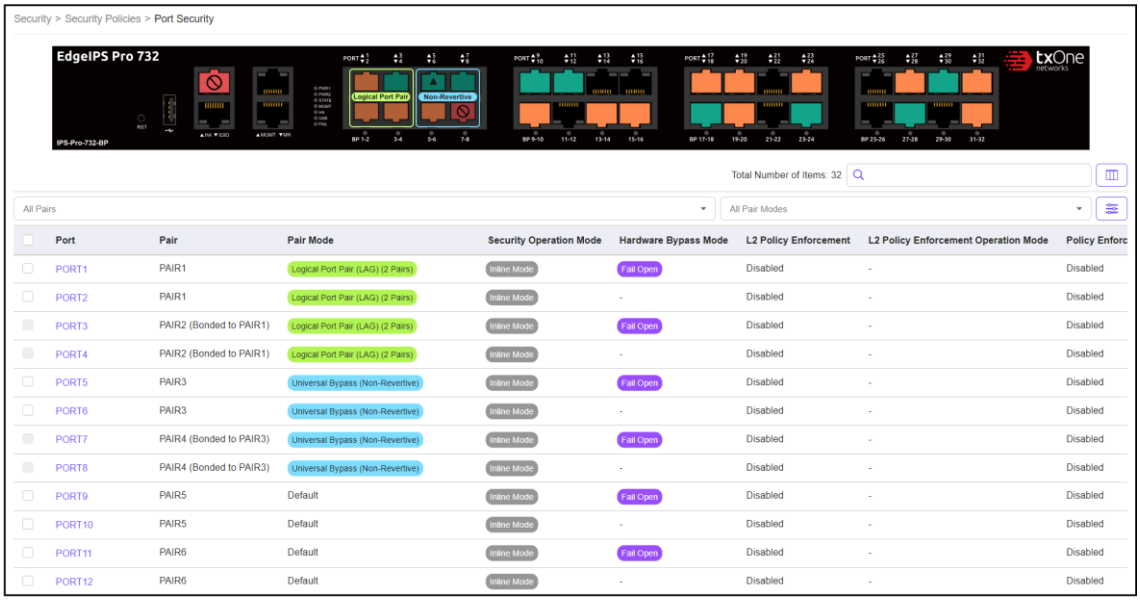
- L2 Policy Enforcement Rule Sets

📖	For more information, see Configuring L2 Policy Enforcement Rule Sets.

- Policy Enforcement Rule Sets

📖	For more information, see Configuring Policy Enforcement Rule Sets.

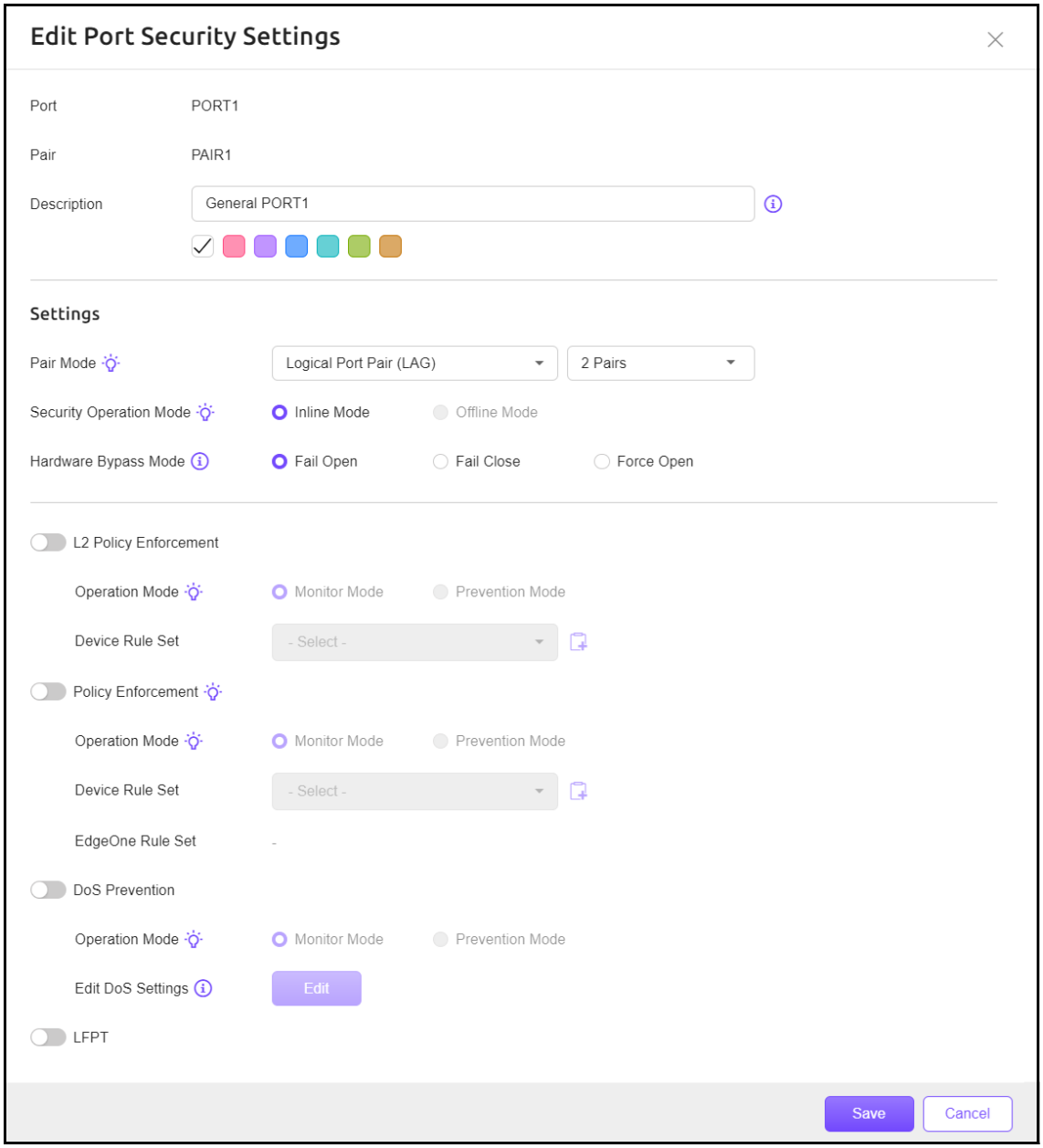
2. Go to [Security] > [Security Policies] > [Port Security].



The table below shows each type of port status.

Port	Status	Description
	Disconnected	Port link down
	Connected	Port link up
	Connected	Port link up (The arrow indicates the uplink traffic toward the original port or spare port when the Pair Mode is Universal Bypass.)
	Disabled	Port disabled
	Bypass	The port bypasses all network traffic to pass through the Edge device when Force Open or Fail Open is enabled.
	LFPT	The port turns to link down status when LFPT is enabled and the other port in the pair is down.

3. Click a port in the [Interface] column. The [Edit Port Security Settings] window will appear.

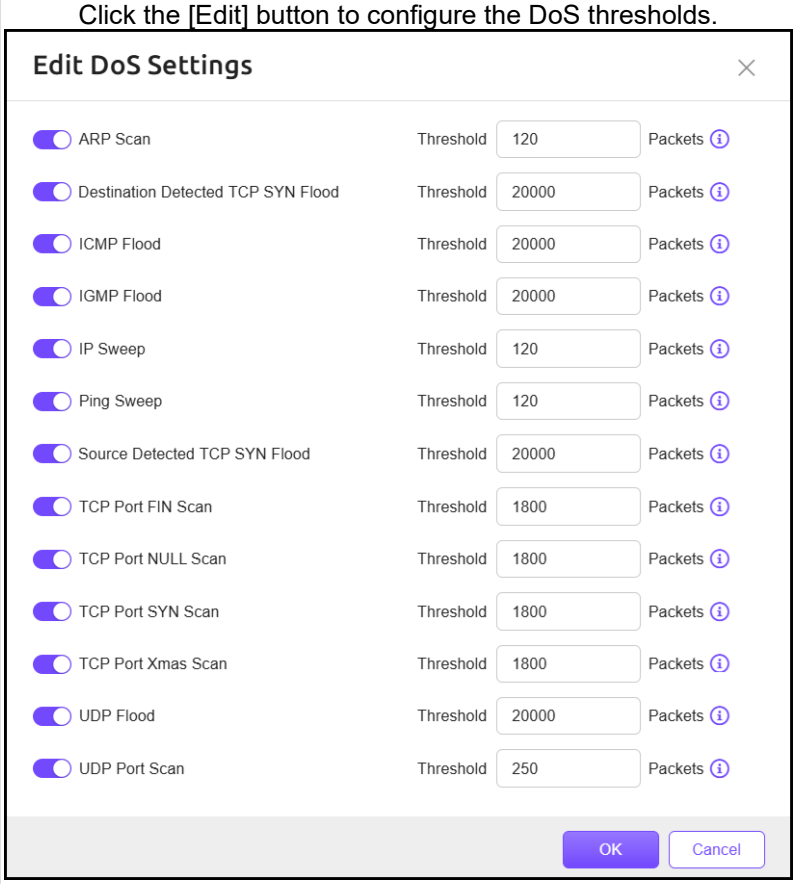


4. Configure the following settings.

Item	Description
Description	(Optional) Type a description for the port.
Pair Mode	Select a pair mode, **Default**, **Universal Bypass**, or **Logical Port Pair (LAG)**. • **Default**: In default mode, each port pair operates independently and has its own security operation mode, hardware bypass mode, Layer 2 (L2)/Layer 3 Policy Enforcement settings, DoS settings, and LFPT settings. • **Universal Bypass**: In Universal Bypass mode, an odd-numbered port pair is combined with its adjacent port pair to become a port pair with a spare uplink port that has redundant capacity to ensure uplink transmission. When the pair mode is Universal Bypass and an uplink disconnection happens in the main port pair, the spare

Item	Description
	port pair will take over the uplink transmission. When the pair mode is Universal Bypass, all the port pairs in a universal bypass port pair share the same security operation mode, hardware bypass mode, Layer 2 (L2)/Layer 3 Policy Enforcement settings, DoS settings, and LFPT settings. If the pair mode is Universal Bypass, further select **Non-Revertive** or **Revertive** for when the uplink disconnection is resolved. ○ **Non-Revertive**: When the uplink disconnection is resolved in the main port pair, the uplink transmission will not be switched back from the spare uplink port to the main port pair unless both uplink ports are disconnected from the upper switch. ○ **Revertive**: When the uplink disconnection is resolved in the main port pair, the uplink transmission will be switched back from the spare uplink port to the main port pair. • **Logical Port Pair (LAG)**: In Logical Port Pair (LAG) mode, an odd-numbered port pair is combined with its adjacent port pair to become a logical port pair for a better uplink/downlink throughput while collaborating with the upper/lower management switches with LAGs (Link Aggregation Groups). LAGs can be used to directly connect two switches and Edge devices when the traffic between them requires high bandwidth and reliability or to provide a higher-bandwidth connection in a network. When the pair mode is Logical Port Pair (LAG), all the port pairs in a logical port pair share the same security operation mode, hardware bypass mode, Layer 2 (L2)/Layer 3 Policy Enforcement settings, DoS settings, and LFPT settings. 📝 Universal Bypass and Logical Port Pair modes are only applicable when the device's security operation mode is set to inline mode.
Security Operation Mode	Select a security operation mode, **Inline Mode** or **Offline Mode**. • **Inline Mode**: The device works as an IPS (Intrusion Prevention System) and checks the traffic passing through the port pair based on Policy Enforcement Rules and IPS profiles for cyber threats. • **Offline Mode**: The device works as an IDS (Intrusion Detection System). The odd-numbered port of the pair will be disabled and the even-numbered port will be enabled to receive the traffic from the mirror port, which is used to manage switch/firewall and detect/log cyber threats. 📝 When the device is under offline mode, the Hardware Bypass Mode and LFPT are not configurable.

Item	Description
Hardware Bypass Mode	Select a hardare bypass mode, **Fail Open**, **Fail Close**, or **Force Open**. • **Fail Open**: The device allows all network traffic to pass through the port pair even when the system failed. With the higher priority on access than security, the system will remain open to operate under failure conditions. • **Fail Close**: The device shuts down links for the port pair and prevents any network traffic from passing through the port pair when failure is detected. Since the security concern overrides the need for access, the further system operation will be prevented. ⚠️ If the hardware bypass mode is Fail Close, you might not be able to access the OT asset when failure is detected. • **Force Open**: The device bypasses all network traffic to pass through the port pair to troubleshoot problems.
L2 Policy Enforcement	Enable or disable the L2 Policy Enforcement rule checking by clicking the toggle.
Operation Mode	If L2 Policy Enforcement is enabled, further select its operation mode, **Monitor Mode** or **Prevention Mode**. • **Monitor Mode**: The device detects and monitors abnormal protocol access attempts via the port pair to OT assets and generate logs, without blocking network attacks. • **Prevention Mode**: The device blocks abnormal protocol access attempts via the port pair to OT assets and generate log.
Device Rule Set	If L2 Policy Enforcement is enabled, further select a predefined L2 Policy Enforcement rule set to apply to the port pair.
Policy Enforcement	Enable or disable the Policy Enforcement rule checking by clicking the toggle. 📝 The device takes control of the Policy Enforcement settings here only when: • The device is not connected to EdgeOne; • The device is connected to EdgeOne, but the option of Policy Enforcement settings in the EdgeOne node management interface is disabled. Except for these conditions, the settings here are always controlled by EdgeOne.
Operation Mode	If Policy Enforcement is enabled, further select its operation mode, **Monitor Mode** or **Prevention Mode**.
Device Rule Set	If Policy Enforcement is enabled, further select a predefined Policy Enforcement rule set to apply to the port pair.
EdgeOne Rule Set	This item displays the applied Policy Enforcement rule set from EdgeOne, if any.

Item	Description
DoS Prevention	Enable or disable the DoS threshold detection by clicking the toggle.
Operation Mode	If DoS Prevention is enabled, further select its operation mode, **Monitor Mode** or **Prevention Mode**.
DoS Settings	Click the [Edit] button to configure the DoS thresholds.  📝 Flood/Scan Attack Protection rules utilize a detection period and threshold mechanisms to detect an attack. During a detection period (typically every five seconds), if the number of anomalous packets reaches the specified threshold, an attack detection occurs. If the rule action is [Block], the security node blocks subsequent anomalous packets until the end of the detection period. After the detection period ends, the security node will again allow anomalous packets until the threshold is once again reached.
LFPT	Enable or disable the LFPT function by clicking the toggle.

5. Click [Save].

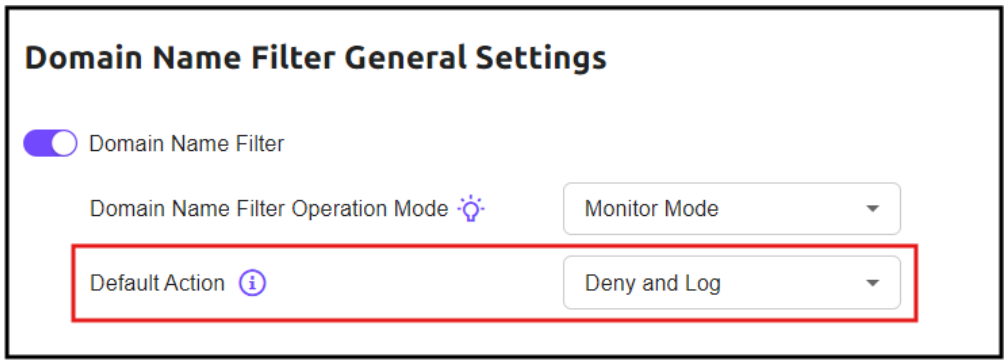
6.2.5 Domain Name Filter Rules

Domain Name Filter rules allow users to define rules to block malicious or allow reliable traffic by identifying the DNS queries sent from the OT assets. This provides users with access controls, ensuring that all traffic passing through their network is secure.

When an OT asset sends a DNS query to a DNS server, the DNS query will be examined by the asset's uplink Edge device, before it arrives at the DNS server. If the Edge device allows the DNS query, it will then be sent to the DNS server. Otherwise, it will be blocked, terminating the DNS query process.

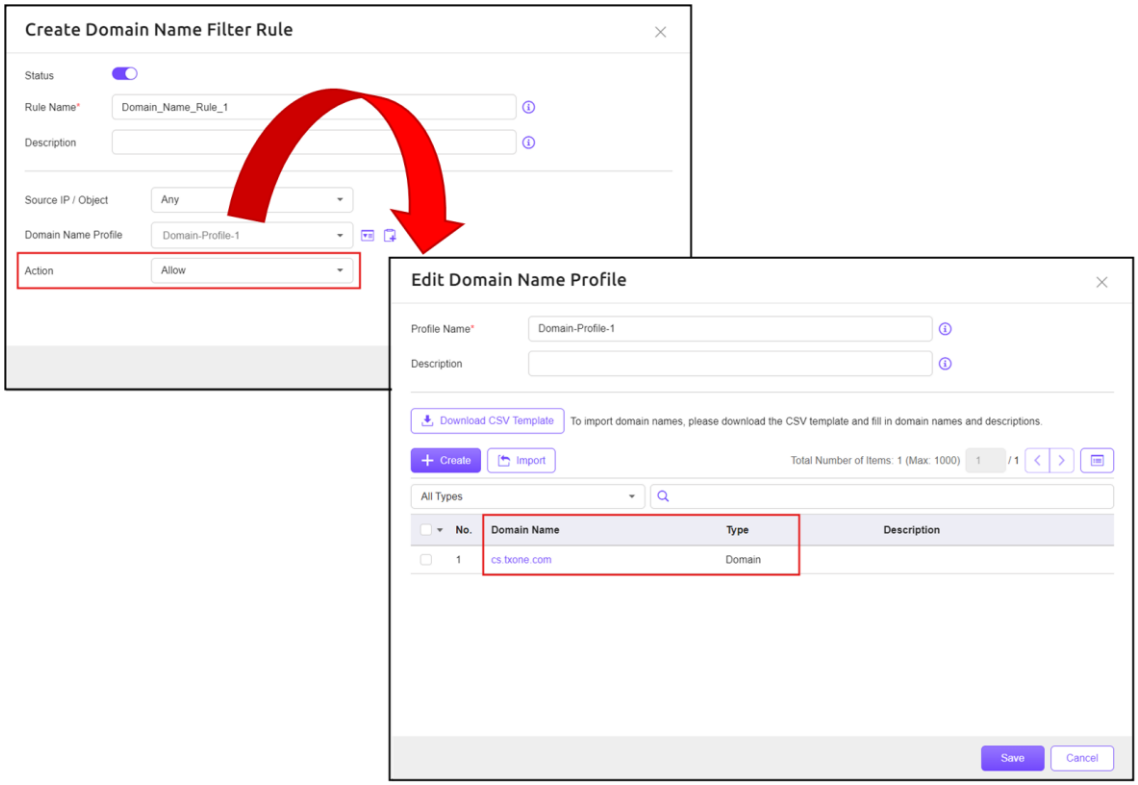
To examine these DNS queries coming from assets, we must define Domain Name Filter rules for the Edge device to determine whether or not a DNS query should be sent out. The Domain Name Filter rule's functioning depends on how it's configured.

Let's assume the default action for the Domain Name Filter rule is "Deny and Log."



We have two Domain Name Filter rules, each containing a Domain Name Object with its action set to "Allow."

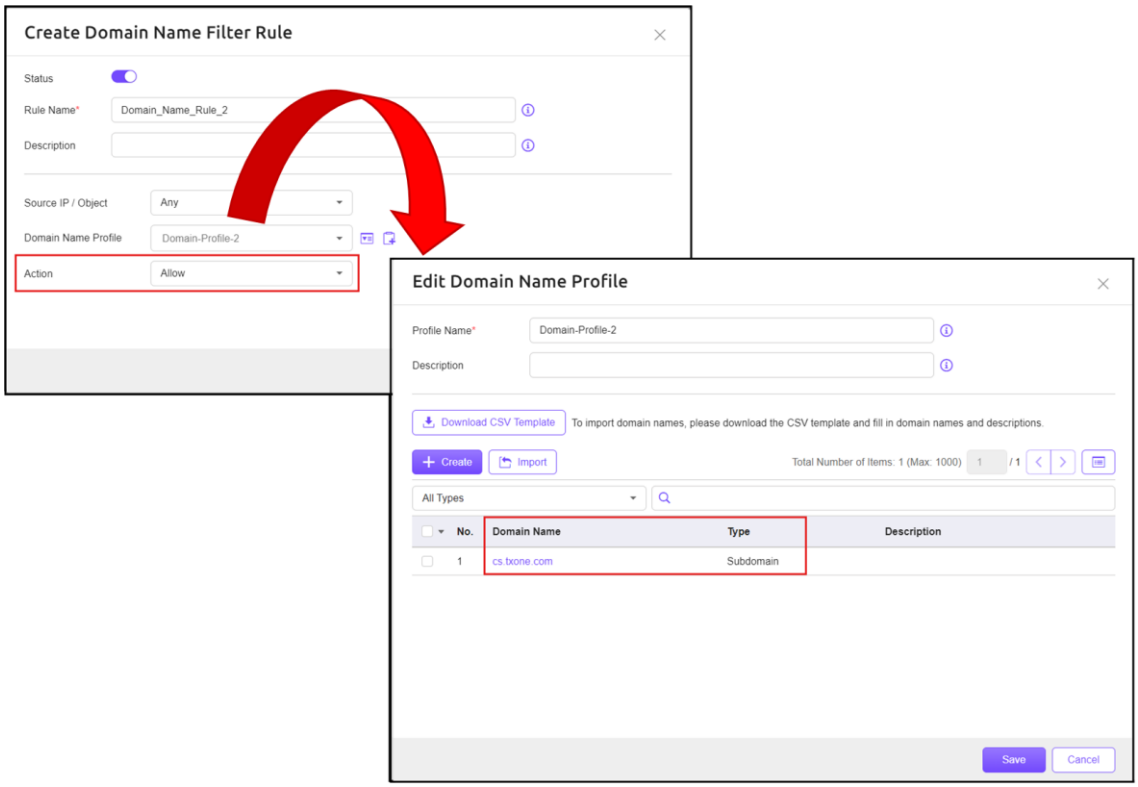
- Domain_Name_Filter_Rule_1:
  - Domain Name Object:
    - Domain Name: cs.txone.com
    - Type: **Domain**
  - Rule Action if Matched: Allow



- Domain_Name_Filter_Rule_2:
  - Domain Name Object:

- Domain Name: cs.txone.com
- Type: **Subdomain**

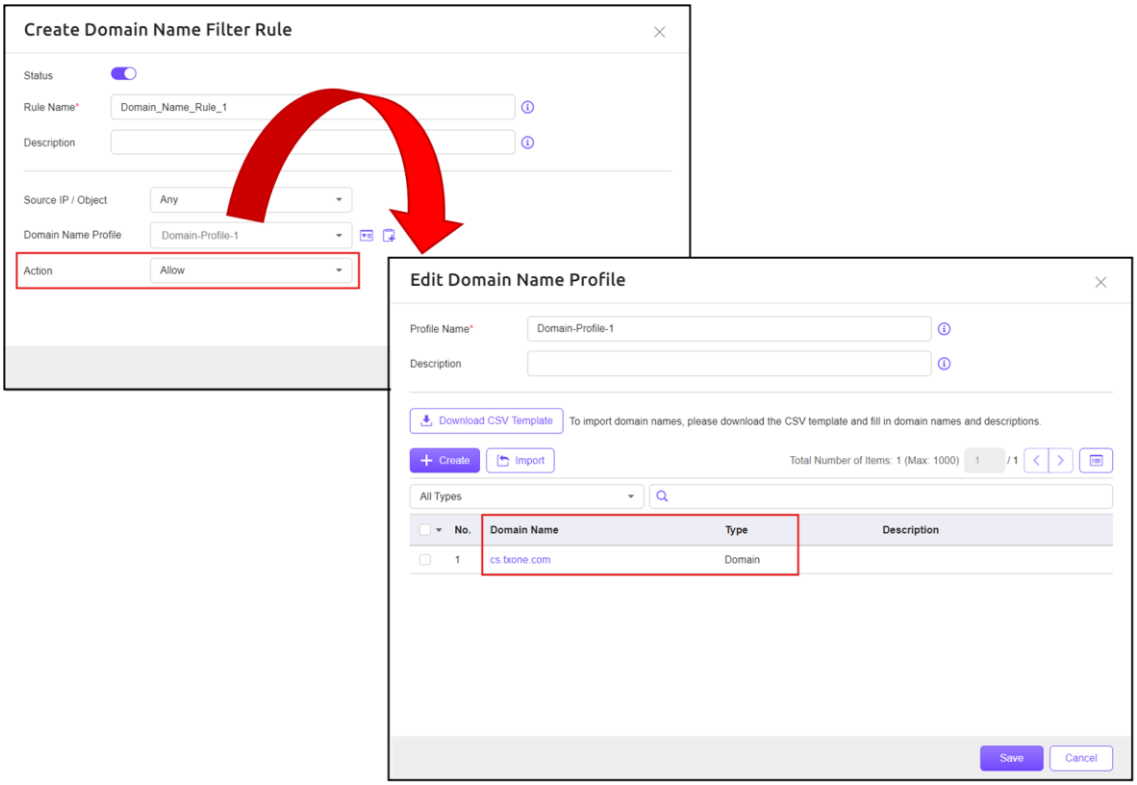
- Rule Action if Matched: Allow



Now, consider DNS queries of these three domains:

- cs.txone.com
- download-center.cs.txone.com
- txone.com

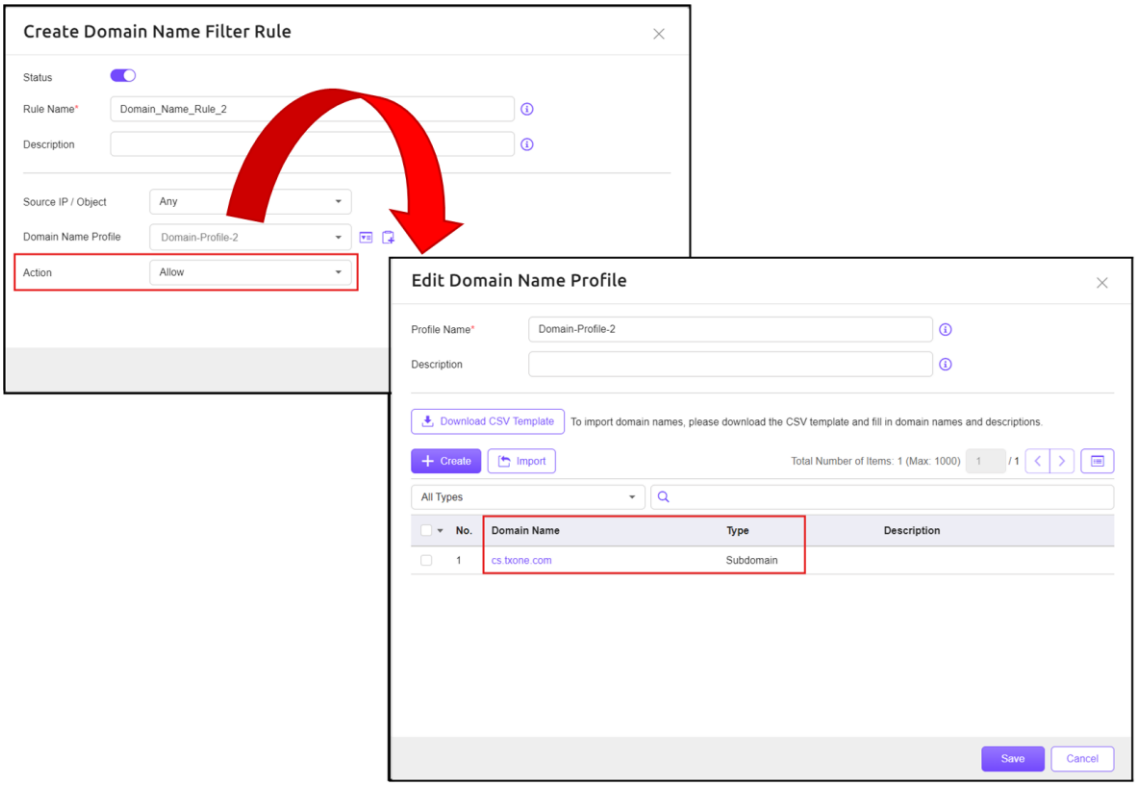
With "Domain_Name_Filter_Rule_1", DNS queries are filtered as follows:



This rule allows the DNS query of "cs.txone.com" and denies queries of all other domains.

- cs.txone.com: This DNS query is **allowed**, as it matches the domain specified.
- download-center.cs.txone.com: This DNS query is **denied**, as it doesn't match the domain specified.
- txone.com: This DNS query is **denied**, as it doesn't match the domain specified.

With "Domain_Name_Filter_Rule_2", DNS queries are filtered differently:



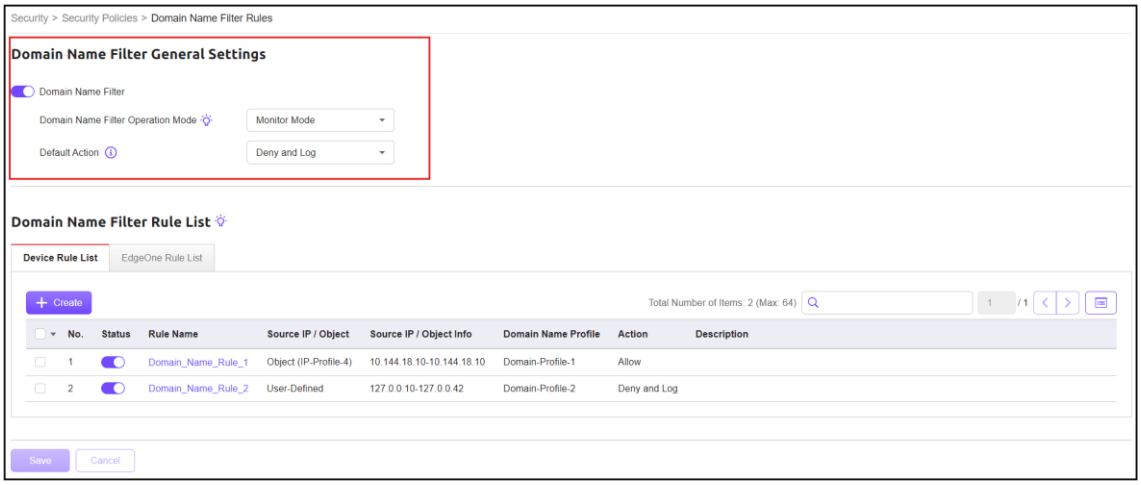
This rule allows DNS queries of any subdomain under "cs.txone.com" and denies all other queries.

- cs.txone.com: This DNS query is **denied**, as it is not a query of a subdomain under "cs.txone.com".
- download-center.cs.txone.com: This DNS query is **allowed**, as it is a query of a subdomain under "cs.txone.com".
- txone.com: This DNS query is **denied**, as it is not a query of a subdomain under "cs.txone.com".

6.2.5.1 Configuring Domain Name Filter General Settings

Procedure

1. Go to [Security] > [Security Policies] > [Domain Name Filter Rules].



2. Enable or disable the [Domain Name Filter] function by clicking the toggle.

3. From the [Domain Name Filter Operation Mode] drop-down list, select a mode, **Monitor Mode** or **Prevention Mode**, for the function.

4. From the [Default Action] drop-down list, select a default action, **Allow**, **Allow and Log** or **Deny and Log**, for when no Domain Name Filter rule is matched.

5. Click [Save].

The following table summarizes the settings:

Security Operation Mode (Security General Settings)	Domain Name Filter Operation Mode	Action Performed
Inline Mode	Monitor Mode	• Detect and monitor abnormal protocol access attempts to the OT assets, without blocking network attacks. • Generate logs. (If the default rule action is [Allow and Log] or [Deny and Log].)
	Prevention Mode	• Block abnormal protocol access attempts to OT assets. • Generate logs. (If the default rule action is [Allow and Log] or [Deny and Log].)
Offline Mode	Monitor Mode	• Passively detect and monitor abnormal protocol access attempts to the OT assets, without blocking network attacks. • Generate logs. (If the default rule action is [Allow and Log] or [Deny and Log].)

6.2.5.2 Configuring Domain Name Filter Rules

Procedure

1. Configure the required objects and profiles.

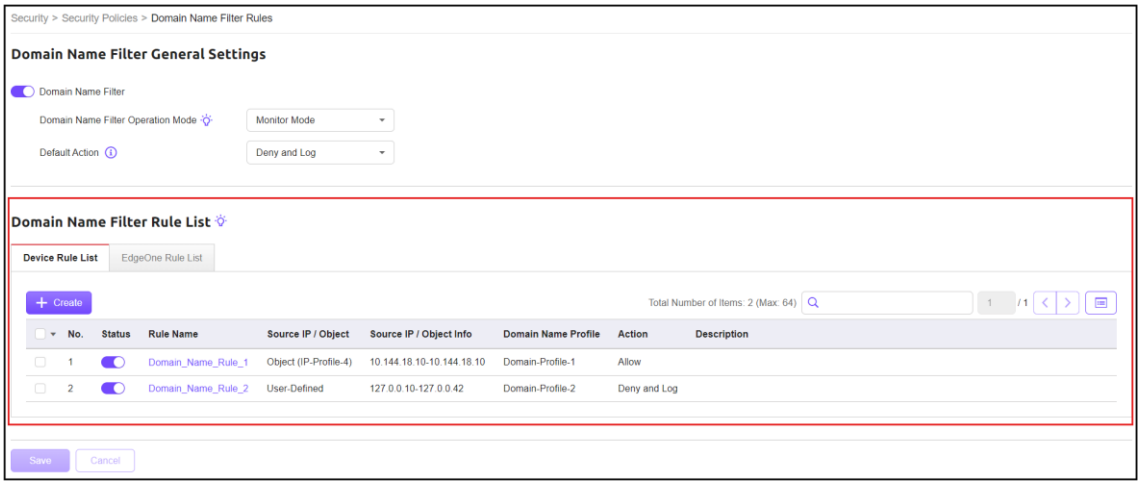
- IP Objects

For more information, see Configuring IP Objects.

- Domain Name Profiles

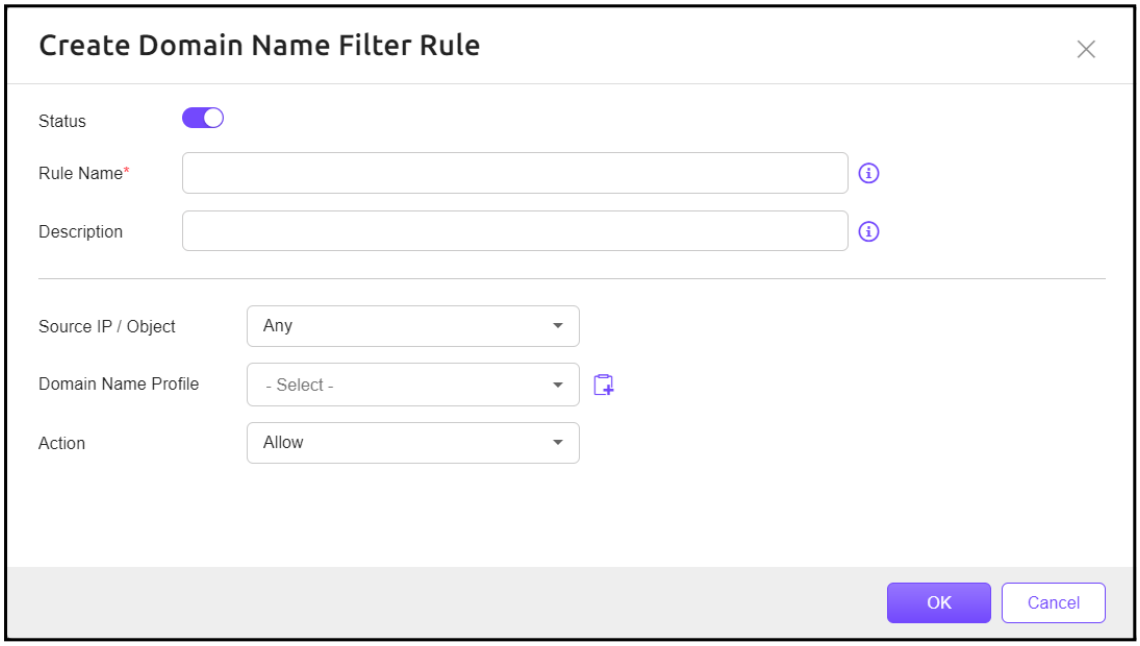
For more information, see Configuring Domain Name Profiles.

2. Go to [Security] > [Security Policies] > [Domain Name Filter Rules].



3. Do one of the following.

- Click [Create] to create a new Domain Name Filter rule. The [Create Domain Name Filter Rule] window will appear.
- Click a rule name to edit settings. The [Edit Domain Name Filter Rule] window will appear.



4. Configure the following settings.

Item	Description
Status	Enable the operational status of this Domain Name Filter rule by clicking the toggle.
Rule Name	Type a rule name for this Domain Name Filter rule.
Description	(Optional) Type a description.
Source IP / Object	Select one of the following for the source IP addresses: • Any • Single IP • IP Range

Item	Description
	• IP Subnet • IP Object If you select [IP Object], you can select an IP object that has been created beforehand on the [IP Objects] page or click the button to create a new IP object.
Domain Name Profile	Select a Domain Name profile you have defined beforehand or click the button to create a new profile.
Action	Select one of the following actions: • **Allow**: Select this option to allow network traffic that matches this rule. • **Allow and Log**: Select this option to allow network traffic that matches this rule and output a log. • **Deny and Log**: Select this option to block network traffic that matches this rule and output a log.

5. Click [OK].
6. Click [Save] on the [Domain Name Filter Rules] page.

6.2.5.3 Managing Domain Name Filter Rules

The following tables list the common tasks for managing Domain Name Filter rules.

- **Device Rule List:**

Task	Action
To create a Domain Name Filter rule	Click the [Create] button to create a new Domain Name Filter rule.
To delete a Domain Name Filter rule	Click the checkbox of a rule and click the [Delete] button.
To duplicate a Domain Name Filter rule	Click the checkbox of a rule and click the [Duplicate] button.
To edit a Domain Name Filter rule	Click the name of a rule, and an [Edit Domain Name Filter Rule] window will appear.
To change the priority of a Domain Name Filter rule	Click the checkbox of a rule, click the [Change Priority] button, and specify a new priority for this rule.

When more than one Domain Name Filter rule is matched, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules listed in the table on the [Domain Name Filter Rules] page are ordered by priority, with the highest priority rule listed on the first row of the table.

- **EdgeOne Rule List:**

Task	Description
N/A	The Domain Name Filter rules on the EdgeOne rule list are view-only.

6.2.6 Suspicious Objects

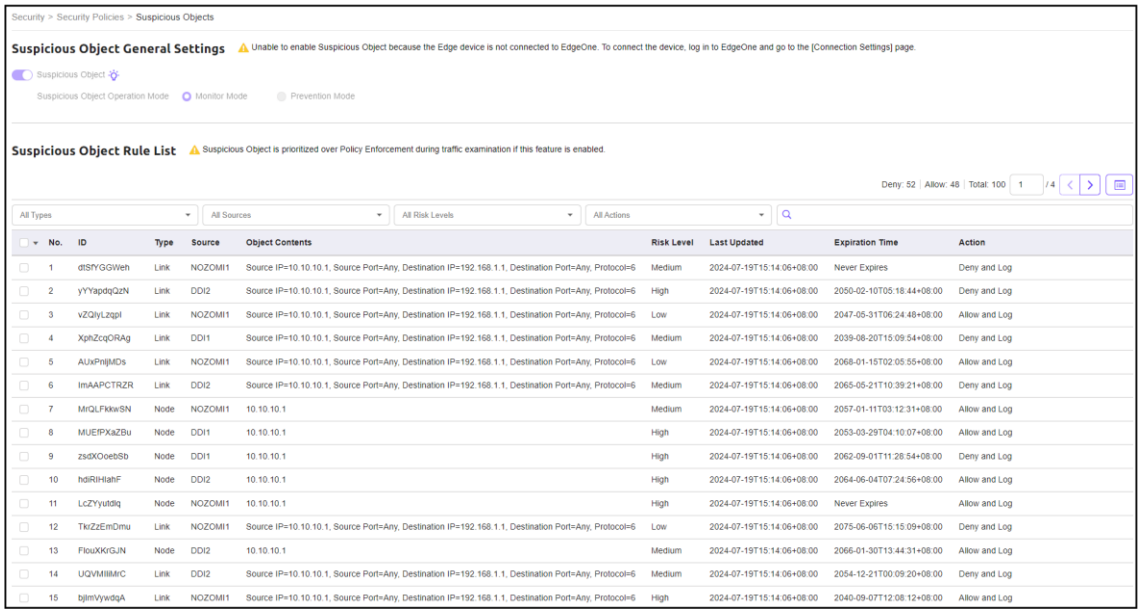
The [Suspicious Objects] feature allows you to define a custom node-based/link-based Suspicious Object list from EdgeOne. If any identical IP address or MAC address on the node level, or identical IP address, protocol and port numbers on the link level are detected, the activity will be allowed or blocked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

> Before you enable the [Suspicious Objects] function, ensure that the Edge device authentication settings ([Admin] > [System] > [EdgeOne Connection Settings]) are properly configured and that EdgeOne is connected with the third-party API from the source of the suspicious objects.

6.2.6.1 Configuring Suspicious Object Settings

Procedure

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



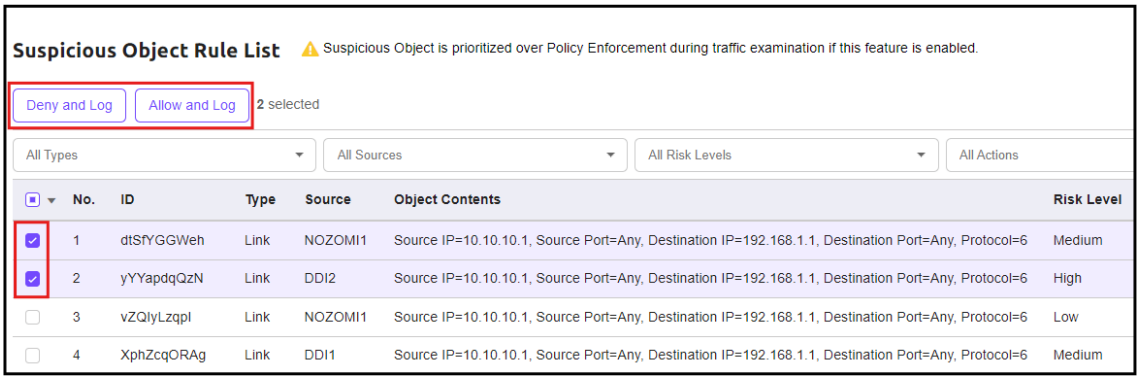
No.	ID	Type	Source	Object Contents	Risk Level	Last Updated	Expiration Time	Action
1	dtSfYGGWeh	Link	NOZOMI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Medium	2024-07-19T15:14:06+08:00	Never Expires	Deny and Log
2	yYYapdqQzN	Link	DDI2	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	High	2024-07-19T15:14:06+08:00	2050-02-10T05:18:44+08:00	Deny and Log
3	vZQlyLzqpl	Link	NOZOMI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Low	2024-07-19T15:14:06+08:00	2047-05-31T06:24:48+08:00	Allow and Log
4	XphZcqORAg	Link	DDI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Medium	2024-07-19T15:14:06+08:00	2039-08-20T15:09:54+08:00	Deny and Log
5	AUxPnljMDs	Link	NOZOMI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Low	2024-07-19T15:14:06+08:00	2068-01-15T02:05:55+08:00	Allow and Log
6	ImAAPCTRZR	Link	DDI2	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Medium	2024-07-19T15:14:06+08:00	2065-05-21T10:39:21+08:00	Deny and Log
7	MrQLFkkwSN	Node	NOZOMI1	10.10.10.1	Medium	2024-07-19T15:14:06+08:00	2057-01-11T03:12:31+08:00	Allow and Log
8	MUEfPXaZBu	Node	DDI1	10.10.10.1	High	2024-07-19T15:14:06+08:00	2053-03-29T04:10:07+08:00	Allow and Log
9	zsdXOoebSb	Node	DDI1	10.10.10.1	High	2024-07-19T15:14:06+08:00	2062-09-01T11:28:54+08:00	Deny and Log
10	hdiRIHlahF	Node	DDI2	10.10.10.1	High	2024-07-19T15:14:06+08:00	2064-06-04T07:24:56+08:00	Allow and Log
11	LcZYyutdlq	Node	NOZOMI1	10.10.10.1	High	2024-07-19T15:14:06+08:00	Never Expires	Allow and Log
12	TkrZzEmDmu	Link	NOZOMI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Low	2024-07-19T15:14:06+08:00	2075-06-06T15:15:09+08:00	Deny and Log
13	FlouXKrGJN	Node	DDI2	10.10.10.1	Medium	2024-07-19T15:14:06+08:00	2066-01-30T13:44:31+08:00	Allow and Log
14	UQVMIIlMrC	Link	DDI2	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	Medium	2024-07-19T15:14:06+08:00	2054-12-21T00:09:20+08:00	Deny and Log
15	bjlmVywdqA	Link	NOZOMI1	Source IP=10.10.10.1, Source Port=Any, Destination IP=192.168.1.1, Destination Port=Any, Protocol=6	High	2024-07-19T15:14:06+08:00	2040-09-07T12:08:12+08:00	Allow and Log

2. Enable the [Suspicious Objects] function by clicking the toggle.

> You cannot enable Suspicious Objects if:
>
> 1. The Edge device is not connected to EdgeOne.
> 2. The Edge device is not managed within an Edge group in EdgeOne.
> 3. The [Suspicious Objects] group setting is not enabled for the Edge group to which the Edge device belongs.
> 4. The [Dispatch Suspicious Objects to Edge Devices] option in EdgeOne ([Nodes] > [Suspicious Objects] > [Suspicious Object Settings]) is not enabled.

3. Select a mode, **Monitor Mode** or **Prevention Mode**, for the function.

4. To change the action (listed in the [Action] column) of a suspicious object, check the checkbox of an item and select an action, **Deny and Log** or **Allow and Log**, for when the pattern is matched.



5. Click [Save].

The following table summarizes the settings.

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

The Suspicious Object is of higher priority than the Policy Enforcement.

6.3 CPSDR Policies

Create and manage network detection policy rules for early identification and prediction of anomalous network behaviors.

- CPSDR Rules
- CPSDR Allow Lists & Alert Lists

6.3.1 CPSDR Rules

TXOne CPSDR (Cyber-Physical System Detection and Response) is designed to identify and predict anomalous network behaviors through a comprehensive analysis of traffic patterns, rather than just inspecting individual packets for abnormalities like traditional IPS features. Unlike IPS, which scrutinizes individual packets within a traffic flow for any anomalies, CPSDR assesses the relationships between sequential traffic flows.

For example, if the system observes Traffic Type A followed by Traffic Type B, and this sequence is determined to be suspicious based on established behavioral patterns, the system

will then predict the impact severity of this network behavior. This method allows CPSDR to provide a holistic view of network behavior and calculate impact severities more effectively.

You can manage the CPSDR network detection policy rules on the [CPSDR Rules] page or go to [CPSDR Allow Lists & Deny Lists] for advanced settings. If network traffic matches a specific rule, a log is generated on the [CPSDR Logs] page.

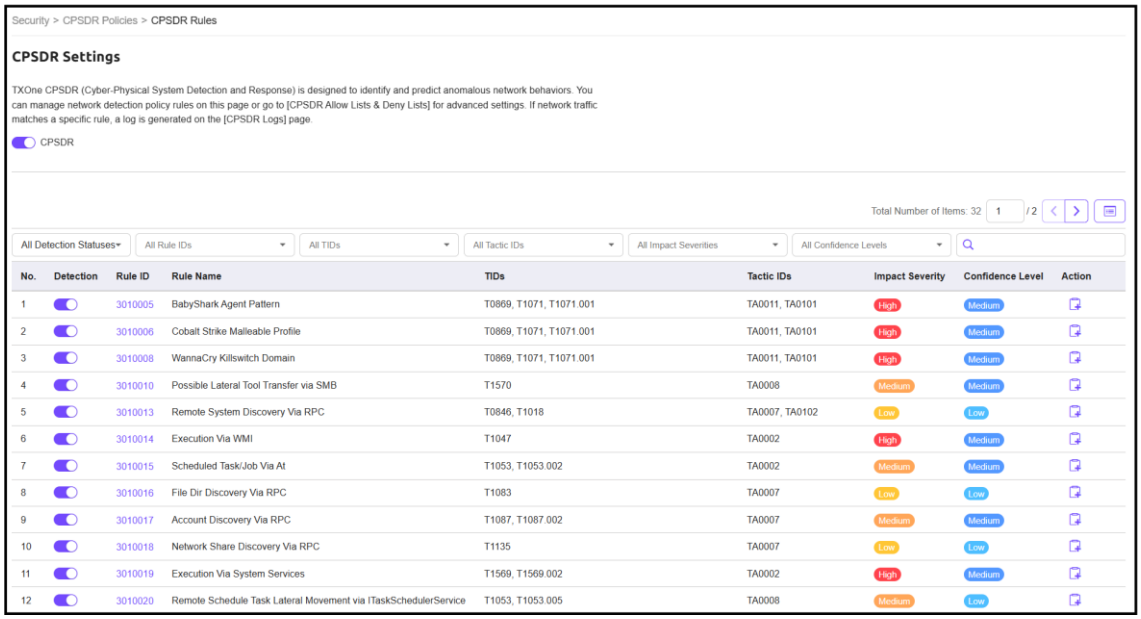
For more information about CPSDR allow lists and deny lists, see *CPSDR Allow Lists & Deny Lists*.

For more information about CPSDR logs, see CPSDR Logs.

6.3.1.1 Viewing and Configuring CPSDR Rules

Procedure

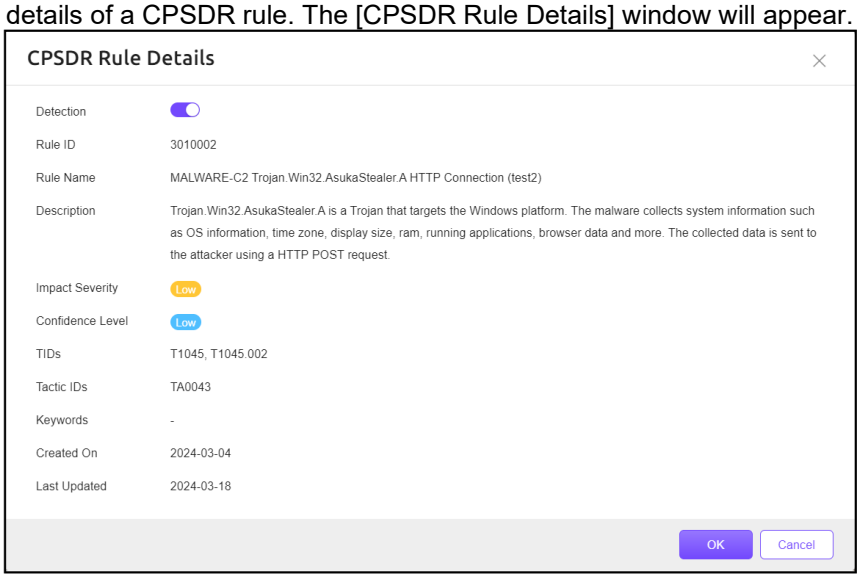
1. Go to [Security] > [CPSDR Policies] > [CPSDR Rules].



2. Enable the [CPSDR] function by clicking the toggle.

The following table describes the CPSDR rule information.

Item	Description
No.	The ordinal number of the CPSDR rule.
Detection	The detection status of the CPSDR rule. **Use the toggles to enable/disable rules and click [Save] on the [CPSDR Rules] page.**

Item	Description
Rule ID	The ID number of the CPSDR rule. Click a specific rule ID to view details of a CPSDR rule. The [CPSDR Rule Details] window will appear.  • **Detection**: The detection status of the CPSDR rule. **Use the toggle to enable/disable this rule, click [OK] on the window, then click [Save] on the [CPSDR Rules] page.** • **Rule ID**: The ID number of the CPSDR rule. • **Rule Name**: The name of the CPSDR rule regarding the cyber attack. • **Description**: A brief overview of this type of cyber attack. • **Impact Severity**: The severity level (Low, Medium, High) of the cyber attack assessed and predicted by the system. • **Confidence Level**: The likelihood (Low, Medium, High) of the cyber attack assessed and predicted by the system. • **TIDs**: MITRE TID information. • **Tactic IDs**: The ID numbers of the cyber tactics. • **Keywords**: The keywords for searching this CPSDR rule. • **Created On**: The date when this CPSDR rule was initially created. • **Last Updated**: The date of the most recent update to the rule's details.
Rule Name	The name of the CPSDR rule regarding the cyber attack.
TIDs	MITRE TID information.
Tactic IDs	The ID numbers of the cyber tactics.
Impact Severity	The severity level (Low, Medium, High) of the cyber attack assessed and predicted by the system.
Confidence Level	The likelihood (Low, Medium, High) of the cyber attack assessed and predicted by the system.

Item	Description
Action	Click the button to create a CPSDR allow list or deny list profile. For more information about creating CPSDR allow lists and deny lists, see *Configuring CPSDR Allow Lists and Deny Lists*.

3. Click [Save].

6.3.2 CPSDR Allow Lists & Alert Lists

You can configure allow lists, deny lists, and threshold settings to enhance CPSDR detection accuracy. The Edge device responds to suspicious network behaviors based on the alert list. The CPSDR detection threshold (disabled by default) is designed to block network behaviors matching both CPSDR rules and the specified risk level. When all three are configured, the Edge device examines traffic in this order: Allow Lists > Deny Lists > CPSDR Detection Threshold.

6.3.2.1 Configuring CPSDR Allow Lists and Deny Lists

Procedure

1. Configure the required objects and profiles.

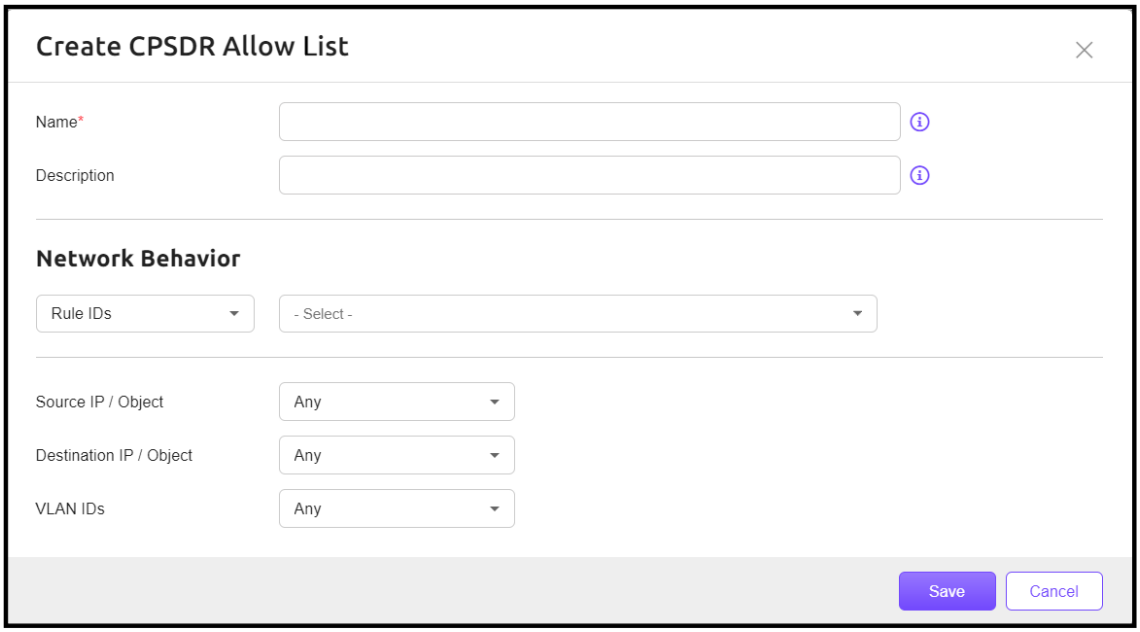
- IP Objects

For more information, see Configuring IP Objects.

2. Go to [Security] > [CPSDR Policies] > [CPSDR Allow Lists & Deny Lists]. Then switch to the [Allow Lists] or [Deny Lists] tab.

3. Do one of the following.

- Click [Create] to create an allow list or deny list. The [Create CPSDR Allow List] or [Create CPSDR Deny List] window will appear.
- Click an allow list or deny list name to edit settings. The [Edit CPSDR Allow List] or [Edit CPSDR Deny List] window will appear.



4. Configure the following settings.

Item	Description
Name	Type a name for this CPSDR allow list/deny list.
Description	(Optional) Type a description.

- **Network Behavior**: Select **Rule IDs**, **TIDs**, or **Tactic IDs**, then select one or multiple IDs from the drop-down list.

Item	Description
Source IP / Object	Select one of the following for the source IP addresses: • Any • Single IP • IP Range • IP Subnet • IP Object If you select [IP Object], you can select an IP object that has been created beforehand on the [IP Objects] page or click the button to create a new IP object.
Destination IP / Object	Select one of the following for the destination IP addresses: • Any • Single IP • IP Range • IP Subnet • IP Object
VLAN IDs	Select either one of the following for the VLAN IDs: • Any

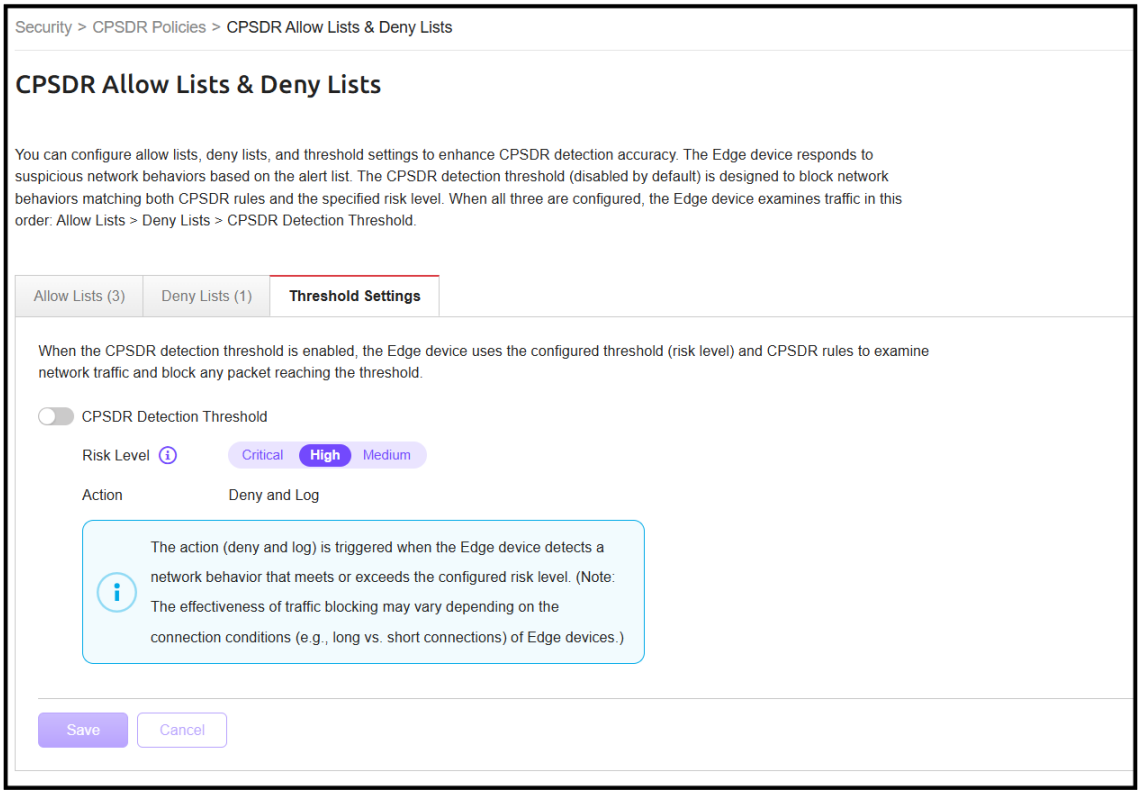
Item	Description
	• Custom: Specify at least one VLAN ID for this protocol. A maximum of five VLAN IDs can be applied to one policy rule.

5. Click [Save].

6.3.2.2 Configuring CPSDR Detection Threshold Settings

Procedure

1. Go to [Security] > [CPSDR Policies] > [CPSDR Allow Lists & Deny Lists]. Then switch to the [Threshold Settings] tab.



2. Click the [CPSDR Detection Threshold] toggle to enable the feature.
3. Select a threshold (risk level), **Critical**, **High**, or **Medium**.
4. Click [Save].

The CPSDR action (deny and log) is triggered when the Edge device detects a network behavior that meets or exceeds the configured risk level.

7 Patterns

This chapter describes how to view the pattern information and import security and CPSDR patterns to the Edge series device.

7.1 Pattern Updates

Manage and update patterns for up-to-date threat prevention.

- Security Patterns
- CPSDR Patterns

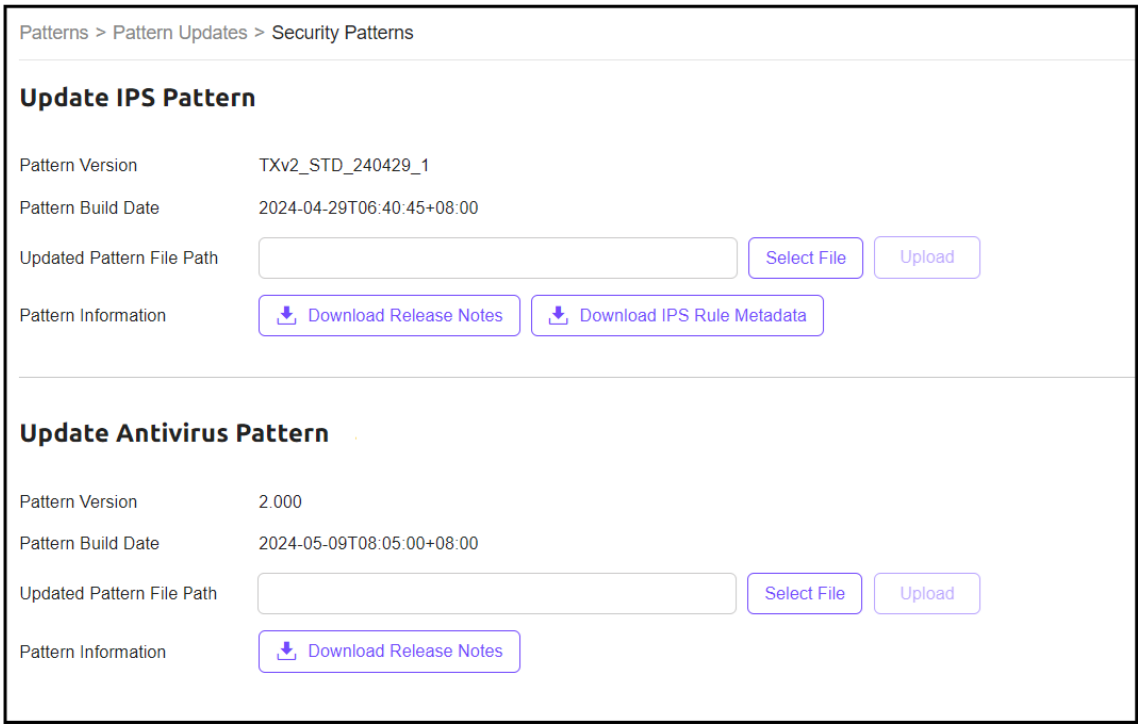
7.1.1 Security Patterns

Security Patterns contain antivirus patterns and DPI (Deep Packet Inspection) patterns (a.k.a. IPS patterns) with signatures to enable intrusion prevention features on the device. The intrusion prevention feature detects and prevents behaviors related to network intrusion attempts or targeted attacks at the network level.

7.1.1.1 Viewing IPS and Antivirus Pattern Information

Procedure

1. Go to [Patterns] > [Pattern Updates] > [Security Patterns].

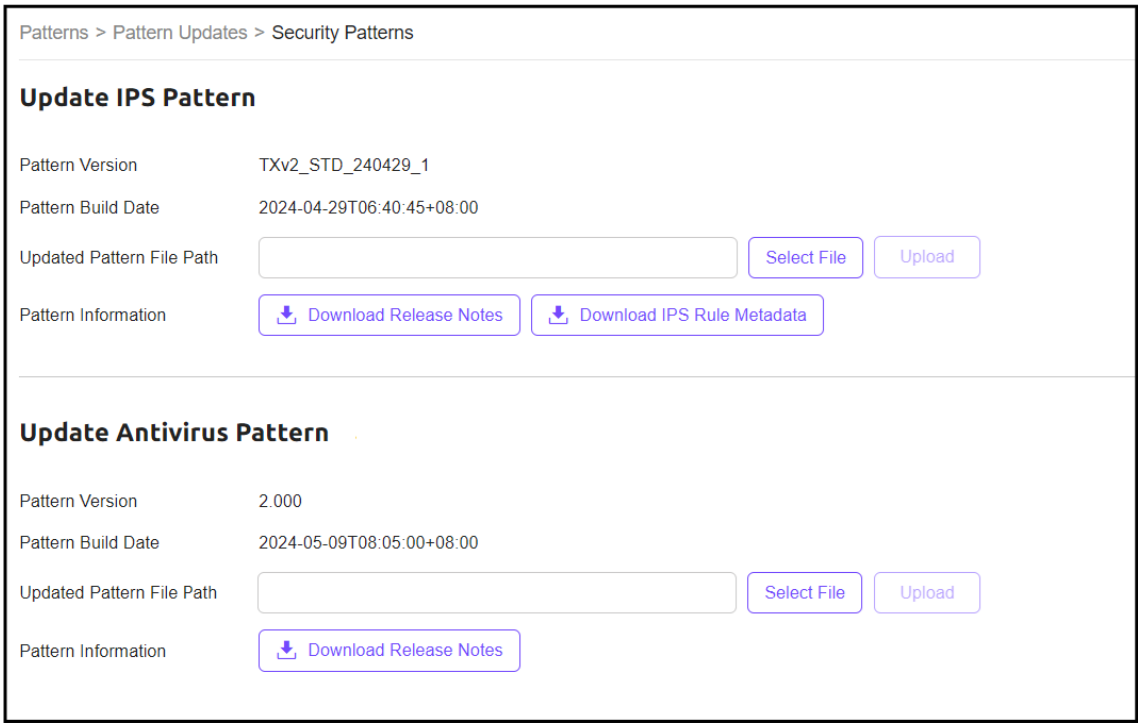


2. In the [Update IPS Pattern] and [Update Antivirus Pattern] panes, you will see the pattern version, pattern build date, release notes, and IPS rule metadata.

7.1.1.2 Updating IPS and Antivirus Patterns

Procedure

1. Go to [Patterns] > [Pattern Updates] > [Security Patterns].



2. In the [Update IPS Pattern] or [Update Antivirus Pattern] pane, click [Select File].
3. Select a pattern file from your local disk.
4. Click [Upload].

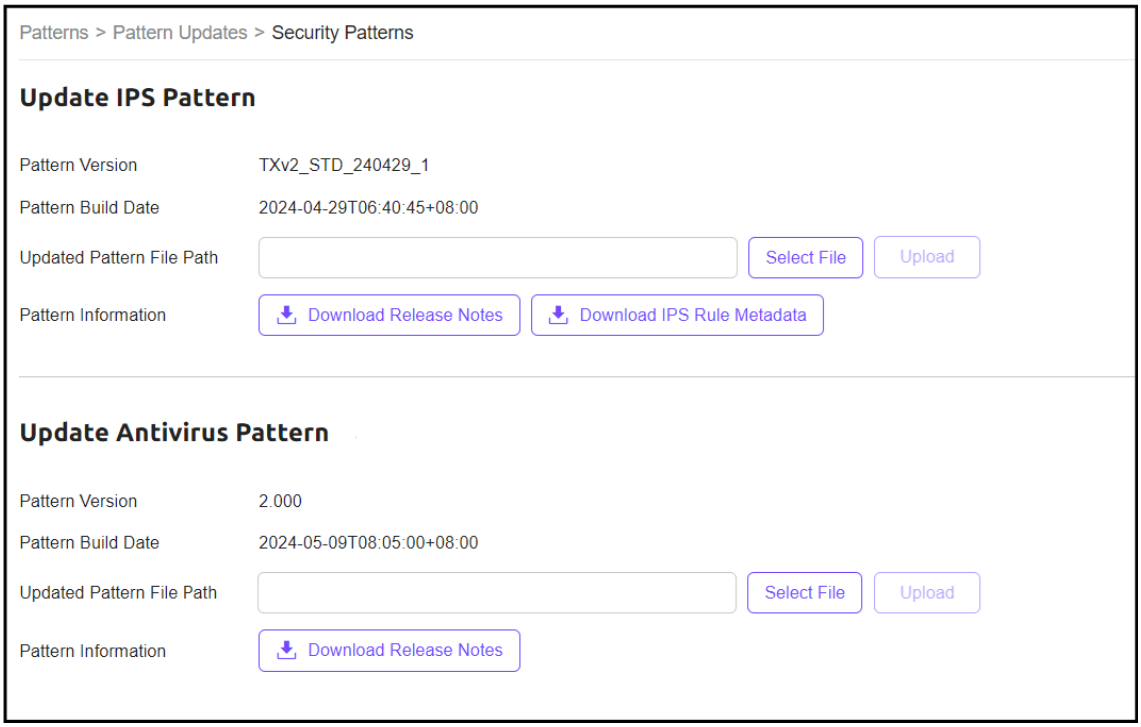
⚠	Before updating the IPS and antivirus patterns, ensure that you have activated the Edge device software license.

📝	Various versions of the pattern files can be downloaded at the MyTXOne Portal at https://my.txone.com/.

7.1.1.3 Downloading Pattern Release Notes and IPS Rule Metadata

Procedure

1. Go to [Patterns] > [Pattern Updates] > [Security Patterns].



2. Click the [Download Release Notes] button to download and view detailed pattern release information.

3. Click the [Download IPS Rule Metadata] button to download and view the IPS rule metadata.

7.1.2 CPSDR Patterns

CPSDR (Cyber-Physical System Detection and Response) patterns are specifically designed for the TXOne CPSDR feature, which the Edge device employs to identify and predict anomalous network behaviors.

For more information about the CPSDR feature, see CPSDR Policies.

7.1.2.1 Viewing CPSDR Pattern Information

Procedure

1. Go to [Patterns] > [Pattern Updates] > [CPSDR Patterns].

2. In the [Update CPSDR Pattern] pane, you will see the pattern version, pattern build date, release notes, and CPSDR rule metadata.

7.1.2.2 Updating CPSDR Patterns

Procedure

1. Go to [Patterns] > [Pattern Updates] > [CPSDR Patterns].

2. In the [Update CPSDR Pattern] pane, click [Select File].

3. Select a pattern file from your local disk.

4. Click [Upload].

⚠️	Before updating the CPSDR pattern, ensure that you have activated the Edge device software license.

📝	Various versions of the pattern files can be downloaded at the MyTXOne Portal at https://my.txone.com/.

7.1.2.3 Downloading Pattern Release Notes and CPSDR Rule Metadata

Procedure

1. Go to [Patterns] > [Pattern Updates] > [CPSDR Patterns].

2. Click the [Download Release Notes] button to download and view detailed pattern release information.

3. Click the [Download CPSDR Rule Metadata] button to download and view the CPSDR rule metadata.

8 Applications

This chapter describes how to configure and use additional applications and tools for advanced network management and control.

8.1 Backup Storage

Configure settings for storing device configuration backup files in a compatible USB disk.

- USB Disk Storage

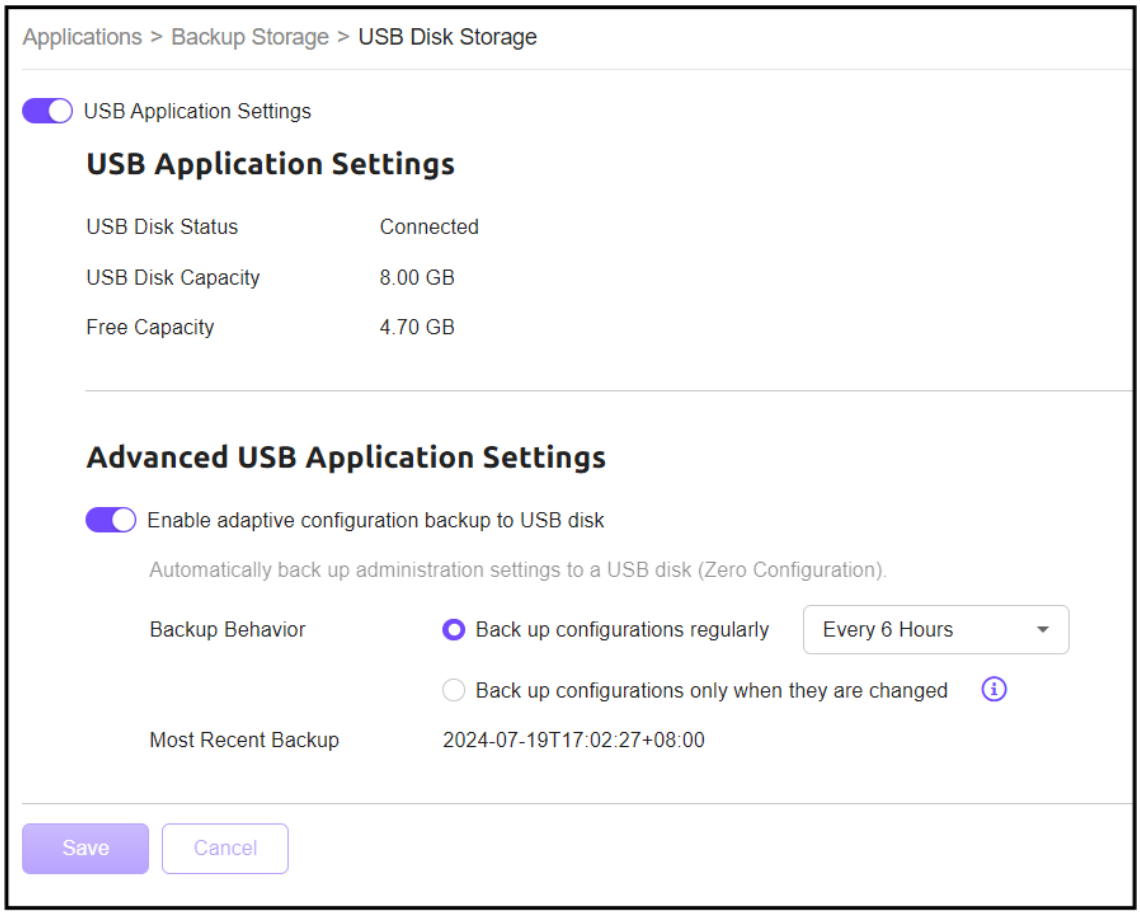
8.1.1 USB Disk Storage

The Edge device supports backing up configurations and loading patterns, configurations, and firmware from a compatible USB disk. On the [USB Disk Storage] page, you can configure the relevant USB backup settings to meet your specific needs.

8.1.1.1 Configuring USB Application Settings

Procedure

1. Go to [Applications] > [Backup Storage] > [USB Disk Storage].



2. Click the [USB Application Settings] toggle to enable the USB backup storage.

3. Once the USB Application function is enabled and a compatible USB disk is plugged in, you can view the status and information about the disk capacity and remaining free space.

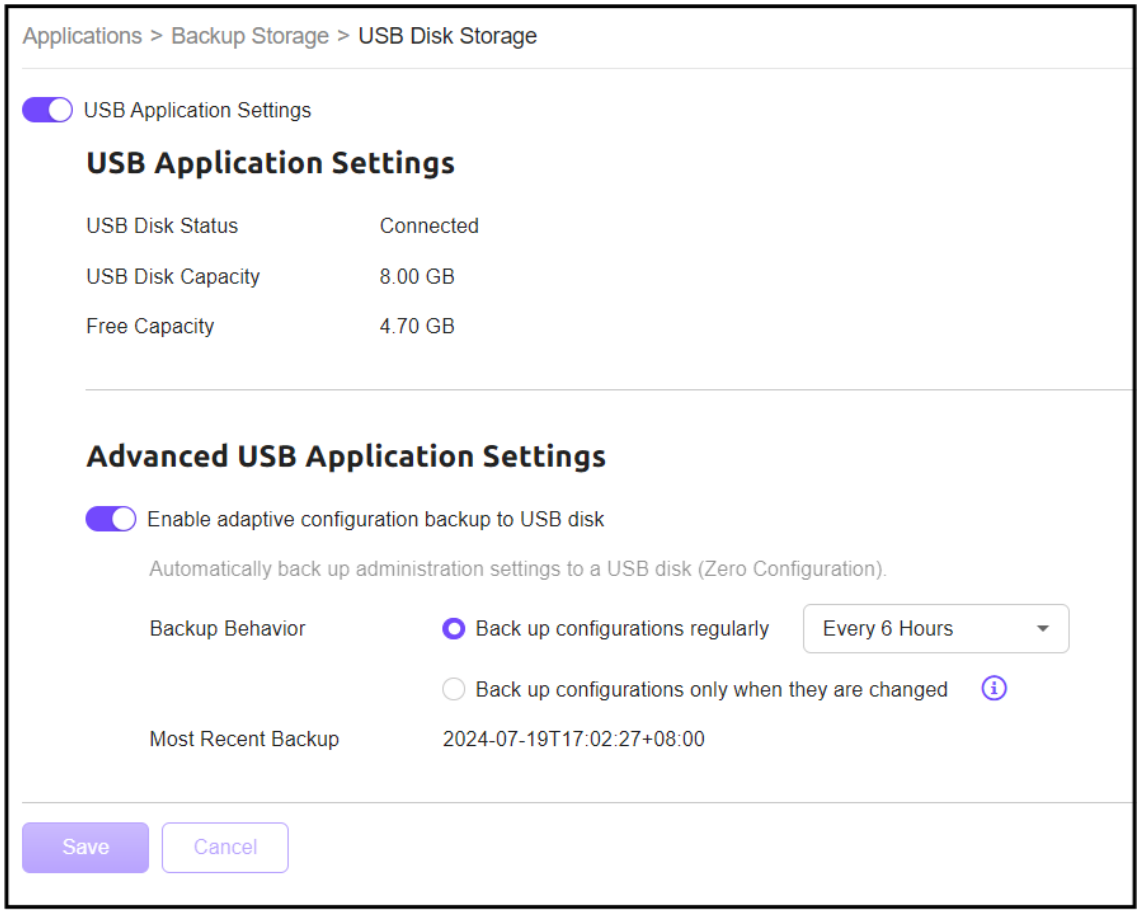
⚠	If the USB Application function is disabled, the USB port on the front panel will not be active and cannot be used.

For more information about the supported USB devices and functions, see Extended Functions via Supported USB Device.

8.1.1.2 Configuring Advanced USB Application Settings

Procedure

1. Go to [Applications] > [Backup Storage] > [USB Disk Storage].



2. Click the [Enable adaptive configuration backup to a USB disk] toggle to allow backups of configurations to a compatible USB disk.

3. Select one of the following backup behavior options:

- **Back up configurations regularly**: If this option is selected, further specify the backup interval:
  - Every 6 Hours
  - Every 12 Hours
  - Every 24 Hours
  - Every 48 Hours
  - Every 72 Hours
- **Back up configurations only when they are changed**: If this option is selected, the Edge device creates backed-up configuration files whenever settings are updated in the web console.

The advanced USB application settings are configurable only when the [USB Application Settings] option is enabled.

8.2 Cyber Forensic Tools

Utilize forensic tools for cybersecurity analysis.

- IPS Event Packet Capture
- Captured Packet Downloads
- Pcap File Server Settings

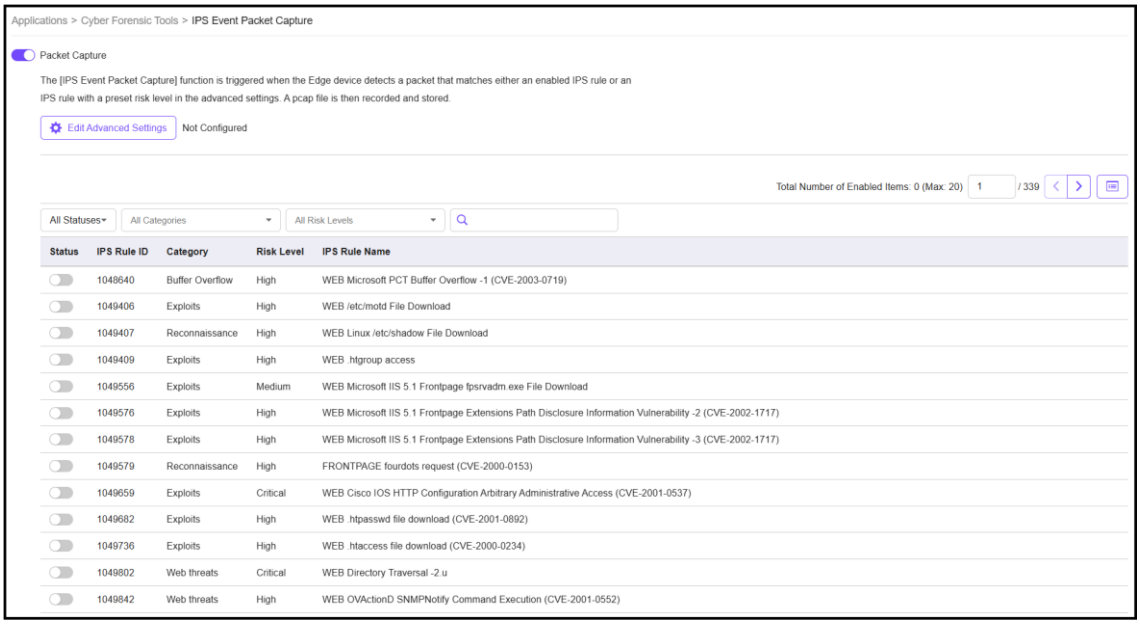
8.2.1 IPS Event Packet Capture

The IPS Event Packet Capture feature enables you to capture packets that trigger IPS events for detailed analysis. This capability allows precise control over packet capture settings for each IPS event rule, aiding support teams in quickly addressing false positive/false negative matching of IPS rules in the security module.

8.2.1.1 Enabling IPS Event Packet Capture

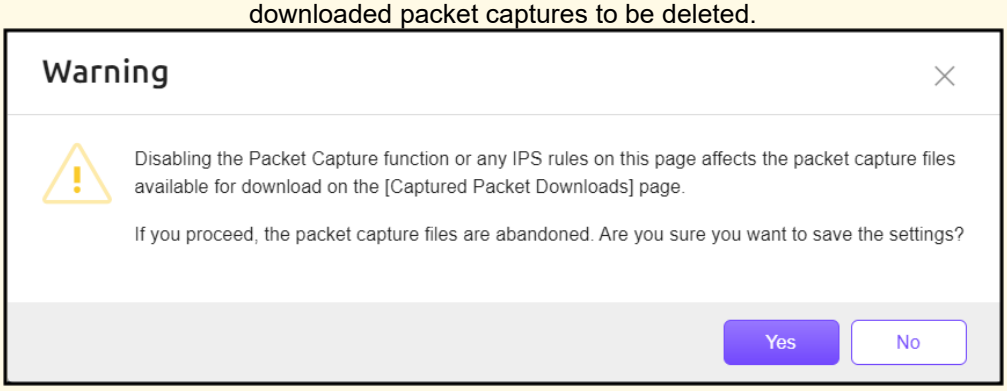
Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [IPS Event Packet Capture].



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

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



3. After the function is enabled, you can see the entire IPS rule list. Select and enable one or multiple rules for IPS event packet capture.

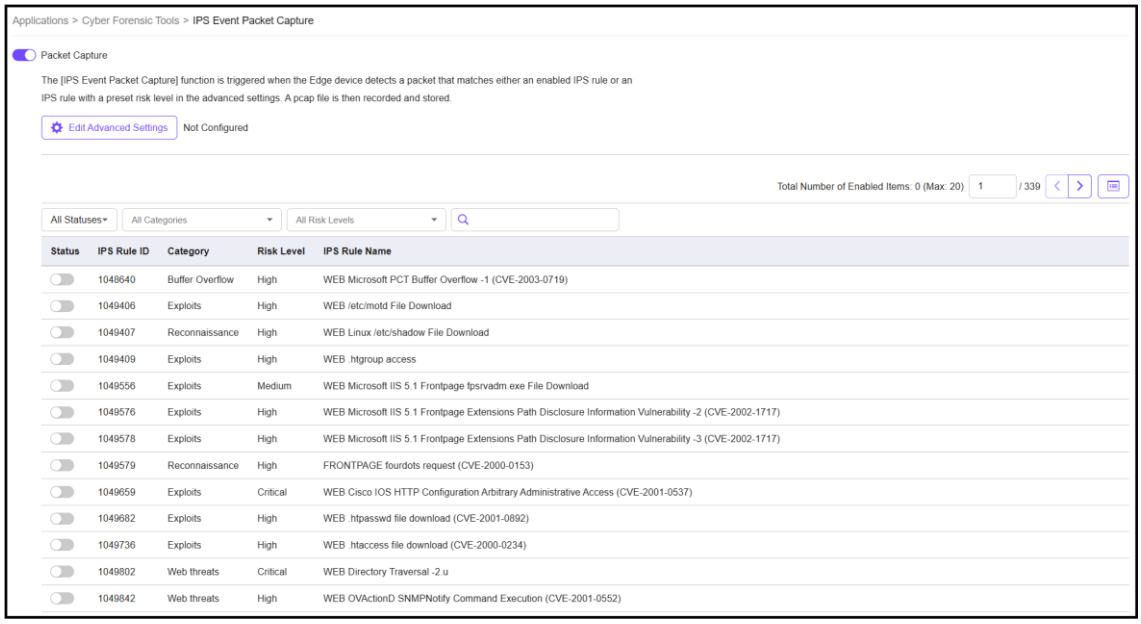
1. You can select up to 20 rules for the IPS Event Packet Capture feature.
2. The Edge device will save IPS event packets when the selected IPS rules are triggered. Only the last 10 packets of each IPS rule are saved. Older event packets will be overwritten.

4. Click [Save].

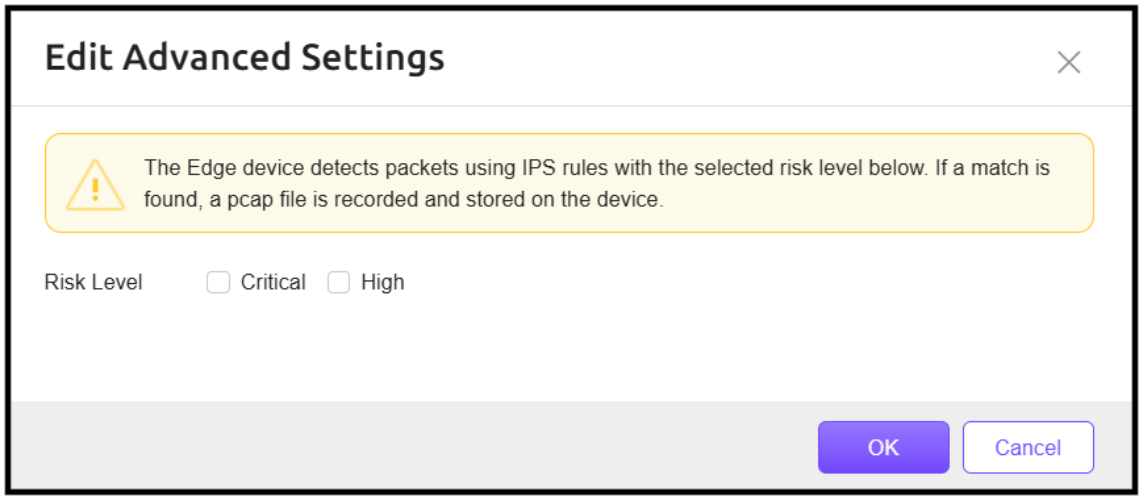
8.2.1.2 Configuring IPS Event Packet Capture Advanced Settings

Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [IPS Event Packet Capture].



2. Enable the Packet Capture function by clicking the [Packet Capture] toggle.
3. Click [Edit Advanced Settings]. The [Edit Advanced Settings] window will appear.



4. Select one or multiple risk levels. When the Edge device detects packets matching IPS rules with the specified risk levels, it will record and store the relevant pcap files.
5. Click [OK] on [Edit Advanced Settings] window, then click [Save] on the packet capture page.

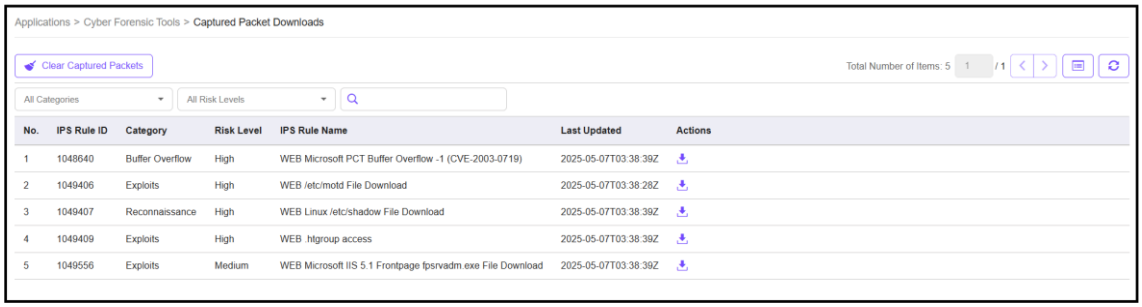
8.2.2 Captured Packet Downloads

When the Edge device captures IPS event packets, you can download the captured packets on the [Captured Packet Downloads] page.

8.2.2.1 Downloading Captured IPS Event Packets

Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [Captured Packet Downloads].



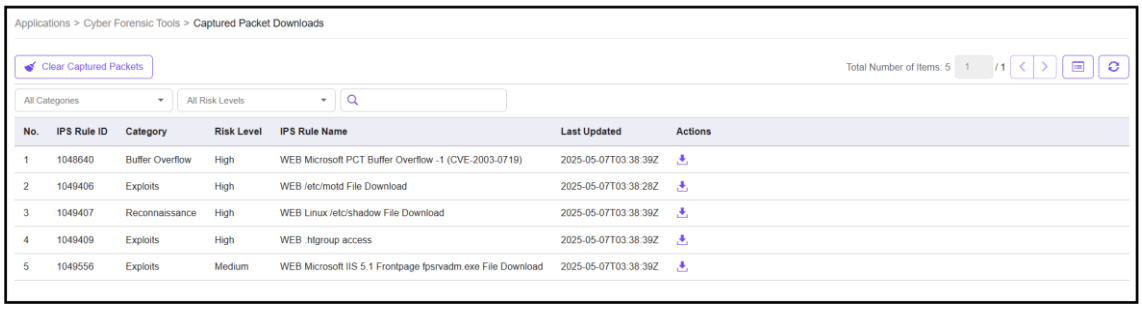
2. Click the download buttons to download the zipped packet files to your local disk.

> The download list is refreshed every 10 seconds. To get the latest update, click the refresh button .

8.2.2.2 Clearing Captured IPS Event Packets

Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [Captured Packet Downloads].



2. Click [Clear Captured Packets].

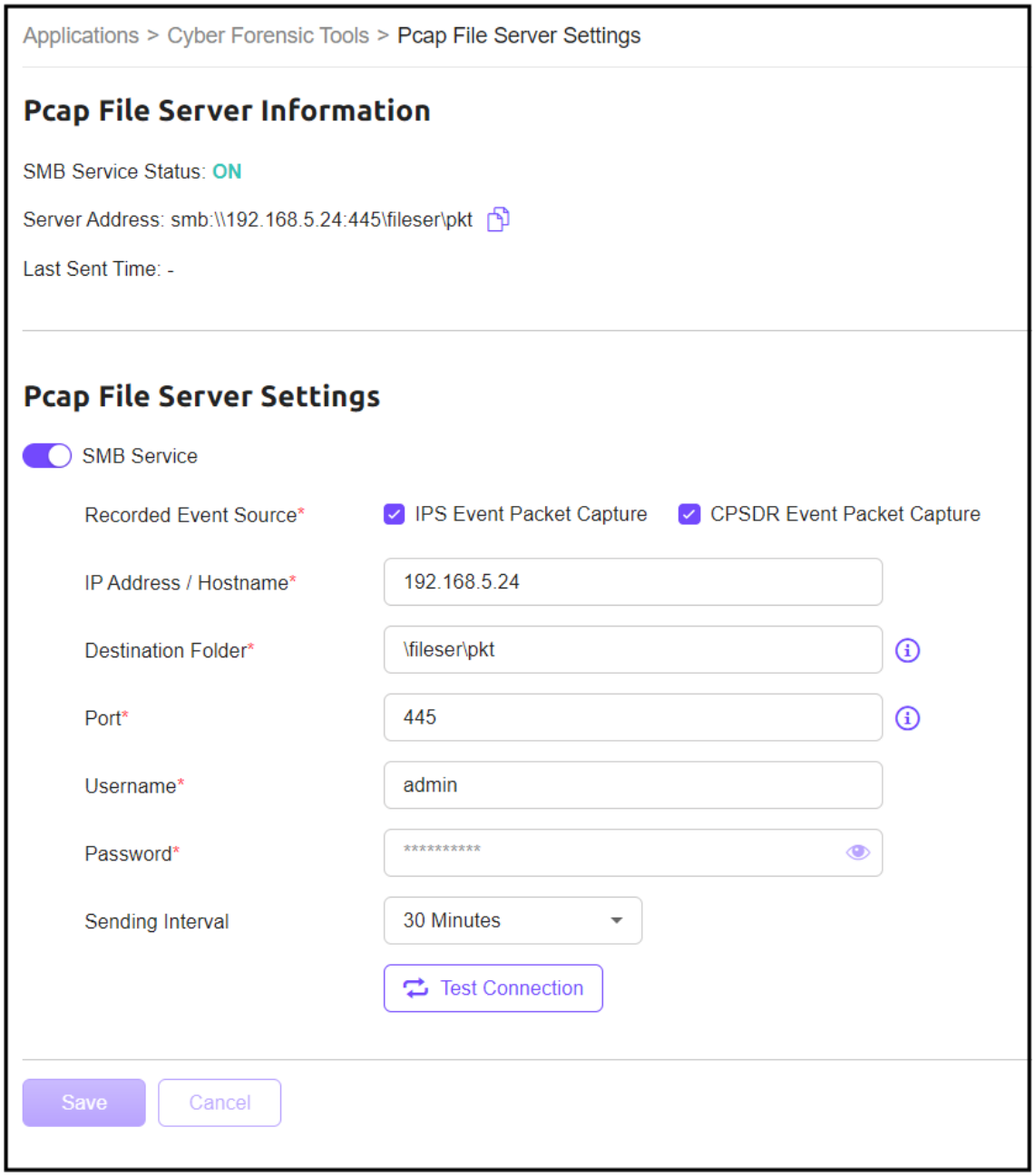
8.2.3 Pcap File Server Settings

In addition to downloading IPS event packets to your local disk, you can also transmit these packet files to a designated remote server using the SMB protocol. On the [Pcap File Server Settings] page, configure the necessary settings to facilitate the transmission of packet files to the server.

8.2.3.1 Viewing Pcap File Server Information

Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [Pcap File Server Settings].

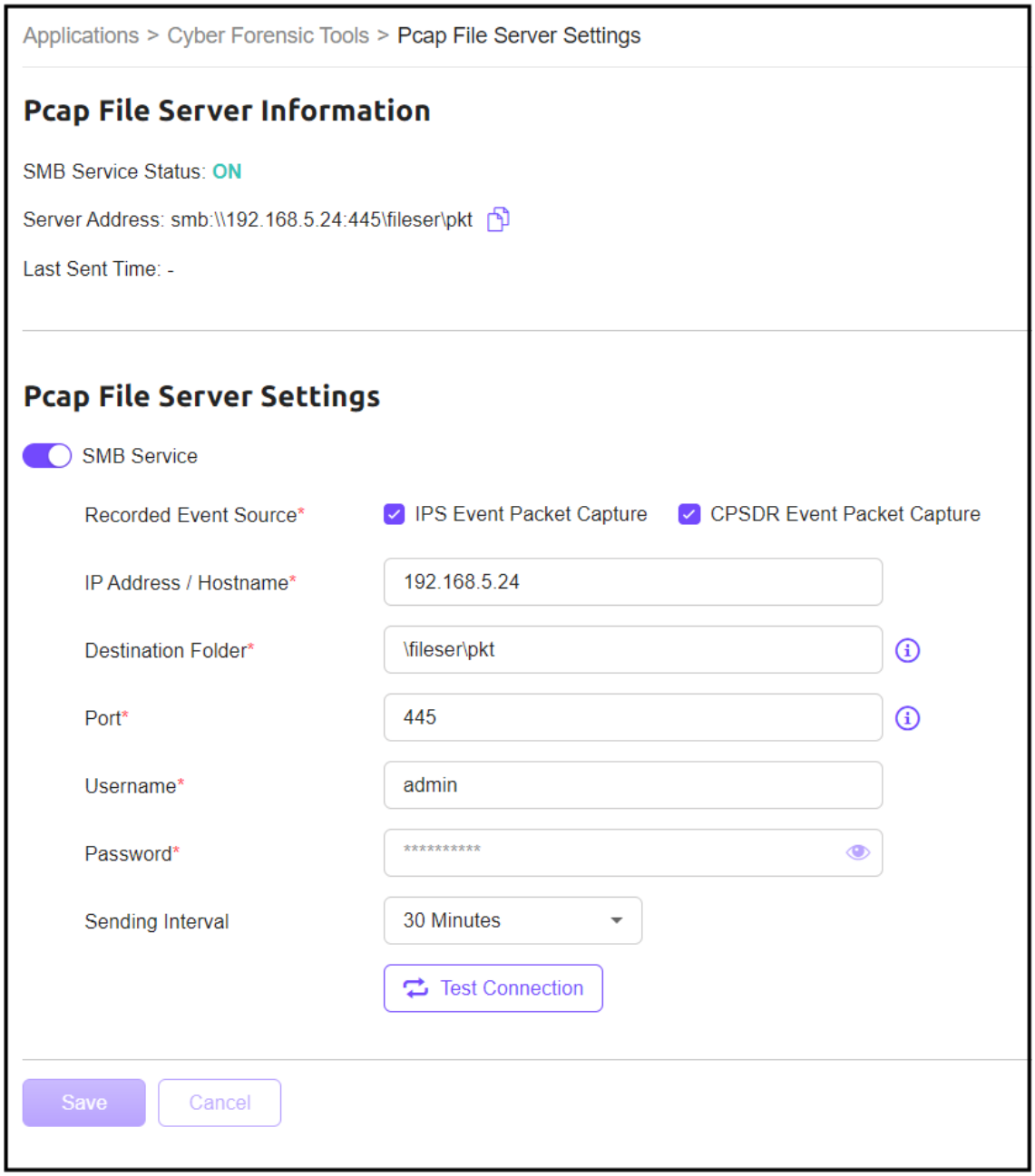


2. In the [Pcap File Server Information] pane, you will see the SMB service status, server address (click the button to copy the address), and last packet file sent time.

8.2.3.2 Configuring Pcap File Server Settings

Procedure

1. Go to [Applications] > [Cyber Forensic Tools] > [Pcap File Server Settings].



2. In the [Pcap File Server Settings] pane, configure the following settings.

Item	Description
SMB Service	Enable the SMB service by clicking the toggle.
Recorded Event Source	Select one or multiple sources of the packet files to be sent to the remote server.
IP Address / Hostname	Input the IP address or hostname of the server where the packet files will be sent.
Destination Folder	Input the destination folder on the server where the packet files will be sent.
Port	Input the port number for initiating an SMB connection. (Default: 445)

Item	Description
Username	Input the username for initiating an SMB connection.
Password	Input the password for initiating an SMB connection.
Sending Interval	Select a packet file sending interval, **30 Minutes**, **1 Hour**, **6 Hours**, **12 Hours**, or **24 Hours**, from the drop-down list.

3. Click [Save].

8.3 Diagnostics

Troubleshoot root causes for device failures.

- Hardware Diagnostics

8.3.1 Hardware Diagnostics

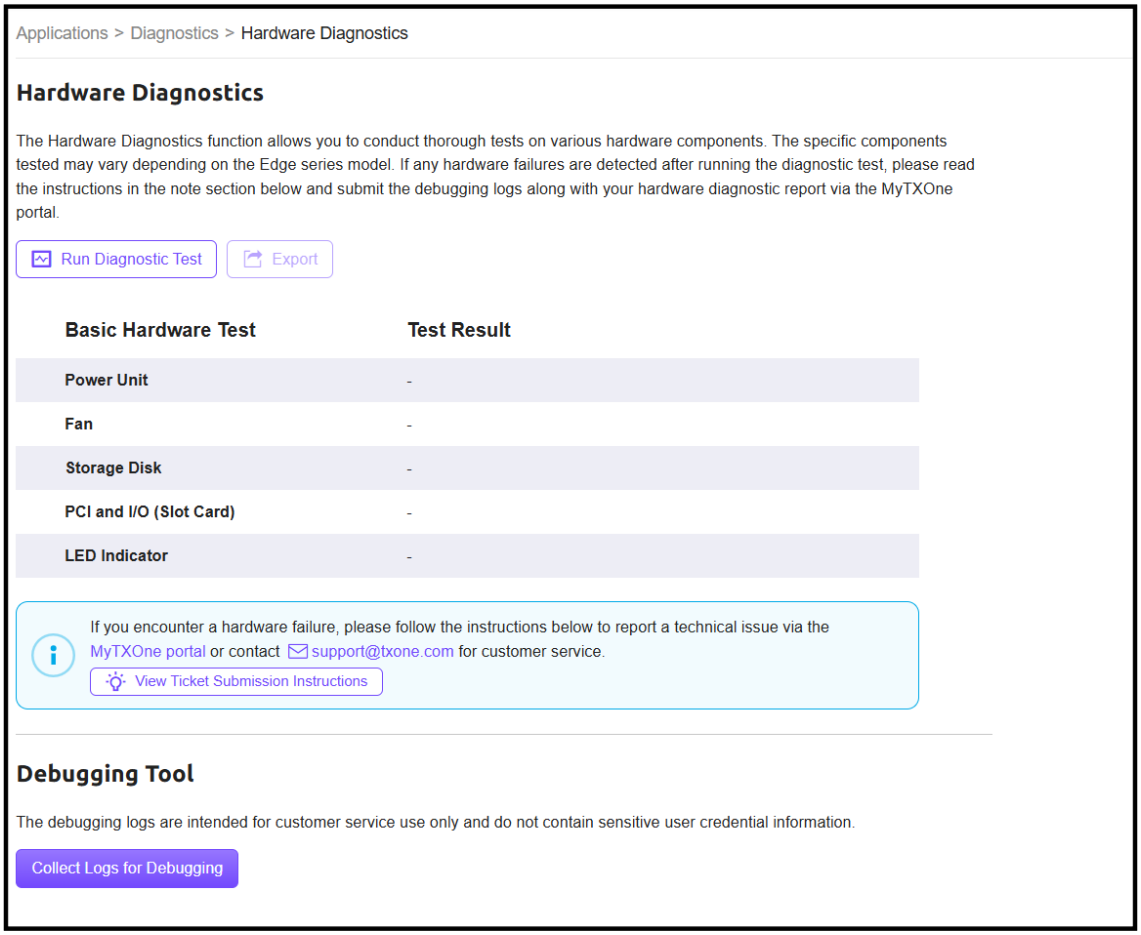
On the [Hardware Diagnostics] page, you can conduct thorough tests on various hardware components. The specific components tested may vary depending on the Edge series model.

If any hardware failures are detected after running the diagnostic test, please report the issue by visiting https://my.txone.com/ or contacting support@txone.com.

8.3.1.1 Running Diagnostic Tests

Procedure

1. Go to [Admin] > [Diagnostics] > [Hardware Diagnostics].

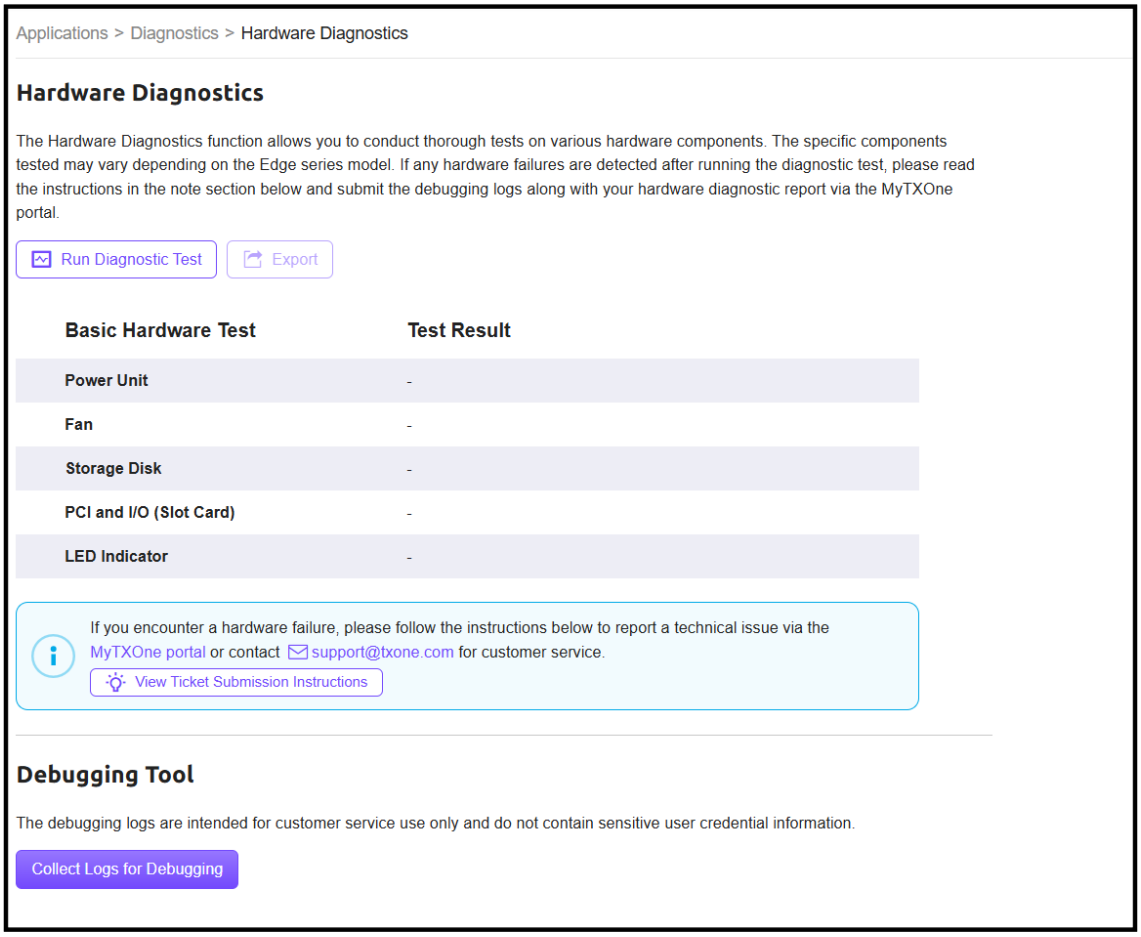


2. Click [Run Diagnostic Test]. Please wait about 10 to 20 seconds for the test result.

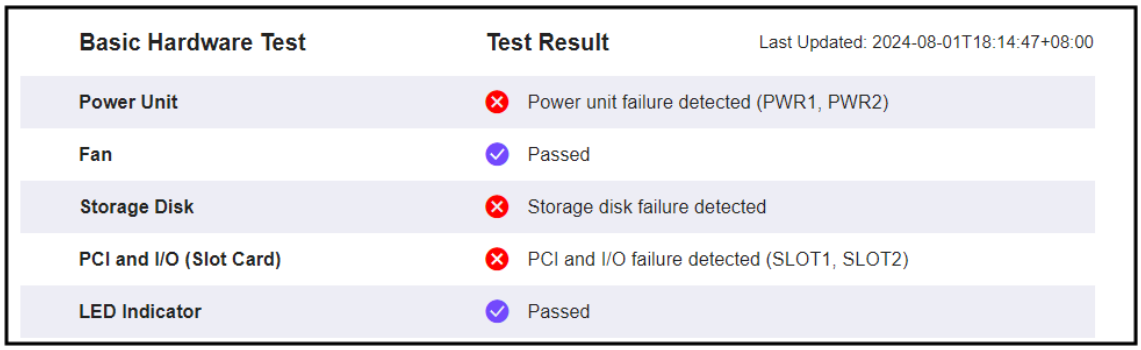
8.3.1.2 Viewing Diagnostic Results

Procedure

1. Go to [Admin] > [Diagnostics] > [Hardware Diagnostics].



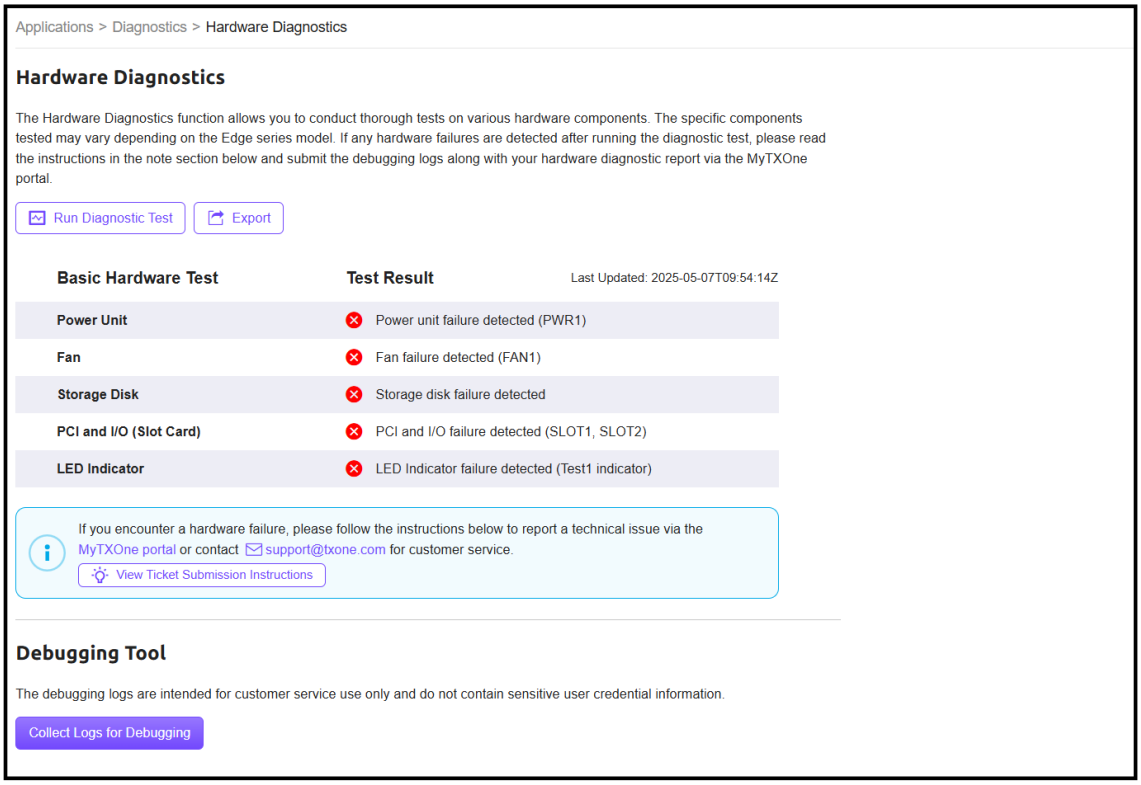
2. On the [Hardware Diagnostics] page, you can view the result of the most recent diagnostic test.



8.3.1.3 Exporting Diagnostic Reports

Procedure

1. Go to [Admin] > [Diagnostics] > [Hardware Diagnostics].

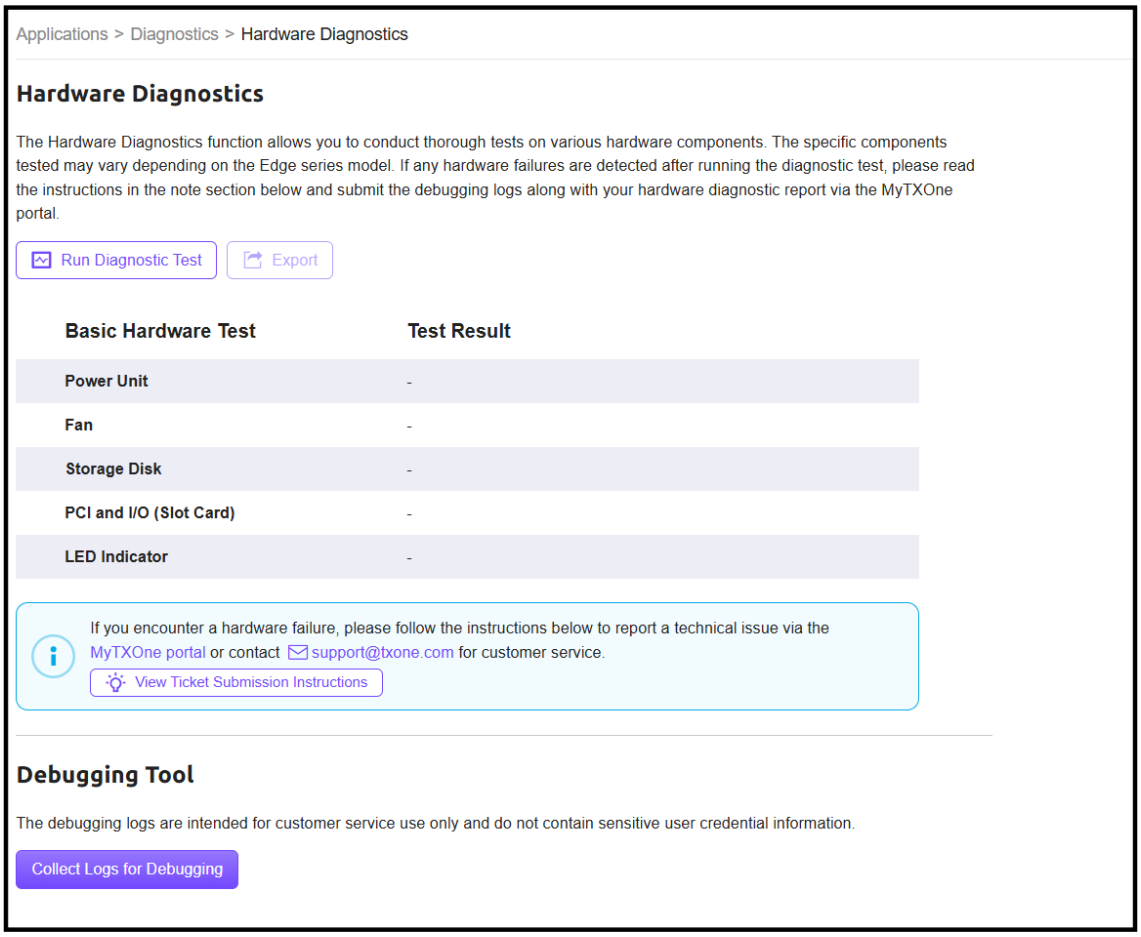


2. Click [Export] to download a PDF file containing the result of the most recent diagnostic test.

8.3.1.4 Collecting Debugging Logs

Procedure

1. Go to [Admin] > [Diagnostics] > [Hardware Diagnostics].



2. In the [Debugging Tool] pane, click [Collect Logs for Debugging]. A tgz file will be downloaded to your local storage.

9 QoS

This chapter describes how to manage and allocate bandwidth for your Edge device.

9.1 Quality of Service

Manage bandwidth allocation for egress ports or port pairs.

- Bandwidth Management

9.1.1 Bandwidth Management

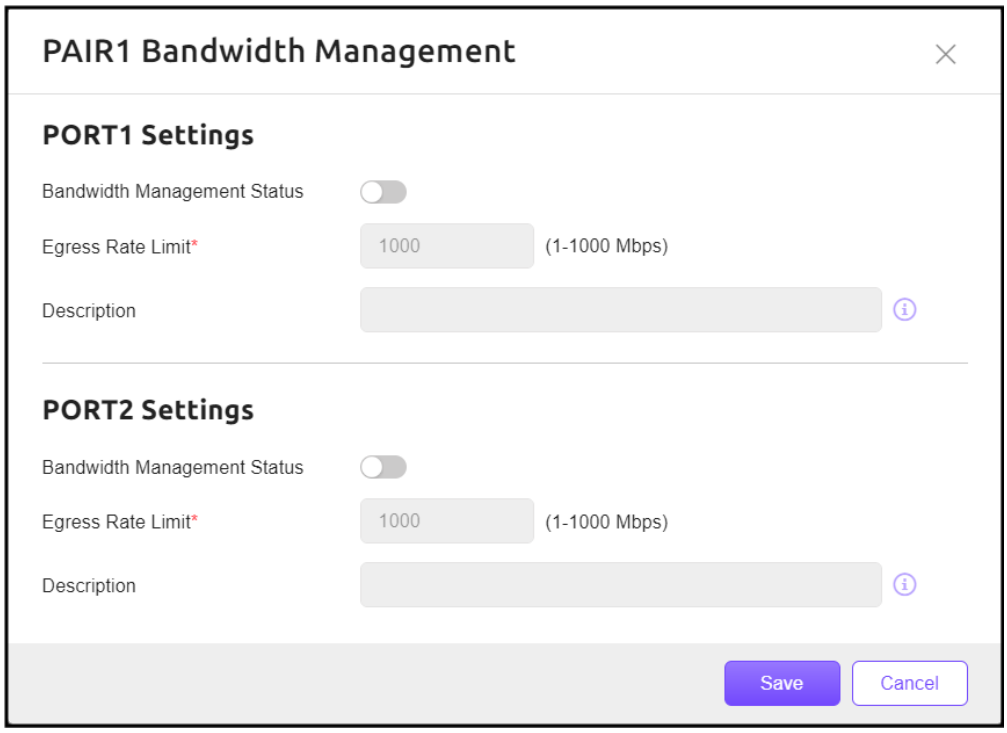
On the [Bandwidth Management] page, network administrators can manage, monitor and allocate bandwidth for the production-critical network traffic of each pair's egress port in real-time.

9.1.1.1 Configuring Bandwidth Management Settings

Procedure

1. Go to [QoS] > [Quality of Service] > [Bandwidth Management].

2. Select a port pair to manage its bandwidth settings.



3. Configure the following settings.

Item	Description
Bandwidth Management Status	Enable this item by clicking the toggle to configure the bandwidth settings.
Egress Rate Limit	Input the maximum data transmission rate for this port. (Default: 1000Mbps)
Description	(Optional) Type a description.

4. Click [Save].

10 Logs

This chapter describes the security and system logs you can view in the management console.

10.1 Security Logs

Review and analyze logs for security incidents.

- Cyber Security Logs
- Policy Enforcement Logs
- Protocol Filter Logs
- Domain Name Filter Logs
- File Filter & Antivirus Logs
- Suspicious Object Logs
- CPSDR Logs

10.1.1 Cyber Security Logs

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

10.1.1.1 Viewing Cyber Security Logs

Procedure

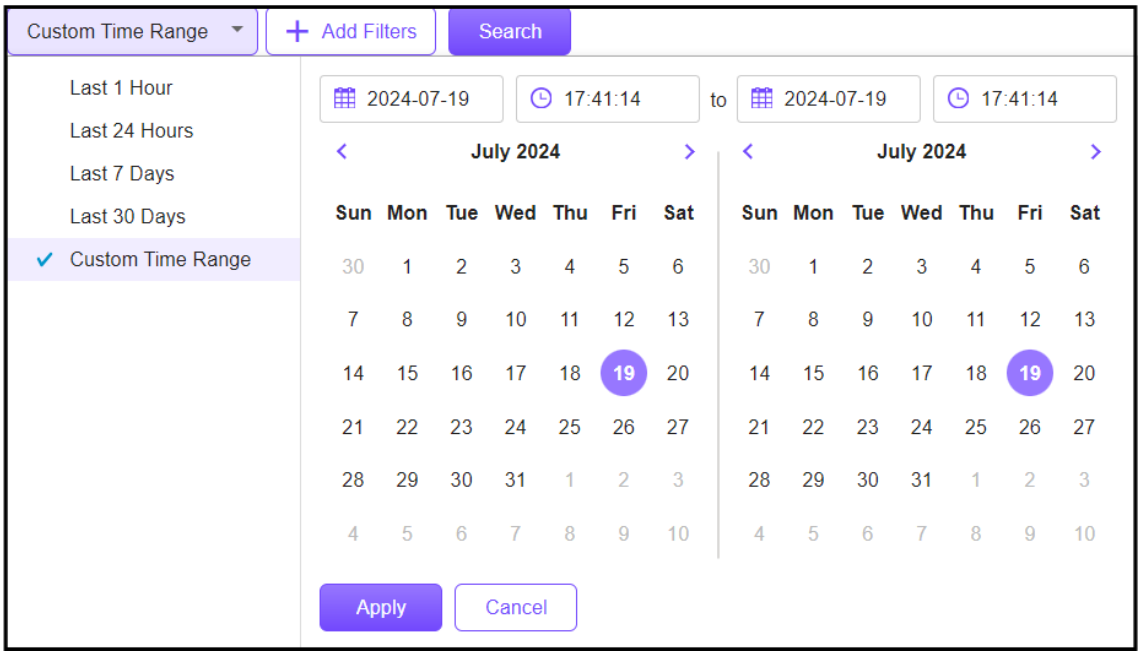
1. Go to [Logs] > [Security Logs] > [Cyber Security Logs].

The following table describes the Cyber Security log information.

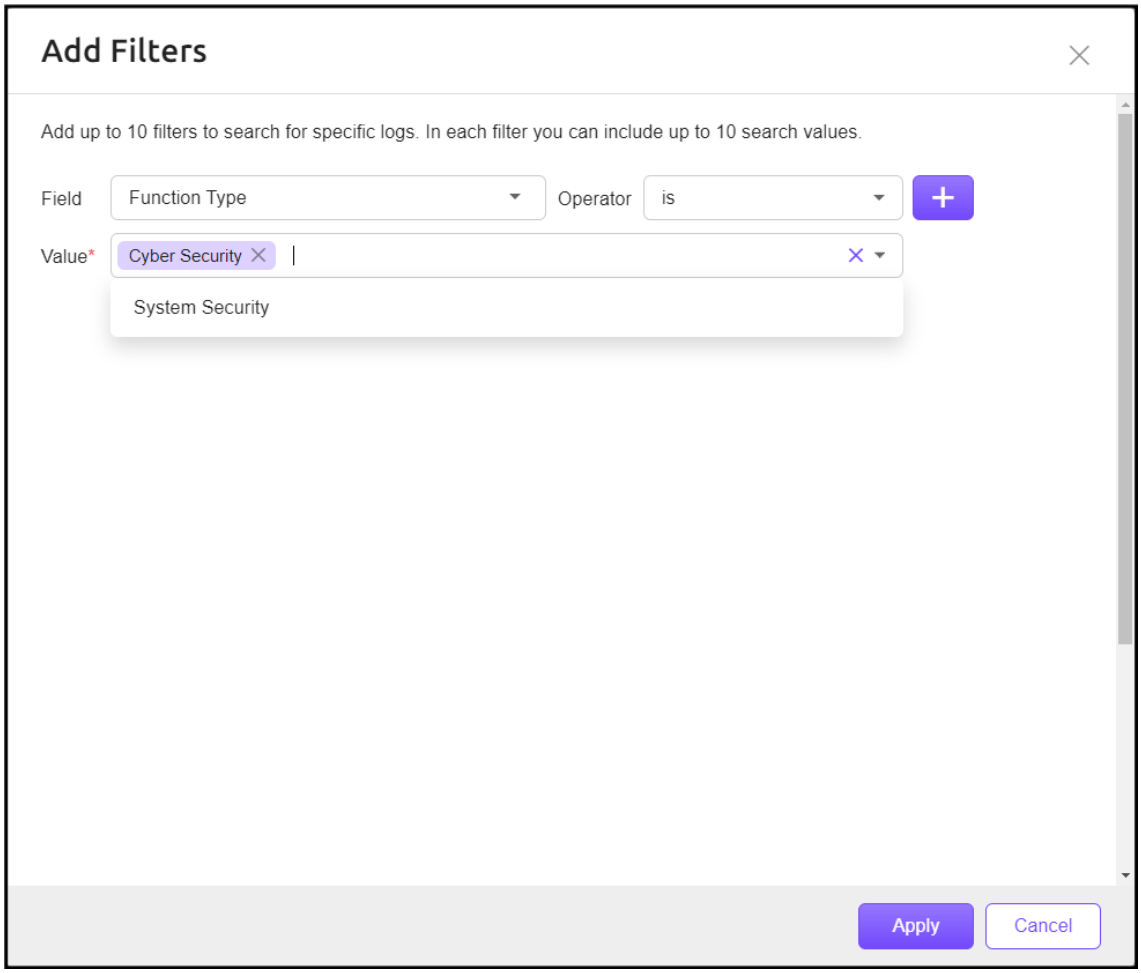
Field	Description
Time	The time when the log entry was created.
Function Type	The function type of the log, either Cyber Security or System Security.
Protocol Layer	The layer of OSI models that the matched signature belongs to.
Policy Rule Name	The name related to the matched policy rule triggering this log.
Profile Name	The name of the IPS profile triggering this log.
Event ID	The ID of the matched signature.
TIDs	MITRE TID Information
Security Category	The category of the matched signature.
Security Severity	The severity level assigned to the matched signature.
Security Rule Name	The name of the matched signature.
Interface	The physical port interface which receives the packet.
Attacker	The IP address of the host device which initiated the cyber incident.
Victim	The IP address of the host device which was attacked in the cyber incident.

Field	Description
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port of the packet, if protocol is TCP/UDP. The ICMP type of the packet, if protocol is ICMP
Destination MAC Address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port of the packet if the protocol is TCP/UDP. The ICMP code of the packet if the protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Ethernet Type	The Ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
Extra Information	Extra information provided with the cyber security log.
Preset Action	The action configured in the policy rule settings.
Enforced Action	The actual action executed by the device.
Count	The number of detected network packets within the detection period after the detection threshold is reached.

2. To query logs, select a time period, **Last 1 Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days** or **Custom Time Range** from the drop-down list.



3. Click the [Add Filters] button and the following [Add Filters] window will appear.



4. Select parameters from the [Field] and [Operator] drop-down lists.
5. Select/Input up to 10 search values in the [Value] field.
6. To add more filters, click the add button +.

7. Click [Apply] to apply these filters for querying logs. Afterwards, the filters that you just applied will be listed.

8. Click the [Search] button to query logs.

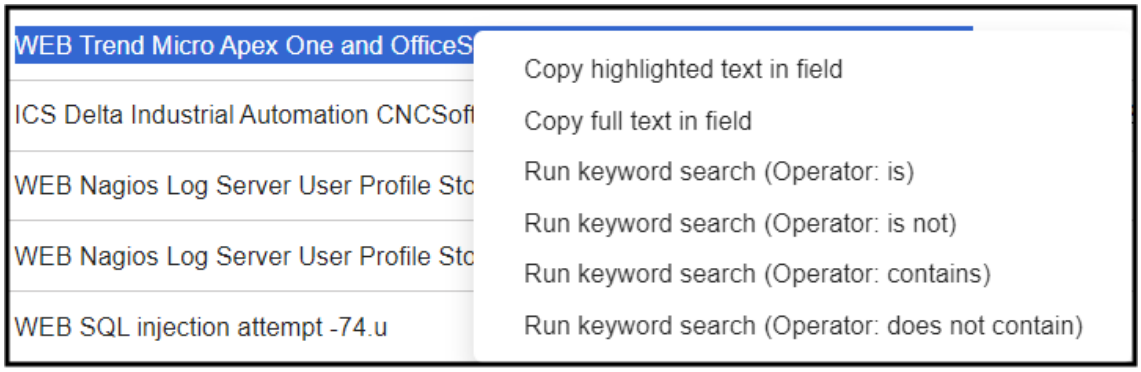
9. Click the [Clear Filters] button to remove all the applied search filters.

10. To export a CSV file of your current search results, click the button.

11. To show/hide certain type of information and adjust the column order, click the button.

For more information, see Viewing in Table View Mode.

12. Right click on a log entry and a pop-up menu will appear. You can take one of the following actions.



10.1.2 Policy Enforcement Logs

Policy Enforcement logs are generated by the [Policy Enforcement] feature without [Protocol Filter] being enabled, i.e., the action of the Policy Enforcement rule is either [Allow] or [Deny]. The Protocol Filter profiles are not used in policy rules.

10.1.2.1 Viewing Policy Enforcement Logs

Procedure

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

The following table describes the Policy Enforcement log information.

Field	Description
Time	The time when the log entry was created.
Protocol Layer	The layer of OSI models that the Policy Enforcement rule belongs to.
Policy Rule Name	The name related to the matched policy rule triggering this log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port, if protocol is TCP/UDP.

Field	Description
	The ICMP type, if protocol is ICMP.
Destination MAC Address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Ethernet Type	The Ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
Preset Action	The action configured in the policy rule settings.
Enforced Action	The actual action executed by the device.

To query logs, see Viewing Cyber Security Logs.

10.1.3 Protocol Filter Logs

Protocol Filter logs contain details about network traffic detected by the [Protocol Filter] feature. The [Protocol Filter] is an advanced setting option that can be configured under the [Policy Enforcement] settings.

10.1.3.1 Viewing Protocol Filter Logs

Procedure

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

The following table describes the Protocol Filter log information.

Field	Description
Time	The time when the log entry was created.
Protocol Layer	The layer of OSI models that the Policy Enforcement rule belongs to.
Policy Rule Name	The name related to the matched policy rule triggering this log.
Profile Name	The name of the Protocol Filter profile triggering this log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.

Field	Description
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port, if protocol is TCP/UDP. The ICMP type, if protocol is ICMP.
Destination MAC Address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Ethernet Type	The Ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd/Fun No.	The command or function number that triggered the log.
Extra Information	Extra information provided with the log.
Preset Action	The action configured in the policy rule settings.
Enforced Action	The actual action executed by the device.
Count	The number of detected network packets.

To query logs, see Viewing Cyber Security Logs.

10.1.4 Domain Name Filter Logs

Domain Name Filter logs are generated by the [Domain Name Filter Rule] feature with the action being either [Allow] or [Deny].

10.1.4.1 Viewing Domain Name Filter Logs

Procedure

1. Go to [Logs] > [Security Logs] > [Domain Name Filter Logs].

The following table describes the Domain Name Filter log information.

Field	Description
Time	The time when the log entry was created.
Policy Rule Name	The name of the Domain Name Filter rule triggering this log.
Interface	The physical port interface which receives the packet.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port, if protocol is TCP/UDP. The ICMP type, if protocol is ICMP.
Destination MAC Address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Domain Name	The domain name in the DNS query.
Preset Action	The action configured in the Domain Name Filter rule settings.
Enforced Action	The actual action executed by the device.

To query logs, see Viewing Cyber Security Logs.

10.1.5 File Filter & Antivirus Logs

File Filter and Antivirus logs contain details about network traffic detected by the [File Filter] or [Antivirus] feature. The [File Filter] and [Antivirus] are advanced setting options that can be configured under the [Policy Enforcement] settings.

10.1.5.1 Viewing File Filter and Antivirus Logs

Procedure

1. Go to [Logs] > [Security Logs] > [File Filter & Antivirus Logs].

The following table describes the File Filter and Antivirus log information.

Field	Description
Time	The time when the log entry was created.
Policy Rule Name	The name related to the matched policy rule triggering this log.
Profile Type	The type of log, either "File Filter" or "Antivirus."
Profile Name	The name of the File Filter profile or Antivirus profile triggering this log.
Interface	The physical port interface which receives the packet.
Attacker	The IP address of the host device which initiated the cyber incident.
Victim	The IP address of the host device which was attacked in the cyber incident.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port, if the protocol is TCP/UDP.
Destination MAC address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port, if protocol is TCP/UDP.
VLAN ID	The VLAN ID of the packet.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Virus Name	The name of the virus.
Extra Information	Extra information provided with the File Filter or Antivirus log.
Preset Action	The action configured in the policy rule settings.
Enforced Action	The actual action executed by the device.

To query logs, see Viewing Cyber Security Logs.

10.1.6 Suspicious Object Logs

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

10.1.6.1 Viewing Suspicious Object Logs

Procedure

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

The following table describes the Suspicious Object log information.

Field	Description
Time	The time when the log entry was created.
ID	The hash ID of the matched suspicious object.
Type	The suspicious object type, which is node type or link type.
Source	The source of the suspicious object.
Risk Level	The threat level of the suspicious object.
Expiration Time	The expiration time of the suspicious object. When the expiration time reaches, the suspicious object will be deleted.
Interface	The physical port interface which receives the suspicious object.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Asset Hostname	The hostname of the asset from which the suspicious object originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the suspicious object originated.
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 Asset Hostname	The hostname of the asset to which the suspicious object was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the suspicious object was sent.
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.
Preset Action	The action configured in the Suspicious Object settings.
Enforced Action	The actual action executed by the device.

Field	Description
Count	The number of detected suspicious object within the detection threshold.

To query logs, see Viewing Cyber Security Logs.

10.1.7 CPSDR Logs

CPSDR logs contain details about network traffic detected by the CPSDR feature with the action being either [Allow] or [Deny].

10.1.7.1 Viewing CPSDR Logs

Procedure

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

The following table describes the CPSDR log information.

Field	Description
Time	The time when the log entry was created.
CPSDR Rule ID	The rule ID of the CPSDR rule triggering this log.
CPSDR Rule Name	The name of the CPSDR rule triggering this log.
TIDs	MITRE TID Information
Tactic IDs	The ID numbers of the cyber tactics.
Impact Severity	The severity level of the cyber incident according to the CPSDR rule.
Confidence Level	The likelihood of the cyber incident according to the CPSDR rule.
Risk Level	The risk level calculated by the system based on the impact severity and confidence level.
Interface	The physical port interface which receives the packet.
Attacker	The IP address of the host device which initiated the cyber incident.
Victim	The IP address of the host device which was attacked in the cyber incident.
Source MAC Address	The source MAC address of the packet.
Source IP Address	The source IP address of the packet.
Source Asset Hostname	The hostname of the asset from which the packet originated.
Source Asset Alias Name	The user-defined alias name of the asset from which the packet originated.
Source Asset Type	The type of the asset from which the packet originated.
Source Port	The source port, if protocol is TCP/UDP. The ICMP type, if protocol is ICMP.

Field	Description
Destination MAC Address	The destination MAC address of the packet.
Destination IP Address	The destination IP address of the packet.
Destination Asset Hostname	The hostname of the asset to which the packet was sent.
Destination Asset Alias Name	The user-defined alias name of the asset to which the packet was sent.
Destination Asset Type	The type of the asset to which the packet was sent.
Destination Port	The destination port, if protocol is TCP/UDP. The ICMP code, if protocol is ICMP.
VLAN ID	The VLAN ID of the packet.
Ethernet Type	The Ethernet type of the packet.
IP Protocol Name	The IP protocol name of the packet.
Extra Information	Extra information provided with the log.
Source	The origin of the log based on the following criteria. • **CPSDR Rule**: The rule triggering this log is not included in an allow list or a deny list. In addition, it does not reach the risk level threshold defined in the CPSDR detection threshold settings. • **Deny List**: The rule triggering this log is included in a deny list. • **Threshold Settings**: The rule triggering this log reaches or exceeds the risk level threshold defined in the CPSDR detection threshold settings. When a rule in an allow list is hit, no log entry is generated.
Preset Action	The action based on the log source. • **Allow**: When the source of the rule triggering this log is **CPSDR Rule**. • **Deny**: When the source of the rule triggering this log is **Deny List** or **Threshold Settings**.
Enforced Action	The actual action executed by the device, corresponding to the preset action.
Count	The number of detected network packets.

To query logs, see Viewing Cyber Security Logs.

10.2 System Logs

Review and analyze logs for system activities and operational events.

- Asset Detection Logs
- System Event Logs
- Audit Logs

10.2.1 Asset Detection Logs

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

10.2.1.1 Viewing Asset Detection Logs

Procedure

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

The following table describes the asset detection log information.

Field	Description
Time	The time when the log entry was created.
Event Type	The log event description.
Interface	The physical port interface which receives the asset information.
Asset MAC Address	The MAC address of the asset.
Asset IP Address	The IP address of the asset.
Asset Hostname	The hostname of the asset.
Asset Type	The type of the asset.

To query logs, see Viewing Cyber Security Logs.

10.2.2 System Event Logs

System event logs contain details about system events on the device.

10.2.2.1 Viewing System Event Logs

Procedure

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

The following table describes the system event log information.

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

To query logs, see Viewing Cyber Security Logs.

10.2.3 Audit Logs

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

📝	To view audit logs, please log in with an auditor account.

10.2.3.1 Viewing Audit Logs

Procedure

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

The following table describes the audit log information.

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

📖	To query logs, see Viewing Cyber Security Logs.

11 Admin

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

📝	Log in to the management console with an admin account to access the Admin tab.

11.1 Accounts

Manage account-related settings, including role-based account management, account logout timer, and third-party account authentication methods.

- Account Management
- Logout Timer
- Auth Services

11.1.1 Account Management

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

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

Task	Description
Create accounts	Click [Create] to create a new user account. 📖 For more information, see Configuring User Accounts.
Delete existing accounts	Select existing user accounts and click [Delete].
Edit existing accounts	Click the name of an existing user account to view or modify the current account settings. 📖 For more information, see Configuring User Accounts.
Configure password policy	Click the [Configure Password Policy] button to adjust password complexity settings. 📖 For more information, see Configuring Password Policy.

📝	The maximum number of user accounts on an Edge web console is 32.

11.1.1.1 User Roles

The following table describes the permission matrix for user roles.

		User Role			
Tab	**Action**	**Admin**	**Operator**	**Viewer**	**Auditor**
Visibility	View	✔	✔	✔	✔

		User Role			
					(Can only view the [System Dashboard] page)
	All operations	✓	✓	✓ (Cannot create profiles)	✗
Device	View	✓	✓	✗	✗
	All operations	✓	✗	✗	✗
Objects & Profiles	View	✓	✓	✗	✗
	All operations	✓	✓	✗	✗
Security	View	✓	✓	✗	✗
	All operations	✓	✓	✗	✗
Patterns	View	✓	✓	✗	✗
	All operations	✓	✓	✗	✗
Applications	View	✓	✓	✓ (Can only view the [Captured Packet Downloads] page)	✗
	All operations	✓	✓	✗	✗
QoS	View	✓	✓	✗	✗
	All operations	✓	✓	✗	✗
Logs - excluding Audit Logs	View	✓	✓	✓	✗
Logs - Audit Logs	View	✗	✗	✗	✓
Admin	View	✓	✗	✗	✗
	All operations	✓	✗	✗	✗

11.1.1.2 Built-in Admin Account Login Credential

The following table lists the default login credential of the built-in admin account.

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

> The built-in admin account cannot be deleted from the system. Ensure that the password of the built-in admin account is changed when you first set up the device.

11.1.1.3 Account Input Format

Input format validation will apply to the account management form text fields. The following table describes the format restrictions on user input.

Field	Length	Format	Reserved Name

ID	1-32 characters	• Letters a-z & A-Z
		• Numbers 0-9
		• Special characters:
		  ○ periods [.]
		  ○ underscores [_]
		1. Leading and trailing characters cannot be special characters.
		2. Successive special characters are not allowed.
			• admin
			• administrator
			• root

Name	1-32 characters	• Letters a-z & A-Z
		• Numbers 0-9
		• Special characters:
		  ○ periods [.]
		  ○ underscores [_]
		  ○ white spaces [ ]
		Single spaces are not allowed.	

Description	0-64 characters	• Letters a-z & A-Z
		• Numbers 0-9
		• Special characters:
		  ○ periods [.]
		  ○ underscores [_]
		  ○ white spaces [ ]
		  ○ parentheses [( ] & [ )]
		  ○ hyphens [-]	

11.1.1.4 Account ID/Password Reset

In some specific situations, for security reasons, users are required to reset their IDs or passwords the next time they log in.

User Role	Scenario	
	First Time Login	**Password Changed by Admin**
Admin	Reset ID and Password	N/A
Operator	Reset Password	Reset Password
Viewer	Reset Password	Reset Password

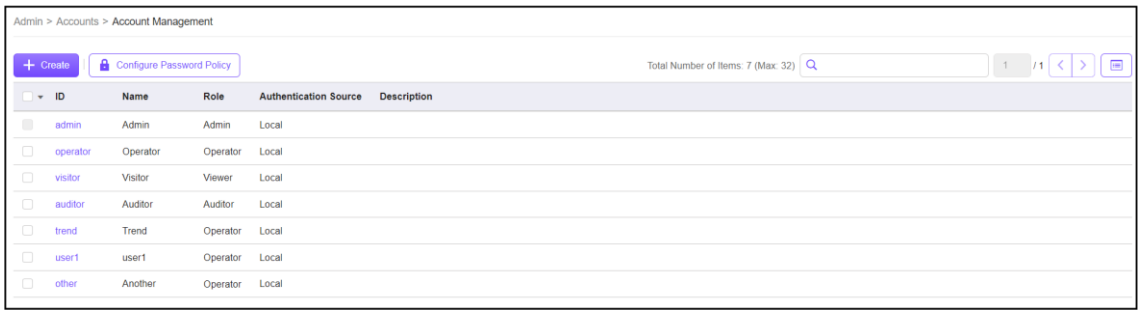
User Role	Scenario	
Auditor	Reset Password	Reset Password

11.1.1.5 Configuring User Accounts

When you log in to the web console using an administrator account (admin), you can create new user accounts to access the system or edit account settings.

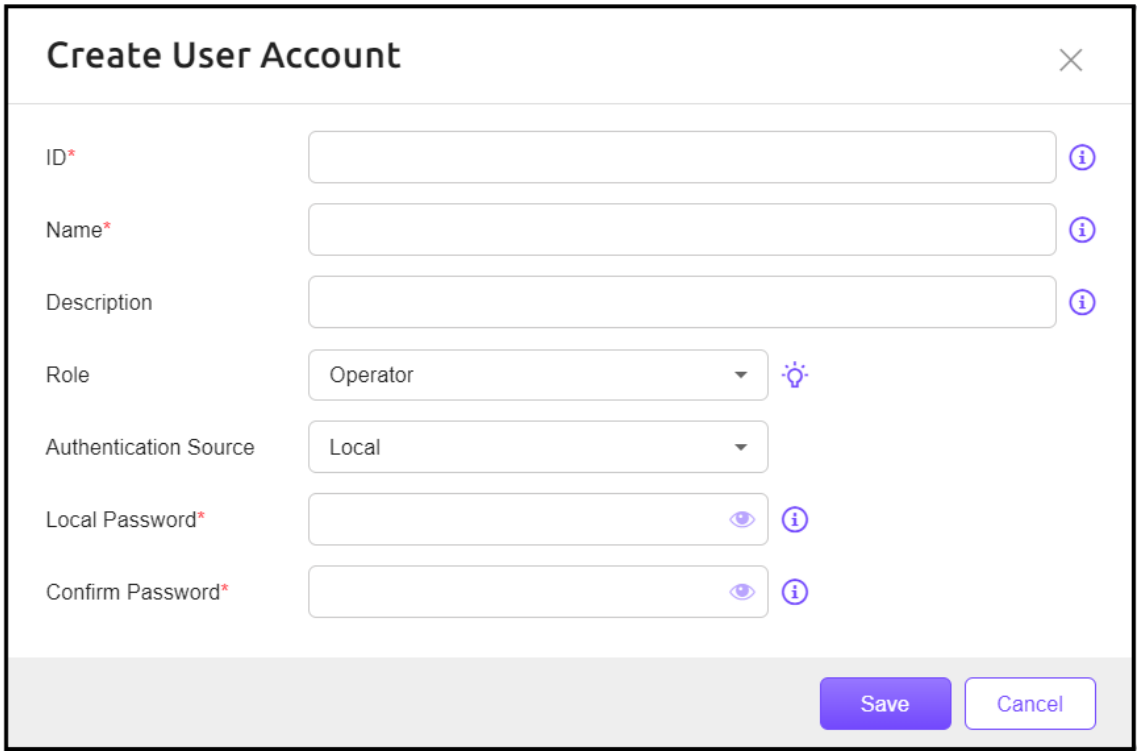
Procedure

1. Go to [Admin] > [Accounts] > [Account Management].



2. Do one of the following.

- Click [Create] to create a new user account. The [Create User Account] window will appear.
- Click a user ID to edit settings. The [Edit User Account] window will appear.



3. Configure the account settings.

Field	Description
ID	Input a user ID to log in to the management console.
Name	Input the name of the user for this account.

Field	Description
Description	(Optional) Add a description for this account.
Role	Select a user role, **Operator**, **Viewer**, or **Auditor**, for this account. For more information, see User Roles.
Authentication Source	Select an authentication source, **Local** or **External Authentication Server**. If you select External Authentication Server, further select an authentication protocol, **TACACS+**, **RADIUS**, or **SAML SSO**, for this account. For more information, see Auth Services.
Local Password	(Only for the "Local" authentication source) Input an account password.
Confirm password	(Only for the "Local" authentication source) Re-type the account password to confirm.

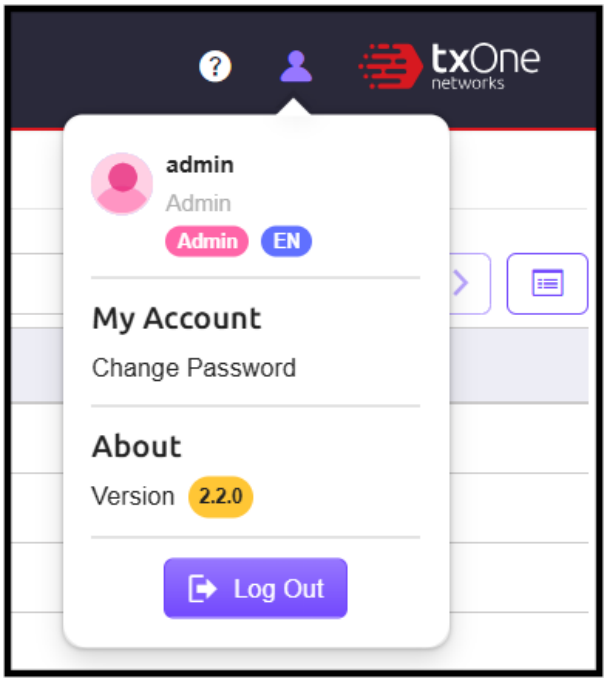
4. Click [Save].

11.1.1.6 Changing Account ID/Password

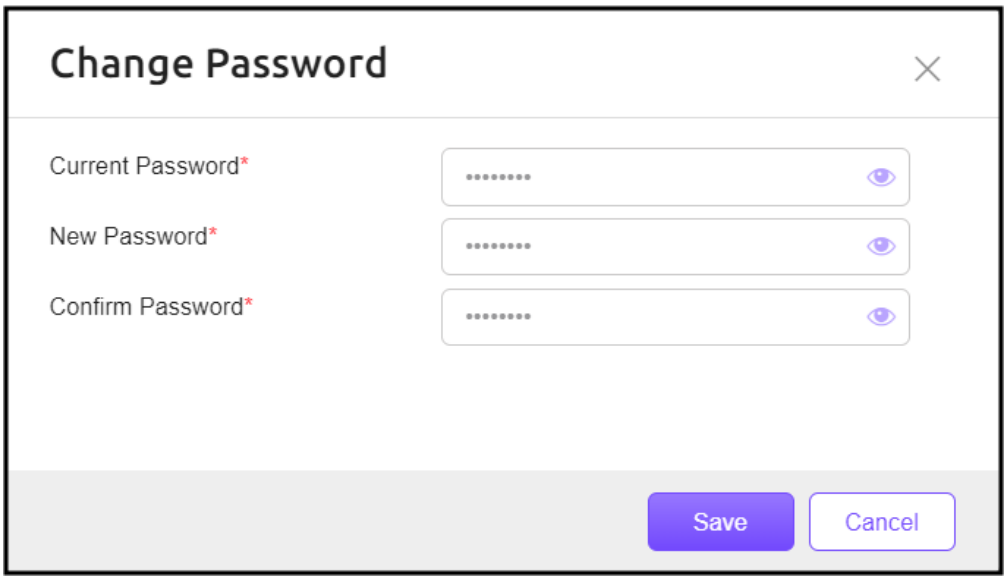
Procedure

- **Method 1: Access [Change Password] Window** (only for changing password)

1. On the web console banner, click your account at the top right corner.



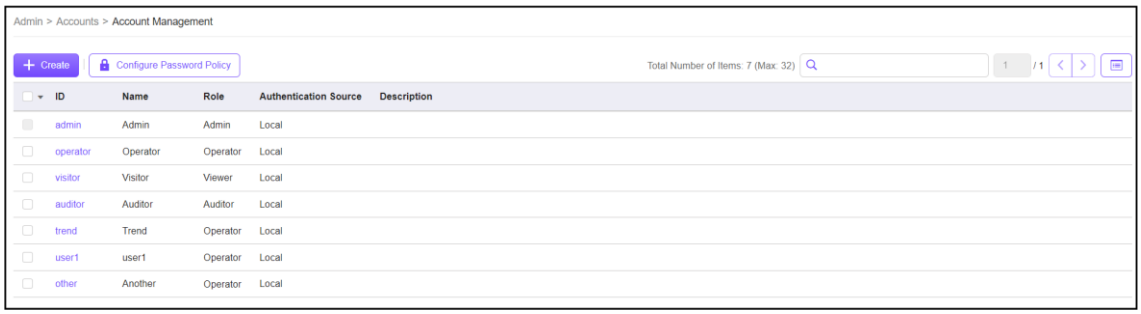
2. Click [Change Password]. The [Change Password] window will appear.



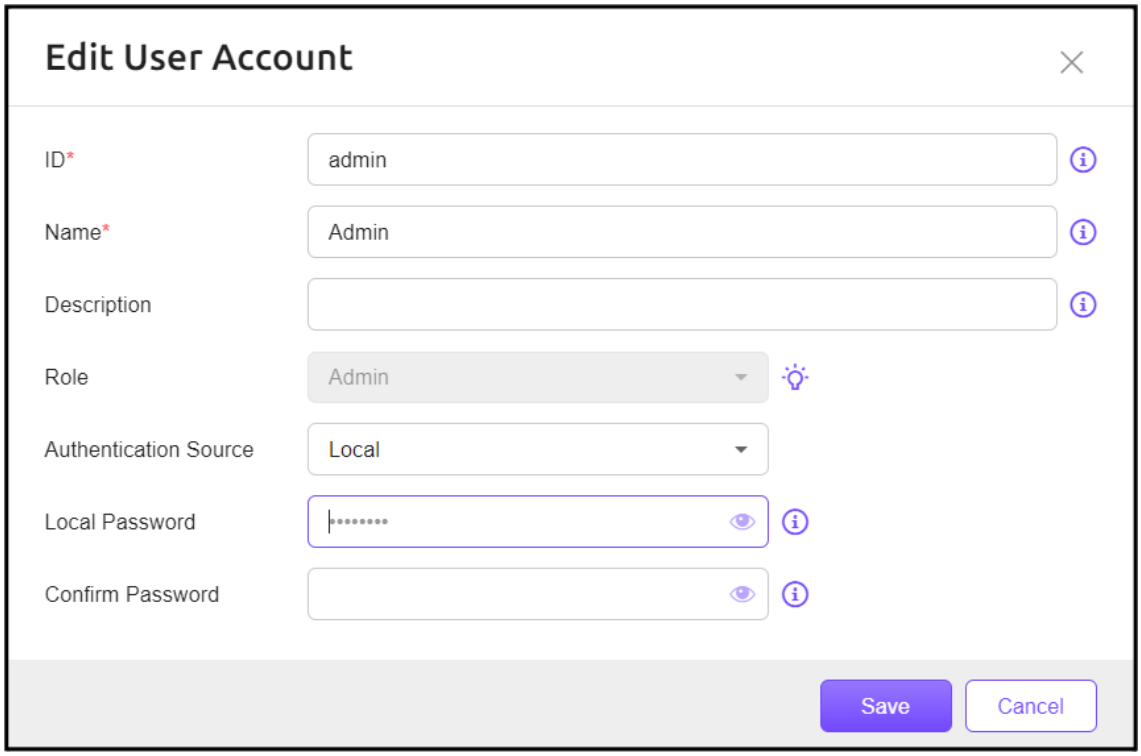
3. Modify the password settings.
   - Current password
   - New password
   - Confirm password
4. Click [Save].

- **Method 2: Access [Account Management] Page** (Only accessible with an admin account)

1. Go to [Admin] > [Accounts] > [Account Management].



2. Click an ID in the [ID] column. The [Edit User Account] window will appear.



3. Modify the ID/password settings.
   - ID
   - Local Password (new password)
   - Confirm Password
4. Click [Save].

11.1.1.7 Configuring Password Policy

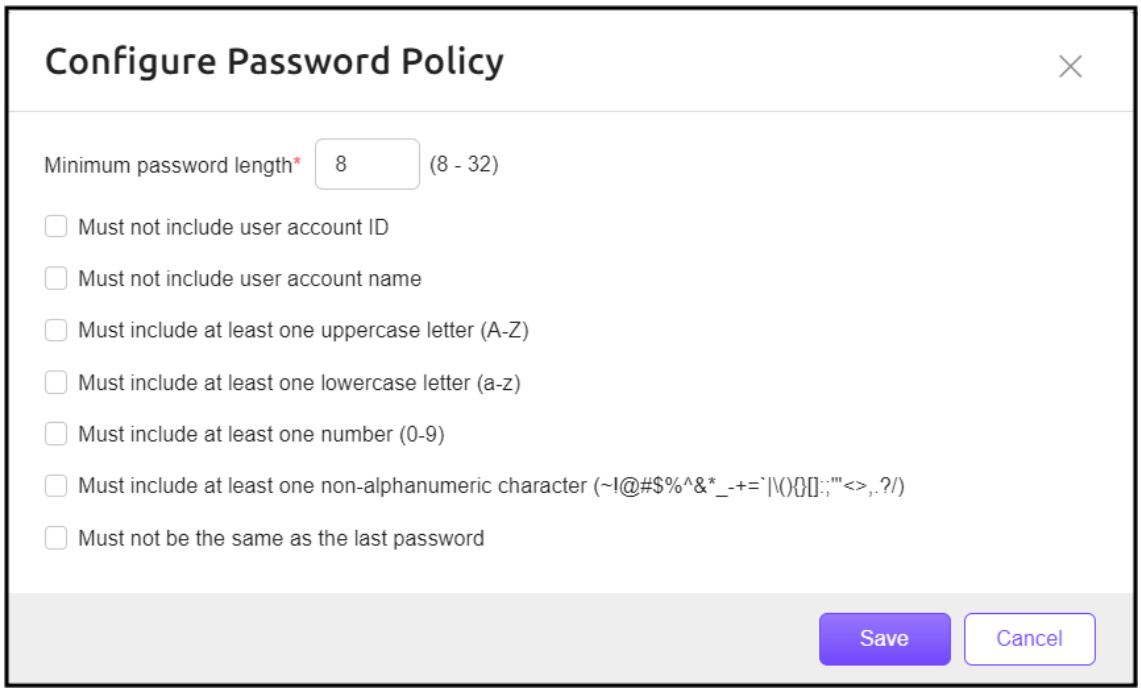
By configuring the password policy, users may enhance web console access security.

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

> ⚠ When a user submits a new password, the password policy determines whether the password meets your company's established requirements. If strong passwords are required, strict password policies may sometimes increase costs to an organization when users select passwords that are too difficult to remember. Users call the help desk when they forget their passwords, or keep passwords in easily accessible locations that would increase their vulnerability to threats. When establishing a password policy, balance the necessity of highly secured password with the utility of easily-recalling password to make the policy easy for users to follow.

Procedure

1. Go to [Admin] > [Accounts] > [Account Management].
2. Click the [Configure Password Policy] button. The [Configure Password Policy] window will appear.



3. Select one or multiple options that meet your required password policy.

4. Click [Save].

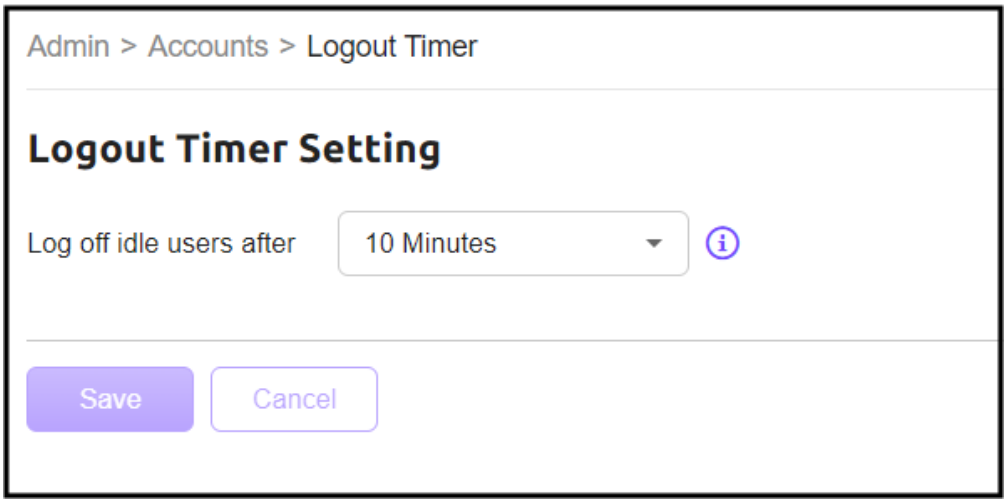
11.1.2 Logout Timer

On the [Logout Timer] page, you may set a specific time to automatically terminate login sessions after users have been idle for a specified time.

11.1.2.1 Configuring Logout Timer

Procedure

1. Go to [Admin] > [Accounts] > [Logout Timer].



2. Select a session timeout value, **10 minutes** (default), **15 minutes**, **30 minutes** or **60 minutes**, from the drop-down list.

3. Click [Save].

📝	The logout timer setting applies to both Edge device web console and CLI.

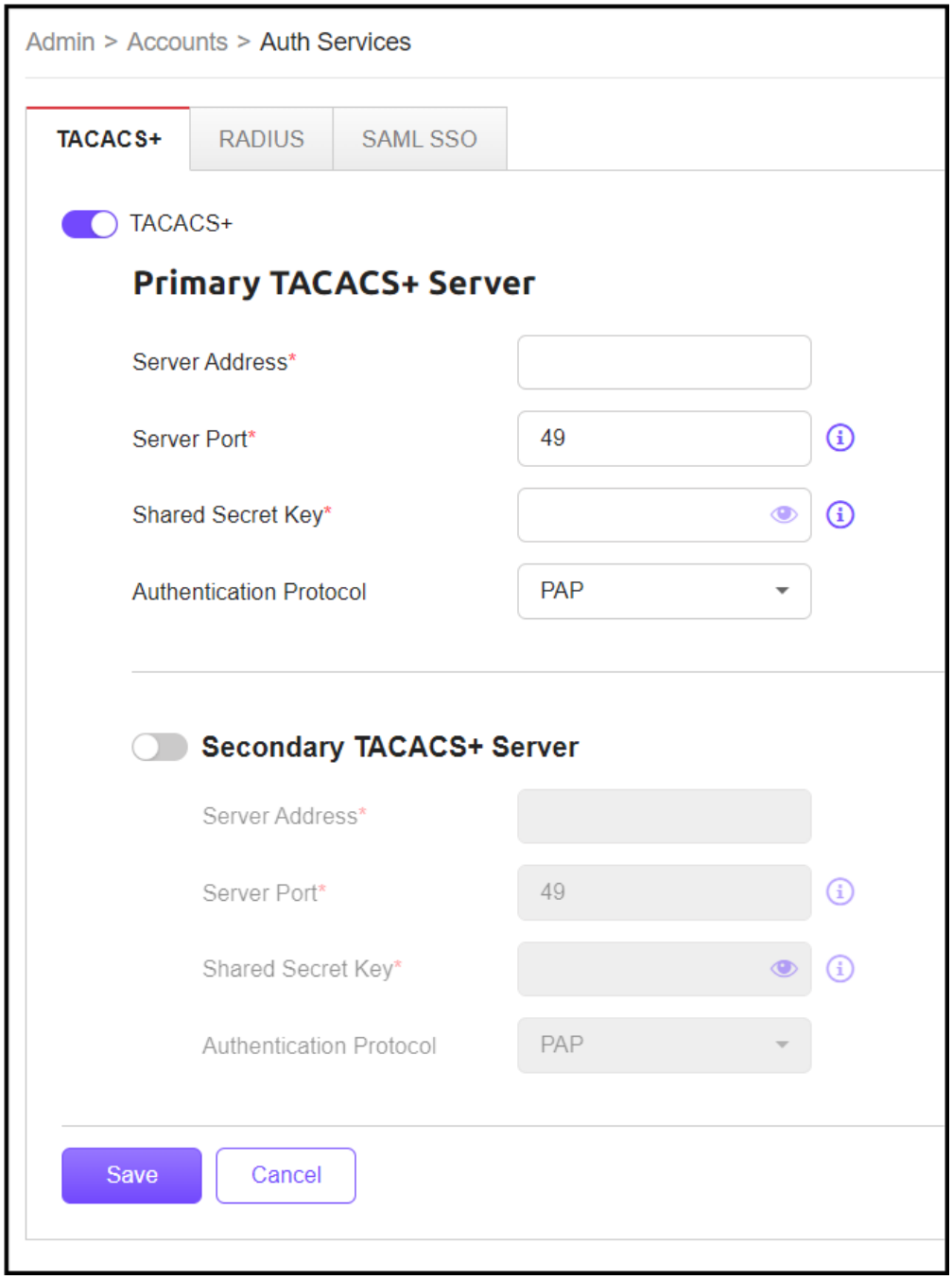
11.1.3 Auth Services

On the [Auth Services] page, you may configure the settings of authentication servers (TACACS+, RADIUS, and SAML SSO) for the Edge device's external authentication service.

11.1.3.1 Configuring TACACS+

Procedure

1. Go to [Admin] > [Accounts] > [Auth Services].



2. Under the [TACACS+] tab, enable TACACS+ and configure the following settings for the primary TACACS+ server.

- Server Address
- Server Port (Default Port: 49)
- Share Secret Key (Maximum Length: 64 characters)

- Authentication Protocol (MS-CHAPv1, CHAP, PAP or ASCII)

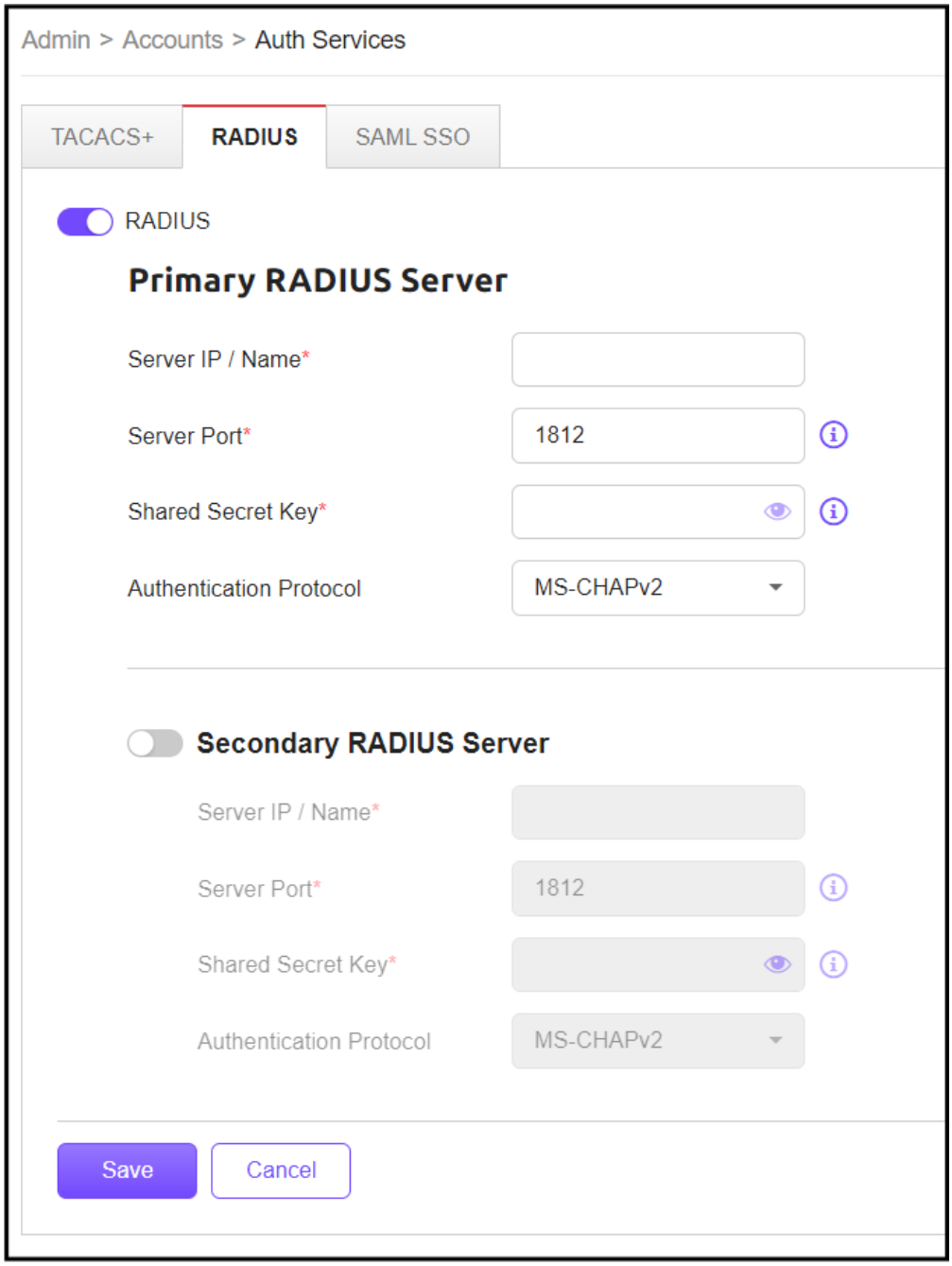
3. (Optional) Enable the secondary TACACS+ server and configure its settings if necessary.
4. Click [Save].

For more information about TACACS+, see the document RFC 8907.

11.1.3.2 Configuring RADIUS

Procedure

1. Go to [Admin] > [Accounts] > [Auth Services].



2. Under the [RADIUS] tab, enable RADIUS server and configure the following settings for the primary RADIUS server.

- Server IP/Name
- Server Port (Default Port: 1812)

- Shared Secret Key (Maximum Length: 64 characters)
- Authentication Protocol (MS-CHAPv2, MS-CHAPv1, CHAP, or PAP)

3. (Optional) Enable the secondary RADIUS server and configure its settings if necessary.
4. Click [Save].

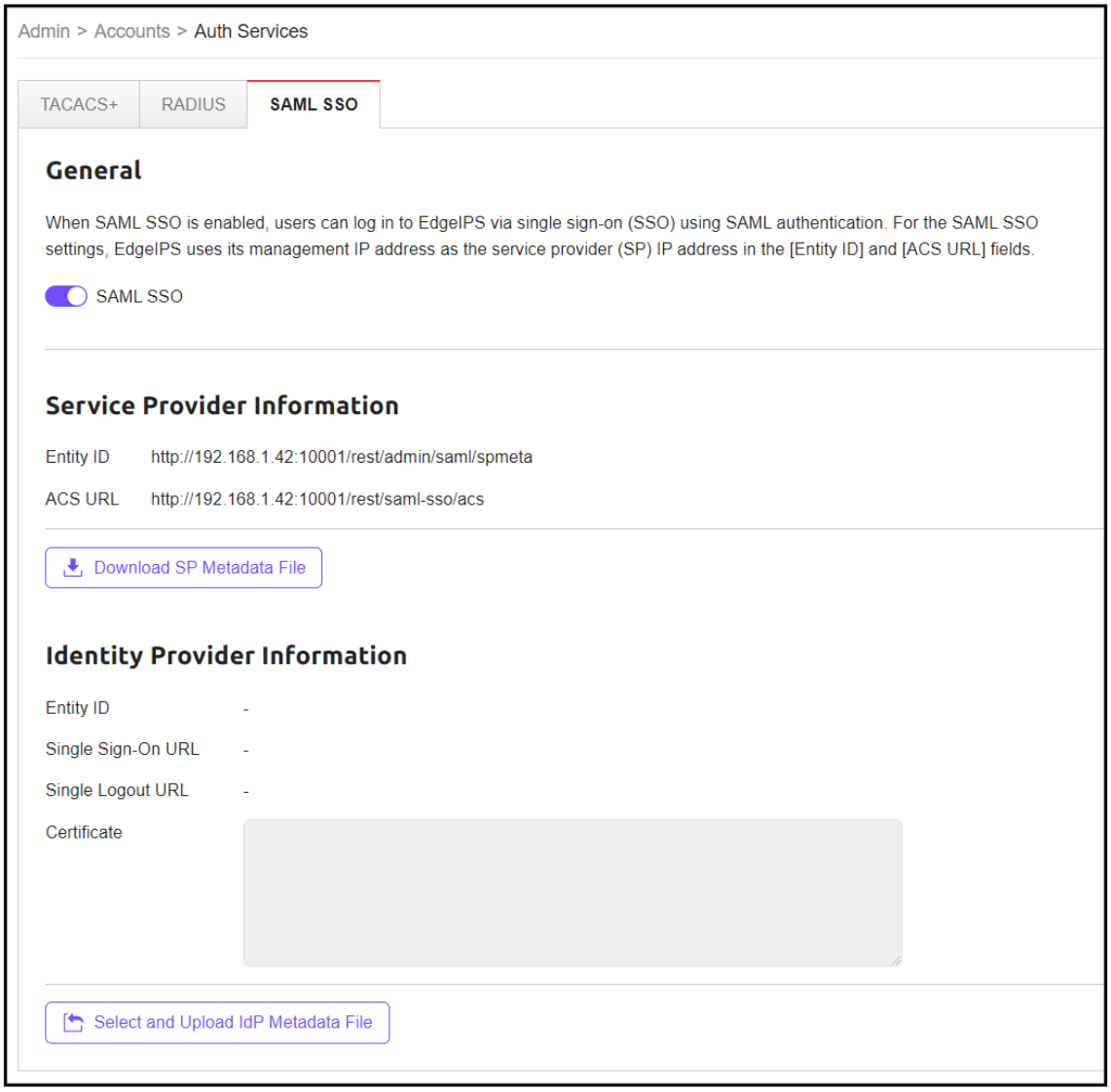
	For more information about RADIUS, see the document RFC 2865.

11.1.3.3 Configuring SAML SSO

SAML SSO (Single Sign-On) allows users to log on to the Edge device after the Edge device metadata file with the external identity provider information is provided. The metadata file indicates the data that provide information about the basic configuration data for authentication and authorization.

Procedure

1. Go to [Admin] > [Accounts] > [Auth Services].
2. Under the [SAML SSO] tab, enable SAML SSO login by clicking the toggle.



3. In the [Service Provider Information] pane, the following information is shown on the page.
   - Entity ID

- ACS URL

4. Click the [Download SP Metadata File] button to download the service provider metadata file in XML format.

5. Go to the external identity provider server and import the metadata file. An integrated metadata file will be generated.

6. In the [Identity Provider Information] pane, the following information will be automatically shown on the screen.

- Entity ID
- Single Sign-On URL
- Single Logout URL
- Certificate

7. After confirming the information above, click the [Select and Upload IdP Metadata File] button to import the integrated authentication and authorization data to the Edge device.

8. Click [Save].

	For more information about SAML SSO, see the document RFC 7522.

11.2 Notifications

Configure notification settings.

- SNMP
- Syslog

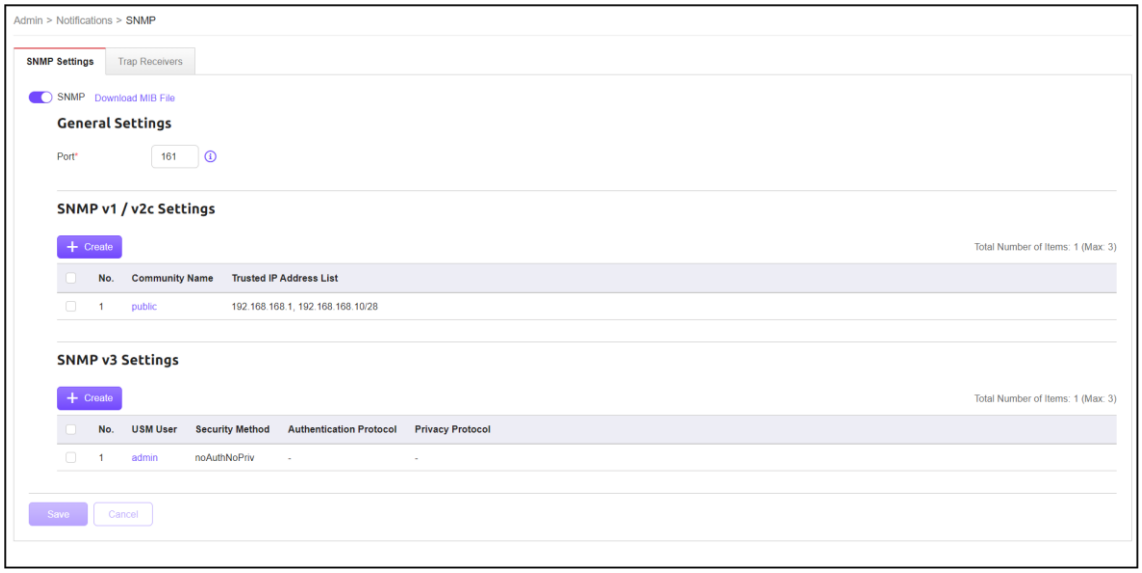
11.2.1 SNMP

The Simple Network Management Protocol is a protocol used for exchanging management information between an Edge series device and its management console. The device supports SNMPv1/v2c and a more secure v3, as well as SNMP traps.

11.2.1.1 Configuring SNMP General Settings

Procedure

1. Go to [Admin] > [Notifications] > [SNMP].

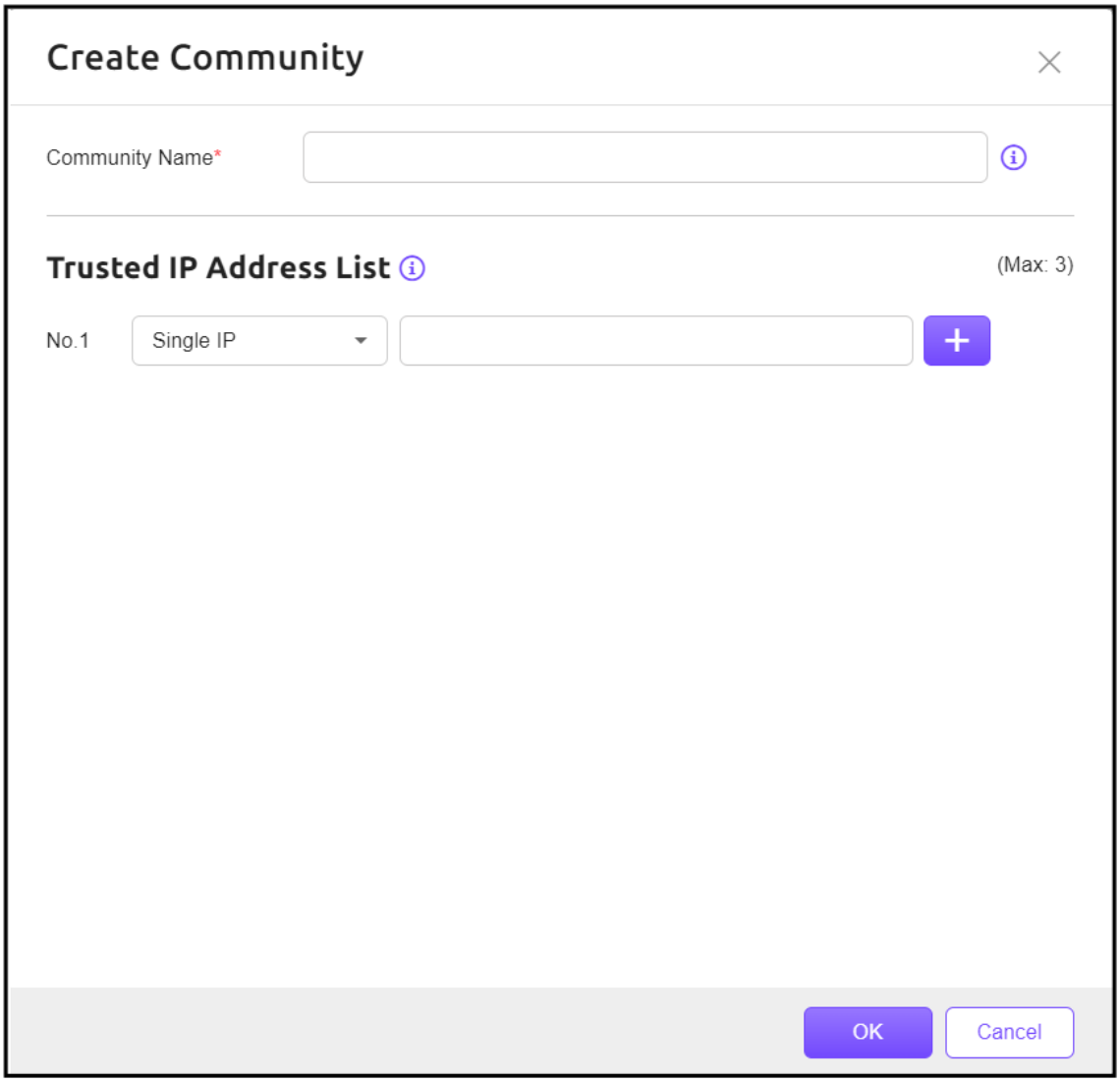


2. Under the [SNMP Settings] tab, enable the SNMP function by clicking the toggle.
3. In the [General Settings] pane, you can change the SNMP port. The default port is 161.
4. To download the Edge device MIB file, click the [Download MIB File] link.

11.2.1.2 Configuring SNMP v1/v2c Communities

Procedure

1. Go to [Admin] > [Notifications] > [SNMP]. Then switch to the [SNMP Settings] tab.
2. In the [SNMP v1/v2c Settings] pane, do one of the following.
   - Click [Create] to create an SNMP v1/v2c community. The [Create Community] window will appear.
   - Click an SNMP v1/v2c community name. The [Edit Community] window will appear.



3. Configure the following settings.

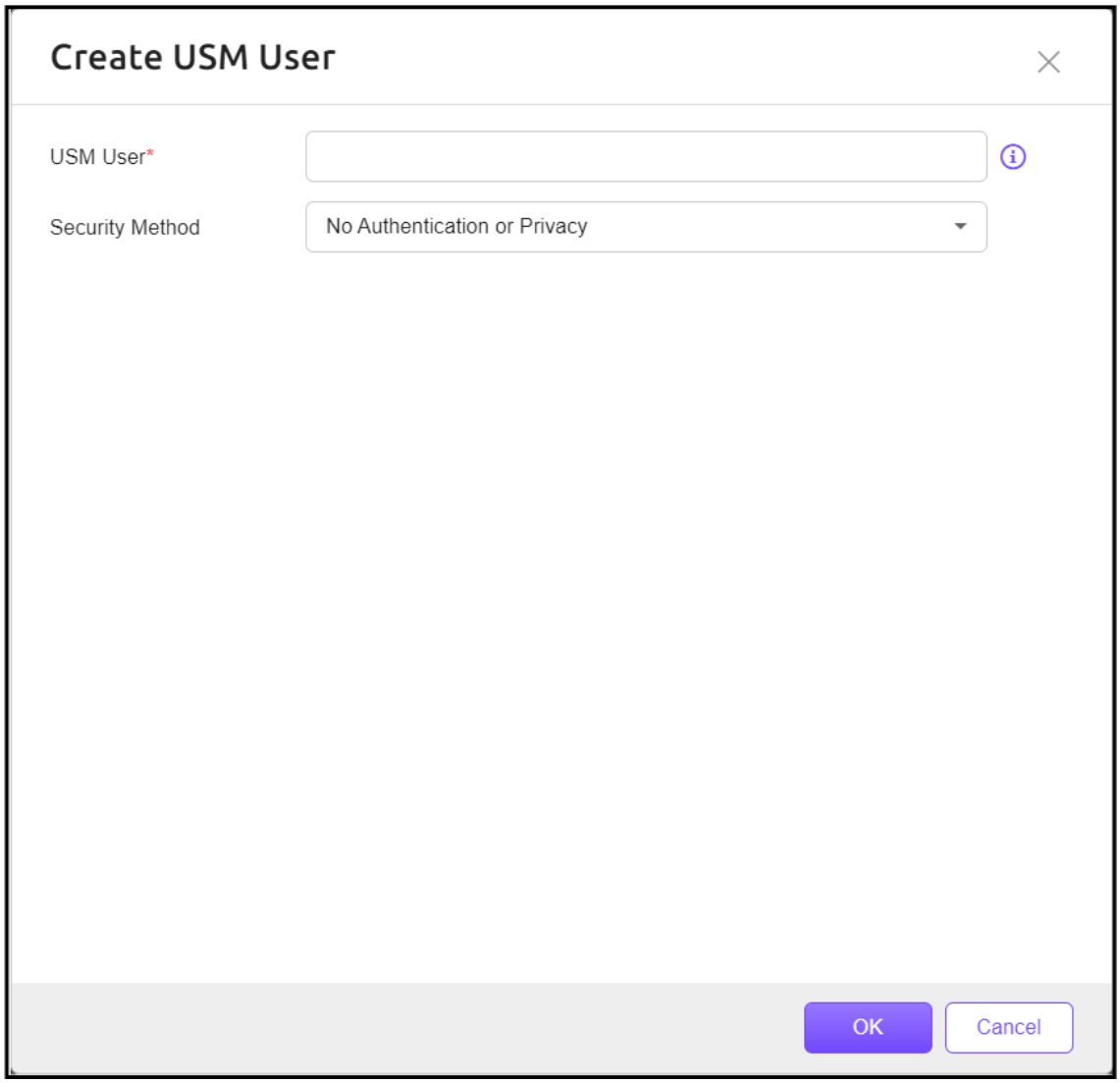
Item	Description
Community Name	Input an SNMP v1/v2c community name.
Trusted IP Address List	Specify an IP address or an IP subnet. Click the add button + to add another entry, or the remove button − to remove an entry.

4. Click [OK].
5. Click [Save] on the [SNMP] page.

11.2.1.3 Configuring SNMP v3 USM Users

Procedure

1. Go to [Admin] > [Notifications] > [SNMP]. Then switch to the [SNMP Settings] tab.
2. In the [SNMP v3 Settings] pane, do one of the following.
   - Click [Create] to create an SNMP v3 USM user. The [Create USM User] window will appear.
   - Click an SNMP v3 USM username. The [Edit USM User] window will appear.



3. Configure the following settings.

Item	Description
USM User	Input an SNMP v3 USM username.
Security Method	Select one of the following options. • **No Authentication or Privacy**

Item	Description
	• **Authentication without Privacy**: Further select an appropriate authentication protocol (SHA or MD5) and enter an authentication key. • **Authentication with Privacy**: Further select an appropriate authentication protocol (SHA or MD5), enter an authentication key, select an appropriate privacy protocol (AES or DES), and enter a privacy key.

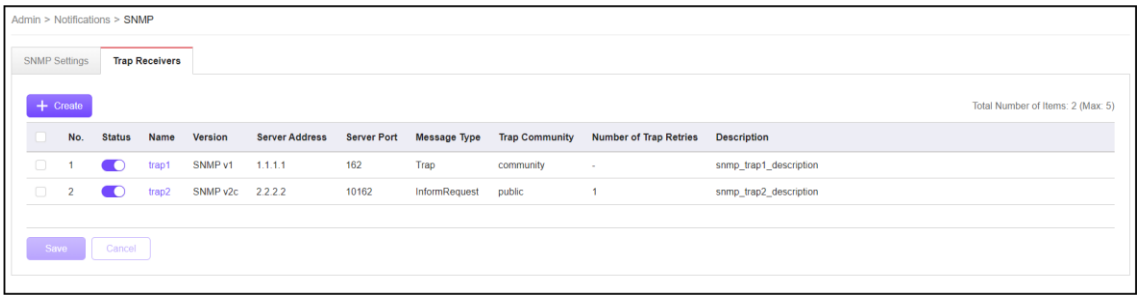
4. Click [OK].

5. Click [Save] on the [SNMP] page.

11.2.1.4 Configuring SNMP Trap Receivers

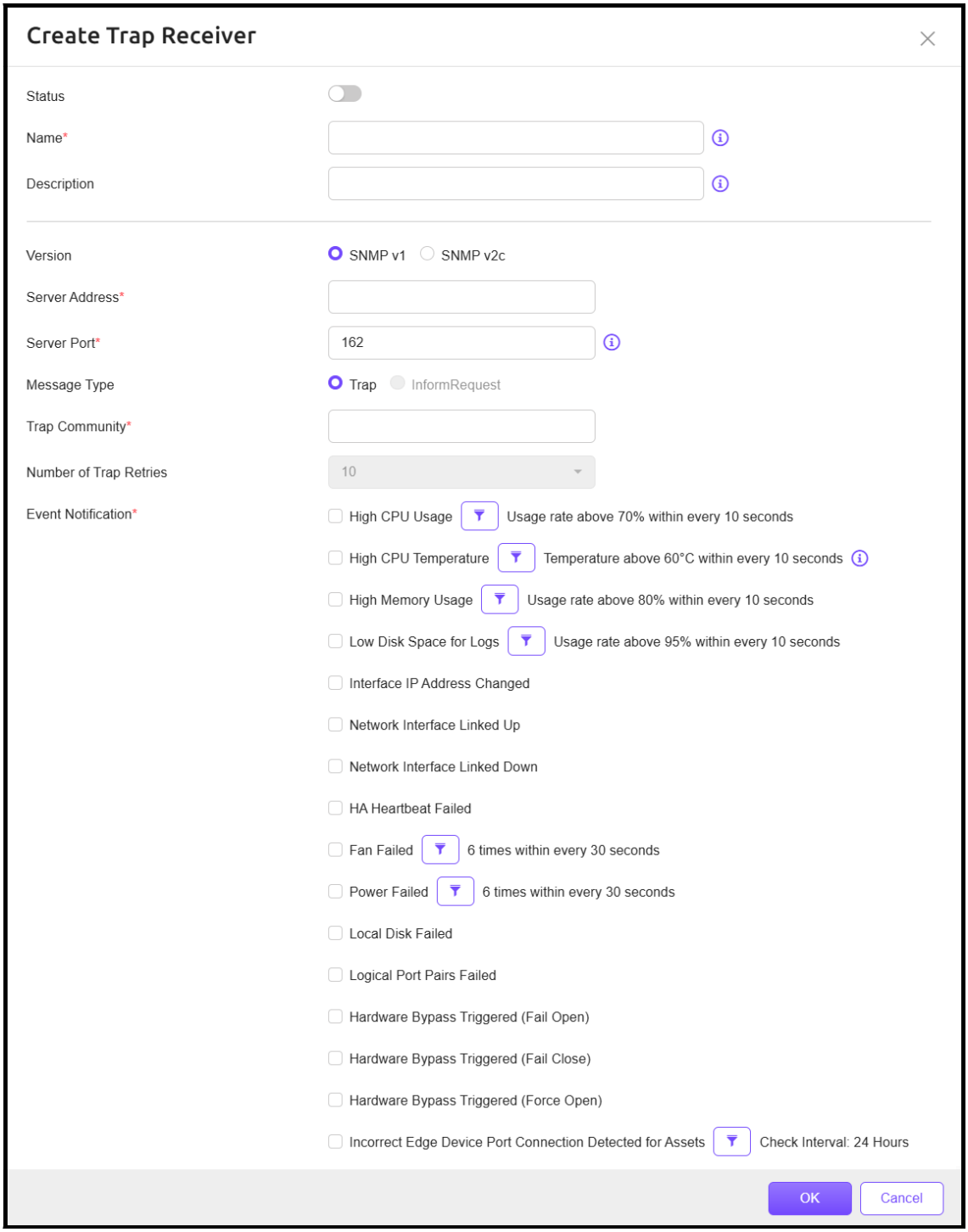
Procedure

1. Go to [Admin] > [Notifications] > [SNMP].



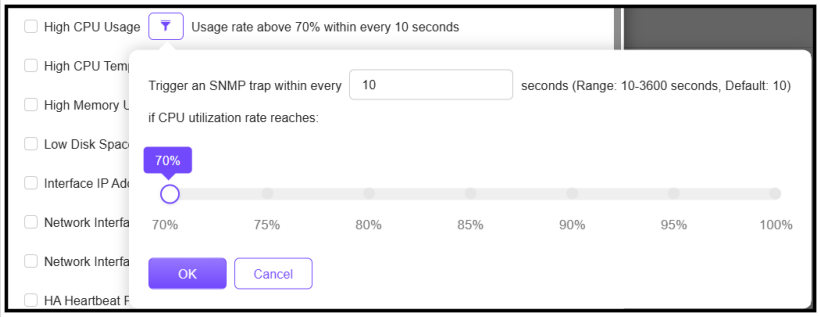
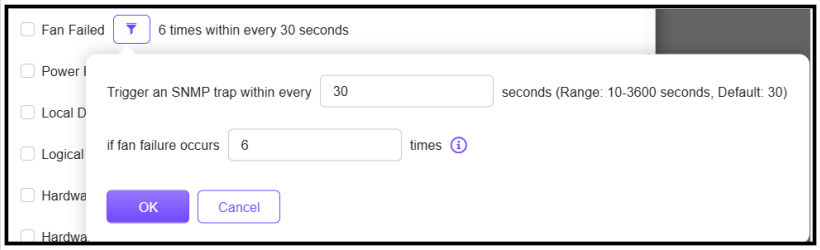
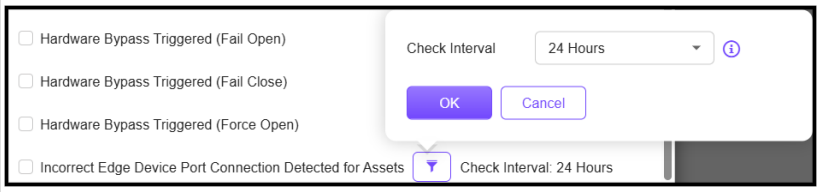
2. Under the [Trap Receivers] tab, do one of the following.

   - Click [Create] to create a new trap receiver. The [Create Trap Receiver] window will appear.
   - Click a trap receiver item. The [Edit Trap Receiver] window will appear.



3. Configure the following trap receiver settings.

Item	Description
Status	Enable this trap receiver by clicking the toggle.
Name	Type a name for this trap receiver.
Description	(Optional) Type a description.
Version	Select an SNMP version, **SNMP v1** or **SNMP v2c**.
Server Address	Input a server IP address.

Item	Description
Server Port	Input a server port. The default server port is 162.
Message Type	Select a message type, **Trap** or **informRequest**.
Trap Community	Input a trap community name. The default name is PUBLIC.
Number of Trap Retries	Set the number of trap retries ranging from 1 to 10.
Event Notification	Select what will trigger an event notification. For [High CPU Usage], [High CPU Temperature], [High Memory Usage], [Low Disk Space for Logs], [Fan Failed], [Power Failed], and [Incorrect Edge Device Port Connection Detected for Assets], click the button to adjust the threshold for triggering the notification and check interval.   

4. Click [OK].
5. Click [Save] on the [SNMP] page.

11.2.2 Syslog

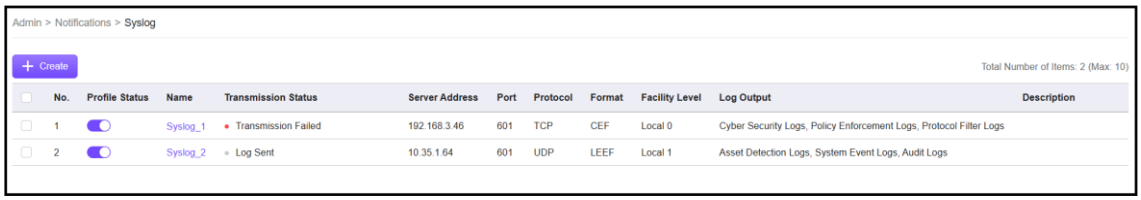
The system of this Edge series device maintains Syslog events that provide summaries of security and system events. Common Event Format (CEF) and Log Event Extended Format (LEEF) syslog messages are used in the device.

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

11.2.2.1 Configuring Syslog Settings

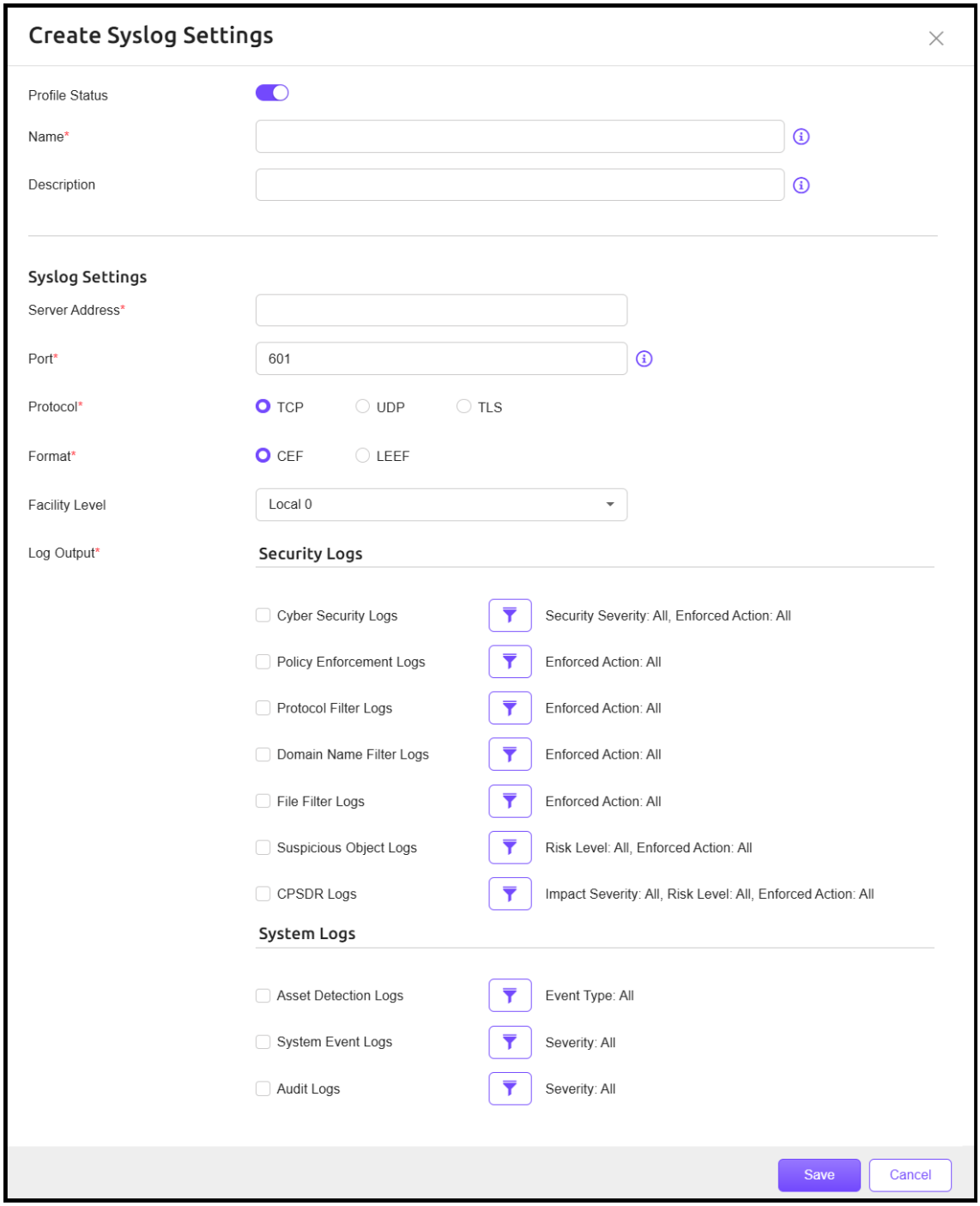
Procedure

1. Go to [Admin] > [Notifications] > [Syslog].



2. Do one of the following.

- Click [Create] to create a Syslog profile. The [Create Syslog Settings] window will appear.
- Click a profile name to edit settings. The [Edit Syslog Settings] window will appear.



3. Configure the following settings.

Field	Description
Profile Status	Click the toggle to enable the Syslog settings configured in this profile.
Name	Type a name for this Syslog profile.
Description	(Optional) Type a description.

- Syslog Settings

Field	Description
Server Address	Type the IP address of the Syslog server.
Port	Type the port number.
Protocol	Select a protocol for the communication.
Format	Select a syslog format, either CEF or LEEF.
Facility Level	Select a facility level to determine the source and priority of the logs.
Log Output	Select the types of logs to send. To configure detailed log filter settings for log output, click the button. For Cyber Security, Suspicious Object, and CPSDR logs, you can configure the severity/risk levels of the output logs. For more information about Syslog severity and risk levels, see Syslog Severity Levels.

1. Click [Save].

11.2.2.2 Syslog Severity Levels

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

Level	Severity	Description
0	Emergency	Complete system failure Take immediate action.
1	Alert	Primary system failure Take immediate action.
2	Critical	Urgent failure Take immediate action.
3	Error	Non-urgent failure Resolve issues quickly.
4	Warning	Error pending Take action to avoid errors.
5	Notice	Unusual events Immediate action is not required.
6	Informational	Normal operational messages useful for reporting, measuring throughput, and other purposes

Level	Severity	Description
		No action is required.
7	Debugging	Useful information when debugging the application. ⚠ Setting the debugging level can lead to a large amount of Syslog traffic in a busy network. Use with caution.

11.2.2.3 Syslog Severity Level Mapping Table

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

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

11.3 Licensing & Updates

Manage product licenses and firmware updates.

- License Management
- Firmware Updates & Management

11.3.1 License Management

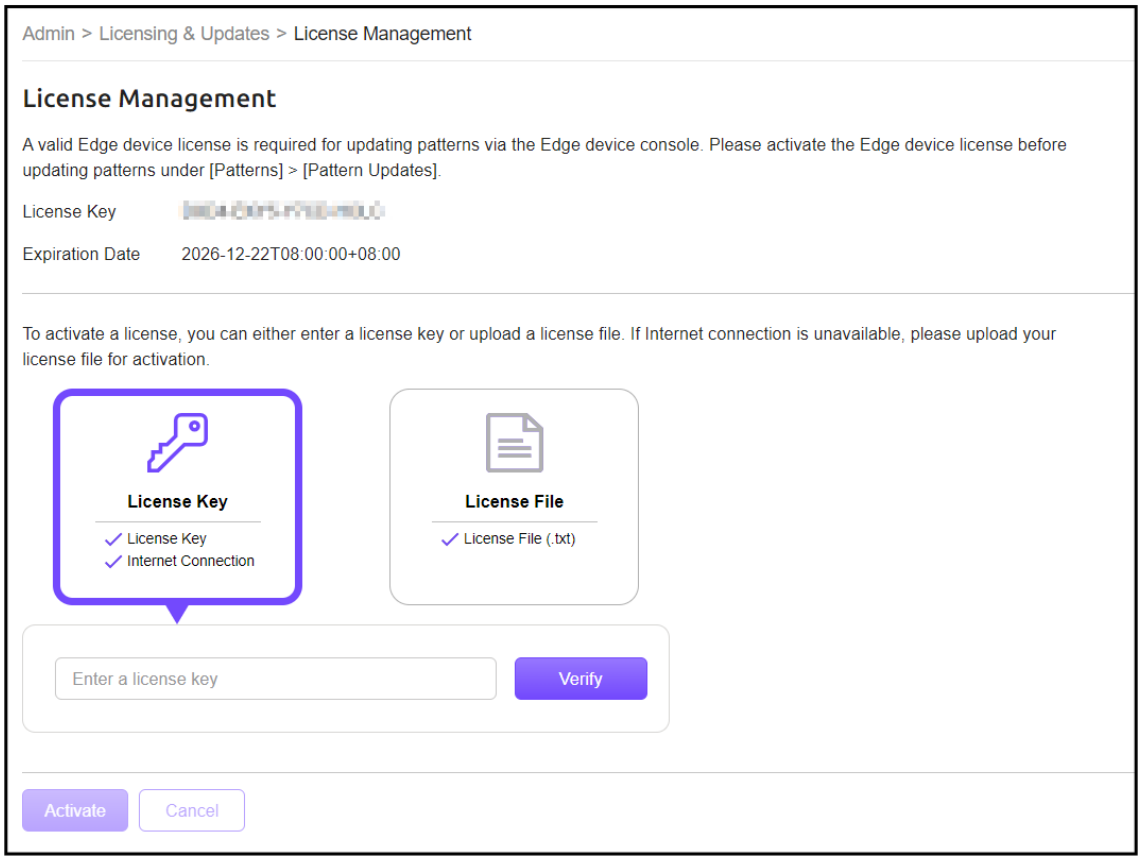
To fully access all functionalities of the Edge device, including pattern updates, you must first activate a valid Edge device software license. On the [License Management] page, you can activate your Edge device license using either a license key or a license file, and view detailed information about your license.

To activate a license, you can either enter a license key or upload a license file. If an Internet connection is unavailable, please upload your license file for activation.

11.3.1.1 Viewing License Information

Procedure

1. Go to [Admin] > [Licensing & Updates] > [License Management].

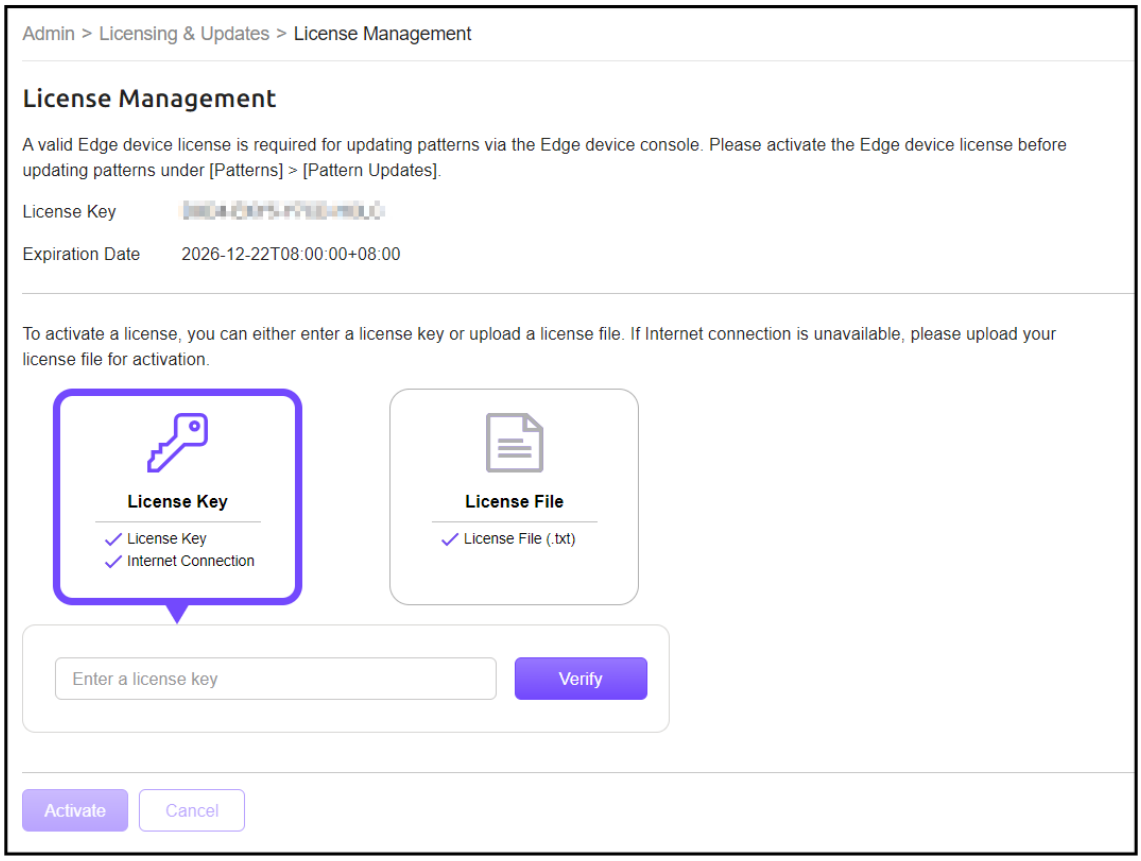


2. On the [License Management] page, you will see the license key and expiration date of the activated license.

11.3.1.2 Activating/Renewing License with License Key

Procedure

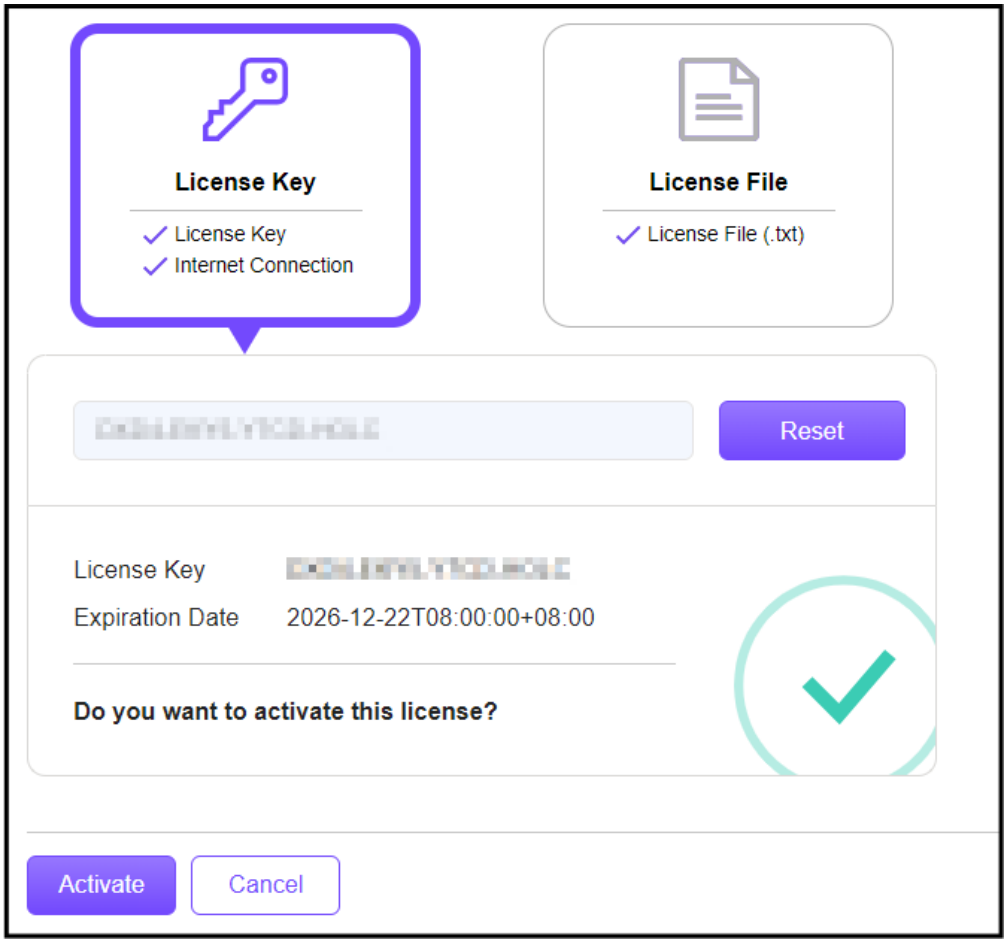
1. Go to [Admin] > [Licensing & Updates] > [License Management].



2. Select [License Key] and input a valid Edge device license key.

3. Click [Verify].

4. Verify the license information shown and click [Activate].

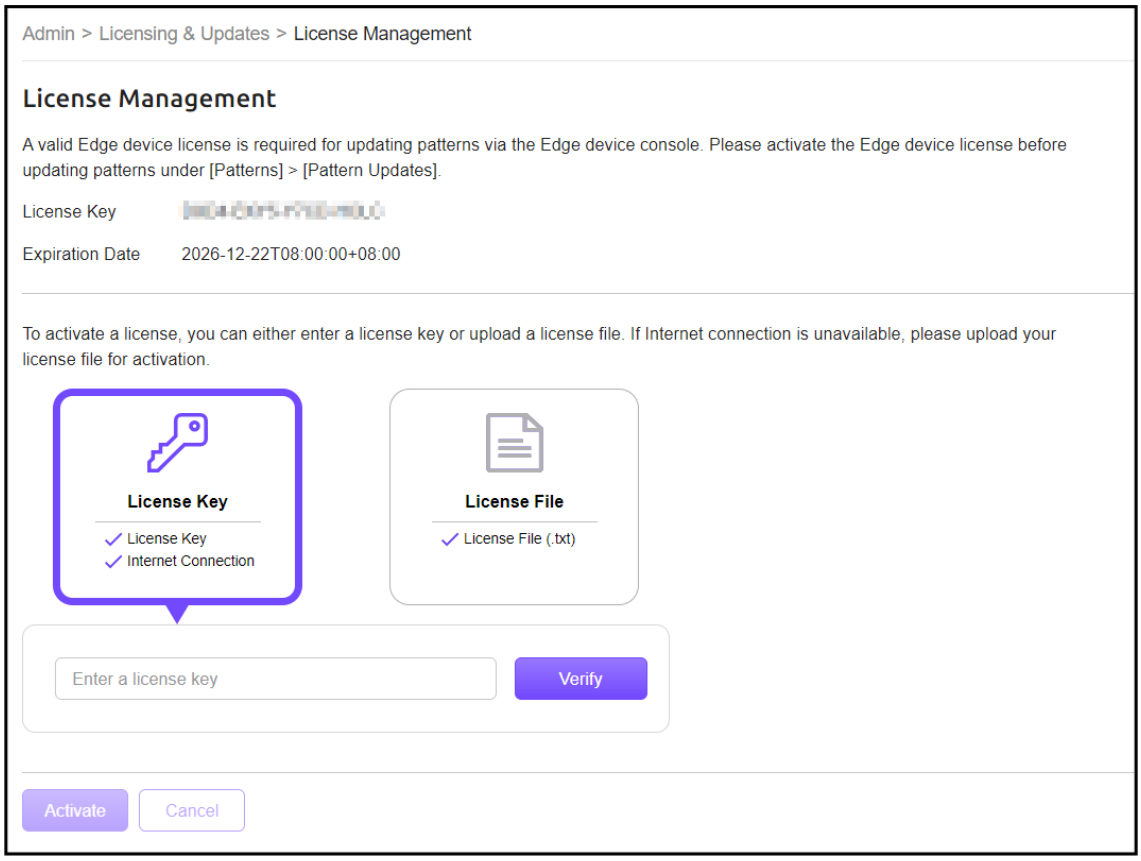


Internet connectivity is required for activating/renewing a license using a license key.

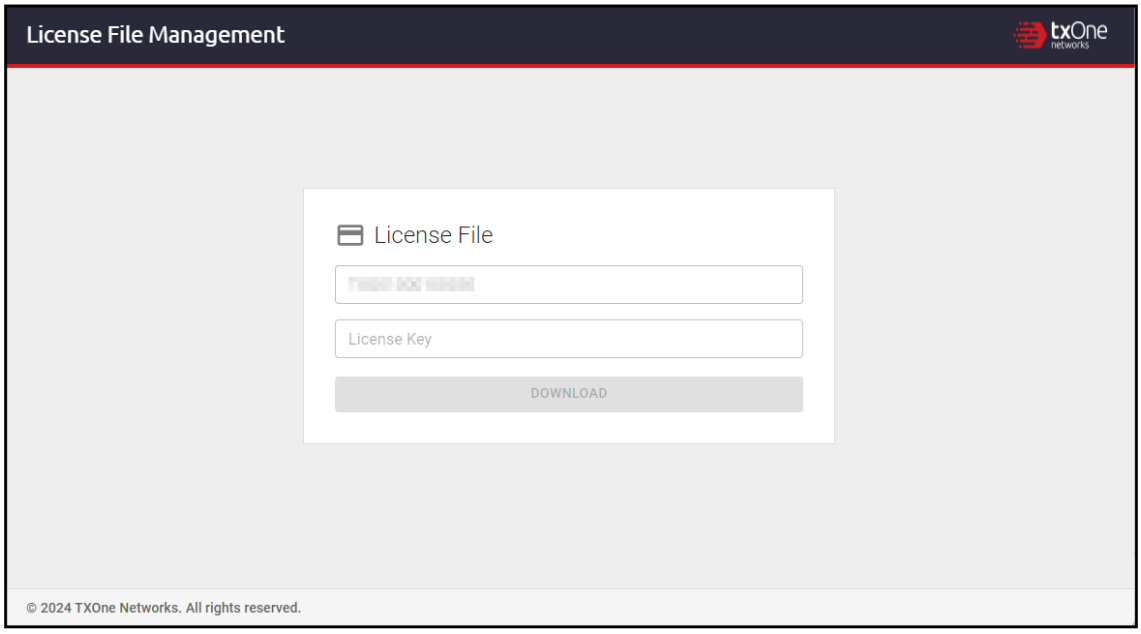
11.3.1.3 Activating/Renewing License with License File

Procedure

1. Go to [Admin] > [Licensing & Updates] > [License Management].



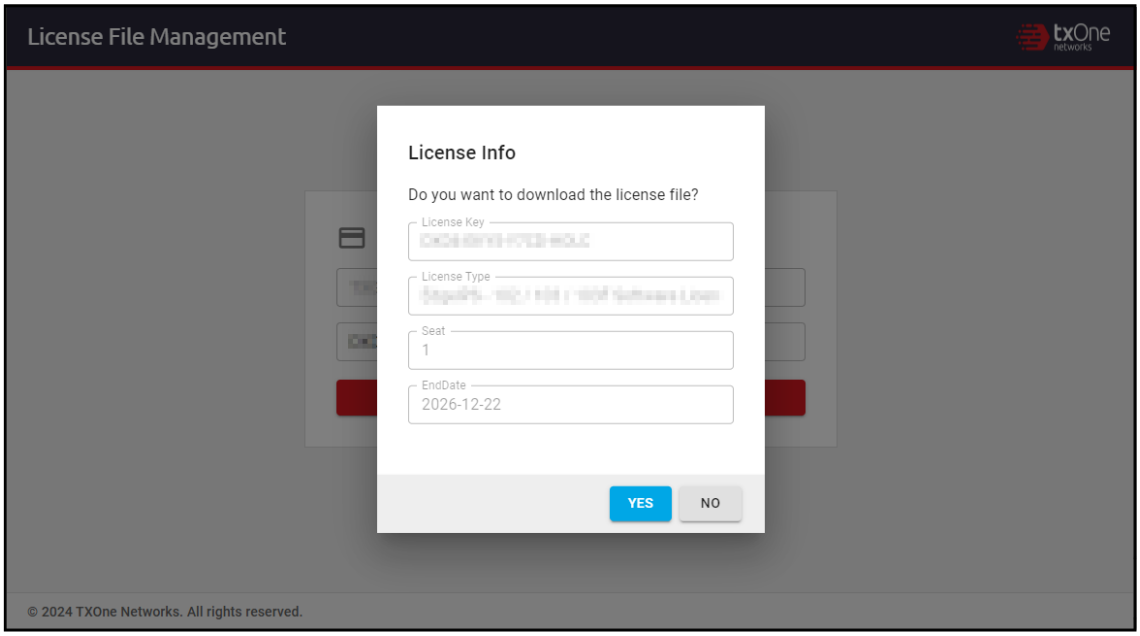
2. Select [License File], and then click [Get License File] to connect to the TXOne License File Management server. (This step requires an Internet connection.)



1. The Edge device serial number is provided on the license file management server.
2. If you do not have an Internet connection, you can click [Copy Download Link] to copy the link of the TXOne License File Management server, and then open the link to download the license file when your Internet connection is restored. The

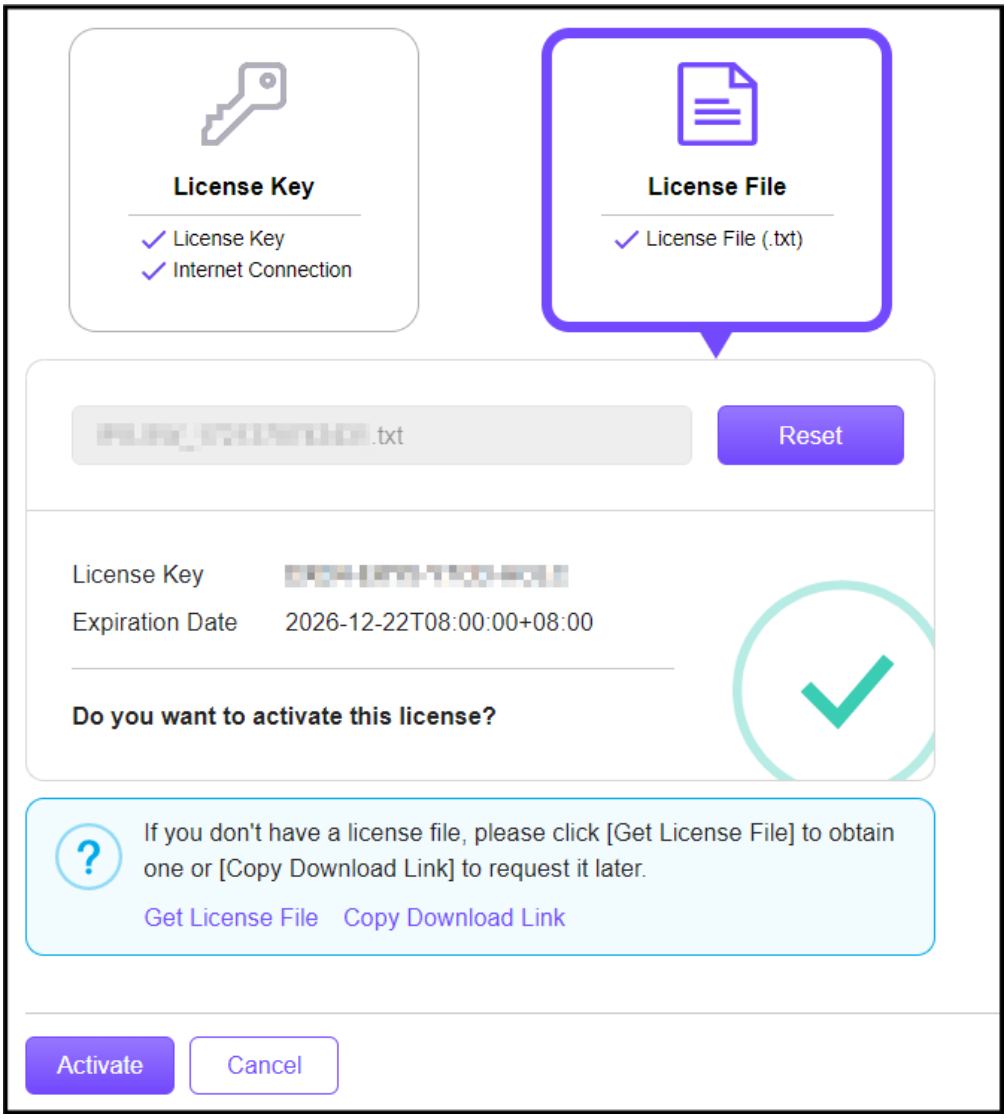
	license file generated by the download link is only valid when it is applied to the same Edge device from which the link was generated.

3. Input your license key to download your license file.



4. Go back to the [License Management] page, and then click [Select File] to upload your license file.

5. Verify the license information shown and click [Activate].



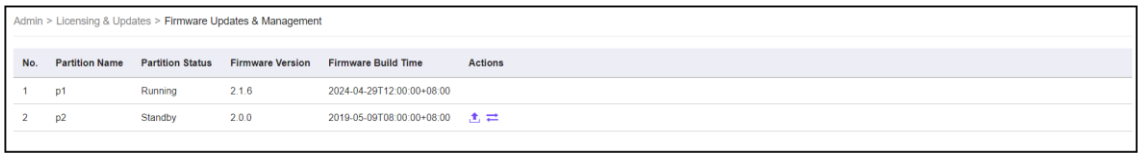
11.3.2 Firmware Updates & Management

On the [Firmware Updates & Management] page, you can view the device firmware information, update the device firmware, and switch to the standby firmware.

11.3.2.1 Viewing Device Firmware Information

Procedure

1. Go to [Admin] > [Licensing & Updates] > [Firmware Updates & Management].



Admin > Licensing & Updates > Firmware Updates & Management

No.	Partition Name	Partition Status	Firmware Version	Firmware Build Time	Actions
1	p1	Running	2.1.6	2024-04-29T12:00:00+08:00	
2	p2	Standby	2.0.0	2019-05-09T08:00:00+08:00	

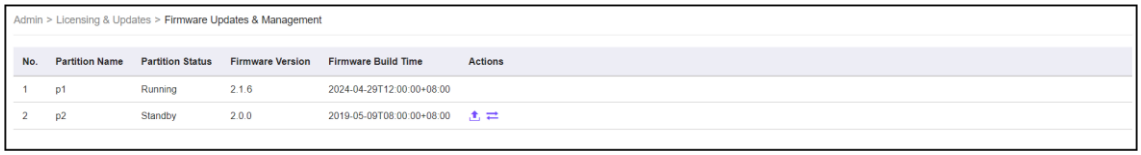
2. The table on this page lists the two available firmware partitions and shows information including the partition name, partition status, firmware version, and firmware build time.

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

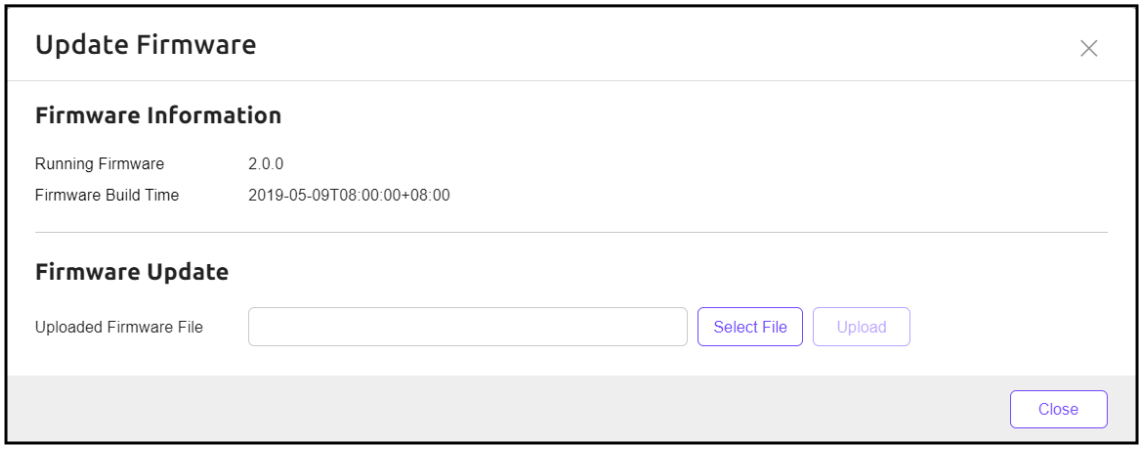
11.3.2.2 Updating Device Firmware

Procedure

1. Go to [Admin] > [Licensing & Updates] > [Firmware Updates & Management].



2. Click the [Update Firmware] button to install firmware to the [Standby] partition. The [Update Firmware] window will appear.



> During a firmware update, firmware will always be installed to the [Standby] partition. As such, the [Update Firmware] button is only available in the [Standby] partition row.

3. On the [Update Firmware] window, click [Select File] to select a firmware file from your local device, and then click [Upload] to install the firmware to the standby partition.

4. Click [Close].

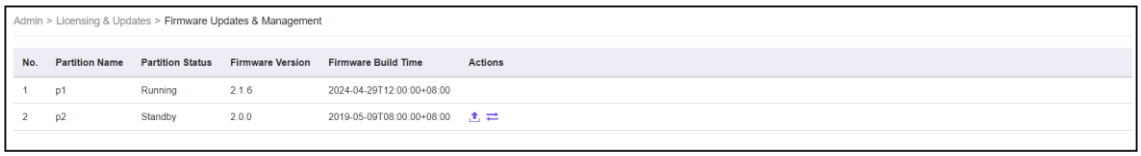
> Various versions of the firmware files can be downloaded at the MyTXOne portal at https://my.txone.com/.

11.3.2.3 Switching to Standby Firmware

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

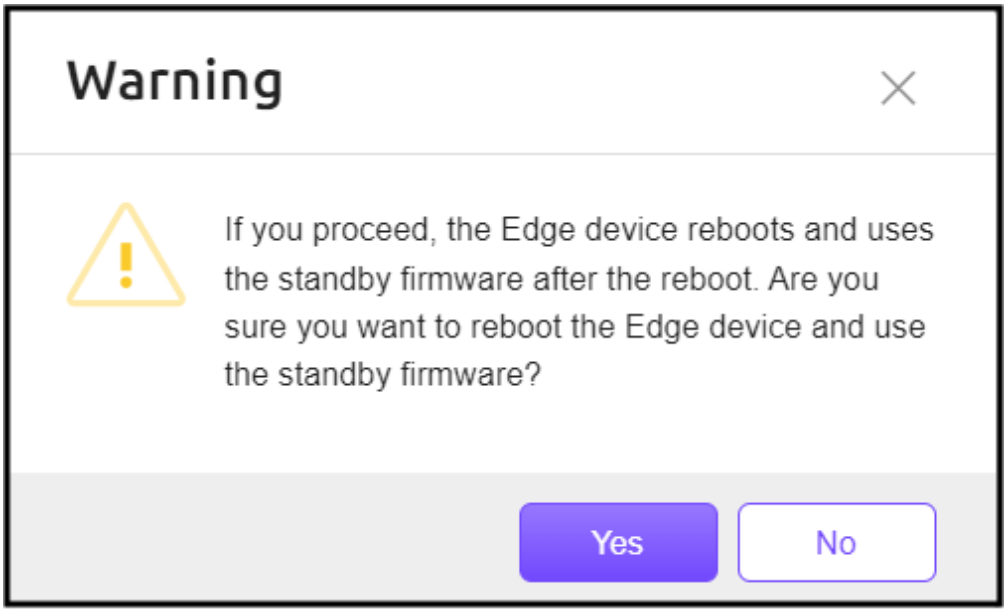
Procedure

1. Go to [Admin] > [Licensing & Updates] > [Firmware Updates & Management].



2. Click the [Switch to Standby Firmware] button in the [Standby] partition row.

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



11.4 System

Configure administrative settings to optimize device operations.

- System Management
- Edge Device Security
- EdgeOne Connection Settings
- Language Package
- API Management
- SSL Certificate
- Backup/Restore
- System Time
- System Reboot

11.4.1 System Management

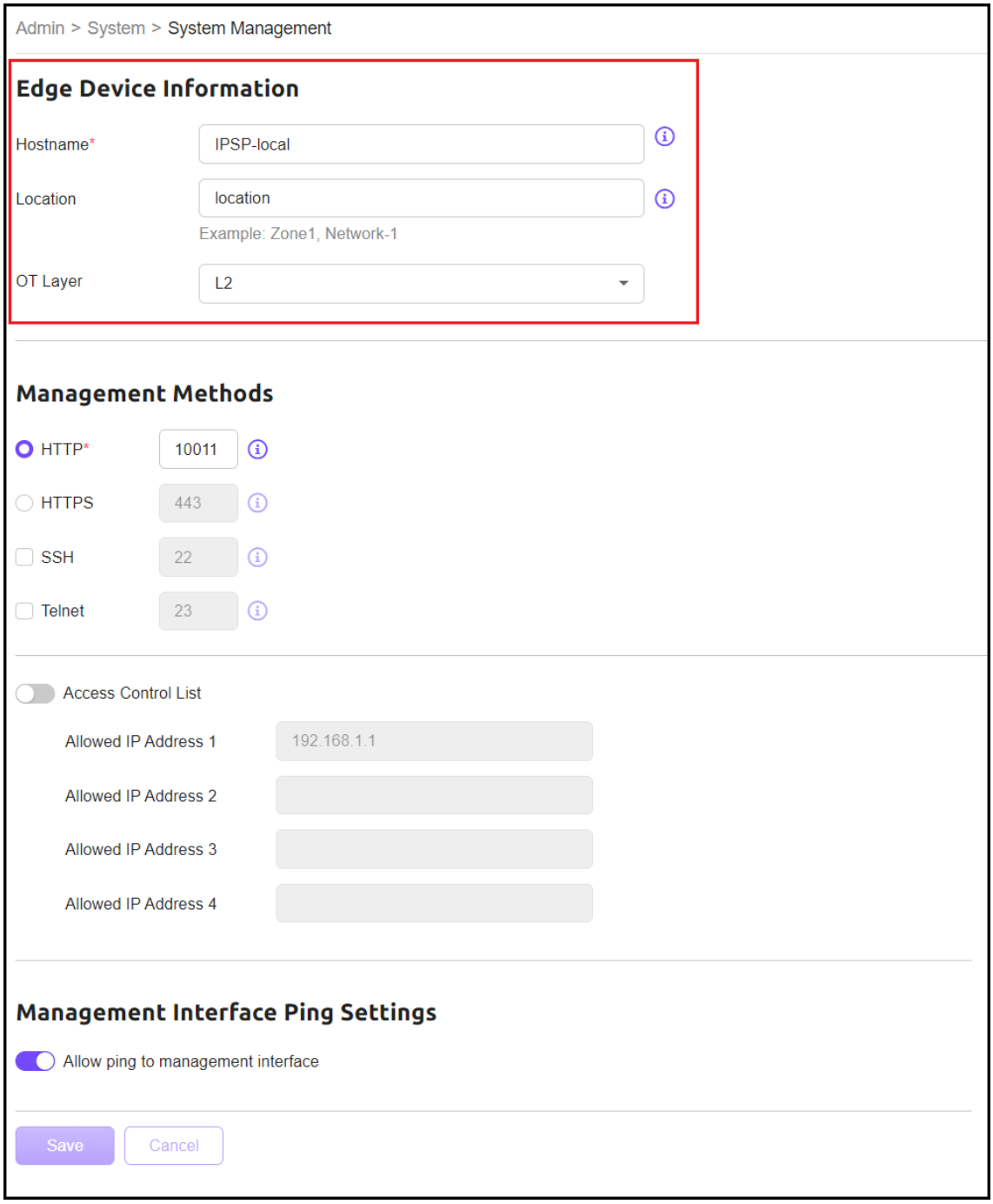
On the [System Management] page, you can do the following:

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

11.4.1.1 Configuring Device Hostname and Location

Procedure

1. Go to [Admin] > [System] > [System Management].



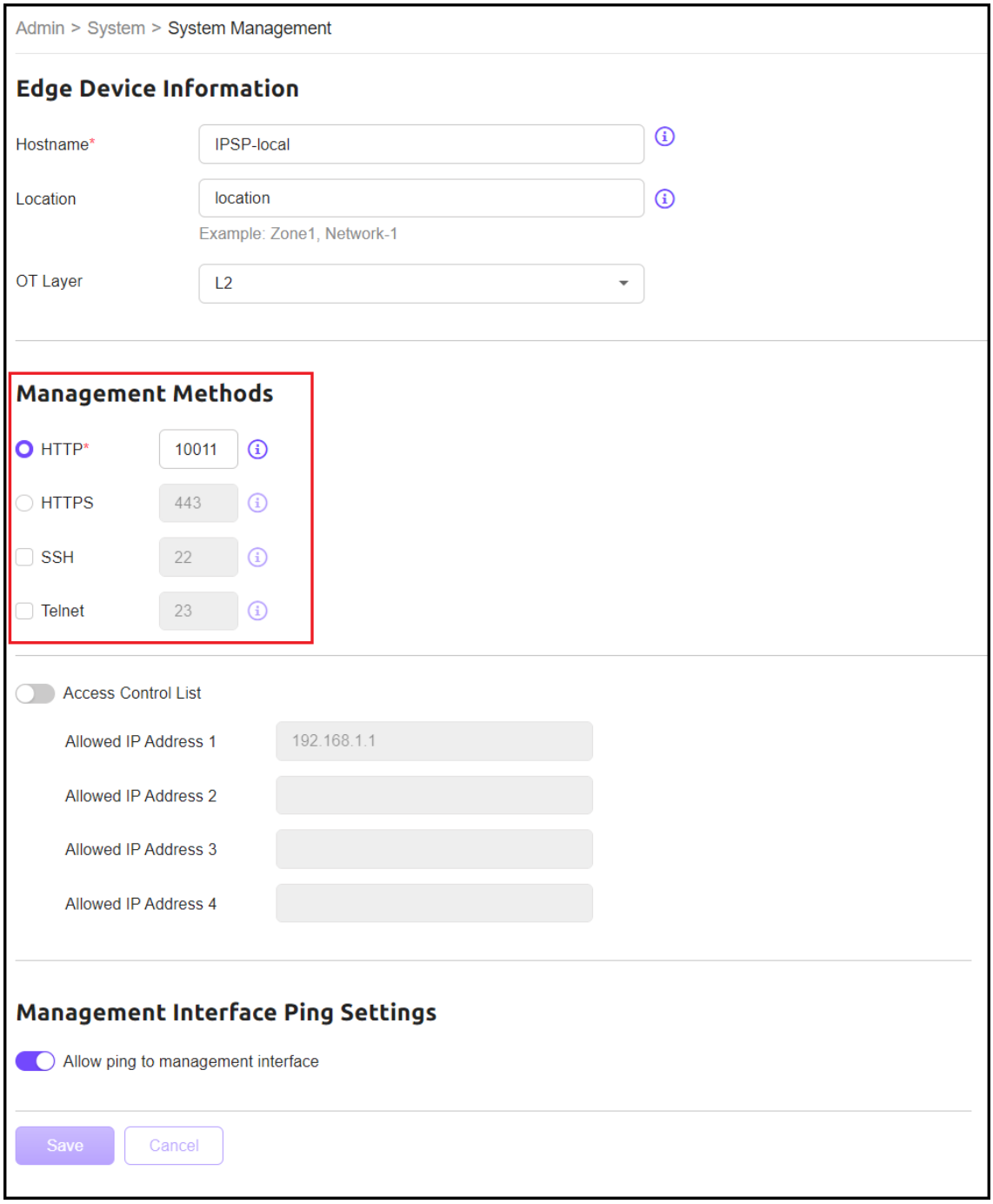
2. In the [Edge Device Information] pane, input a hostname and location, and select an OT layer for the device.

3. Click [Save].

11.4.1.2 Configuring Management Protocols and Ports

Procedure

1. Go to [Admin] > [System] > [System Management].



2. In the [Management Methods] pane:

- Select the protocols that are allowed to be used.
- Input port numbers for the protocols.

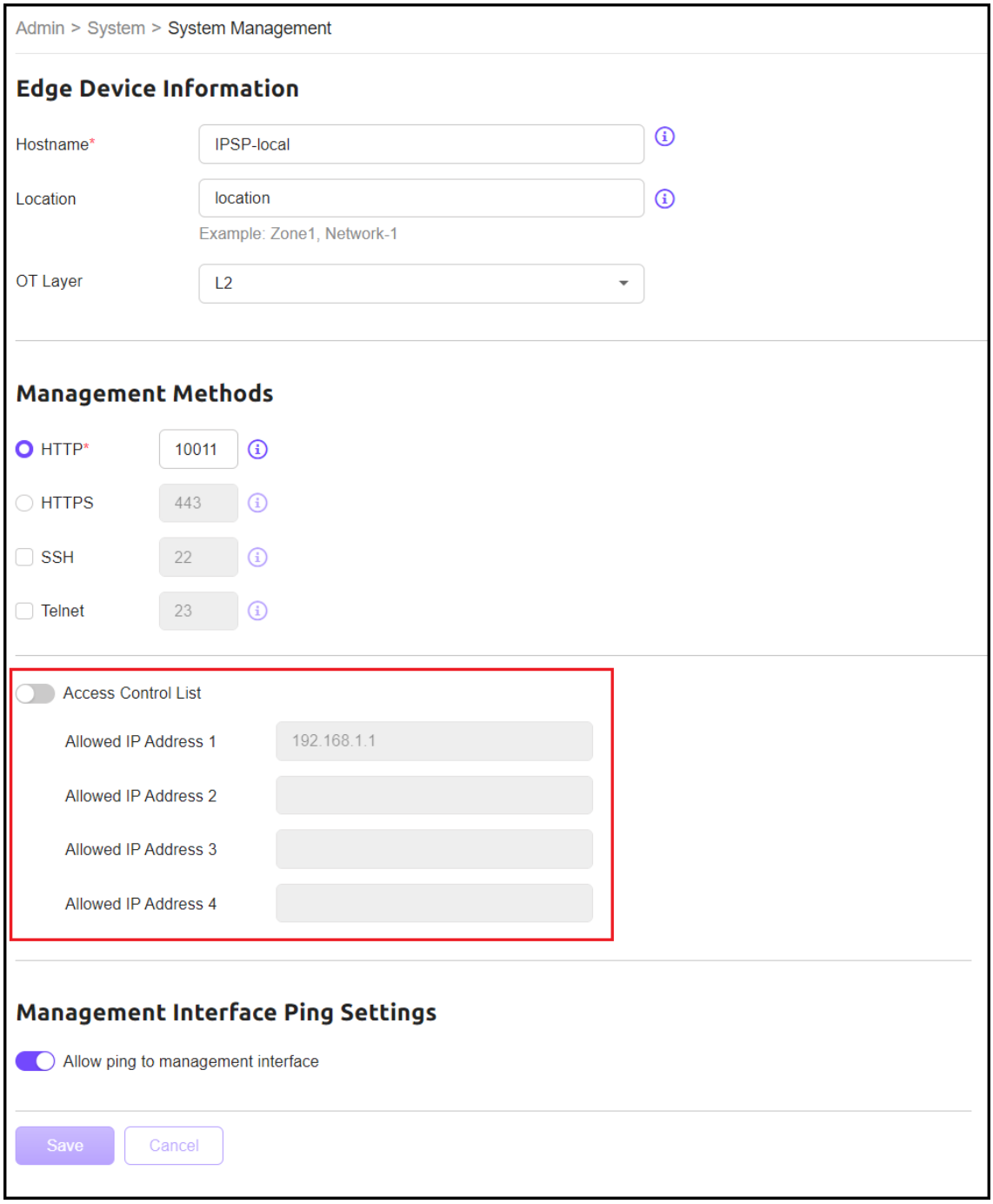
📝	The HTTP and HTTPS protocols are used for connecting to the web management console. The SSH and Telnet protocols are used for connecting to the CLI commands.

3. Click [Save].

11.4.1.3 Configuring Access Control List

Procedure

1. Go to [Admin] > [System] > [System Management].



2. Click the [Access Control List] toggle to enable or disable access control of the management clients.

3. List the IP addresses that are allowed for accessing the device.

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

5. Click [Save].

11.4.2 Edge Device Security

The feature, Edge Device Security, is used to protect the Edge device itself against file vulnerabilities, buffer overflow, denial of service attacks, exploits, etc. by applying pre-defined IPS profiles and configuring the thresholds of the denial of service rules.

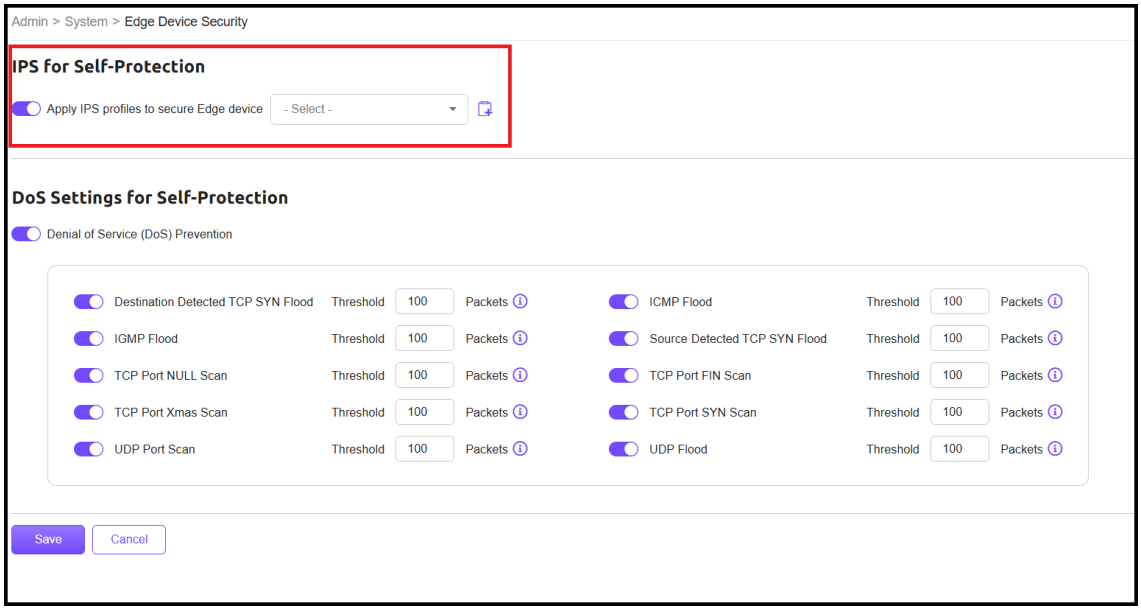
11.4.2.1 Applying IPS Profile for Self-Protection

Procedure

1. Configure the required IPS profile.

> For more information, see Configuring IPS Profiles.

2. Go to [Admin] > [System] > [Edge Device Security].



3. In the [IPS for Self-Protection] pane, enable [Apply IPS profiles to secure Edge device] by clicking the toggle.

4. Select an IPS profile from the drop-down list or click the button to create a profile.

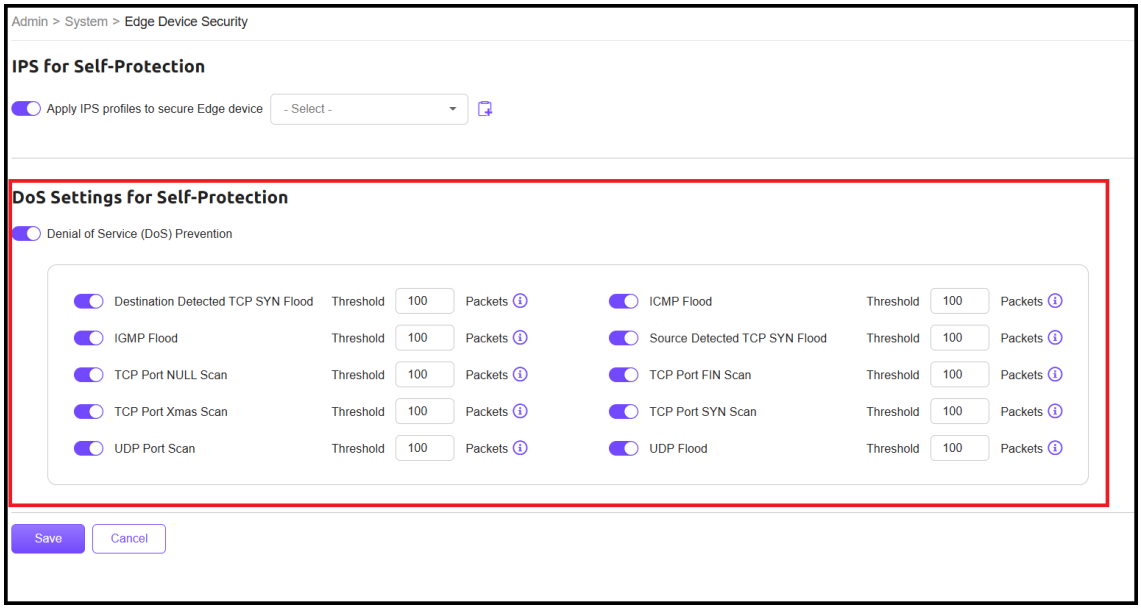
5. Click [Save].

11.4.2.2 Configuring DoS Prevention for Self-Protection

Procedure

1. Go to [Admin] > [System] > [Edge Device Security].

2. In the [DoS Settings for Self-Protection] pane, enable the [Denial of Service (DoS) Prevention] function by clicking the toggle.



3. Configure the thresholds of the denial of service rules.

> The [Source Detected TCP SYN Flood] option is applicable to only Edge devices running firmware 2.2 or later.

4. Click [Save].

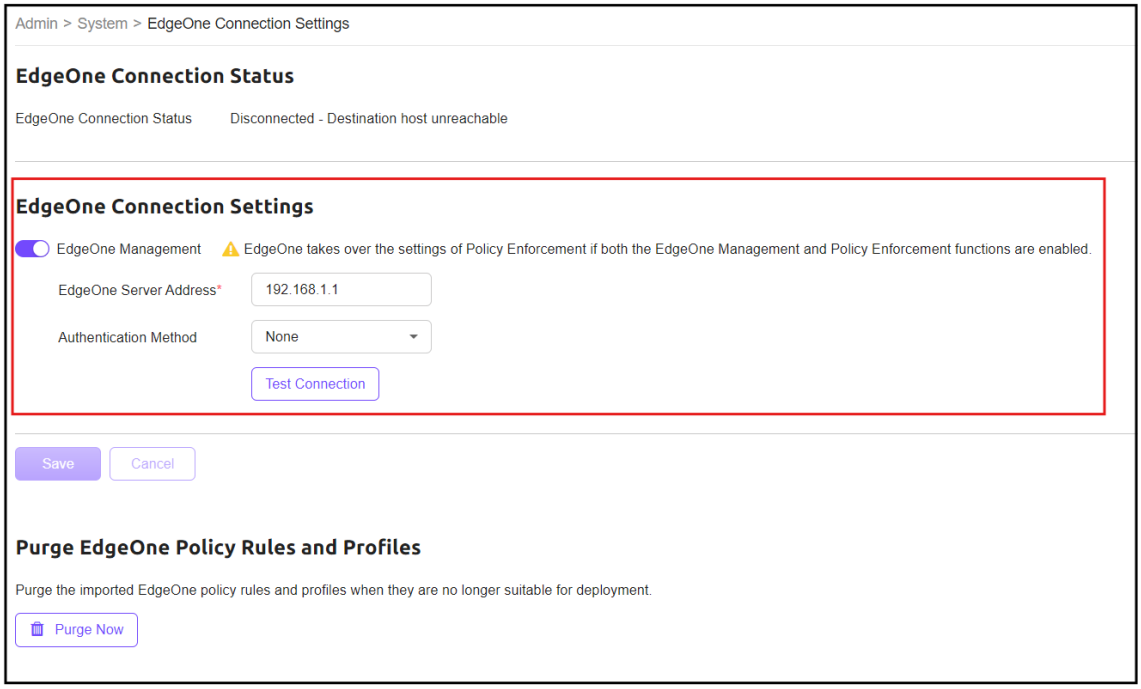
11.4.3 EdgeOne Connection Settings

This Edge series device can be managed by TXOne EdgeOne, a centralized management system. Use this tab to register your device to EdgeOne.

11.4.3.1 Enabling EdgeOne Management

Procedure

1. Go to [Admin] > [System] > [EdgeOne Connection Settings].



2. In the [EdgeOne Connection Settings] pane, enable [EdgeOne Management] by clicking the toggle.

3. Configure the following connection settings.

Item	Description
EdgeOne Server Address	Input the IP address of the EdgeOne server.
Authentication Method	Select **None** or **Passcode** from the drop-down list. To test connectivity between the Edge device and EdgeOne, click the [Test Connection] button. If you have selected passcode as the authentication method in the EdgeOne system, please select "Passcode" as the authentication method here accordingly and input the passcode specified in the EdgeOne system for onboarding. The passcode is used only for first-time onboarding to EdgeOne.

4. Click [Save].

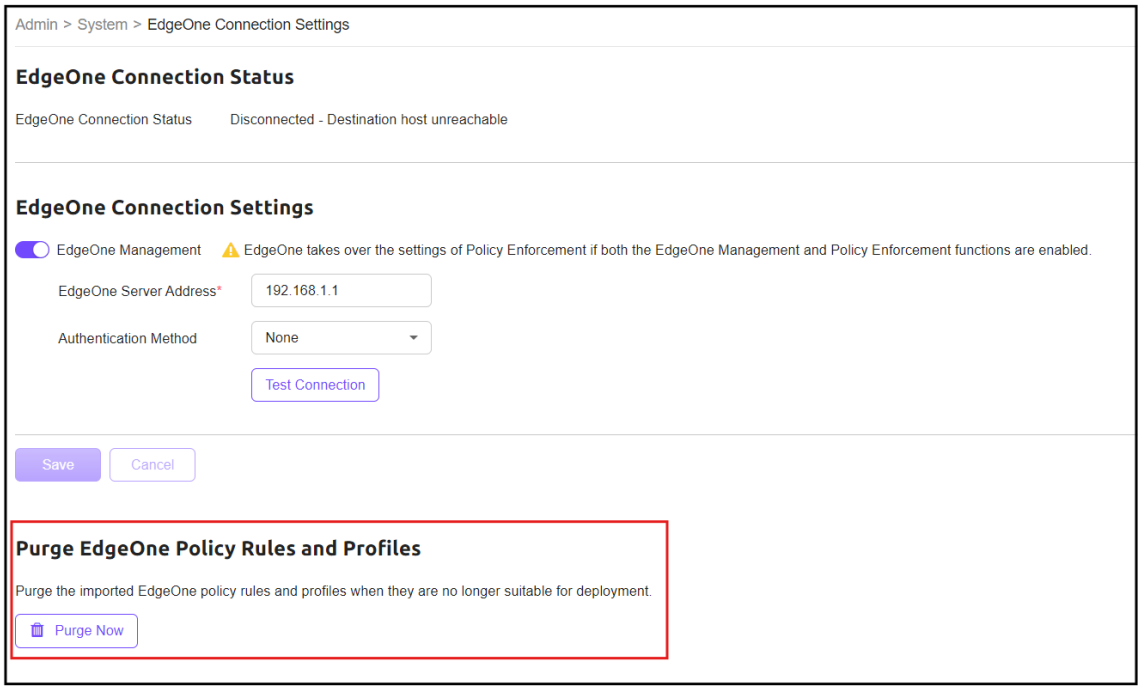
The following settings/functions cannot be configured/performed on the device management console when the Edge device is connected to EdgeOne.

- Cyber Security
- Policy Enforcement
- Packet Capture
- File Exclusion
- Suspicious Objects
- Pattern Update
- EdgeOne Rule & Profile Deletion

11.4.3.2 Purging EdgeOne Policy Rules and Profiles

Procedure

1. Go to [Admin] > [System] > [EdgeOne Connection Settings].



2. In the [Purge EdgeOne Policy Rules and Profiles] pane, click the [Purge Now] button to delete objects, profiles, and Policy Enforcement rules synced from EdgeOne.

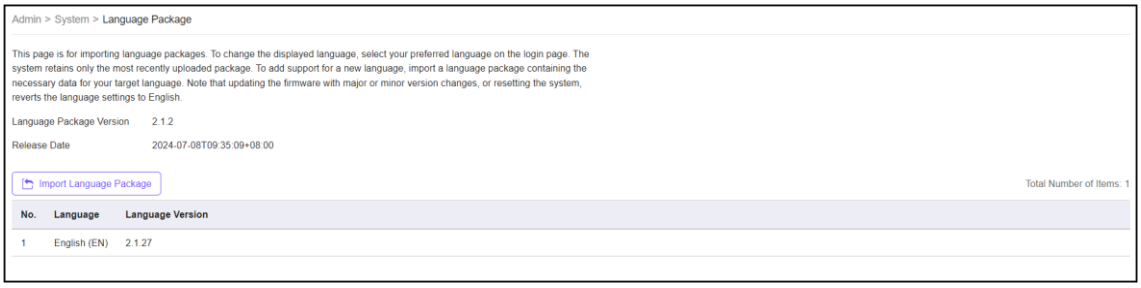
11.4.4 Language Package

You can import language packages on the [Language Package] page. To change the displayed language, select your preferred language on the login page. The system retains only the most recently uploaded package. To add support for a new language, import a language package containing the necessary data for your target language. Note that updating the firmware with major or minor version changes, or resetting the system, reverts the language settings to English.

11.4.4.1 Importing Language Packages

Procedure

1. Go to [Admin] > [System] > [Language Package].



2. Click [Import Language Package] and select a language package file (ACF file) from your local disk. The [Import Language Package] window will appear.

3. Click [Import].

11.4.5 API Management

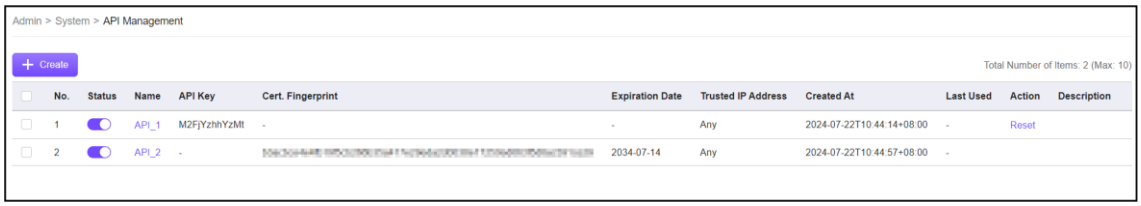
The API Key and API Secret are the software-level credentials for external systems to access the device via the RESTful APIs. It's a common practice to provide separate API Key/Secret for each API client. The API Key Management function allows the administrator to create and manage up to 10 API Keys.

> This API key management function is provided by request. To utilize this function, please contact local sales representative for more information.

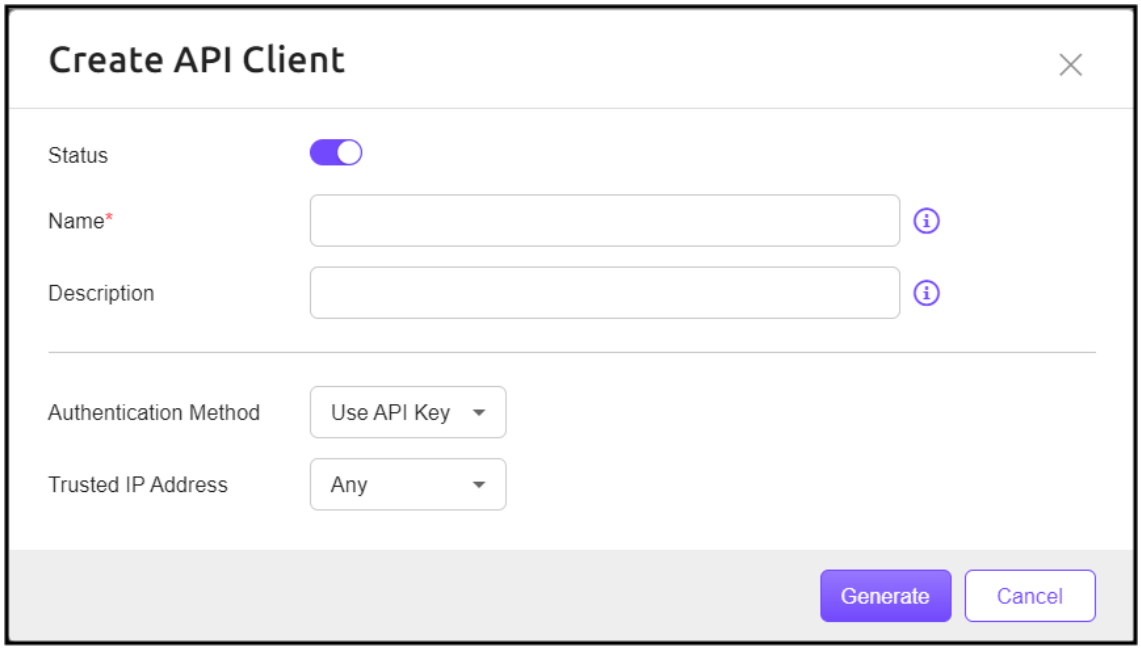
11.4.5.1 Creating API Clients

Procedure

1. Go to [Admin] > [System] > [API Management].



2. Click the [Create] button to create a new API client.

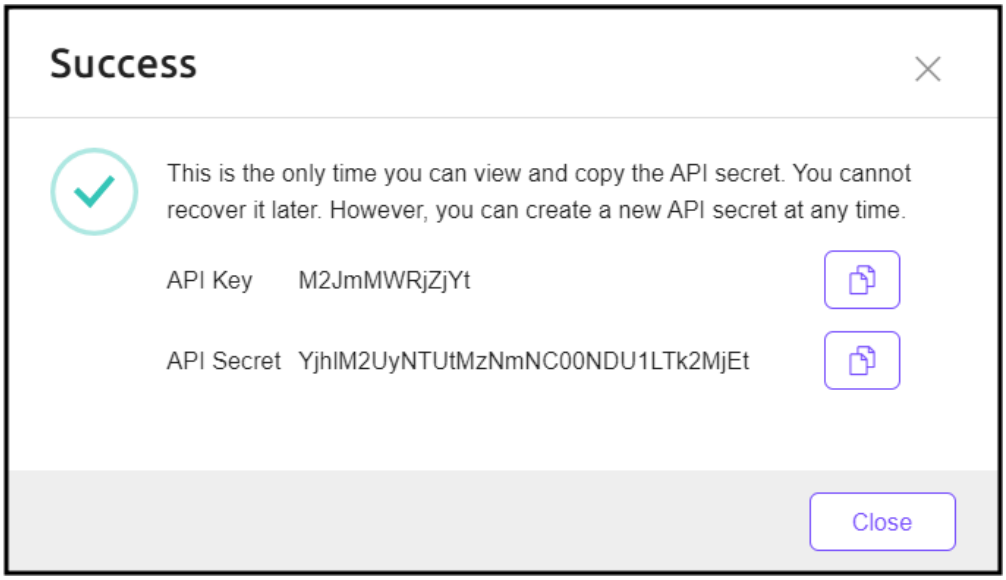


3. Configure the following settings.

Item	Description
Status	Click the toggle to enable this API client.
Name	Type a name for this API client profile.
Description	(Optional) Type a description.
Authentication Method	Select an authentication method for accessing this API client, either **Use API Key** or **Use Certificate**. • **Use API Key**: Authenticate using a randomly generated API key and secret. • **Use Certificate**: Authenticate using a user-defined authentication credential embedded within a certificate. If this option is selected, click [Upload] to import a certificate from your local disk.
Trusted IP Address	Select **Any** or **Custom**. If you select **Custom**, specify an IP address. The system will reject API requests if the client's IP address does not match the given trusted IP address.

4. Click [Generate].

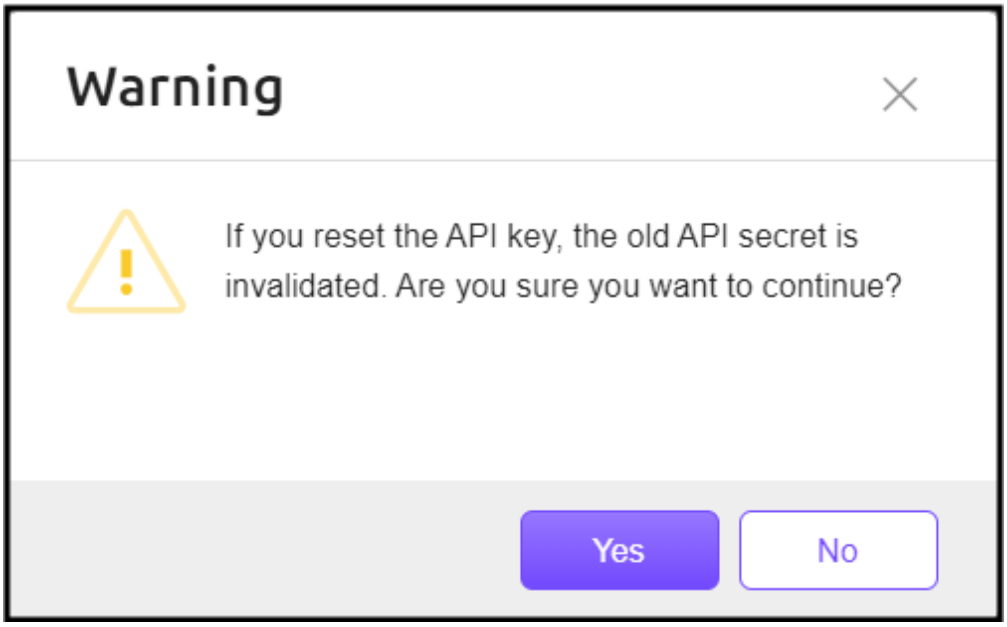
5. If the authentication method is **Use API Key**, a new API key and API secret will be generated and displayed on the screen. Click the copy button to copy the API key and API secret.



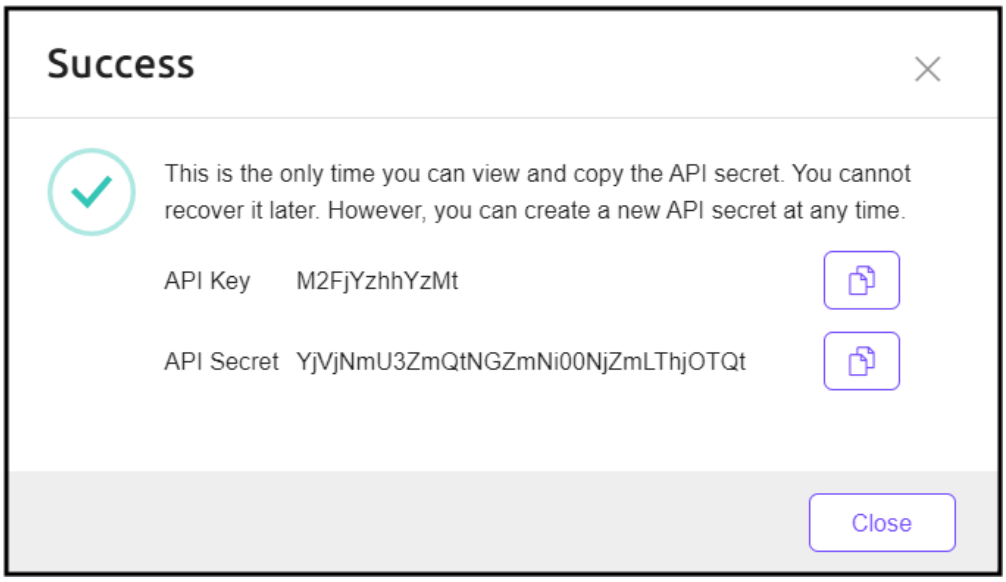
11.4.5.2 Resetting API Clients

Procedure

1. Go to [Admin] > [System] > [API Management].
2. Click [Reset] for the selected API client. A warning window will appear.



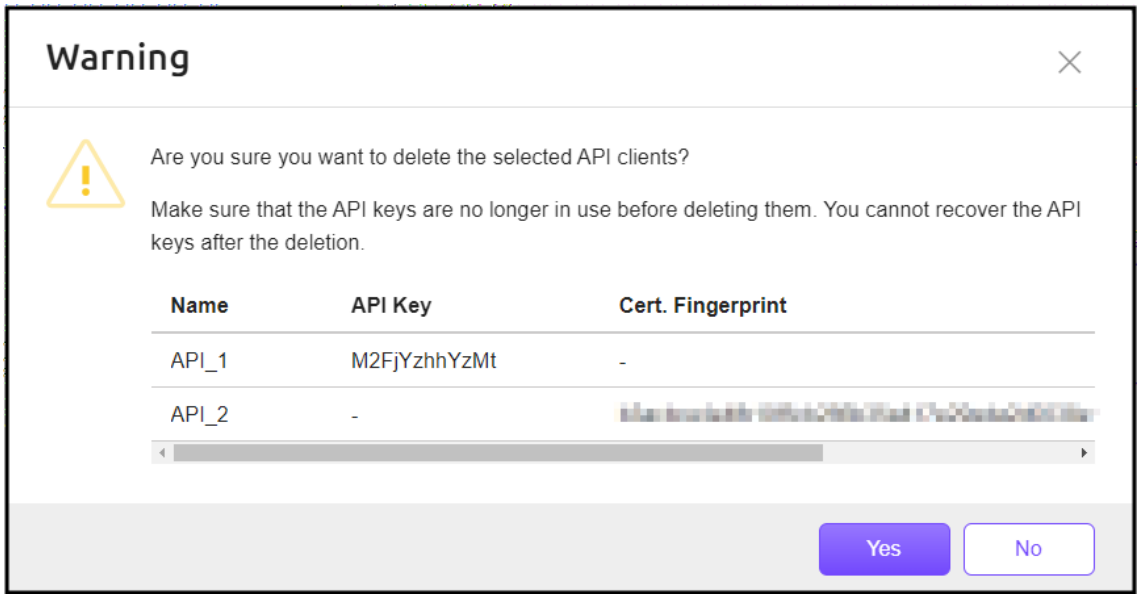
3. Click [Yes]. Please note that the old API secret will be invalidated then.
4. A new API key and API secret will be generated and displayed on the screen. Click the copy button to copy the API key and API secret and paste them onto the API client.



11.4.5.3 Deleting API Clients

Procedure

1. Go to [Admin] > [System] > [API Management].
2. Select the API clients to be deleted.
3. Click the [Delete] button. A warning window will appear.



4. Click [Yes].

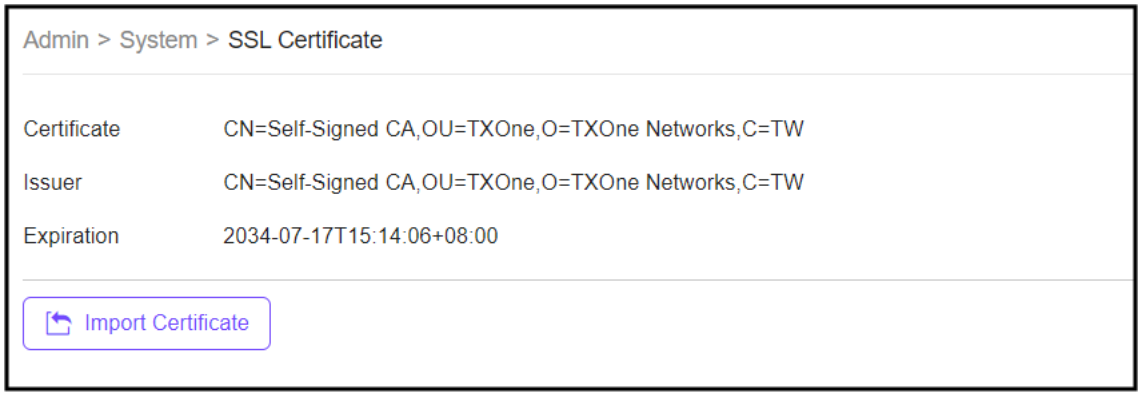
11.4.6 SSL Certificate

The Edge device uses the HTTPS protocol to encrypt web traffic between the user's web browser and the Edge device web server. By default, the Edge device web server uses an auto-generated and self-signed SSL certificate for the HTTPS connections. This chapter introduces how to change the SSL certificate.

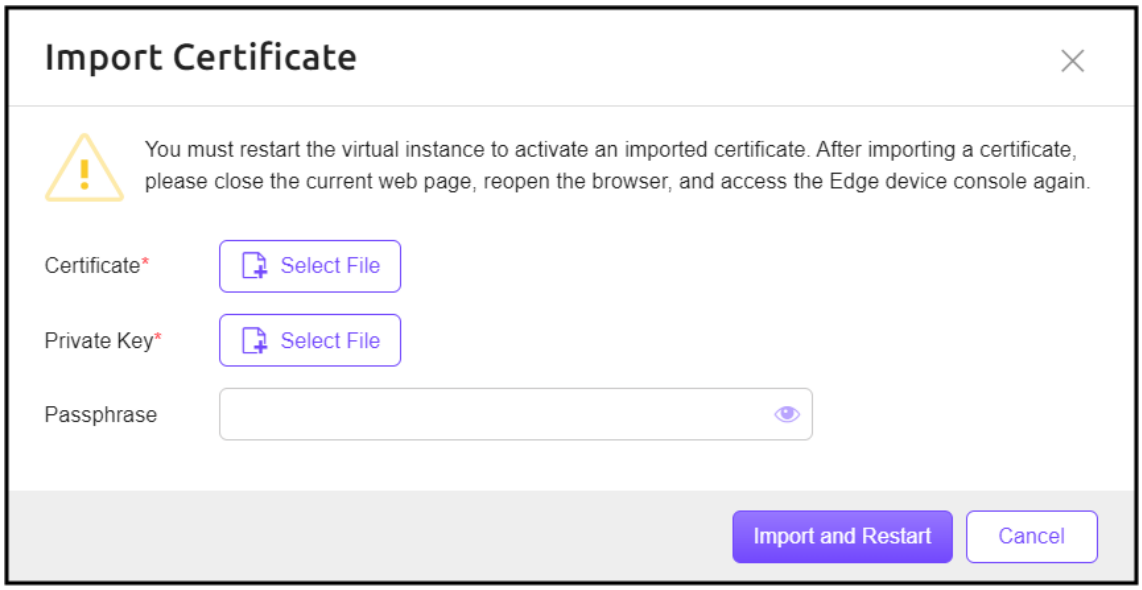
11.4.6.1 Importing SSL Certificates

Procedure

1. Go to [Admin] > [System] > [SSL Certificate]. If the Edge device is currently using its default certificate (auto-generated and self-signed), you will see the following page. The information shown on the page is the default Edge device certificate information.



2. Click [Import Certificate]. The [Import Certificate] window will appear.



3. Import your certificate file by clicking the [Select File] button next to the [Certificate] field.

4. Import the private key (PEM-encoded PKCS#1 format) for the certificate file by clicking the [Select File] button next to the [Private Key] field.

5. Input the passphrase of the private key if the private key is encrypted.

6. Click [Import and Restart].

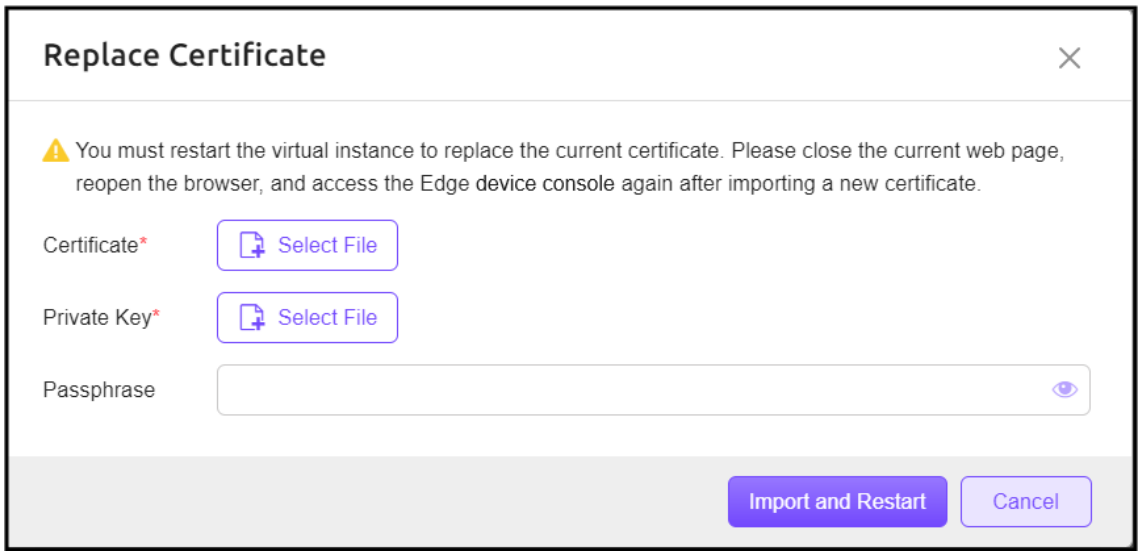
7. Close the current web page, reopen the browser, and access the Edge device web console again.

11.4.6.2 Replacing SSL Certificates

Procedure

1. Go to [Admin] > [System] > [SSL Certificate]. If the Edge device is currently using an imported certificate, you will see the following page. The information shown on the page is the current Edge device certificate information.

2. Click [Replace Certificate]. The [Replace Certificate] window will appear.



3. Import your certificate file by clicking the [Select File] button next to the [Certificate] field.

4. Import the private key (PEM-encoded PKCS#1 format) for the certificate file by clicking the [Select File] button next to the [Private Key] field.

5. Input the passphrase of the private key if the private key is encrypted.

6. Click [Import and Restart].

7. Close the current web page, reopen the browser, and access the Edge device web console again.

11.4.6.3 Verifying SSL Certificates

After adding a new certificate to the Edge device web console, you can verify whether the certificate is valid.

Procedure

1. Log in to the Edge device web console with the Chrome browser.

2. Go to the Three Dots Menu > More Tools > Developer Tools.

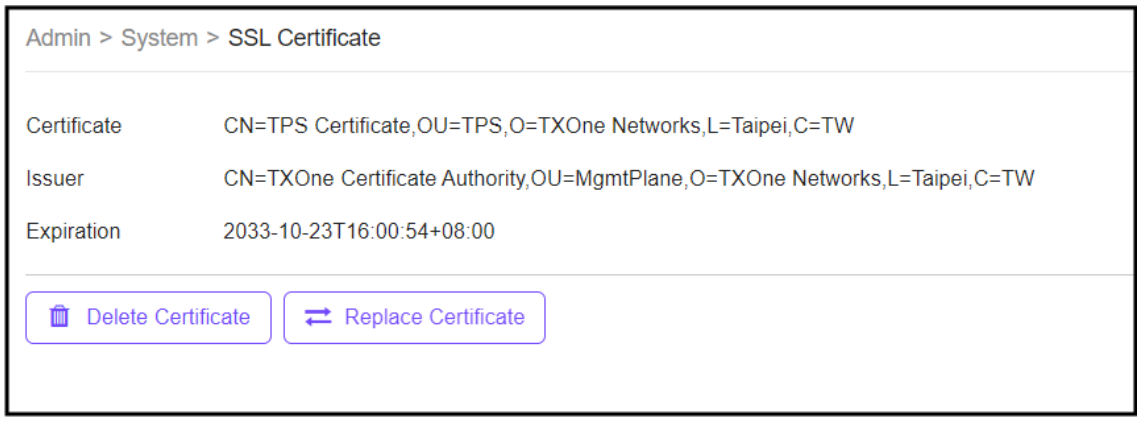
3. Go to the [Security] Tab. It will give you a security overview.

4. In the [Security Overview] pane, click the [View certificate] button, and you will see the certificate details of the Edge device web console.

11.4.6.4 Deleting SSL Certificates

Procedure

1. Go to [Admin] > [System] > [SSL Certificate].



2. Click [Delete Certificate].

3. Close the current web page, reopen the browser, and access the Edge device web console again.

11.4.7 Backup/Restore

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

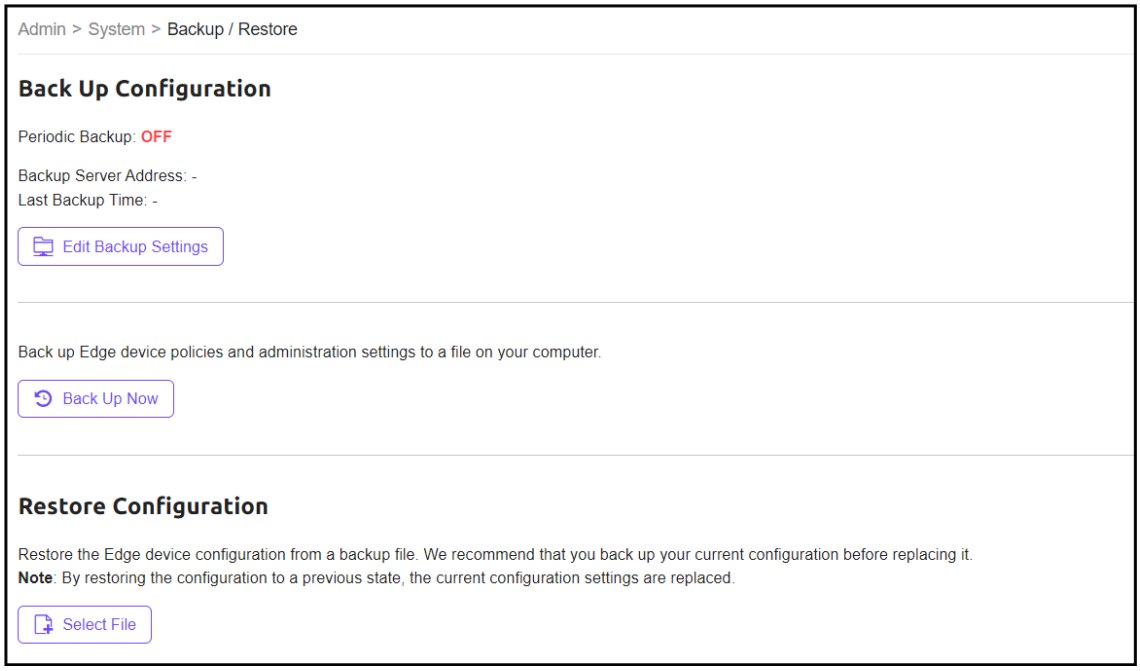
We recommend the following:

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

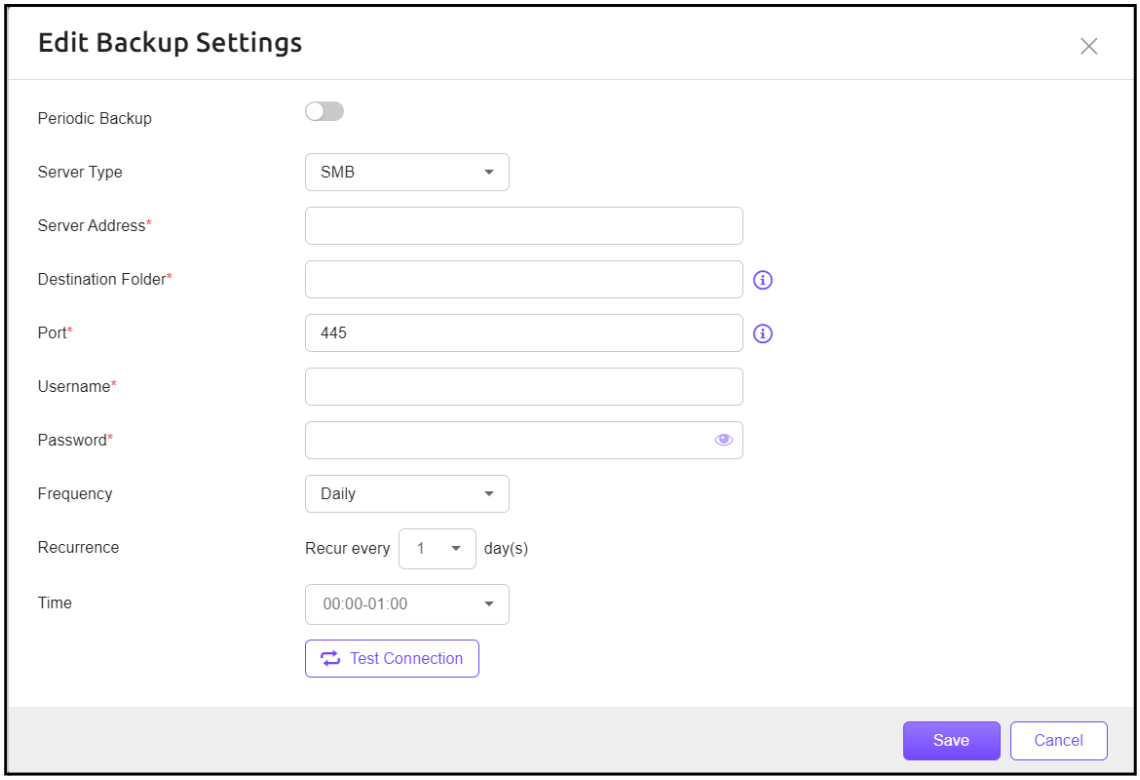
11.4.7.1 Configuring Backup Settings

Procedure

1. Go to [Admin] > [System] > [Backup/Restore].



2. Click [Edit Backup Settings]. The [Edit Backup Settings] window will appear.



3. Configure the following settings.

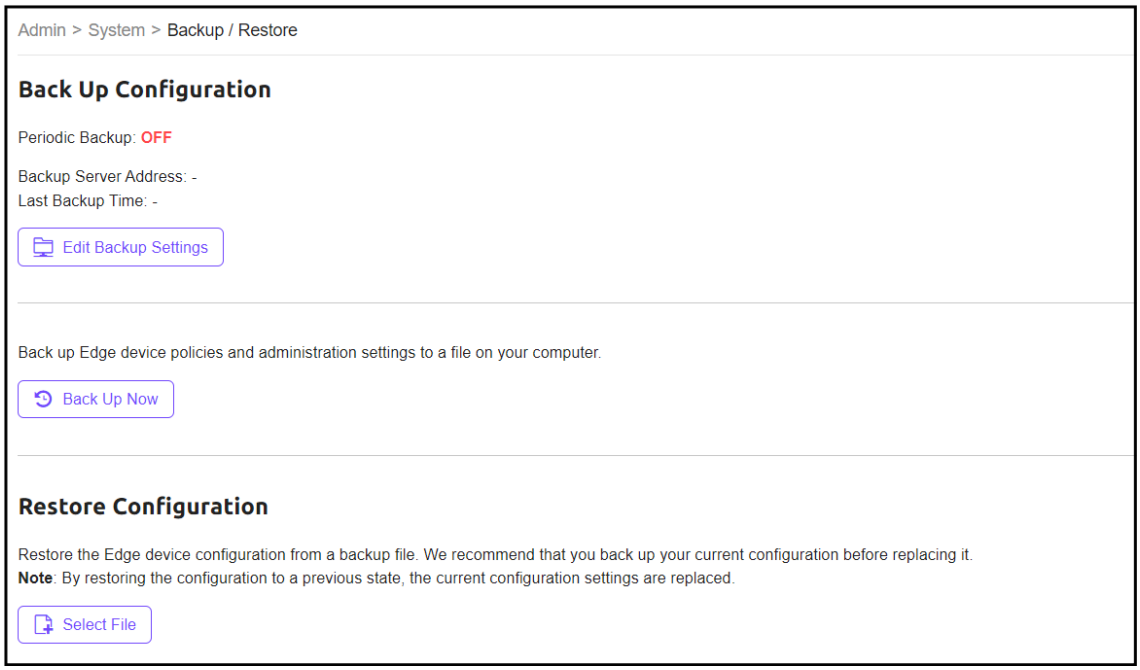
Item	Description
Periodic Backup	Click the toggle to enable or disable backing up configuration to a remote server periodically.
Server Type	Select a protocol, **SMB** or **SFTP**, for sending backed-up files to a remote server.
Server Address	Input the IP address of the server where the backed-up files will be sent.
Destination Folder	Input the destination folder on the server where the backed-up files will be sent.
Port	Input the port number for initializing an SMB or SFTP connection. (Default: 445)
Username	Input the username for initializing an SMB or SFTP connection.
Password	Input the password for initializing an SMB or SFTP connection.
Frequency	Select a backup frequency, **Daily** or **Weekly**, from the drop-down list.
Recurrence	Specify the exact days when the backups should run.
Time	Specify the exact times when the backups should run.

4. Click [Save].

11.4.7.2 Backing Up Device Configuration

Procedure

1. Go to [Admin] > [System] > [Backup/Restore].

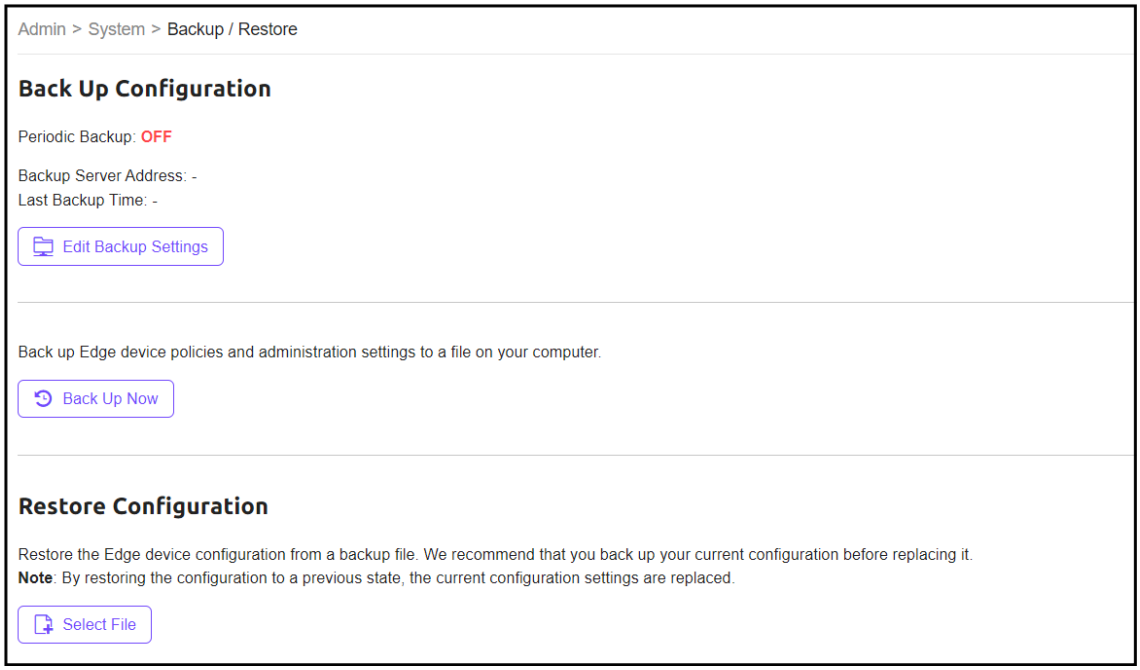


2. Click [Back Up Now]. A configuration backup file will automatically be saved to your computer.

11.4.7.3 Restoring Device Configuration

Procedure

1. Go to [Admin] > [System] > [Backup/Restore].



2. In the [Restore Configuration] pane, click [Select File], then import a configuration file from your local disk. All services will restart. It can take some time to restart services after applying imported settings and rules.

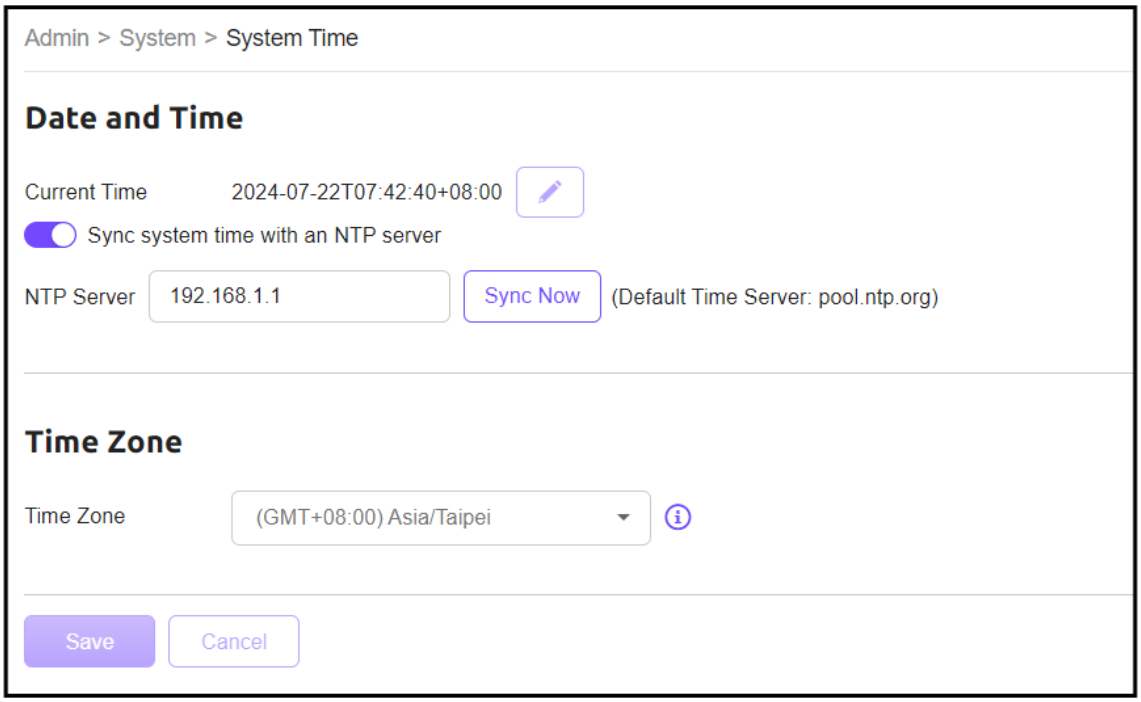
11.4.8 System Time

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

11.4.8.1 Configuring System Time

Procedure

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



2. In the [Date and Time] pane, you can choose to synchronize the system time with an NTP server or set the system time manually.

- Synchronize the system time with an NTP server:

a. Enable the [Sync system time with an NTP server] setting.

b. Specify the domain name or IP address of the NTP server.

c. Click [Sync Now].

- Set the system time manually:

a. Click the edit button .

b. Set the date and time.

c. Click [Apply].

3. From the [Time Zone] drop-down list, select a time zone.

4. Click [Save].

	EdgeOne system synchronizes the system time with its managed instances.

11.4.9 System Reboot

Access the [System Reboot] page to reboot the Edge device.

11.4.9.1 Rebooting Edge Device

Procedure

1. Go to [Admin] > [System] > [System Reboot].

2. Click [Reboot Now] to reboot the Edge device.

Admin > System > System Reboot
Use the current configuration and reboot the Edge device now.
Reboot Now

12 Extended Functions via Supported USB Device

This chapter describes the use of supported USB devices with the Edge series device for extended or supported functions.

To ensure optimal operation, only the USB devices listed below are currently supported.

	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 & 32GB (AH355)		USB Disk Drive

After a supported USB device is plugged in, you can perform the following tasks.

- Back up configuration
- Load pattern from USB device
- Load configuration from USB device
- Load firmware from USB device

⚠	Given that this feature allows anyone with a supported USB disk to perform the above tasks, the physical security of your Edge series device must be considered carefully.

12.1 Backing Up Configuration

Procedure

1. Plug a supported USB disk device into the USB port on the front panel of your Edge series device.

2. Upon successful detection of the USB disk device, the corresponding LED as listed below will change to a steady green. Relevant system logs 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.

State/Action	LED	LED Color/State
Default State – USB Disk Plugged in	USB	Green – Steady

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

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

4. Press the reset button for more than 10 seconds to back up configuration. The corresponding LED as listed below will blink.

State/Action	LED	LED Color/State
Back Up Configuration	USB	Green – Blinking once every 0.5 seconds

5. Once the reset button is released, the LED will be restored to the default state (as shown in the table in step 2).

6. If any error occurs, the corresponding LED as listed below will indicate it.

State/Action	LED	LED Color/State
Error	FAIL	Red – Blinking once every second

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

7. Relevant system logs can be checked to verify if the configuration backup was completed successfully or not.

8. Unplug the USB disk, after which the LEDs will return to their states prior to the USB disk device being plugged in (USB LED off), and relevant system logs will show that the USB disk has been unplugged.

📝	Since configuration files are usually not very large, this process may finish quickly.

12.2 Loading Pattern from USB Device

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

Procedure

1. Create a folder "**TXOne**" and a subfolder "**pattern**" in the TXOne folder on a supported USB disk.

2. Save a pattern file you would like to load onto your Edge series device on your USB disk under the path "**/TXOne/pattern/**". Assuming the filename of the pattern file is "pattern.acf", the file path on the USB disk would be "**/TXOne/pattern/pattern.acf**".

⚠️	Saving pattern files under other paths or incorrect folder names will cause the file to not be detected during the pattern load process.

📝	1. Folder names are case-insensitive. If multiple pattern files exist in the folder, the newest one will be used. 2. Various versions of the pattern files can be downloaded at the MyTXOne portal at https://my.txone.com/.

3. Plug your USB disk into the USB port on the front panel of your Edge series device.

4. Upon successful detection of the USB disk, the corresponding LED as listed below will change to a steady green. Relevant system logs can also be checked to confirm that a supported USB disk was detected when inserted. This state is referred to as the "Default Action" state.

State/Action	LED	LED Color/State
Default State – USB Disk Plugged in	USB	Green – Steady

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

5. The function of the reset button will also change until the USB disk is unplugged. When a USB disk is plugged in, the reset button will not serve the as the reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken during this time.

6. Give the reset button one short press to toggle to the "Load Pattern from USB Disk" action. The LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Toggle to Pattern Load	USB	Green – Steady	STATE	Green – Blinking once every second

7. The action must be confirmed within 10 seconds by holding down the reset button for more than 3 seconds. After the reset button is pressed more than 3 seconds, the LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Pattern Load Action Confirmed	USB	Green – Steady	STATE	Green – Blinking once every 0.5 seconds

8. Once the reset button is released, pattern load will be in progress, and the LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Pattern Load in Progress	USB	Green – Blinking once every 0.5 seconds	STATE	Green – Blinking once every 0.5 seconds

9. If any error occurs, the corresponding LED as listed below will indicate it.

State/Action	LED	LED Color/State
Error	FAIL	Red – Blinking once every second

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

10. Relevant system logs can be checked to verify if the pattern load was completed successfully or not. If so, the LEDs will be restored to the default state (as shown in the table in step 4).

11. Unplug the USB disk, after which the LEDs will return to their states prior to the USB disk device being plugged in (USB LED off), and relevant system logs will show that the USB disk has been unplugged.

12.3 Loading Configuration from USB Device

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

Procedure

1. Create a folder "**TXOne**" and a subfolder "**config**" in the TXOne folder on a supported USB disk.

2. Save a configuration file you would like to load onto your Edge series device on your USB disk under the path "**/TXOne/config/**". Assuming the filename of the configuration file is "config.acf", the file path on the USB disk would be "**/TXOne/config/config.acf**".

> Saving configuration files under other paths or incorrect folder names will cause the file to not be detected during the configuration load process.

> Folder names are case-insensitive. If multiple configuration files exist in the folder, the newest one will be used.

3. Plug your USB disk into the USB port on the front panel of your Edge series device.

4. Upon successful detection of the USB disk, the corresponding LED as listed below will change to a steady green. Relevant system logs can also be checked to confirm that a supported USB disk was detected when inserted. This state is referred to as the "Default Action" state.

State/Action	LED	LED Color/State
Default State – USB Disk Plugged in	USB	Green – Steady

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

5. The function of the reset button will also change until the USB disk is unplugged. When a USB disk is plugged in, the reset button will not serve the as the reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken during this time.

6. Give the reset button two short presses to toggle to the "Load Configuration from USB Disk" action. The LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Toggle to Configuration Load	USB	Green – Steady	MGMT	Green – Blinking once every second

7. The action must be confirmed within 10 seconds by holding down the reset button for more than 3 seconds. After the reset button is pressed more than 3 seconds, the LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Configuration Load Action Confirmed	USB	Green – Steady	MGMT	Green – Blinking once every 0.5 seconds

8. Once the reset button is released, the configuration load will be in progress, and the LEDs will change to the following colors/states.

State/Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State
Configuration Load in Progress	USB	Green – Blinking once every 0.5 seconds	MGMT	Green – Blinking once every 0.5 seconds

9. If any error occurs, the corresponding LED as listed below will indicate it.

State/Action	LED	LED Color/State
Error	FAIL	Red – Blinking once every second

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

10. Relevant system logs can be checked to verify if the configuration load was completed successfully or not. If so, the LEDs will be restored to the default state (as shown in the table in step 4).

11. Unplug the USB disk, after which the LEDs will return to their states prior to the USB disk device being plugged in (USB LED off), and relevant system logs will show that the USB disk has been unplugged.

12.4 Loading Firmware from USB Device

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

Procedure

1. Create a folder "**TXOne**" and a subfolder "**firmware**" in the TXOne folder on a supported USB disk.

2. Save a firmware file you would like to load onto your Edge series device on your USB disk under the path "**/TXOne/firmware/**". Assuming the filename of the firmware file is "firmware.acf", the file path on the USB disk would be "**/TXOne/firmware/firmware.acf**".

⚠️	Saving firmware files under other paths or incorrect folder names will cause the file to not be detected during the firmware load process.

📝	1. Folder names are case-insensitive. If multiple firmware files exist in the folder, the newest one will be used. 2. Various versions of the firmware files can be downloaded at the MyTXOne portal at https://my.txone.com/.

3. Plug your USB disk into the USB port on the front panel of your Edge series device.

4. Upon successful detection of the USB disk, the corresponding LED as listed below will change to a steady green. Relevant system logs can also be checked to confirm that a supported USB disk was detected when inserted. This state is referred to as the "Default Action" state.

State/Action	LED	LED Color/State
Default State – USB Disk Plugged in	USB	Green – Steady

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

5. The function of the reset button will also change until the USB disk is unplugged. When a USB disk is plugged in, the reset button will not serve the as the reboot/factory reset button. It will instead serve as a button to cycle through a set of possible actions that may be taken during this time.

6. Give the reset button three short presses to toggle to the "Load Firmware from USB Disk" action. The LEDs will change to the following colors/states.

State/ Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State	LED 3	LED 3 Color/State
Toggle to Firmware Load	USB	Green – Steady	STATE	Green – Blinking once every second	MGMT	Green – Blinking once every second

7. The action must be confirmed within 10 seconds by holding down the reset button for more than 3 seconds. After the reset button is pressed more than 3 seconds, the LEDs will change to the following colors/states.

State/ Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State	LED 3	LED 3 Color/State
Firmware Load Action Confirmed	USB	Green – Steady	STATE	Green – Blinking once every 0.5 seconds	MGMT	Green – Blinking once every 0.5 seconds

8. Once the reset button is released, the firmware load will be in progress, and the LEDs will change to the following colors/states.

State/ Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State	LED 3	LED 3 Color/State
Firmware Load in Progress	USB	Green – Blinking	STATE	Green – Blinking once	MGMT	Green – Blinking once

State/ Action	LED 1	LED 1 Color/State	LED 2	LED 2 Color/State	LED 3	LED 3 Color/State
		once every 0.5 seconds		every 0.5 seconds		every 0.5 seconds

9. If any error occurs, the corresponding LED as listed below will indicate it.

State/Action	LED	LED Color/State
Error	FAIL	Red – Blinking once every second

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

10. Relevant system logs can be checked to verify if the firmware load was completed successfully or not. If so, the LEDs will be restored to the default state (as shown in the table in step 4).

11. Unplug the USB disk, after which the LEDs will return to their states prior to the USB disk device being plugged in (USB LED off), and relevant system logs will show that the USB disk has been unplugged.

13 Technical Support

This chapter includes the following topics.

- Troubleshooting Resources
- Contacting TXOne
- Other Resources

13.1 Troubleshooting Resources

Before contacting technical support, consider visiting the following TXOne online resources.

13.1.1 Help Center

TXOne Help Center provides 24/7 online resources that contain the most up-to-date information about both common and unusual problems.

To access the TXOne Help Center, click the ? icon in the top right corner of the console or visit https://help.txone.com/ , where you can learn more about:

- News & Releases
- Technical Advisory
- Security Advisory

13.1.2 Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. TXOne combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Visit https://www.encyclopedia.txone.com/ to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

13.2 Contacting TXOne

In the United States, TXOne representatives are available by phone or email:

Address	TXOne Networks, Incorporated 222 West Las Colinas Boulevard, Irving, Texas 75062, U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.txone.com/

Email Address	

- Contact us: https://www.txone.com/contact/ or mail to support@txone.com

13.2.1 Expediting Support Call

To accelerate the speed to reply and solve the problem, ensure that you have the following details available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand and model, as well as any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received

13.3 Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

13.3.1 MyTXOne Portal

MyTXOne portal (https://my.txone.com/) is designed to consolidate everything you need all through a single pane of glass, aiming to maximize your efficiency when using TXOne products.

By visiting our MyTXOne portal, you are able to:

- Manage your TXOne product licenses, including license activation and license renewal, all at one place;
- Download the firmware and pattern files for your security appliances' regular updates and enhancement;
- Access our product documentation, such as user's guides, quick start guides, and release notes, enabling you to use our products efficiently and effectively;
- Read our white papers, case studies, security reports, etc. to gain insights into OT security and stay ahead of the curve;
- Submit support case tickets to resolve technical issues or other concerns.

13.3.2 Documentation Feedback

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any other TXOne document, please mail to support@txone.com.

14 Appendix A: Terms and Acronyms

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

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