



OT Defense Console™

Administrator's Guide

V 1.5
2022-09-05



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

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

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

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

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

Table of Contents

Chapter 1.....	7
About OT Defense Console™.....	7
Introduction.....	7
Main Functions.....	8
Extensive Support for Industrial Protocols.....	8
Policy Enforcement for Mission-Critical Machines.....	8
Intrusion Prevention and Intrusion Detection.....	8
Asset Management of Mission-Critical Machines.....	8
Centralized Management.....	8
Chapter 2.....	9
Getting Started.....	9
Getting Started: Task List.....	9
Opening the Management Console.....	9
Chapter 3.....	11
Dashboard and Widgets.....	11
Introduction to the Widgets.....	12
Tab and Widget Management.....	22
Chapter 4.....	24
The Visibility Tab.....	24
Common Tasks.....	24
Displaying Asset Information.....	25
Basic Asset Information.....	26
Real Time Network Application Traffic.....	27
Exporting Data.....	27
Pattern View.....	28
Chapter 5.....	30
Node Management.....	30
Common Tasks.....	30
Device Group Management.....	32
Managing EdgeIPS™ Devices.....	33
Accessing the Management Tab.....	33
Upgrading the Firmware.....	34
Editing Name / Location of a Node.....	34
Rebooting the Node.....	35
Configuring Cyber Security.....	36
Configuring Policy Enforcement.....	37
Configuring Packet Capture.....	40
Configuring Suspicious Objects.....	41
Configuring Pattern Settings.....	43
Sharing Management Permissions to Other User Accounts.....	44
Managing EdgeFire™ Devices.....	45
Accessing the Management Tab.....	45
Upgrading the Firmware.....	45
Editing Name / Location of a Node.....	46
Rebooting the Node.....	46
Configuring Cyber Security.....	46
Configuring Policy Enforcement.....	46
Configuring Packet Capture.....	52
Configuring Suspicious Objects.....	52
Configuring Pattern Settings.....	52
Sharing Management Permissions to Other User Accounts.....	52
Managing EdgeIPS™ Pro Devices.....	52
Accessing the Management Tab.....	53
Upgrading the Firmware.....	54

Editing Name / Location of a Node	54
Rebooting the Node	54
Configuring Port Security	54
Configuring Policy Enforcement	57
Configuring Packet Capture	61
Configuring Suspicious Objects	61
Configuring Pattern Settings	61
Sharing Management Permissions to Other User Accounts	61
Managing EdgeIPS™ LE Devices	61
Accessing the Management Tab	61
Upgrading the Firmware	62
Editing Name / Location of a Node	63
Rebooting the Node	63
Configuring Cyber Security	64
Configuring Policy Enforcement	65
Configuring Packet Capture	69
Configuring Suspicious Objects	70
Configuring Pattern Settings	72
Sharing Management Permissions to Other User Accounts	73
Chapter 6	75
Object Profiles	75
Configuring IP Object Profiles	75
Configuring Service Object Profiles	76
Configuring Protocol Filter Profiles	77
Specifying Commands Allowed in an ICS Protocol	79
Applying the Drop Malformed Option to an ICS Protocol	79
Advanced Settings	80
Configuring IPS Profiles	97
Configuring a Pattern Rule for Granular Control	99
Configuring File Filter Profiles	100
Configuring File Exclusions	102
Configuring Antivirus Profiles	104
Configuring File Exceptions	105
Chapter 7	107
Logs	107
Viewing Cyber Security Logs	107
Viewing Policy Enforcement Logs	111
Viewing Protocol Filter Logs	113
Viewing File Filter and Antivirus Logs	115
Viewing Suspicious Object Logs	116
Viewing Asset Detection Logs	118
Viewing System Logs	119
Viewing Audit Logs	121
Chapter 8	123
The Report Tab	123
Report List	123
Report Task	124
Report Sample	126
Chapter 9	127
The Application Tab	127
Packet Capture	127
Suspicious Object Pool	128
Reviewing Imported Suspicious Objects	128
Configuring Suspicious Objects Import Settings	129
Chapter 10	130
Administration	130

Account Management	130
User Roles	130
Account Input Format	132
Adding a User Account.....	133
Changing Your Password	134
Password Complexity	134
Login Protection	135
ID/Password Reset	135
Auth Services	136
Configuring TACACS+.....	136
Configuring SAML SSO	137
Adding User Account with Local and SAML SSO Authentication	138
Logging on via SAML	139
API Key Management	140
Adding API Key	140
Resetting API Key	141
Deleting API Key	141
Integrating Products/Services	141
Configuring System Time	142
Configuring Syslog Settings.....	143
Syslog Severity Levels.....	144
Syslog Severity Level Mapping Table.....	144
The SNMP	145
Configuring SNMP v1/v2c	146
Configuring SNMP v3	146
Configuring SNMP Trap Settings	147
Updates	148
Device Update - Components	149
Updating the Components Manually.....	150
Importing a Component File	150
Scheduling Component Updates.....	150
Managing the Component Repository	151
ODC System Update - Components	151
Importing an SSL Certificate	152
Log Purge	152
Back-Up / Restore	154
Backing Up a Configuration.....	154
Restoring a Configuration	155
License	155
Introduction to the Licenses	155
Viewing Your Product License Information	156
Alert Messages.....	157
Activating or Renewing Your Product License.....	158
Manually Refreshing the License	160
Proxy	160
Configuring Proxy Settings	160
Notification Service	161
Configuring Email	161
Configuring Event Notification	161
Chapter 11.....	164
Technical Support.....	164
Troubleshooting Resources	164
Using the Support Portal.....	164
Threat Encyclopedia.....	164
Contacting Trend Micro	165
Expediting the Support Call.....	165

Other Resources	165
Download Center	165
Documentation Feedback	165
Appendix A	166
Terms and Acronyms	166
Appendix B	167
Setting Up Connection to ODC via EdgeFire, EdgeIPS or EdgeIPS Pro Web Console	167
Appendix C	168
Introduction to the vShell	168
First Time Using vShell	168
Signing in to vShell	168
Changing Default Password to Activate	168
How to Set Up a Network	169
Displaying the Network Settings	169
Updating the Interface Settings	169
How to Set Up ACL (Access Control List)	171
Querying the Status	172
Adding Clients to the Trust List	172
Deleting Clients from the Trust List	172
Enabling/Disabling the ACL of modules	172
Shortcut Table	173
List of Command Prompt Commands	173
Summary	173
access-list	173
env	174
exit	174
help	174
iface	175
ping	177
poweroff	177
reboot	177
resolv	177
scp	178
service	178
sftp	178
ssh	178
pwd	178
dx	178
web	179
Appendix D	180
Supported MIB Objects	180
SNMP Queries	180
SNMP Traps	181

About OT Defense Console™

Introduction

OT Defense Console™ (Operational Technology Defense Console™, or ODC™) is a web-based management console that provides a graphical user interface for device configuration and security policy settings. The management process is designed to comply with the manufacturing SOP of the industry. ODC centrally monitors operational information, edits network protection policies, sets patterns of attack behaviors, and generates reports of security events. All safeguards are deployed throughout the entire information technology (IT) and operational technology (OT) infrastructure.

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

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

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

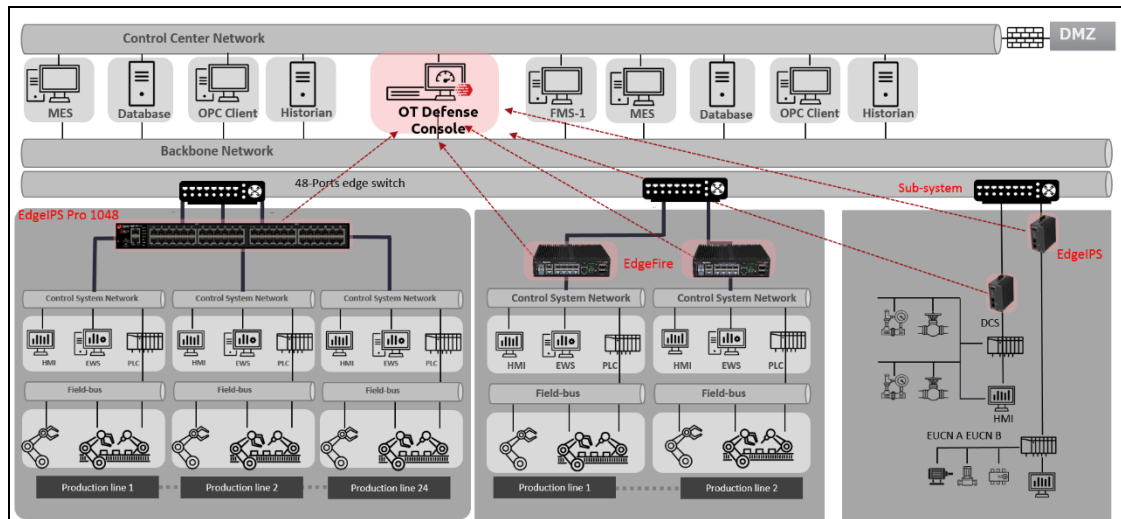


Figure 1. TXOne Networks security solutions for OT networks

Main Functions

OT Defense Console™ is capable of managing the security devices EdgeIPS™, EdgeIPS™ Pro, and EdgeFire™. The following describes the main functions of the product suite:

Extensive Support for Industrial Protocols

The Edge series 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 defensive measures in appropriate network segments and seamlessly connects them to existing factory networks.

Policy Enforcement for Mission-Critical Machines

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

Intrusion Prevention and Intrusion Detection

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

Asset Management of Mission-Critical Machines

The Edge series, when deployed at the forefront of critical production equipment, can be viewed as security sensors. Each Edge series node grants network traffic control without interfering with production line performance. The deployed security devices also analyze network traffic and visualize network topology, as well as key devices, on the OT Defense Console™. In addition to providing detailed analysis of events, the OT Defense Console™ also helps operators to control and monitor legacy devices.

Centralized Management

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

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

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

Getting Started

This chapter describes how to get started with OT Defense Console™ and configure initial settings.

Getting Started: Task List

Getting Started Tasks provides a high-level overview of all procedures required to get OT Defense Console up and running as quickly as possible. Each step links to more detailed instructions later in the document.

Procedure

1. Open the management console.
For more information, see [Opening the Management Console on page 9](#).
2. Change administrator's default login name and password at the first login.
3. Activate the license.
For more information, [Activating or Renewing Your Product License on page 158](#).
4. Configure the system time.
For more information, see [Configuring System Time on page 142](#).
5. [Optional] Configure the Syslog settings.
For more information, see [Configuring Syslog Settings on page 143](#).
6. Update the components.
For more information, see [Updates on page 148](#).
7. Create the device groups for the EdgeIPS™, EdgeFire™ and EdgeIPS™ Pro devices.
For more information, see [Device Group Management on page 32](#).
8. Assign policies to the device groups.
For more information, see [Node Management on page 30](#) and [Object Profiles on page 75](#).
9. Create user accounts and share device group management permissions to the related user accounts.
For more information, see [Account Management on page 130](#) and [Sharing Management Permissions to Other User Accounts on page 44](#).

Opening the Management Console

OT Defense Console provides a built-in management console that you can also use for configuration. View the management console using a web browser.

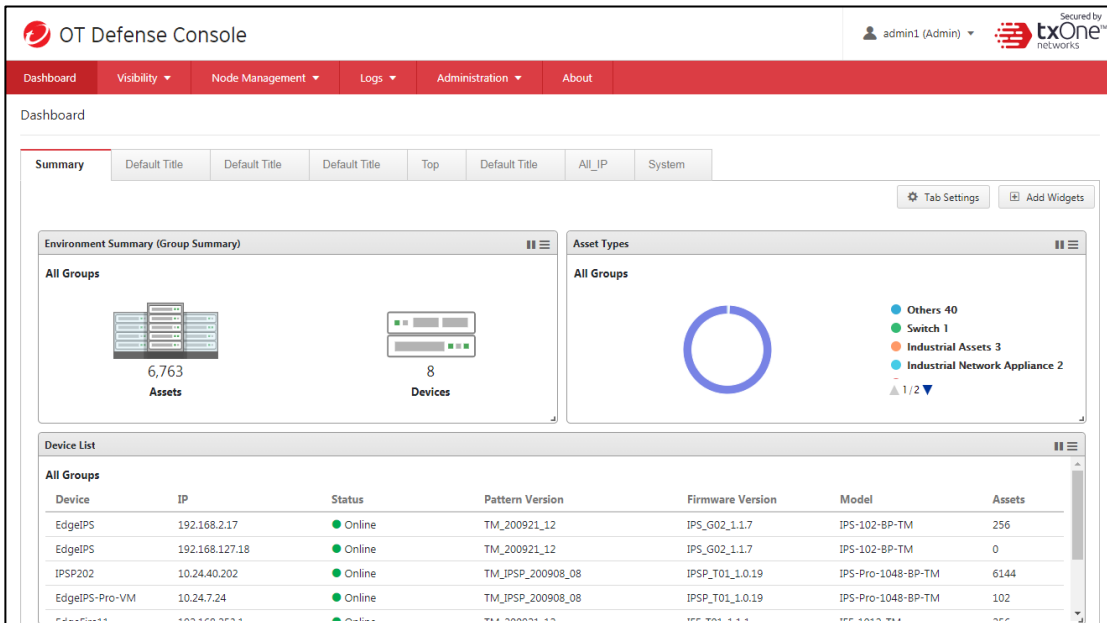
- View the management console using Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; Edge version 15 or later.

Procedure

1. In a web browser, type the address of the OT Defense Console in the following format:
`https://<target server IP address or FQDN>`
The logon screen will appear.
2. Enter your logon credentials (user ID and password).
Use the default administrator logon credentials when logging on for the first time:
 - User ID: admin
 - Password: txone
3. Click [Log On].

If this is your first log on, the Login Information Setup frame will appear.

- The first time you log on, you must change the default login name and password before you can access the management console.
- New login name can not be "root", "admin", "administrator" or "auditor" (case-insensitive).
 - a. Confirm your password settings.
 - New Login Name
 - New Password
 - Retype Password
 - b. Click [Confirm].
You will be automatically logged out of the system. The Log On screen will appear.
 - c. Log on again using your new credentials.



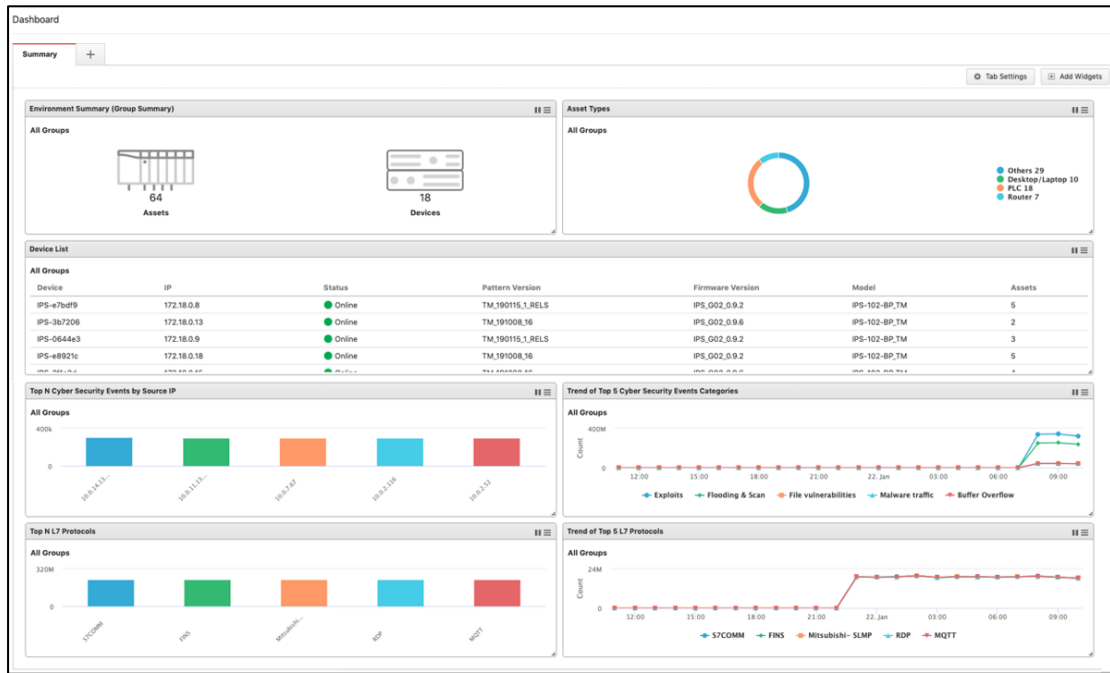
The screenshot shows the OT Defense Console interface. At the top, there is a navigation bar with tabs for Dashboard, Visibility, Node Management, Logs, Administration, and About. The user is logged in as 'admin1 (Admin)'. The main dashboard area is titled 'Dashboard' and contains several widgets:

- Environment Summary (Group Summary):** Shows 6,763 Assets and 8 Devices.
- Asset Types:** A donut chart showing the distribution of asset types: Others (40), Switch (1), Industrial Assets (3), and Industrial Network Appliance (2).
- Device List:** A table listing individual devices with their IP addresses, status, pattern and firmware versions, and models.

Device	IP	Status	Pattern Version	Firmware Version	Model	Assets
EdgeIPS	192.168.2.17	Online	TM_200921_12	IPS_G02_1.1.7	IPS-102-BP-TM	256
EdgeIPS	192.168.127.18	Online	TM_200921_12	IPS_G02_1.1.7	IPS-102-BP-TM	0
IPSP202	10.24.40.202	Online	TM_IPSP_200908_08	IPSP_T01_1.0.19	IPS-Pro-1048-BP-TM	6144
EdgeIPS-Pro-VM	10.24.7.24	Online	TM_IPSP_200908_08	IPSP_T01_1.0.19	IPS-Pro-1048-BP-TM	102

Dashboard and Widgets

Monitor your assets, devices, network status, and threat detection on the Summary tab. The Summary tab is automatically added to the Dashboard by default when there's no user-defined tab. Default widgets included in Summary tab are [Environment Summary], [Asset Types], [Device List], [Top N Cyber Security Events by Source IP], [Top N L7 Protocols], [Trends of Top 5 Cyber Security Events Categories] and [Trends of Top 5 L7 Protocols].



■ The amount of statistical information shown to you depends on your user account role and whether permission to manage each particular device group has been shared with you. For more information, see [Sharing Management Permissions to Other User Accounts on page 44](#) and [User Roles on page 130](#).

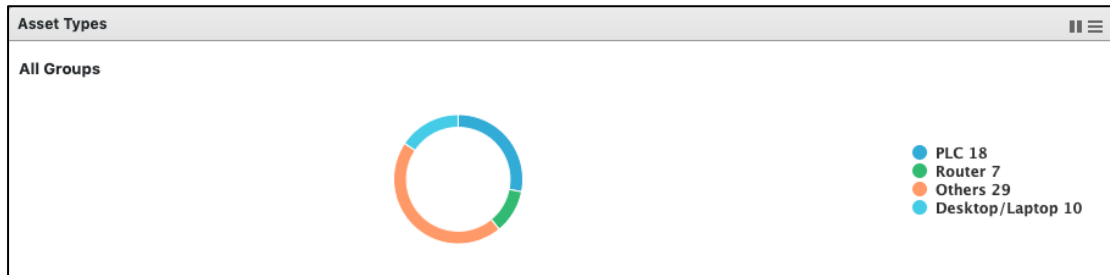
■ The six widgets Top N Cyber Security Events by Source IP, Top N Cyber Security Events by Destination IP, Top N Protocol Filter Events by Source IP, Top N Protocol Filter Events by Destination IP, Top N Policy Enforcement Events by Source IP and Top N Policy Enforcement Events by Destination IP might encounter a performance issue when the event log has recorded too many events during the last 24 hours. We suggest setting the auto refresh to **5 minutes** if dashboards are unable to present the results.

Introduction to the Widgets

This section describes available widgets on the dashboard.

Assets > Asset Types

This widget displays the numbers of assets by asset type in the selected device group(s).



Assets > Environment Summary (Group Summary)

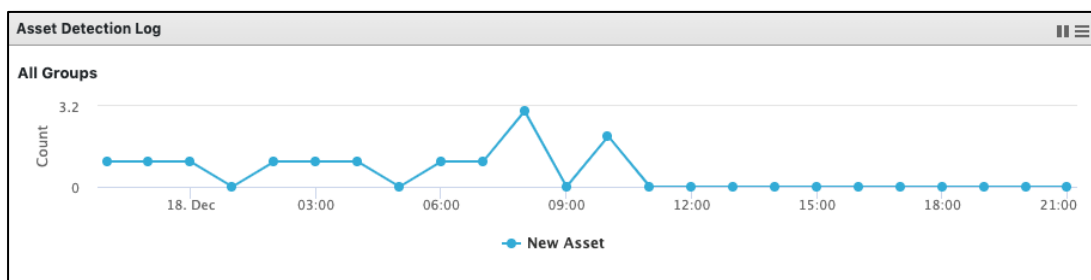
The Environment Summary widget displays a quick summary of your network environment, including the machines that are protected by Edge Series product, the Edge series devices managed by the OT Defense Console™, and the protocol types identified in your network environment.



Item	Description
Assets	Click this item to view a summary of the machines protected by the Edge series devices.
Devices	Click this item to view a summary of the Edge series devices managed by the OT Defense Console™.

Assets > Asset Detection Log

This widget displays the event trends for new assets detected in the selected device group(s) during the last 24 hours.



Devices > Device List

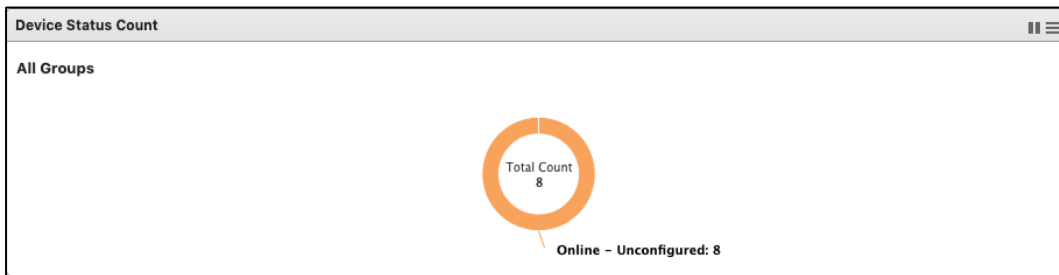
This widget lists the information for all devices in the selected device group(s), including the device model name, host name, IP, status, and so on.

Device	IP	Status	Pattern Version	Firmware Version	Model	Assets
IPS-e70df9	172.18.0.8	Online	TM_190115_1_REL5	IPS_G02_0.9.2	IPS-102-BP, TM	5
IPS-3b7206	172.18.0.13	Online	TM_191008_16	IPS_G02_0.9.6	IPS-102-BP, TM	2
IPS-0644e3	172.18.0.9	Online	TM_190115_1_REL5	IPS_G02_0.9.2	IPS-102-BP, TM	3
IPS-e8921c	172.18.0.18	Online	TM_191008_16	IPS_G02_0.9.2	IPS-102-BP, TM	5

Item	Description
Device	Name of the device
IP	IP address of the device
Status	Status (online or offline) of the device
Pattern Version	Pattern version of the device
Firmware Version	The firmware version of the device
Model	The model name of the device
Assets	The number of assets that are managed by the device

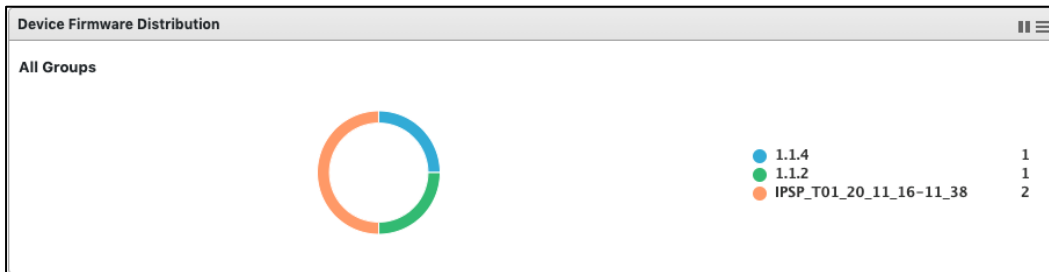
Devices > Device Status Count

This widget lists the information for all devices in the selected device group(s), including the device model name, host name, IP, status, and so on.



Devices > Firmware Distribution

This widget displays the devices in the selected device group(s) organized by firmware version.



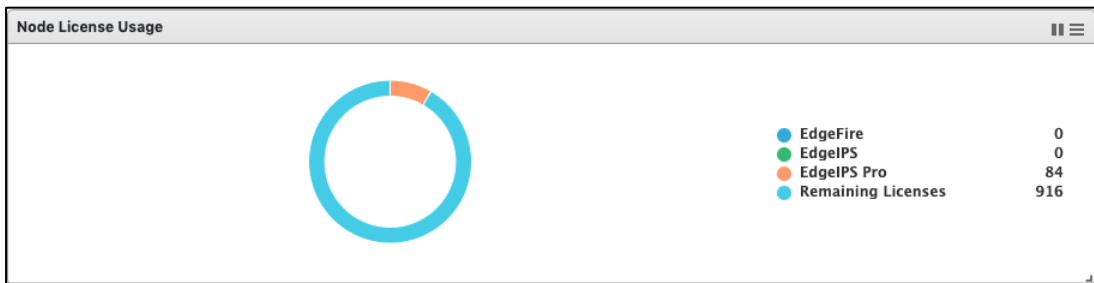
Devices > Device Pattern Distribution

This widget displays the devices in the selected device group(s) organized by pattern.



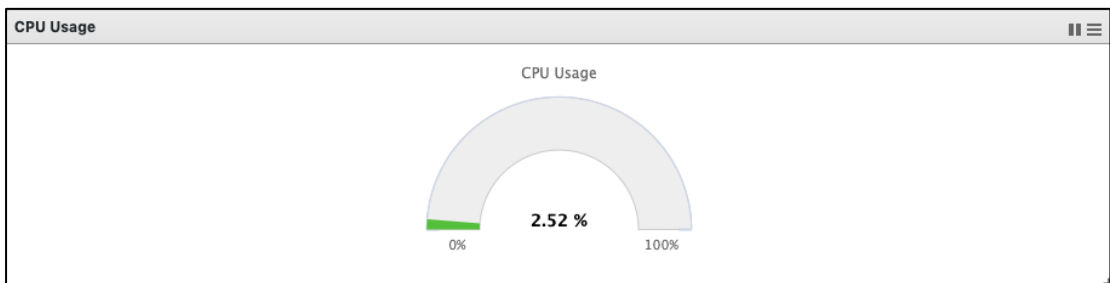
License > Node License Usage

This widget displays the numbers of registered EdgeIPS/EdgeFire devices and unused node license count.



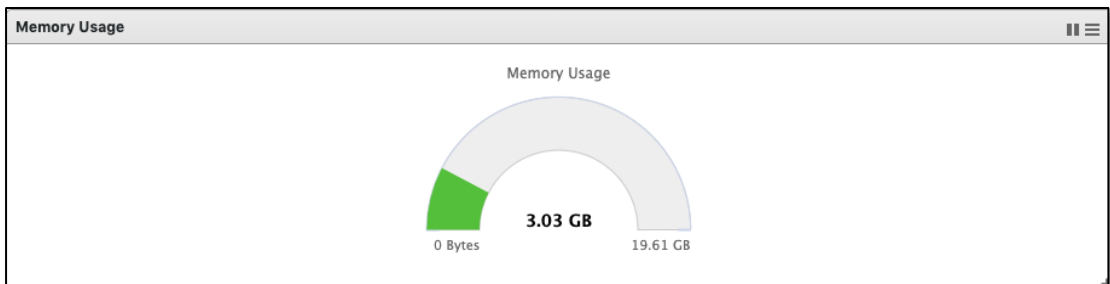
System > CPU Usage

Show ODC's CPU Usage.



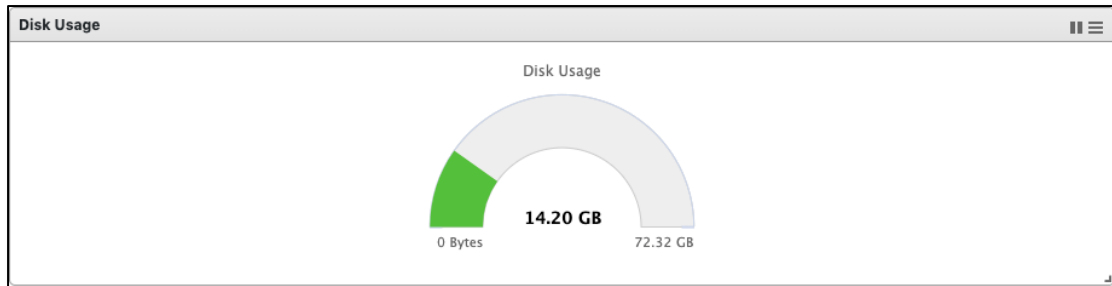
System > Memory Usage

Show ODC's Memory Usage.



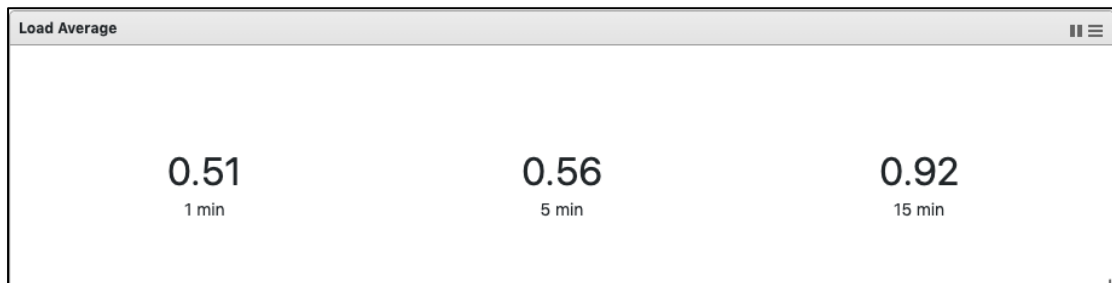
System > Disk Usage

Show ODC's Disk Usage.



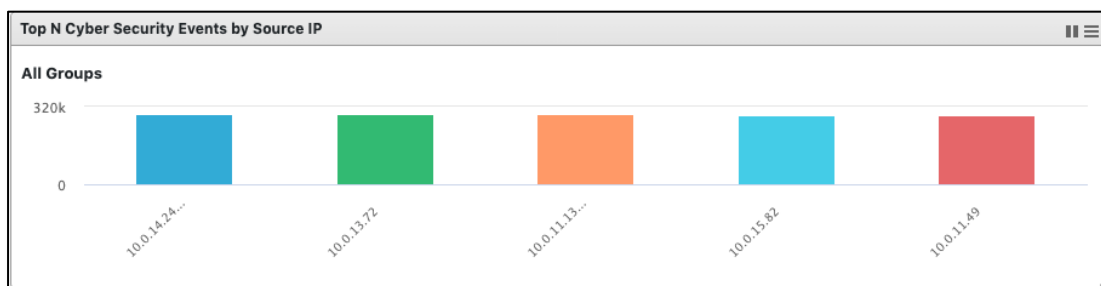
System > Load Average

Show ODC's Load Average. This refers to the average amount of work the system is doing, based on how many processes are using or waiting for CPU, over these three periods of time.



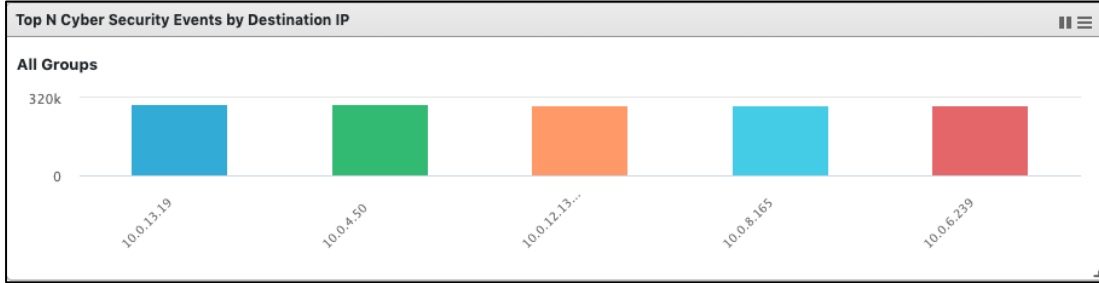
Cyber Security > Top N Cyber Security Events by Source IP

This widget displays the top N (5 or 10) source IP addresses of the cyber security events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues; please see the **note** above.)



Cyber Security > Top N Cyber Security Events by Destination IP

This widget displays the top N (5 or 10) destination IP addresses of the cyber security events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues; please see **note** above.)



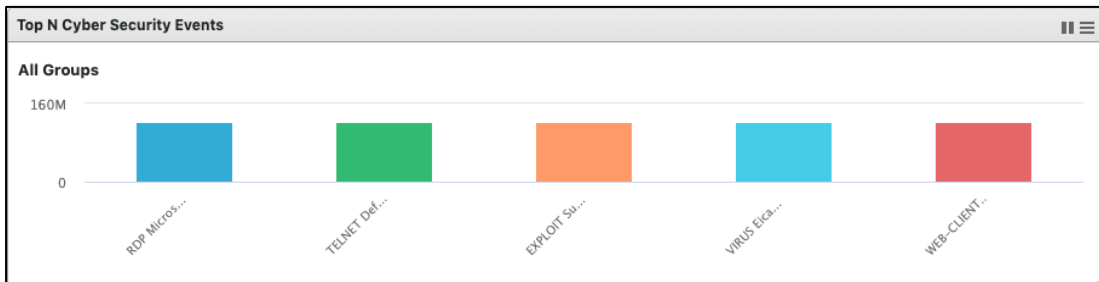
Cyber Security > Top N IPS Attack Events Categories

This widget displays the top N (5 or 10) categories of the cyber security events found in the selected device group(s) in the last 24 hours.



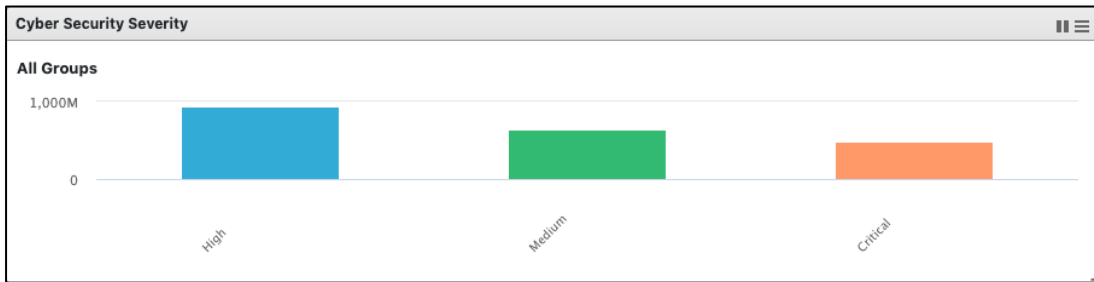
Cyber Security > Top N Cyber Security Events

This widget displays the top N (5 or 10) cyber security events found in the selected device group(s), in the last 24 hours.



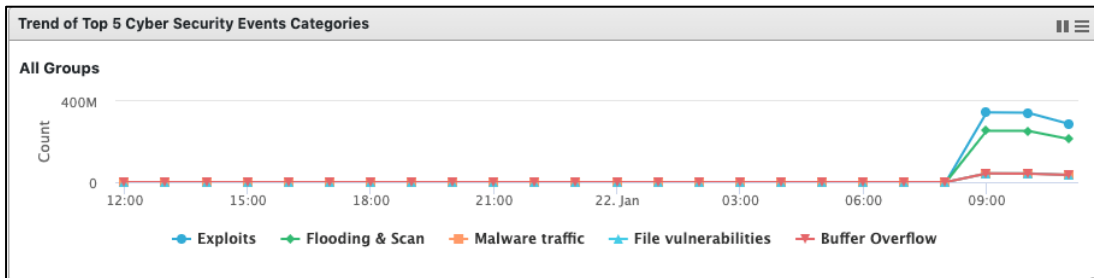
Cyber Security > Top N Cyber Security Severity

This widget displays the numbers of the cyber security events by severity levels in the selected device group(s) in the last 24 hours.



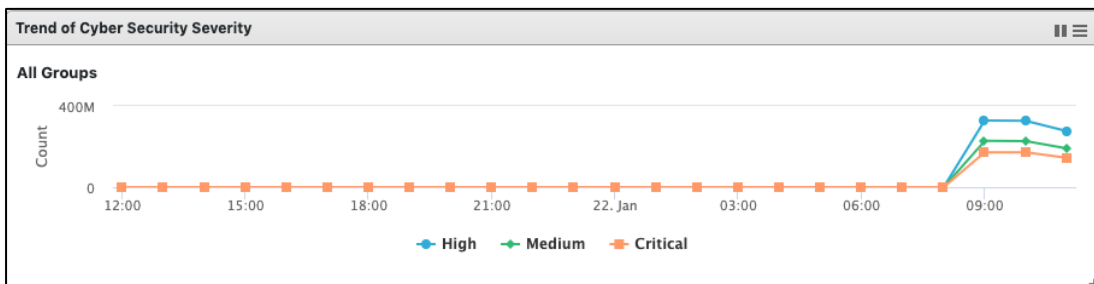
Cyber Security > Trends of Top N Cyber Security Events Categories

This widget displays the event trends for the top five cyber security categories in the selected device group(s) in the last 24 hours.



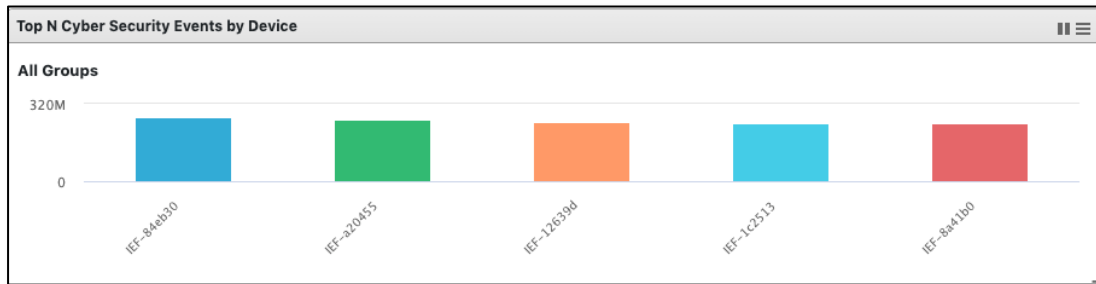
Cyber Security > Trends of Top N Cyber Security Severity

This widget displays the event trends of the cyber security severity levels in the selected device group(s) in the last 24 hours.



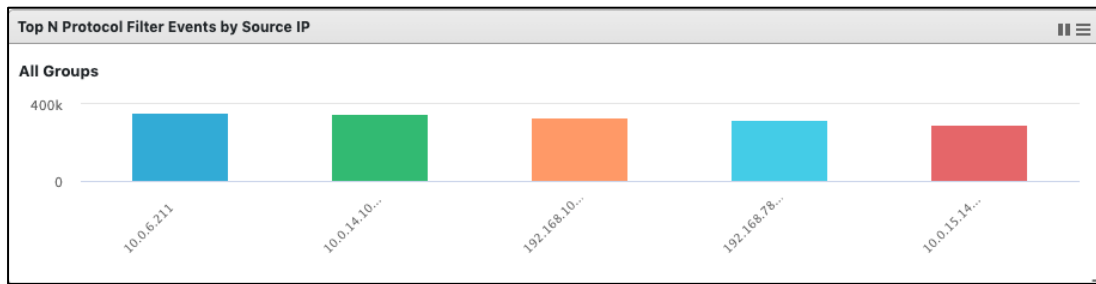
Cyber Security > Top N Cyber Security by Device

This widget displays the top N (5 or 10) devices in the selected device group(s) that have detected the most cyber security events in the last 24 hours.



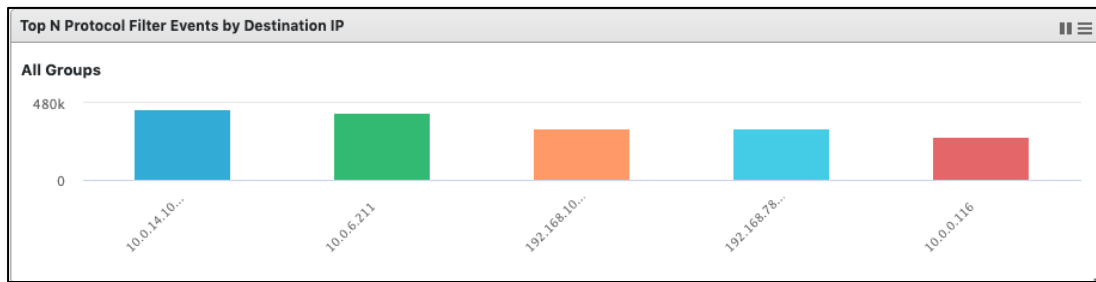
Protocol Filter > Top N Protocol Filter Events by Source IP

This widget displays the top N (5 or 10) source IP addresses of the protocol filter events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues, please see the note above.)



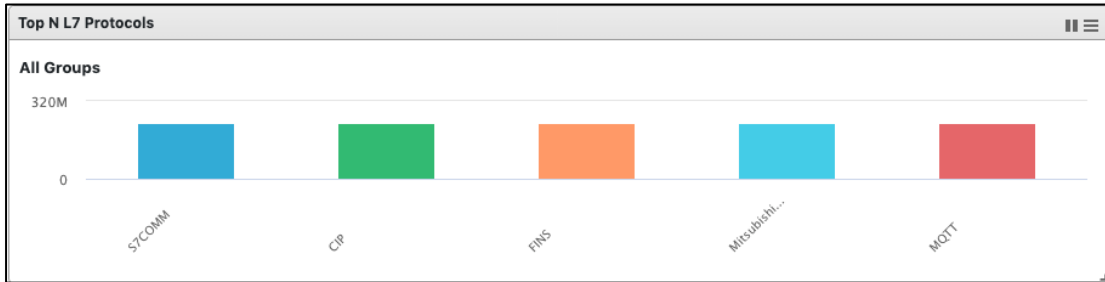
Protocol Filter > Top N Protocol Filter Events by Destination IP

This widget displays the top N (5 or 10) destination IP addresses of the protocol filter events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues, please see the note above.)



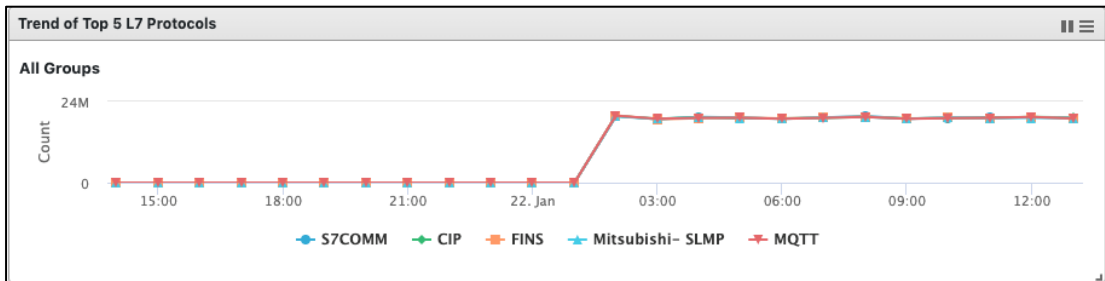
Protocol Filter > Top N L7 Protocols

This widget displays the top N (5 or 10) L7 protocol names of the protocol filter events found in the selected device group(s) in the last 24 hours.



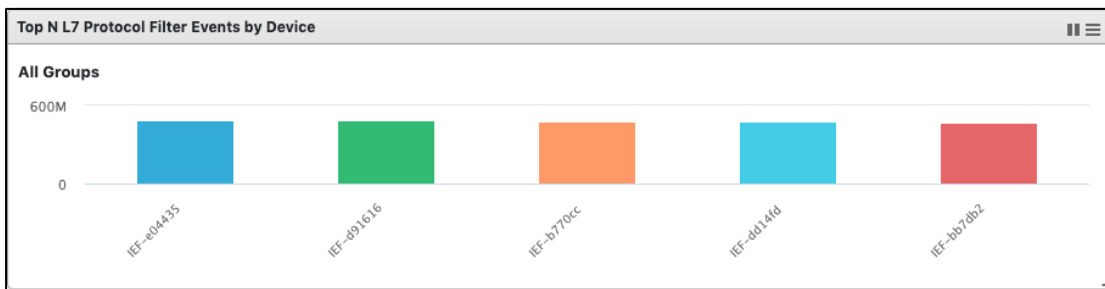
Protocol Filter > Trends of Top 5 L7 Protocols

This widget displays the event trends of the top five L7 protocol names found in the selected device group(s) in the last 24 hours.



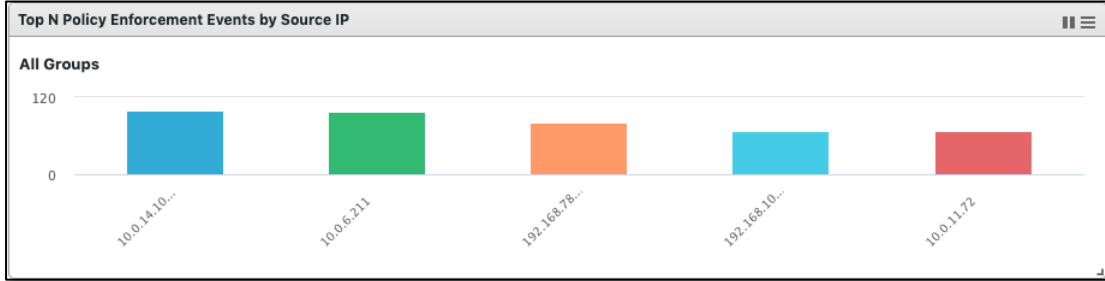
Protocol Filter > Top N L7 Protocol by Device

This widget displays the top N (5 or 10) devices in the selected device group(s) that have detected the most protocol filter events in the last 24 hours.



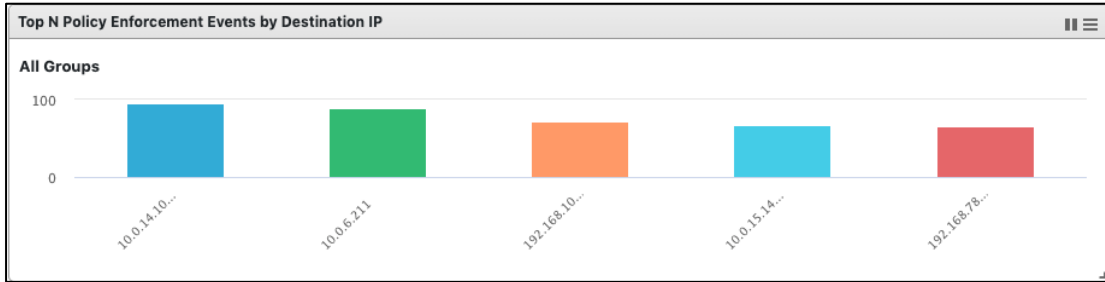
Policy Enforcement > Top N Policy Enforcement Events by Source IP

This widget displays the top N (5 or 10) source IP addresses of the policy enforcement events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues, please see the **note** above.)



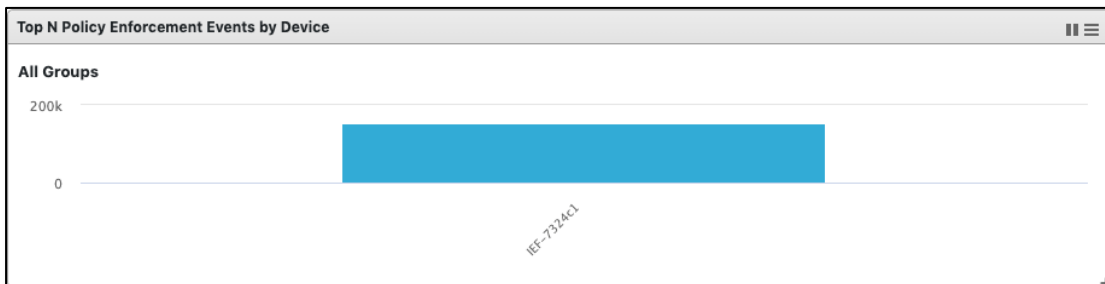
Policy Enforcement > Top N Policy Enforcement Events by Destination IP

This widget displays the top N (5 or 10) destination IP addresses of the policy enforcement events found in the selected device group(s) in the last 24 hours. (This feature may encounter performance issues, please see **note** above.)



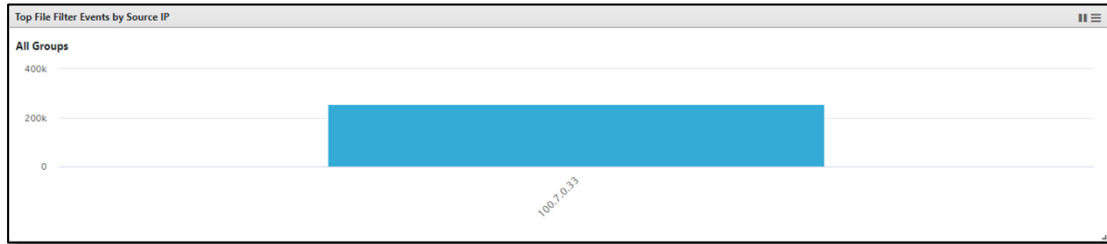
Policy Enforcement > Top N Policy Enforcement Events by Device

This widget displays the top N (5 or 10) devices in the selected device group(s) that have detected the most policy enforcement events in the last 24 hours.



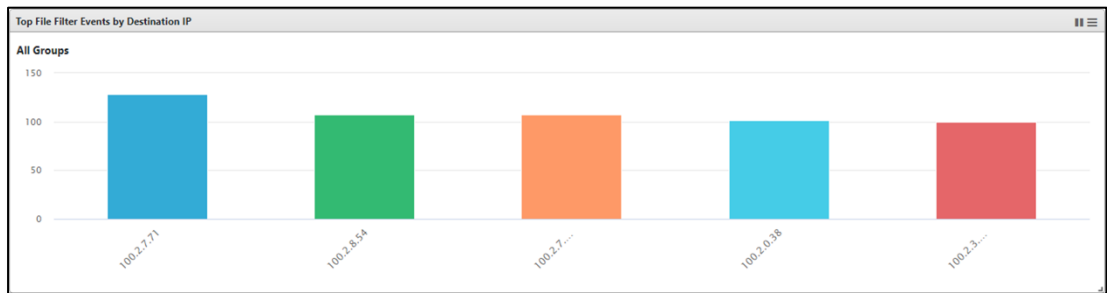
File Filter > Top File Filter Events by Source IP

This widget displays the top 5 or 10 source IP addresses for file filter events found in the selected device group(s) over the last 24 hours.



File Filter > Top File Filter Events by Destination IP

This widget displays the top 5 or 10 destination IP addresses of file filter events found in the selected device group(s) over the last 24 hours.



File Filter > Top File Filter Events by Device

This widget displays the top 5 or 10 devices in the selected device group(s) that detected the most file filter events over the last 24 hours.



Tab and Widget Management

This section describes how to manage the tabs and widgets in the web management console.

Add a Tab to the Dashboard

1. Click [Tab Settings].
2. Provide a name for the new tab then click [Ok].


Delete a Tab on the Dashboard

Mouse over the tab name. The delete button, [x], will appear. Click on the [x] button to delete the tab.


Add a Widget to the Dashboard

1. Click [Add Widgets].
2. Select one or multiple widgets by checking the checkbox. You can browse different categories of widgets by clicking different category names. The max amount of widgets for a tab is set to 10.
3. Click [Add] to add selected widgets to tab.

Remove a Widget from the Dashboard

Hover the mouse over the  button on the top right corner of the widget, click [Remove Widget], then click [OK] to confirm.



Resize the Size of a Widget

Hover the mouse over the bottom right corner of the widget. Click and drag the  button to resize the widget.

Move Widget Position

Hover the mouse over the title of the widget. The pointer will change to a cross icon. Click and drag the widget to the place you want it, then release the mouse. The widget will be placed automatically in an appropriate position.

Pause and Resume Widget Refresh

Click on the  button to pause automatic widget refresh on the widget title bar. To resume automatic refresh, click on the  button.

Widget Setting

Click [Widget Settings], and the following setting options will be shown in a popup dialog.

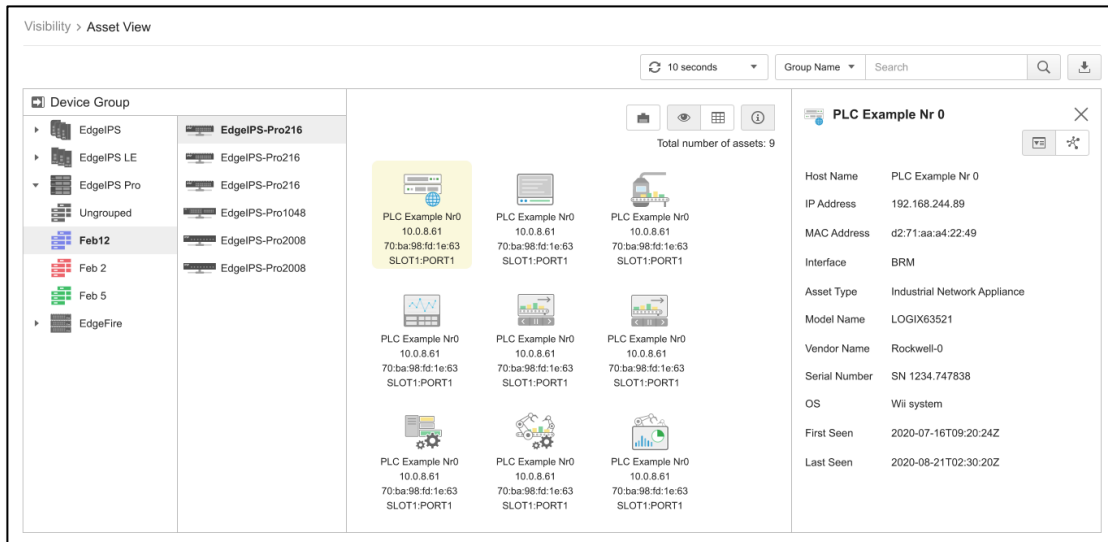
Setting	Procedure
Widget Name	Edit the widget name in the input box. The widget name will be displayed on the title of the widget in the Dashboard.
Auto Refresh Settings	Click on the drop-down button on the right of the option name to select a different frequency of data refresh such as [Every 30 seconds] or [Every minute]. You can choose [Manual Refresh] if the widget doesn't need to be refreshed automatically.
Top Statistics (selected widget only)	Click on the drop-down button on the right of the option name to show options for Top Statistics. Choose [Top 5] or [Top 10] for different counts of statistics.

Setting	Procedure
Chart Type (selected widget only)	Click on different chart icons for different chart types on the widget, such as a bar chart or a pie chart.
Device Type (selected widget only)	Click on the device type, EdgeFire/EdgeIPS, to get the corresponding group list. Select a group by clicking its group name on the [Groups] panel or deselect a group by clicking its group name on the [Selected Groups] panel.

When the configuration is done, click [OK] to save the settings.

The Visibility Tab

The [Visibility] tab gives you an overview of asset visibility for your managed assets. This tab provides you with timely and accurate information about the assets managed by Edge series devices.




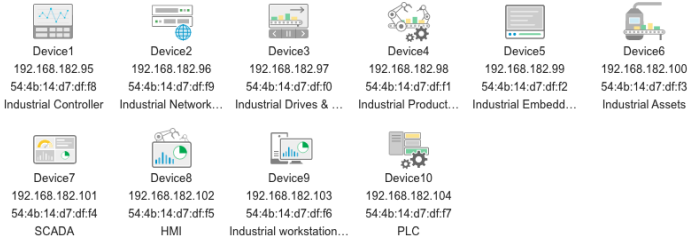

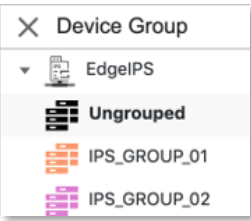
The assets, listed on the tab, are automatically detected by Edge series devices.

- The term **assets** in this chapter refers to the devices or hosts that are protected by Edge series solutions.
- The statistical information presented to you depends on your user account role and whether permission to manage the device groups has been shared with you. For more information, see [Sharing Management Permissions to Other User Accounts on page 44](#) and [User Roles on page 130](#).

Common Tasks


The following table lists the common tasks that are done under this tab.

Task	Action
To search an asset	<p>Specify the fields you want to search under, input the search string, and click the [Search] button.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Group Name ▾ <input style="width: 100%; border: none;" type="text" value="Search"/> Q </div> <p>Possible options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Group Name ■ Device Serial Number ■ Asset Hostname ■ Asset IP Address ■ Asset MAC Address ■ Asset Interface ■ Asset Type ■ Asset Vendor Name

Task	Action																																			
	<ul style="list-style-type: none"> Asset Model Name Asset Firmware Version Asset OS Name Asset Serial Number 																																			
To list devices and assets as icons	Click the Grid View  button. 																																			
To list devices in a table list	Click the Table View  button. <table border="1" data-bbox="515 790 1337 1032"> <thead> <tr> <th><input type="checkbox"/></th> <th>Host Name</th> <th>Asset Type</th> <th>IP Address</th> <th>MAC Address</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Device 1</td> <td>Industrial Controller</td> <td>192.168.182.95</td> <td>54:4b:14:d7:df:f8</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Device 2</td> <td>Industrial Network appliance</td> <td>192.168.182.96</td> <td>54:4b:14:d7:df:f9</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Device 3</td> <td>Industrial Drives & I/O Device</td> <td>192.168.182.97</td> <td>54:4b:14:d7:df:f0</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Device 4</td> <td>Industrial Production Machines</td> <td>192.168.182.98</td> <td>54:4b:14:d7:df:f1</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Device 5</td> <td>Industrial Embedded PC</td> <td>192.168.182.99</td> <td>54:4b:14:d7:df:f2</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Device 6</td> <td>Industrial assets</td> <td>192.168.182.100</td> <td>54:4b:14:d7:df:f3</td> </tr> </tbody> </table>	<input type="checkbox"/>	Host Name	Asset Type	IP Address	MAC Address	<input type="checkbox"/>	Device 1	Industrial Controller	192.168.182.95	54:4b:14:d7:df:f8	<input type="checkbox"/>	Device 2	Industrial Network appliance	192.168.182.96	54:4b:14:d7:df:f9	<input type="checkbox"/>	Device 3	Industrial Drives & I/O Device	192.168.182.97	54:4b:14:d7:df:f0	<input type="checkbox"/>	Device 4	Industrial Production Machines	192.168.182.98	54:4b:14:d7:df:f1	<input type="checkbox"/>	Device 5	Industrial Embedded PC	192.168.182.99	54:4b:14:d7:df:f2	<input type="checkbox"/>	Device 6	Industrial assets	192.168.182.100	54:4b:14:d7:df:f3
<input type="checkbox"/>	Host Name	Asset Type	IP Address	MAC Address																																
<input type="checkbox"/>	Device 1	Industrial Controller	192.168.182.95	54:4b:14:d7:df:f8																																
<input type="checkbox"/>	Device 2	Industrial Network appliance	192.168.182.96	54:4b:14:d7:df:f9																																
<input type="checkbox"/>	Device 3	Industrial Drives & I/O Device	192.168.182.97	54:4b:14:d7:df:f0																																
<input type="checkbox"/>	Device 4	Industrial Production Machines	192.168.182.98	54:4b:14:d7:df:f1																																
<input type="checkbox"/>	Device 5	Industrial Embedded PC	192.168.182.99	54:4b:14:d7:df:f2																																
<input type="checkbox"/>	Device 6	Industrial assets	192.168.182.100	54:4b:14:d7:df:f3																																
To fold up a device group	Click the X button to fold up the device group. 																																			

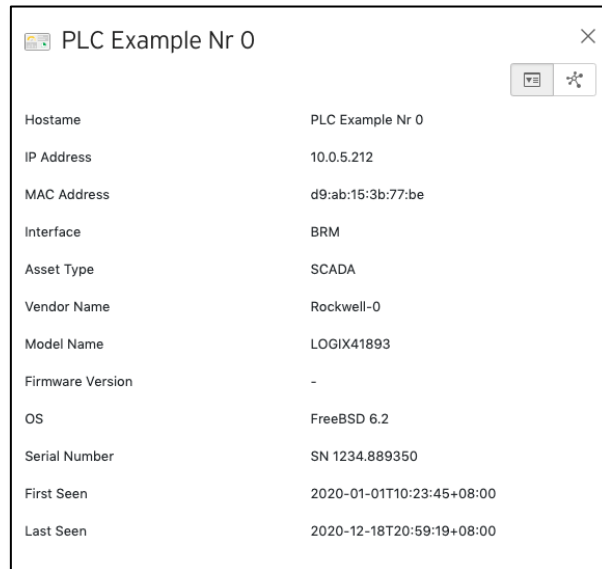
Displaying Asset Information

Procedure

1. Go to [Visibility] > [Assets View].
2. Click the  button to display asset information.

Basic Asset Information

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



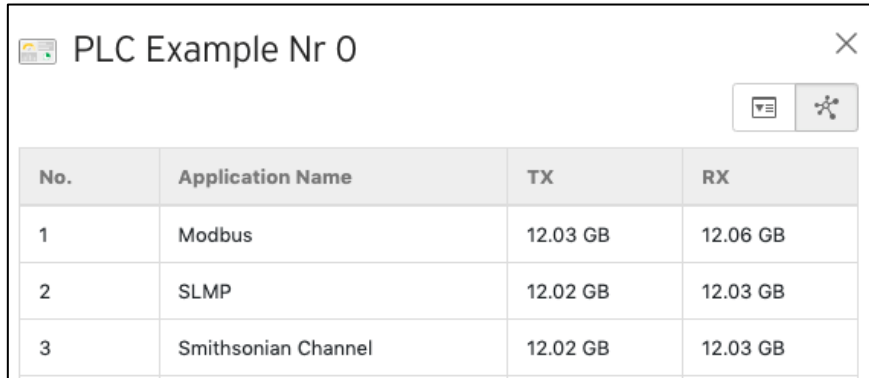
Field	Description	Example
Hostname	The name of the asset	Rockwell
IP Address	The IP address of the asset	10.24.254.94
MAC Address	The MAC address of the asset	00:0c:29:da:14:1c
Interface	The network interface of the device	PORT1
Asset Type	The type of the asset	Industrial Controller
Vendor Name	The vendor name of the asset	Rockwell Automation/Allen-Bradley
Model Name	The model name of the asset	1756-L61/B LOGIX5561
Firmware Version	The firmware version of the asset	1.0.0
OS	The system OS of the asset	Linux 2.6
Serial Number	The serial number of the asset	7079450
First Seen	The date and time the asset was first seen	2020-01-22T11:26:39+08:00
Last Seen	The date and time the asset was last seen	2020-01-22T11:44:28+08:00

Field	Description	Example
Hostname	The name of the asset	Rockwell
IP Address	The IP address of the asset	10.24.254.94
MAC Address	The MAC address of the asset	00:0c:29:da:14:1c
Interface	The network interface of the device	PORT1
Asset Type	The type of the asset	Industrial Controller
Vendor Name	The vendor name of the asset	Rockwell Automation/Allen-Bradley
Model Name	The model name of the asset	1756-L61/B LOGIX5561
Firmware Version	The firmware version of the asset	1.0.0
OS	The system OS of the asset	Linux 2.6
Serial Number	The serial number of the asset	7079450
First Seen	The date and time the asset was first seen	2020-01-22T11:26:39+08:00
Last Seen	The date and time the asset was last seen	2020-01-22T11:44:28+08:00

- EdgeIPS, EdgeFire and EdgeIPS Pro attempt to automatically collect the above information from an asset, and then transfer the information to the OT Defense Console™.

Real Time Network Application Traffic

The [Real Time Network Application Traffic] panel shows a list of network traffic statistics for the asset:




No.	Application Name	TX	RX
1	Modbus	12.03 GB	12.06 GB
2	SLMP	12.02 GB	12.03 GB
3	Smithsonian Channel	12.02 GB	12.03 GB

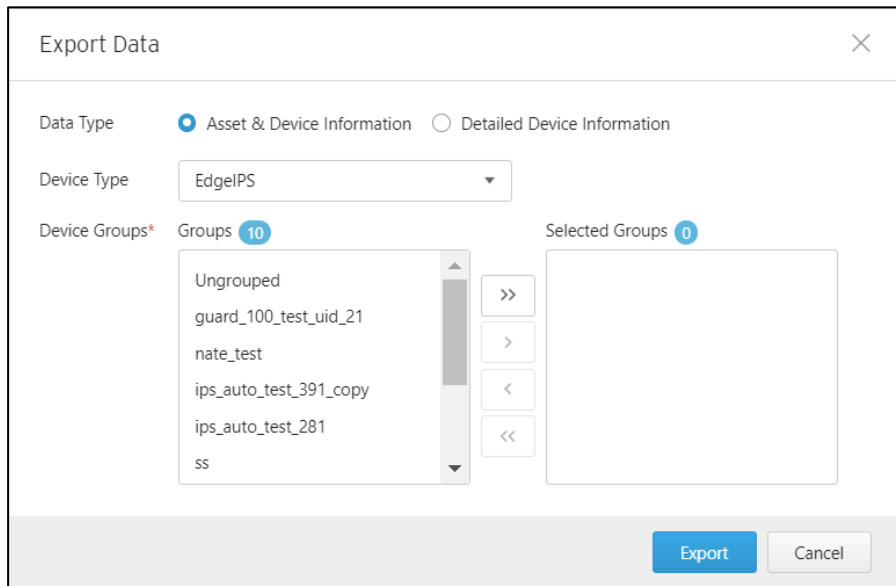
Field	Description
No.	Ordinal number of the application.
Application Name	The application type.
TX	The amount of traffic transmitted for this application.
RX	The amount of traffic received for this application.

- Click the [Manual asset info refresh] to refresh the information displayed.
- Specify the refresh time under the [Refresh Time] drop-down menu.

Exporting Data

Procedure

1. Go to [Visibility] > [Assets View].
2. Selected the target asset.
3. Click the  button to export asset/device information in a CSV file. The Export Data screen will appear.



4. Select one radio button for Data Type, **Asset & Device Information** or **Detailed Device Information**.
5. Select a device model from Device Type drop-down menu and the selected Device Groups will be shown accordingly.
6. Click button to move all groups for that type of device into the selected groups.
7. Click button to move the specified group(s) for that type of device into the selected groups.
8. Click [Export] to export data.

Pattern View

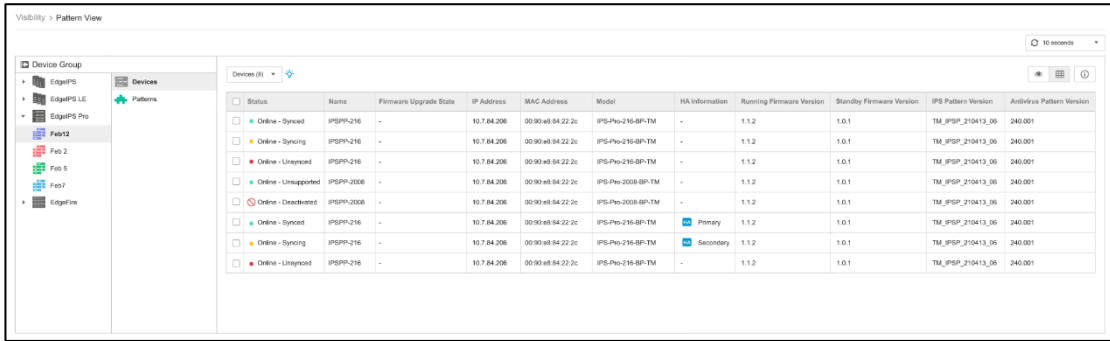
Pattern view allows all user roles to know the latest status of pattern for a device.

User Role	Access Pattern View
Master Admin	Yes
System Admin	Yes
Operator	Yes
Viewer	Yes

Procedure

1. Go to [Visibility] > [Pattern View].

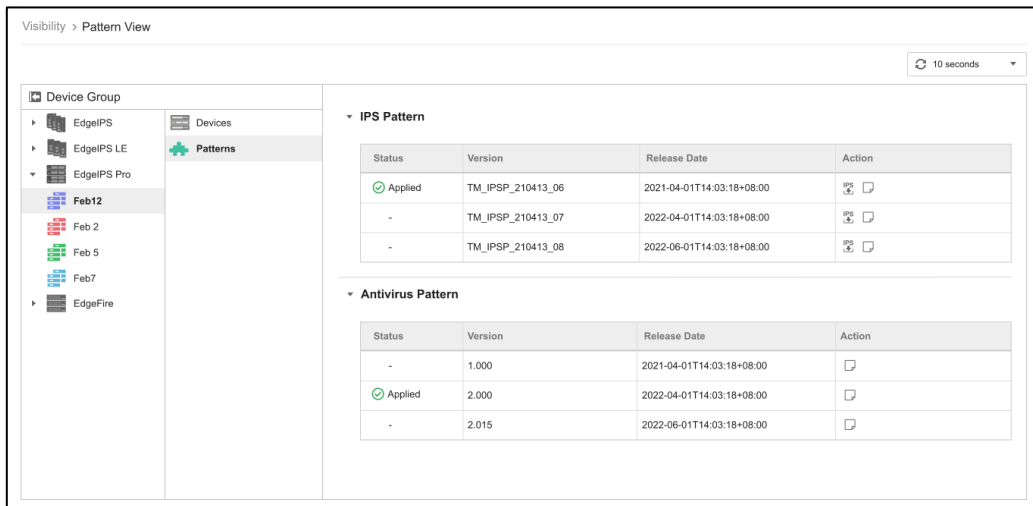
2. Click the target device group and the following screen will appear.



3. The following is an example for EdgeIPS™ Pro, which includes two types of patterns, IPS Pattern and Antivirus Pattern. All pattern history will be recorded.

The pattern details include pattern status (applied or unavailable), pattern version, release date, and actions as follows:

- Click to download IPS rule metadata
- Click to view release notes



Node Management

This chapter describes how to manage the TXOne Networks Edge series devices that have been registered to your OT Defense Console™. The [Node Management] tab show two levels of operations: device-level operation and group-level operation. You can operate the nodes directly or arrange them in several groups to share the same configurations. All the nodes are put in the [Ungroup] group by default.

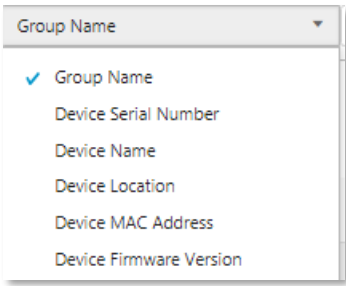



The following types of nodes can be managed by the OT Defense Console™:

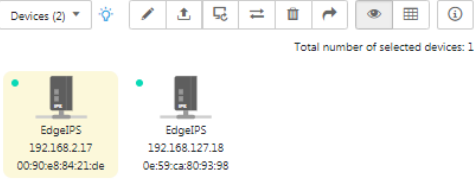
- **EdgeIPS™**
- **EdgeFire™**
- **EdgeIPS™ Pro**
- **EdgeIPS™ LE**

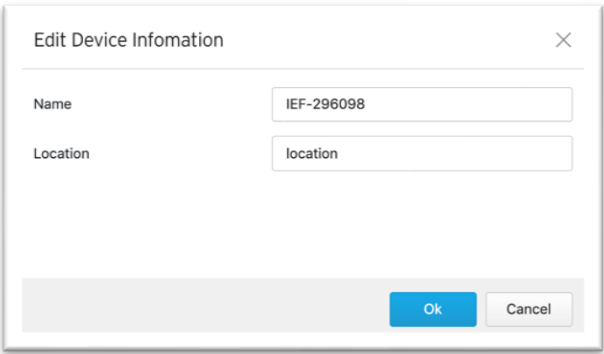

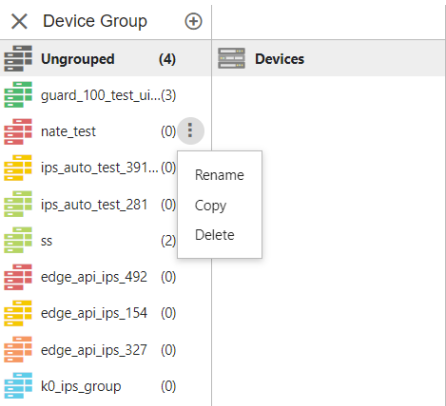
- The term **node** here refers to a TXOne Networks security device that has been registered to the OT Defense Console™.
- The maximum number of supported managed nodes depends on the ODC model (physical appliance) or the resources allocated to the ODC (virtual appliance). See the datasheet for more details.
- The information presented to you depends on your user account role and whether the permission to manage the device groups has been shared with you. For more information, see [Sharing Management Permissions to Other User Accounts on page 44](#) and [User Roles on page 130](#).

Common Tasks

The following table lists the common tasks that are used under this tab.

Task	Action
To search a device	Specify the fields you want to search under, input the search string, and click the [Search] button. 
To add a new device group	Click the  button to add a new device group.
To view devices that are not yet grouped	Click the [Ungroup] icon.
To view devices that are removed	Click the [Recycle Bin] icon.
To list devices as icons	Click the Grid View  button.
To list devices in a table list	Click the Table View  button.


Task	Action
To show the detailed information of a device	Click the Detailed Information  button. 
To edit/delete/move/reboot a device when in grid view	Select one or multiple nodes. You can make changes to the nodes via the top-right buttons. <ul style="list-style-type: none"> EdgeIPS  EdgeFire  EdgeIPS Pro 
To edit a device when in table view	Select a device and click the edit button at the top-right corner.

Task	Action
	
<p>To rename/copy/delete a group</p>	<p>Hover over the group icon, click the  button of the group, and select the desired action:</p>  <p>Rename: Rename the device group. Copy: Clone all source profile info to create a new profile for the new device group. Notice that the user role and permission and the managed node device won't be copied. Delete: Delete the device group.</p>


Device Group Management

Given the massive volume of devices that can be managed by ODC, ODC features device grouping so that the same security policy configurations can be shared among the devices that belong to the same group.


Creating a New Device Group

1. Under the [Device Group] panel, click .
2. Provide a name for the group and click [Confirm].
 - o Length: 1-32 characters
 - o Only a-z / A-Z / 0-9, underline "_", hyphen "-", parentheses "()", and dot "." are supported in group names.

Renaming or Deleting a Device Group

1. Hover over a group icon and click the  button of the group.
2. Select the desired action.

Moving a Node into a Group

1. Select one or multiple nodes, click the  button in the function area located at the top-right, and move the node(s) to a group.
2. Click [Move].
3. Select the name of the group which the node will be moved to.

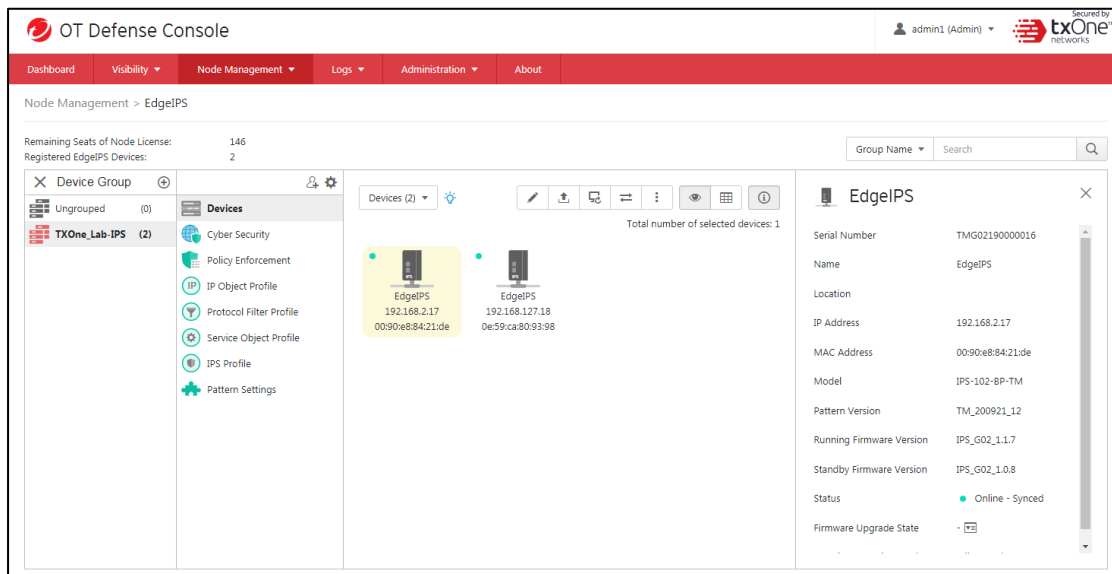
Managing EdgeIPS™ Devices

This section describes how to manage the EdgeIPS™ devices that have been registered to the OT Defense Console™.

Accessing the Management Tab

Procedure


1. Go to [Node Management] > [EdgeIPS].
2. Click a node icon to view the details of this node.

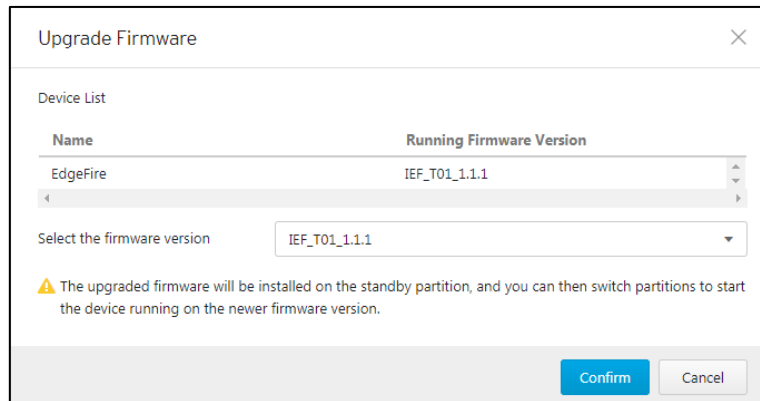


See [Common Tasks on page 30](#) for general tasks that can be performed under this tab.


Upgrading the Firmware


Procedure when in Table View

1. Click one or multiple nodes.
2. Click the  button.
3. Select a desired version number from the [Select the firmware version] drop-down menu, then click [Confirm].



Procedure when in Grid View


1. Click one or multiple nodes.
2. Click the  button.
3. Select a desired version number from the [Select the firmware version] drop-down menu, then click [Confirm].

■ Only firmware versions that are the same as or newer than the [Running Firmware Version] can be upgraded. After the new firmware is uploaded to the node, the new firmware will be stored in the standby disk partition of the node. You can click the  button to switch between the active and standby disk partition with which to boot the node, thus allowing the node to boot between the old and the new firmware. If the node does not support standby disk partition, then the new uploaded firmware will be installed automatically and become effective after the node is rebooted.


■ If the node is in **inline mode**, then during the firmware upgrade the network will be disconnected for a few minutes depending on CPU and traffic load on the node.

Editing Name / Location of a Node

Procedure when in Table View


1. Click the node and click the  button.
2. Provide name or location information for the node.

Procedure when in Grid View


1. Click the node and click the  button.
2. Provide name or location information for the node.

Rebooting the Node

Procedure When in Table View

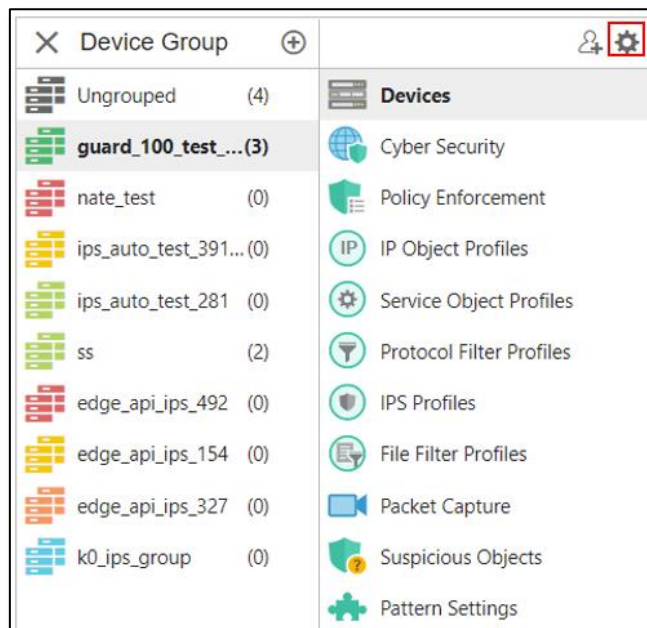
1. Select one or multiple nodes.
2. Click the  button.

Procedure When in Grid View

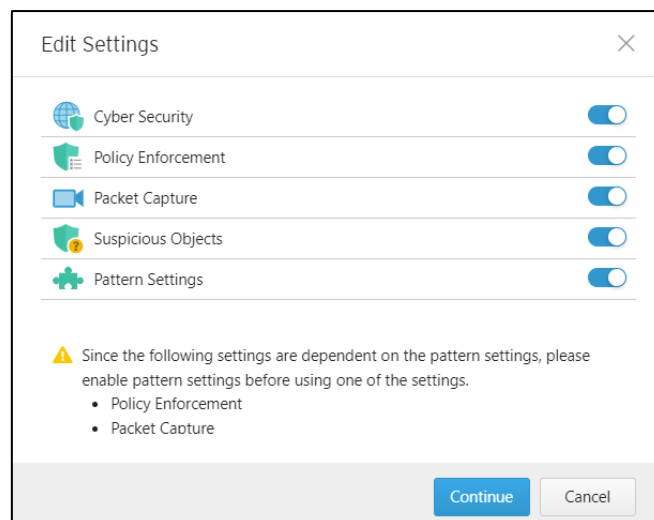
1. Select one or multiple nodes.
2. Click the  button.

Enabling Device Group Settings

1. Click the device group you want to manage.
2. Click the [Edit Settings] button.



An [Edit Settings] screen will appear.



Configuring Cyber Security

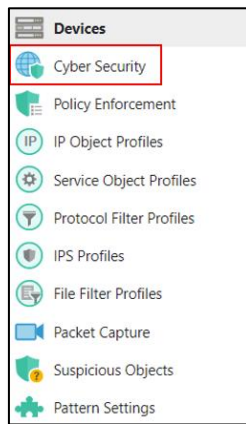
EdgeIPS features cyber security, which covers both intrusion prevention and denial of service attack prevention. The signature rules of intrusion prevention are called 'Trend Micro DPI Pattern'. This pattern is provided by Trend Micro and can be regularly updated through ODC.

Enabling Cyber Security

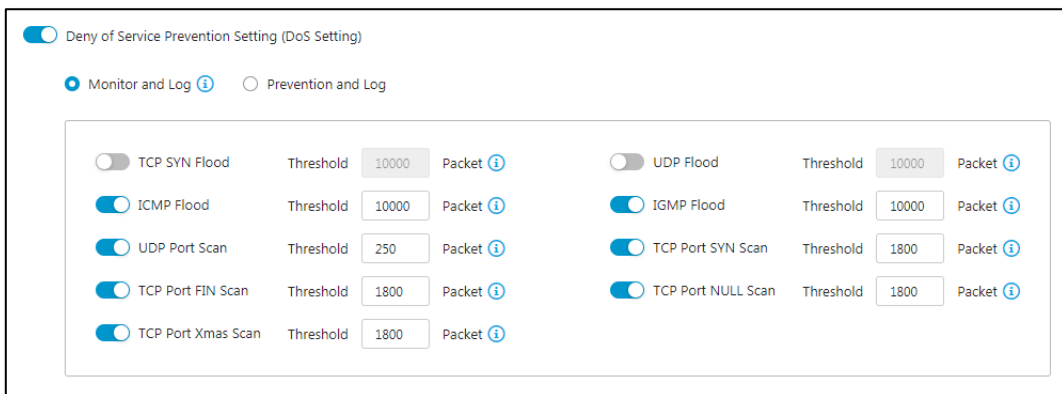
1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that [Cyber Security] is enabled, and click [Continue].

Configuring Cyber Security

1. Click the device group you want to manage.
2. Click the [Cyber Security] tab for the device group.



3. Use the toggle to enable or disable the 'Denial of Service Prevention' feature.



4. Select an action ([Monitor and Log] or [Prevent and Log]) for the feature.
5. (Optional) Configure the thresholds of the denial of service rules.

- Flood/Scan Attack Protection rules use detection period and threshold mechanisms to detect an attack. During a detection period (typically every 5 seconds), if the number of anomalous packets reaches the specified threshold, an attack detection occurs. If the rule action is "block", the security node blocks subsequent anomalous packets until the end of the detection period. After the detection period, the security node allows anomalous packets until the threshold is reached.

The following table summarizes the settings:

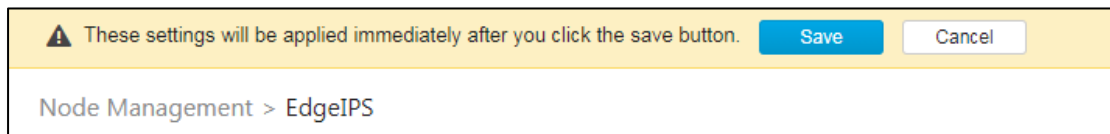
Mode (Security General Setting)	Action Setting	Action Performed
Inline Mode	Monitor and Log	<ul style="list-style-type: none"> ▪ Detects and monitors network attacks, but does not block network attacks. ▪ Generates logs.
	Prevent and Log	<ul style="list-style-type: none"> ▪ Blocks network attacks. ▪ Generates logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none"> ▪ Passively detects and monitors network attacks. ▪ Generates logs.

Configuring Policy Enforcement

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

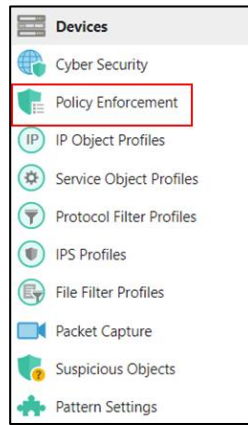
Enabling Policy Enforcement

1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that [Policy Enforcement] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

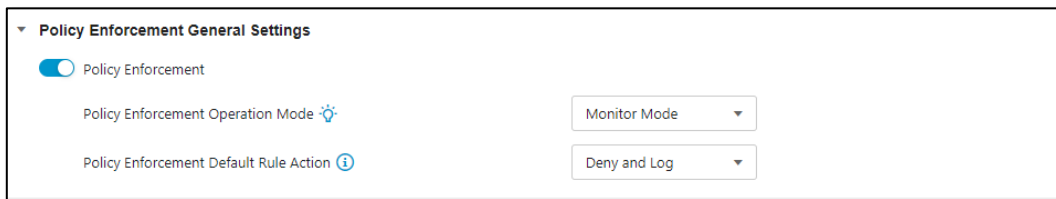


Configuring Policy Enforcement

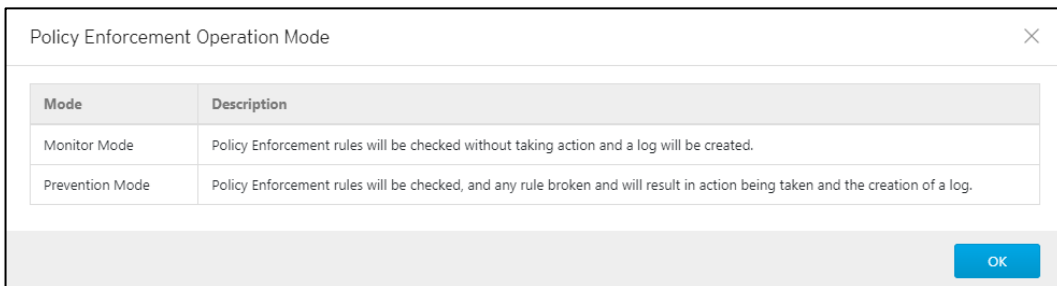
1. Configure the required object profiles.
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 75](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 76](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 77](#).
 - IPS profiles
For more information, see [Configuring IPS Profiles on page 97](#).
 - File Filter profiles
For more information, see [Configuring File Filter Profiles on page 100](#).
2. Click the device group you want to manage.
3. Click the [Policy Enforcement] tab.



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



5. Select a mode ([Monitor Mode], or [Prevention Mode]) for policy enforcement.



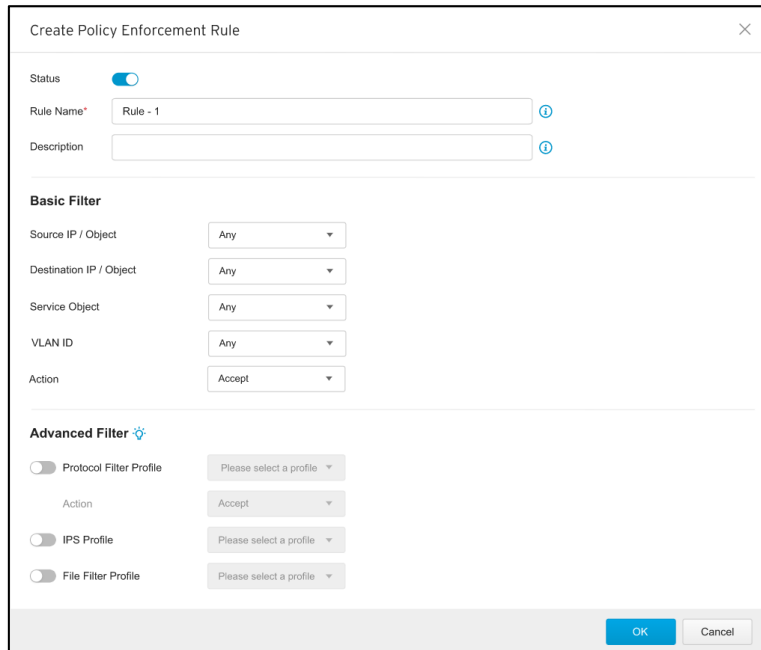
6. Under the [Policy Enforcement Default Rule Action] drop-down menu, select a default action for when no pattern is matched.

The following table summarizes the settings:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	<ul style="list-style-type: none"> ▪ Detects and monitors packets that violate a policy, but does not block network attacks. ▪ Generates logs.
	Prevention Mode	<ul style="list-style-type: none"> ▪ Blocks packets that violate a policy. ▪ Generates logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none"> ▪ Not supported.

Adding Policy Enforcement Rules

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



2. Use the toggle to enable or disable the policy rule.
3. Input a name for the rule and a description for the rule.
4. At the [Source IP / IP Object] drop-down menu, select one of the following for the source IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - Object

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

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

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

7. Under the [VLAN ID] , please enter the VLAN ID number. The number of maximum supported VLAN IDs is up to 5 IDs for each rule, and the VLAN ID Range is from 1 to 4094.
8. Under the [Action] drop-down menu, select one of the following:
 - a. **Accept:** Select this option to allow network traffic that matches this rule.
 - b. **Deny:** Select this option to block network traffic that matches this rule.
 - c. **Protocol Filter:** The node will further take actions based on the protocol filter:
 - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
 - Under the [Protocol Filter Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.
 - Under the [IPS Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
9. Click [Save] to save the configuration.

Managing Policy Enforcement Rules

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

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

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

Configuring Packet Capture

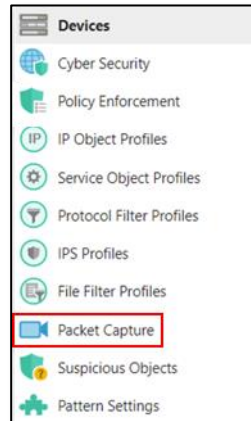
Packet Capture allows you to select one or multiple IPS rules to capture packets that meet their definitions, and this feature can help users to quickly collect hit IPS rule packets as well as help support teams to quickly address false positive or false negative IPS rule enforcements.

Enabling Packet Capture

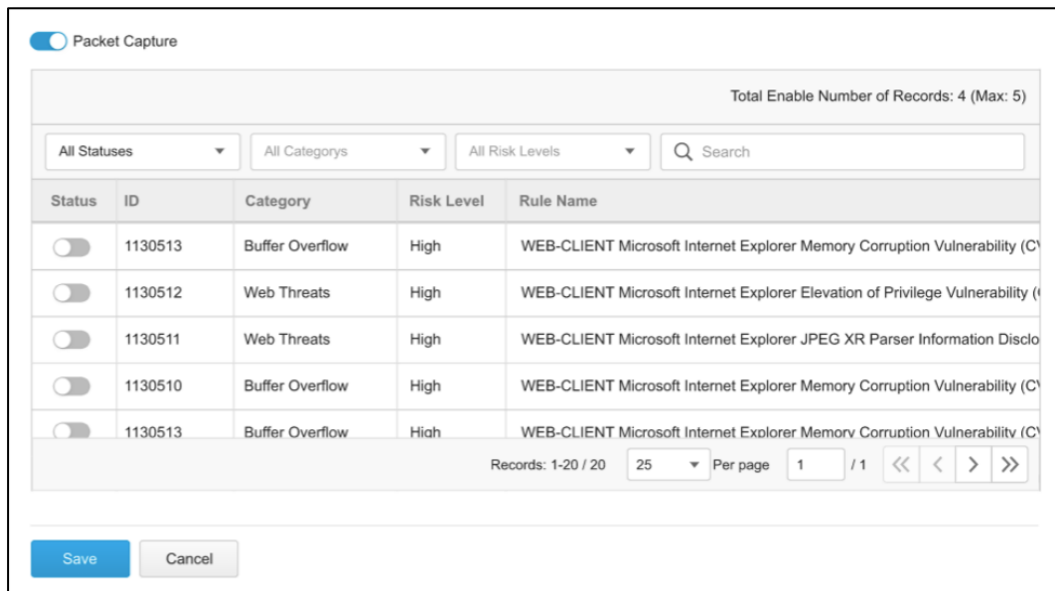
1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that [Packet Capture] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

Configuring Packet Capture

1. Click the device group you want to manage.
2. Click the [Packet Capture] tab.



3. Click [Enable] to enable IPS packet capture.



You can see the IPS rule list and select a rule to "Enable" for IPS packet capture. The IPS packet capture supports up to 20 rules being selected.

- The packet capture will collect selected IPS Rules. Once an IPS rule gets a hit, it will always collect the latest packet.

Configuring Suspicious Objects

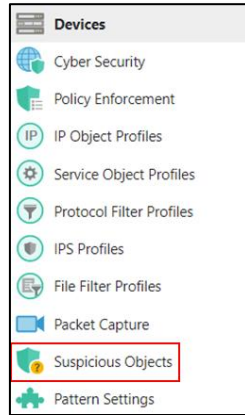
The Suspicious Object tab allows you to define the filter rules to pull suspicious objects from the global Suspicious Object Pool into a device group.

Enabling Suspicious Objects

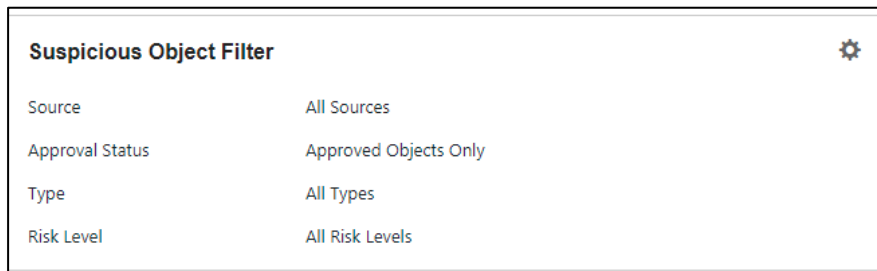
1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that [Suspicious Object] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

Configuring Suspicious Object Filter

1. Click the device group you want to manage.
2. Click the [Suspicious Object] tab.



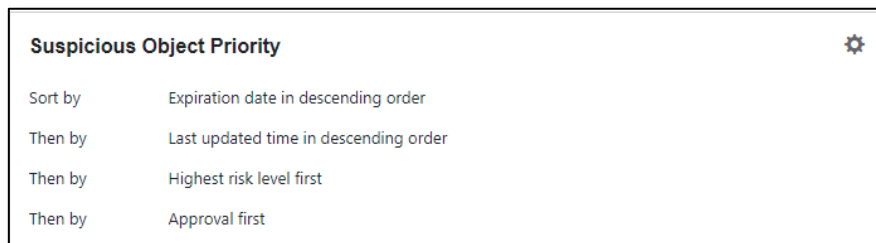
3. Click the gear button on the "Suspicious Object Filter" pane to configure the following settings:
 - Sources – the sources of the suspicious objects (SO); either "All Sources" or "Custom". You may further specify the names of the SO sources when "Custom" is selected.
 - Approval Status – either "Approved Objects Only" or "Approved and New Objects".
 - Types – "All Types", "Node" or "Link".
 - Risk Level – "All Risk Levels", "High Only" or "High and Medium".

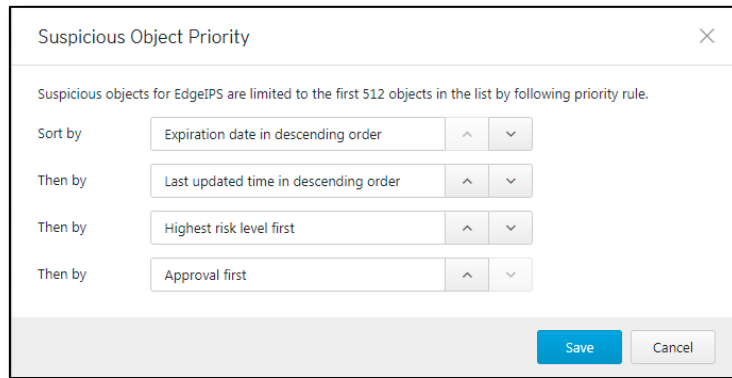


4. Click the "Save" button to save the changes.

Configuring Suspicious Object Priority

1. Click the gear button on the "Suspicious Object Priority" pane to configure the priority of different sorting methods for the system to determine which suspicious objects should be kept first when the list has reached the upper limit. (For EdgeIPS, the upper limit is 512 objects.)

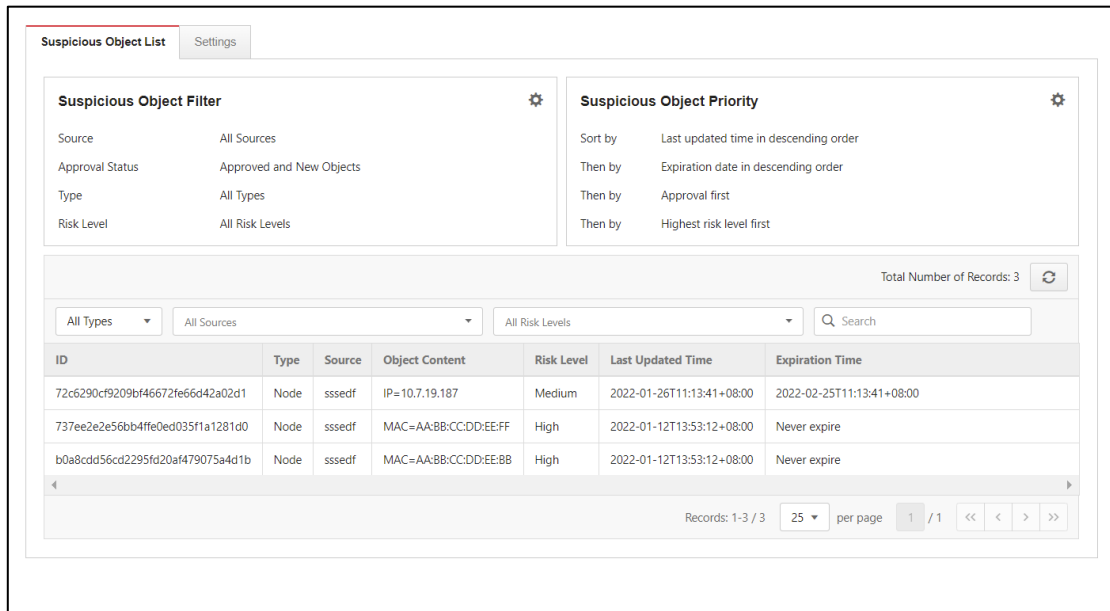




2. Click the "Save" button to save the changes.

Viewing the Suspicious Objects

The system will pull the suspicious objects from the global Suspicious Object Pool to this device group according to the given filter and display the objects in the table below the configuration panes. ODC will synchronize the suspicious object list to all devices in the group automatically.



Configuring Pattern Settings

Pattern Settings allows you to view the pattern information and to import a DPI (Deep Packet Inspection) pattern to the device from ODC. The DPI pattern, prepared by Trend Micro, contains signatures to enable the intrusion prevention features on the device. The intrusion prevention feature detects and prevents behaviors related to network intrusion attempts or targeted attacks at the network level.

Enabling Pattern Settings

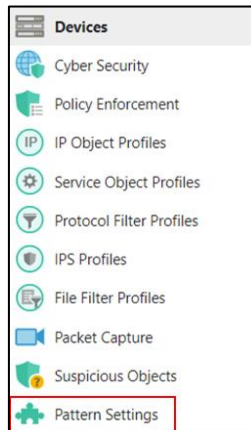
1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that the [Pattern Setting] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

⚠ These settings will be applied immediately after you click the save button. Save Cancel

Node Management > EdgeIPS

Configuring Pattern Settings

1. Click the device group you want to manage.
2. Click the [Pattern Settings] tab.



3. Select the DPI pattern to be deployed to the EdgeIPS™ nodes:
 - Latest: Always deploy the latest DPI pattern available on the OT Defense Console™.
 - Fixed version: Deploy the fixed DPI version specified.

Sharing Management Permissions to Other User Accounts

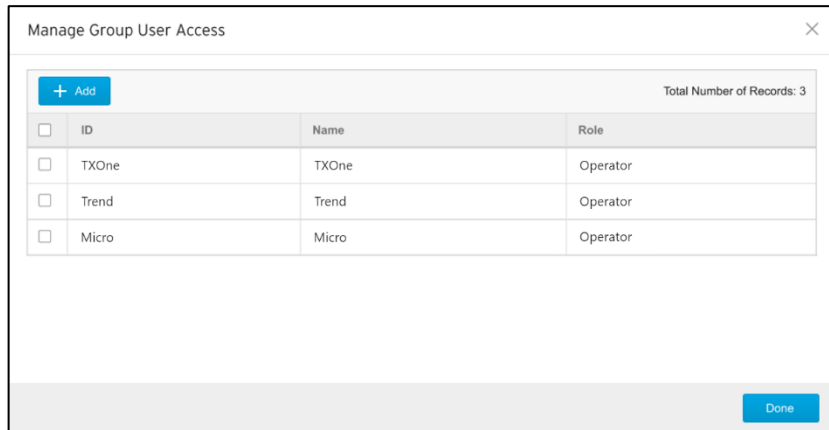
By default, the device group can only be created or managed by the [admin] account. However, you as the administrator can share management permissions to other users after a device group is created. See and [User Roles on page 130](#) for the details.

Procedure

1. Click the device group you want to manage.
2. Click the [Share with Others] button.



A [Manage Group User Access] screen will appear.



3. Add the user accounts with which you want to share management of the device group.

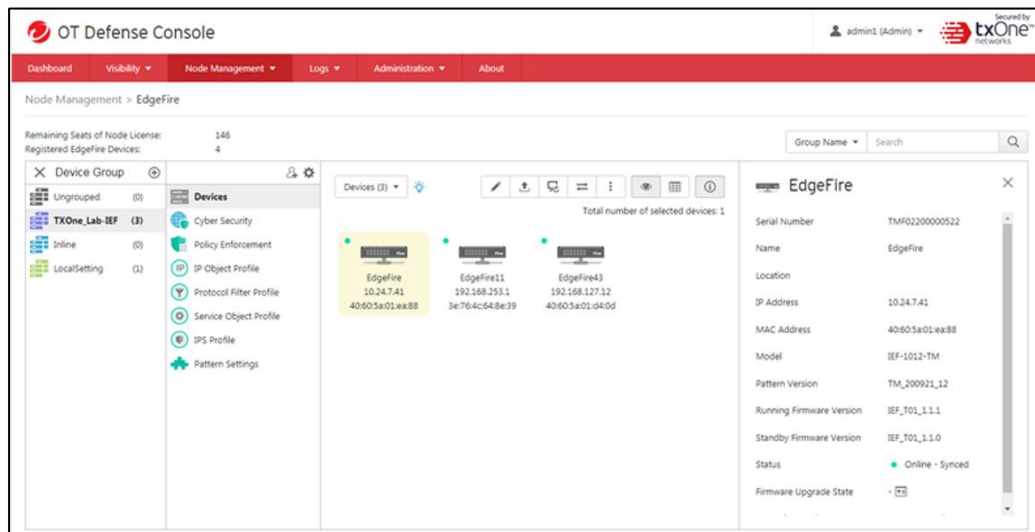
Managing EdgeFire™ Devices

This section describes how to manage the EdgeFire™ devices that have been registered to the OT Defense Console.

Accessing the Management Tab

Procedure

1. Go to [Node Management] > [EdgeFire].
2. Click a node icon to view the details of this node.



See [Common Tasks on page 30](#) for general tasks that can be performed under this tab.

Upgrading the Firmware

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Editing Name / Location of a Node

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Rebooting the Node

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Cyber Security

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

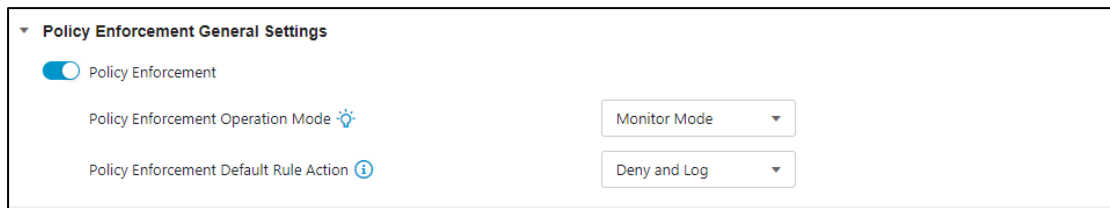
Configuring Policy Enforcement

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

Configuring Policy Enforcement

Procedure

1. Go to [Node Management] > [Policy Enforcement]

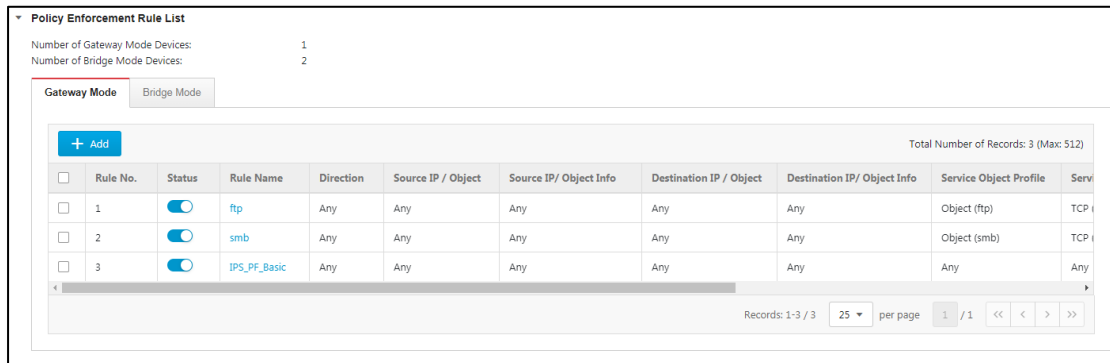


2. At the [Policy Enforcement] tab you will see the [Policy Enforcement General Settings] panel
3. Use the toggle to enable or disable the policy enforcement feature.
4. Select a mode ([Monitor Mode], or [Prevention Mode]) for the policy enforcement.
5. Under the [Policy Enforcement Default Rule Action] drop-down menu, select a default action when no pattern is matched.

The following table summarizes the settings:

Mode (Policy Enforcement)	Action Performed
Monitor Mode	<ul style="list-style-type: none"> ▪ Detects and monitors protocol access to OT assets, but does not block network attacks. ▪ Generates logs.
Prevention Mode	<ul style="list-style-type: none"> ▪ Blocks abnormal protocol access to OT assets. ▪ Generates logs.

Adding Policy Enforcement Rules in Gateway Mode



Policy Enforcement Rule List

Number of Gateway Mode Devices: 1
Number of Bridge Mode Devices: 2

Gateway Mode | Bridge Mode

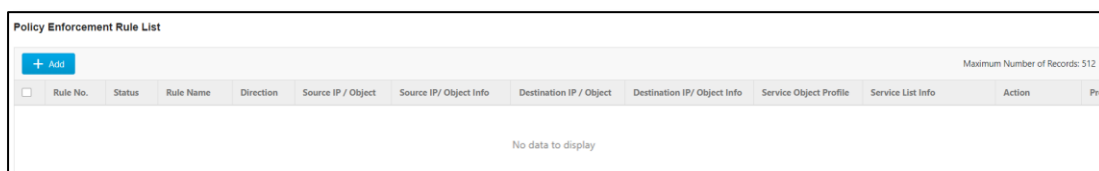
+ Add Total Number of Records: 3 (Max: 512)

<input type="checkbox"/>	Rule No.	Status	Rule Name	Direction	Source IP / Object	Source IP / Object Info	Destination IP / Object	Destination IP / Object Info	Service Object Profile	Service List Info
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	ftp	Any	Any	Any	Any	Any	Object (ftp)	TCP
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	smb	Any	Any	Any	Any	Any	Object (smb)	TCP
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	IPS_PF_Basic	Any	Any	Any	Any	Any	Any	Any

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

Procedure

1. Configure the required object profiles.
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 75](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 76](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 77](#).
 - IPS profiles
For more information, see [Configuring IPS Profiles on page 97](#).
 - File Filter profiles
For more information, see [Configuring File Filter Profiles on page 100](#).
2. Go to [Node Management] > [Policy Enforcement]
3. Under the [Policy Enforcement] tab you will see the following pane.

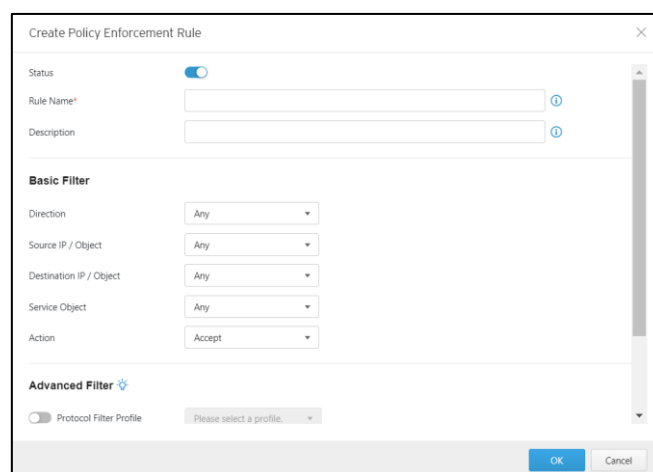


Policy Enforcement Rule List

+ Add Maximum Number of Records: 512

<input type="checkbox"/>	Rule No.	Status	Rule Name	Direction	Source IP / Object	Source IP / Object Info	Destination IP / Object	Destination IP / Object Info	Service Object Profile	Service List Info	Action	Pro
No data to display												

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



Create Policy Enforcement Rule

Status:

Rule Name*

Description

Basic Filter

Direction: Any

Source IP / Object: Any

Destination IP / Object: Any

Service Object: Any

Action: Accept

Advanced Filter

Protocol Filter Profile: Please select a profile.

OK Cancel

6. Input a name for the rule.
7. Input a description for the rule.
8. Under the [Interface Direction] drop-down menu, select one of the following for the network traffic direction:
 - Any
 - WAN to LAN
 - LAN to WAN
 - WAN to DMZ
 - DMZ to WAN
 - LAN to DMZ
 - DMZ to LAN
 - LAN to LAN

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

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

9. Under the [Source IP / IP Object Profile] drop-down menu, select one of the following for the source IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object

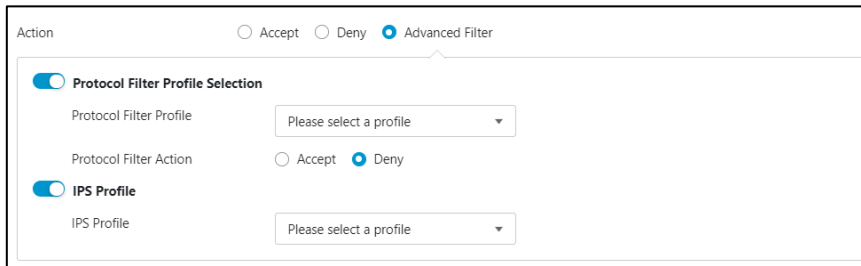
■ If you select [IP Object], then you need to select the IP object from an IP object profiles that have been created beforehand.

10. Under the [Destination IP / IP Object Profile] drop-down menu, select one of the following for the destination IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object

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

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

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



13. Click [Save] to save the configurations.

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

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

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

- When more than one policy enforcement rule is matched, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules are listed in the table under the UI tab ordered by priority, starting with the highest priority rule at the top.

Adding Policy Enforcement Rules in Bridge Mode

Rule No.	Status	Rule Name	Source IP / Object	Source IP / Object Info	Destination IP / Object	Destination IP / Object Info	Service Object Profile	Service List Info
1	<input checked="" type="checkbox"/>	smb	Any	Any	Any	Any	Object (smb)	TCP (139), TCP (445)
2	<input checked="" type="checkbox"/>	ftp	Any	Any	Any	Any	Object (ftp)	TCP (20 ~ 21)
3	<input checked="" type="checkbox"/>	IPS_PF_Basic	Any	Any	Any	Any	Any	Any

Procedure

- Configure the required object or objects.
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 75](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 76](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 77](#).
 - IPS profiles
For more information, see [Configuring IPS Profiles on page 97](#).
 - File Filter profiles
For more information, see [Configuring File Filter Profiles on page 100](#).
- Go to [Node Management] > [Policy Enforcement]
- Under the [Policy Enforcement] tab you will see the following pane:

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

Create Policy Enforcement Rule

Status:

Rule Name*

Description

Basic Filter

Direction: Any

Source IP / Object: Any

Destination IP / Object: Any

Service Object: Any

Action: Accept

Advanced Filter

Protocol Filter Profile: Please select a profile.

OK Cancel

6. Input a name for the rule.
7. Input a description for the rule.
8. Under the [Source IP / IP Object Profile] drop-down menu, select one of the following for the source IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object

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

9. Under the [Destination IP / IP Object Profile] drop-down menu, select one of the following for the destination IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object

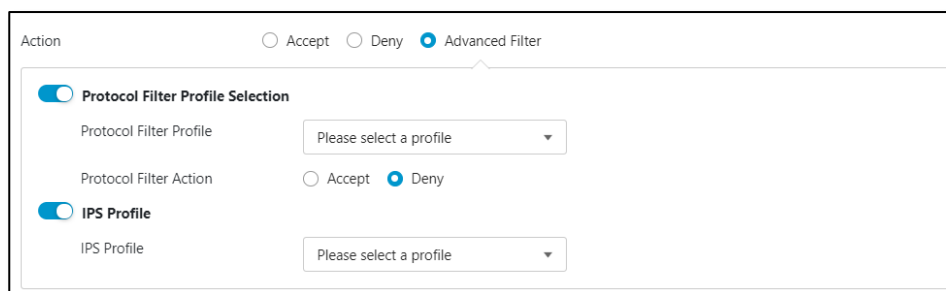
10. Under the [Service Object] drop-down menu, select one of the following for the layer 4 criteria:
 - TCP (You can further specify the port range for this protocol.)
 - UDP (You can further specify the port range for this protocol.)
 - ICMP (You can further specify the type and code for this protocol.)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

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

11. Use the toggle to enable or disable the VLAN ID, then input one or multiple VLAN IDs.

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

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



13. Click [Save] to save the configurations.

Managing Policy Enforcement Rules

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

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

- When more than one policy enforcement rule is matched, the device takes action based on the rule with the highest priority and ignores the rest of the rules. The rules are listed in the table under the UI tab ordered by priority, starting with the highest priority rule at the top.

Configuring Packet Capture

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Suspicious Objects

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Pattern Settings

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Sharing Management Permissions to Other User Accounts

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Managing EdgeIPS™ Pro Devices

EdgeIPS™ Pro series include three models, EdgeIPS™ Pro 1048/2096, EdgeIPS™ Pro 216, and EdgeIPS™ Pro 2008.

EdgeIPS™ Pro 1048 and EdgeIPS™ Pro 2096 now support the fiber module cards in addition to the copper module cards. Each device slot can be accommodated with Copper LAN module or Fiber LAN module. Various arrangements of interface can be provided to cater the need on your OT network, but notice that only copper module cards support hardware bypass mode. For EdgeIPS™ Pro 1048, up to 2 slots can be inserted with module cards. For EdgeIPS™ Pro 2096, up to 4 slots can be inserted with module cards.

Features of the fiber module cards are as below:

- 24 fiber ports (12 pairs of ports) for each fiber module card
- Maximum speed: 1 Gbps
- LFPT (Link Fault Pass Through) feature



Figure 2. EdgeIPS™ Pro 1048

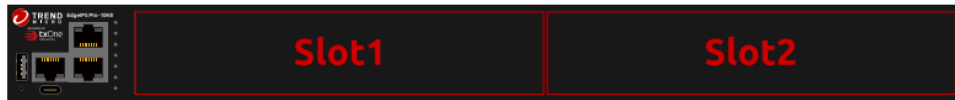


Figure 3. Slots of EdgeIPS™ Pro 1048

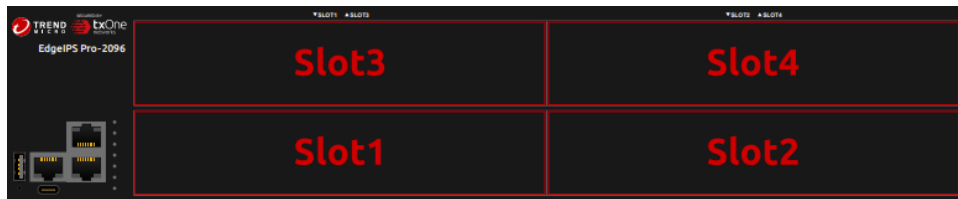


Figure 4. Slots of EdgeIPS™ Pro 2096

EdgeIPS™ Pro 216 and EdgeIPS™ Pro 208 are Transparent Security Appliances, supporting up to 8 pairs (EdgeIPS™ Pro 216)/4 pairs (EdgeIPS™ Pro 208) of IPS segments. Users can efficiently adapt the rack mounted EdgeIPS™ Pro 216 and EdgeIPS™ Pro 208 to a flexible solution for Ethernet communications.

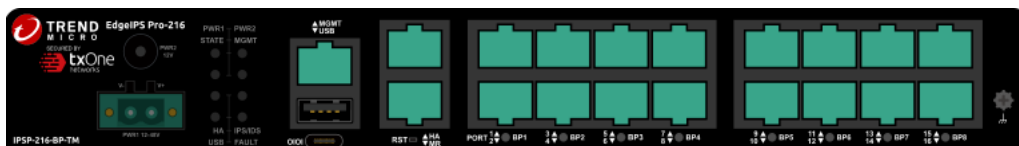


Figure 5. EdgeIPS™ Pro 216



Figure 6. EdgeIPS™ Pro 208

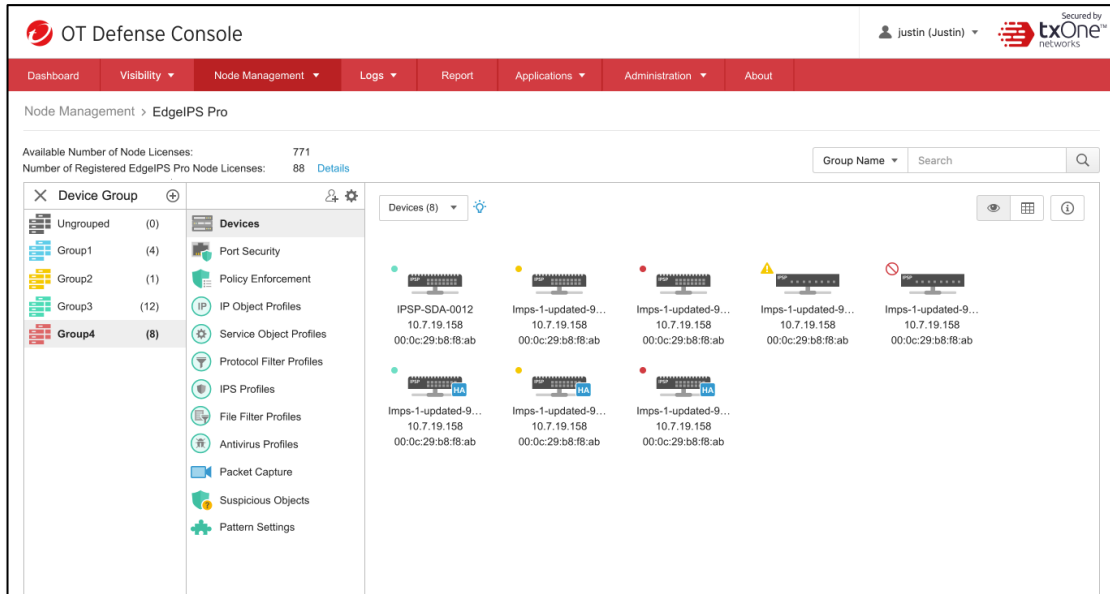
The following step-by-step instructions are for EdgeIPS™ Pro 1048.

Accessing the Management Tab

Procedure

1. Go to [Node Management] > [EdgeIPS Pro].

2. Click a node icon to view the details of this node.



See [Common Tasks on page 30](#) for general tasks that can be performed on this tab.

Upgrading the Firmware

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Editing Name / Location of a Node

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Rebooting the Node

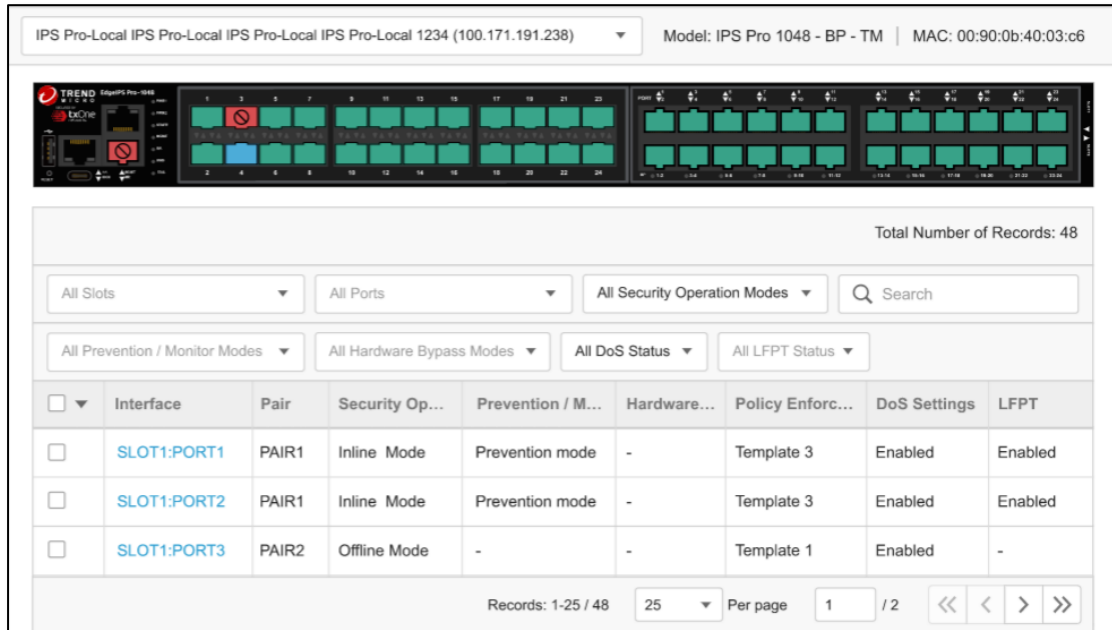
- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Port Security

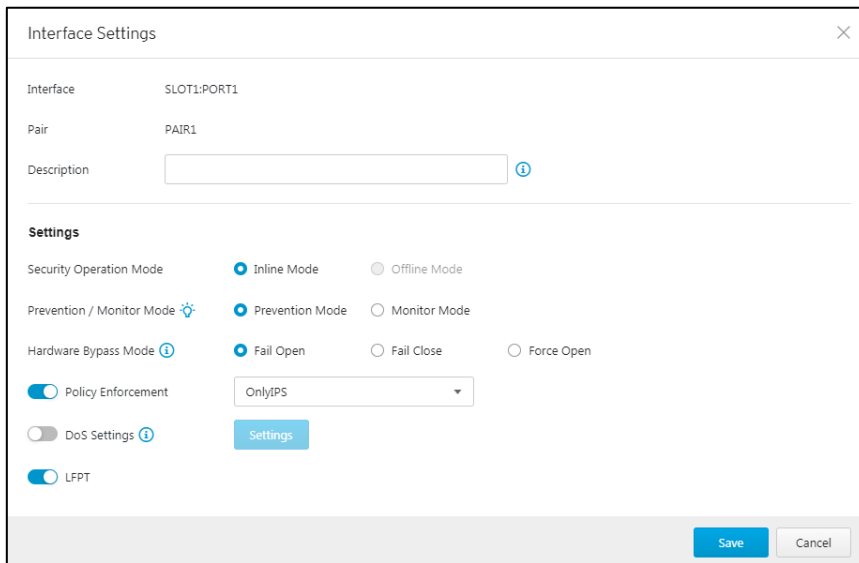
Procedure

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

- Port security page will show the EdgeIPS Pro's installed I/O module card and the connection status on the page tab.



- Click a specific [Interface] to configure port security.



- Input a clear, easily identifiable [Description] for the port security setting.
- Select an operation mode and configure the operation mode for the port of device

Task	Action
Inline Mode	Choose [Inline Mode] to have EdgeIPS Pro operate in Inline Mode. The pane can be connected from Port 1 or Port 2 at the same time.
Offline Mode	Choose [Offline Mode] to have EdgeIPS Pro operate in Offline Mode.

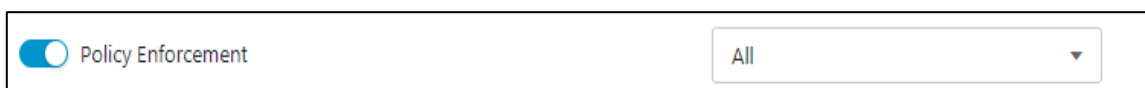
7. The [Prevention and Monitoring] setting allows you to configure prevention and monitor mode for port security.

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

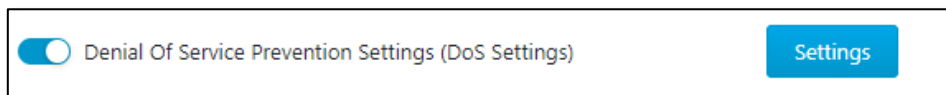
8. Configure [Hardware bypass] mode as 'fail open' or 'fail closed'. The following table lists hardware bypass mode definitions.

Setting	Description
Hardware Bypass	<p>Bypass ports allow uninterrupted network traffic even if a single in-line appliance is shut down or hangs. The settings for hardware bypass mode are:</p> <ul style="list-style-type: none"> ▪ Fail Open: Allows all network traffic to pass through the appliance when a system fails. ▪ Fail Closed: Closes the links for the interface pair and prevents any network traffic from passing through the appliance when a system fails. ▪ Force Open: Always allows all network traffic to pass through the appliance.

9. Use the toggle to enable policy enforcement and apply a created policy enforcement rule set



10. Use the toggle to enable [Denial of Service Prevention]



11. Click the [Settings] tab you will see the [Denial of Service Prevention] pane.

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

DoS Settings ✕

<input checked="" type="checkbox"/> TCP SYN Flood	Threshold	<input type="text" value="10000"/>	Packet	ⓘ
<input checked="" type="checkbox"/> UDP Flood	Threshold	<input type="text" value="10000"/>	Packet	ⓘ
<input checked="" type="checkbox"/> ICMP Flood	Threshold	<input type="text" value="10000"/>	Packet	ⓘ
<input checked="" type="checkbox"/> IGMP Flood	Threshold	<input type="text" value="10000"/>	Packet	ⓘ
<input checked="" type="checkbox"/> UDP Port Scan	Threshold	<input type="text" value="250"/>	Packet	ⓘ
<input checked="" type="checkbox"/> TCP Port SYN Scan	Threshold	<input type="text" value="1800"/>	Packet	ⓘ
<input checked="" type="checkbox"/> TCP Port FIN Scan	Threshold	<input type="text" value="1800"/>	Packet	ⓘ
<input checked="" type="checkbox"/> TCP Port NULL Scan	Threshold	<input type="text" value="1800"/>	Packet	ⓘ
<input checked="" type="checkbox"/> TCP Port Xmas Scan	Threshold	<input type="text" value="1800"/>	Packet	ⓘ

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

13. Use the toggle to enable [LFPT] function.

LFPT

■ The Link Fault Pass Through (LFPT) provides constant monitoring of the links connected to the media converters. If either of the copper interface links fails, the media converter will pass the fail state on throughout the link then taking down the middle fiber link as well as the copper link on the opposite end.

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

Configuring Policy Enforcement

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

Procedure

1. Go to [Node Management] > [Policy Enforcement].
At the [Policy Enforcement] tab you will see the [Policy Enforcement rule set] pane.
2. Click "Add" button to create Policy Enforcement Rule set.

	No.	Rule Set Name	Number of Rules	Description	Last Update
+ Add	Total Number of Records: 1 (Max: 64)				
<input type="checkbox"/>	1	All	3		2020-08-27T00:38:23+08:00

3. Create rule set name and description if necessary.
4. At the [Policy Enforcement Default Rule Action] pane, select a default action [Accept] or [Deny] for when no pattern is matched.

▼ Policy Enforcement General Settings

Policy Enforcement

Policy Enforcement Operation Mode Monitor Mode ▼

Policy Enforcement Default Rule Action Deny and Log ▼

Adding Policy Enforcement Rules

Procedure

1. Configure the required object or objects.
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 75](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 76](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 77](#).
 - IPS profiles
For more information, see [Configuring IPS Profiles on page 97](#).
 - File Filter profiles
For more information, see [Configuring File Filter Profiles on page 100](#).
 - Antivirus profiles
For more information, see [Configuring Antivirus Profiles on page 104](#).
2. Go to [Node Management] > [Policy Enforcement].
3. Under the [Policy Enforcement] tab you will see the following panes.

Security > Policy Enforcement					
Total Number of Records: 1 (Max: 64)					
No.	Rule Set Name	Number of Rules	Description	Last Update	
1	Rule_Set_1	2		2020-09-17T17:34:53+08:00	<input type="checkbox"/>

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

▼ Policy Enforcement General Settings

Policy Enforcement

Policy Enforcement Operation Mode Monitor Mode ▼

Policy Enforcement Default Rule Action Deny and Log ▼

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

Edit Policy Enforcement Rule

Status

Rule Name* i

Description i

Basic Filter

Source IP / Object ▼

Destination IP / Object ▼

Service Object ▼

VLAN ID ▼

Action ▼

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

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

9. At the [Destination IP / IP Object Profile] drop-down menu, select one of the following for the destination IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - IP Object

10. At the [Service Object] drop-down menu, select one of the following for the layer 4 criteria:
 - TCP (You can further specify the port range for this protocol.)
 - UDP (You can further specify the port range for this protocol.)
 - ICMP (You can further specify the type and code for this protocol.)
 - Custom (You can further specify the protocol number for this protocol. The term protocol number refers to the one defined in the internet protocol suite.)
 - Service Object


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

11. Use the toggle to enable or disable the VLAN ID, then input one or multiple VLAN IDs.

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

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

- a. **Accept:** Select this option to allow network traffic that matches this rule.
- b. **Deny:** Select this option to block network traffic that matches this rule.
- c. **Advanced Filter:** Select "Accept" and "Accept and log", and you will be able to do further actions based on the protocol filter:

Advanced Filter 

<input checked="" type="checkbox"/>	Protocol Filter Profile	All ▼
	Protocol Filter Action	Deny and Log ▼
<input checked="" type="checkbox"/>	IPS Profile	default ▼
<input checked="" type="checkbox"/>	File Filter Profile	All ▼
<input checked="" type="checkbox"/>	Antivirus Filter Profile	default ▼

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

Click [OK] to save the configuration.

Managing Policy Enforcement Rules

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

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

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

Configuring Packet Capture

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Suspicious Objects

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

Configuring Pattern Settings

- Click the device group you want to manage.
- Click the [Pattern Settings] tab.
- Select a DPI pattern to be deployed to the EdgeIPS™ Pro nodes:
 - Latest: Always deploy the latest DPI pattern available on the OT Defense Console.
 - Fixed version: Deploy the fixed DPI version specified.

IPS Pattern Update

Latest TM_IPSP_210719_21

Fixed version

Antivirus Pattern Update

Latest 2.004

Fixed version

Sharing Management Permissions to Other User Accounts

- The configurations are the same as those of managing EdgeIPS™ devices. Please see [Managing EdgeIPS™ Devices on page 33](#) for more details.

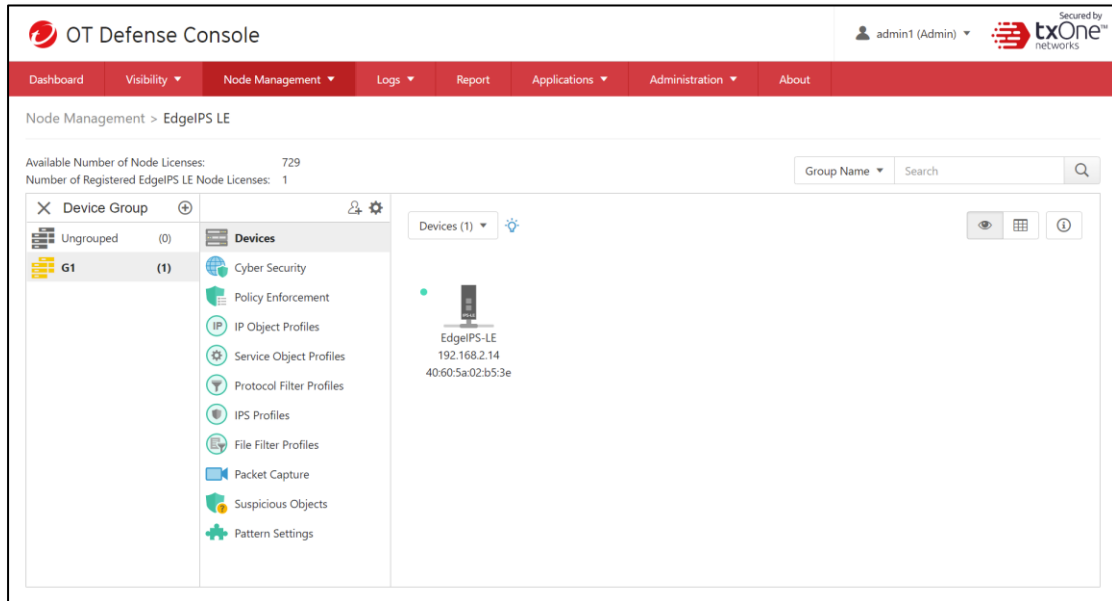
Managing EdgeIPS™ LE Devices

This section describes how to manage the EdgeIPS™ LE devices that have been registered to the OT Defense Console.

Accessing the Management Tab

Procedure

- Go to [Node Management] > [EdgeIPS LE].
- Click a node icon to view the details of this node.

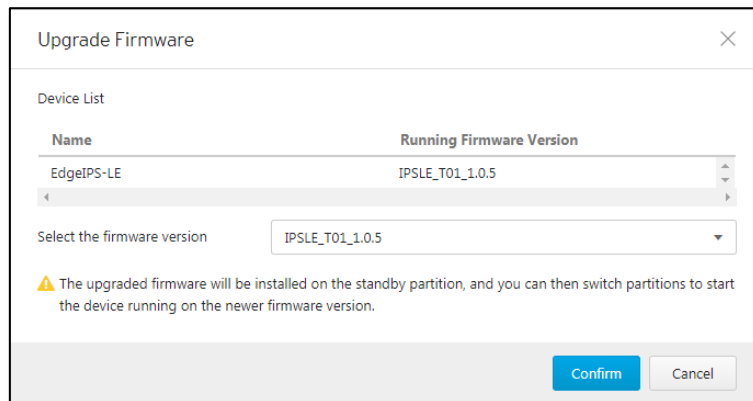


See [Common Tasks on page 30](#) for general tasks that can be performed under this tab.

Upgrading the Firmware


Procedure when in Table View

1. Click one or multiple nodes.
2. Click the button.
3. Select a desired version number from the [Select the firmware version] drop-down menu, then click [Confirm].




Procedure when in Grid View

1. Click one or multiple nodes.
2. Click the button.
3. Select a desired version number from the [Select the firmware version] drop-down menu, then click [Confirm].


- Only firmware versions that are the same as or newer than the [Running Firmware Version] can be upgraded. After the new firmware is uploaded to the node, the new firmware will be stored in the standby disk partition of the node. You can click the  button to switch between the active and standby disk partition with which to boot the node, thus allowing the node to boot between the old and the new firmware. If the node does not support standby disk partition, then the new uploaded firmware will be installed automatically and become effective after the node is rebooted.
- If the node is in **inline mode**, then during the firmware upgrade the network will be disconnected for a few minutes, depending on CPU and traffic load on the node.

Editing Name / Location of a Node

Procedure When in Table View


1. Click the node and click the  button.
2. Provide name or location information for the node.

Procedure When in Grid View


1. Click the node and click the  button.
2. Provide name or location information for the node.

Rebooting the Node

Procedure When in Table View

1. Select one or multiple nodes.
2. Click the  button.

Procedure When in Grid View

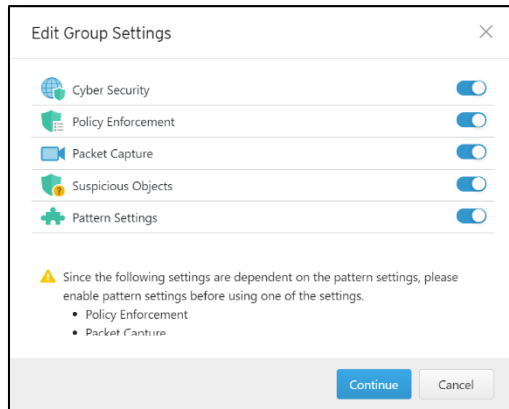
1. Select one or multiple nodes.
2. Click the  button.

Enabling Device Group Settings

1. Click the device group you want to manage.
2. Click the [Edit Group Settings] button.



An [Edit Group Settings] screen will appear.



Configuring Cyber Security

EdgeIPS™ LE features cyber security, which covers both intrusion prevention and denial of service attack prevention. The signature rules of intrusion prevention are called the 'Trend Micro DPI Pattern'. This pattern is provided by Trend Micro and can be regularly updated through ODC.

Enabling Cyber Security

1. Click the device group you want to manage.
2. Click the [Edit Settings] button. An [Edit Settings] screen will appear.
3. Ensure that [Cyber Security] is enabled, and click [Continue].

Configuring Cyber Security - Intrusion Prevention

Click the [Cyber Security] tab for the device group.



Configuring Cyber Security - Denial of Service Prevention

1. Click the device group you want to manage.
2. Click the [Cyber Security] tab for the device group.

- Use the toggle to enable or disable the 'Denial of Service Prevention' feature.

- Select an action ([Monitor and Log] or [Prevent and Log]) for the feature.

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

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

The following table summarizes the settings:

Mode (Security General Setting)	Action Setting	Action Performed
Inline Mode	Monitor and Log	<ul style="list-style-type: none"> Detects and monitors network attacks, but does not block network attacks. Generates logs.
	Prevent and Log	<ul style="list-style-type: none"> Blocks network attacks. Generates logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none"> Passively detects and monitors network attacks. Generates logs.

Configuring Policy Enforcement

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

Enabling Policy Enforcement

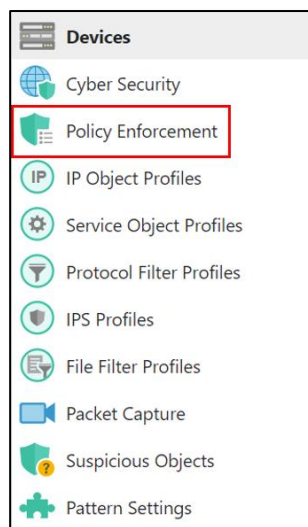
- Click the device group you want to manage.
- Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
- Ensure that [Policy Enforcement] is enabled, and click [Continue].
- Click the [Save] button to apply the settings.

⚠ These settings will be applied immediately after you click the save button. Save Cancel

Node Management > EdgeIPS

Configuring Policy Enforcement

1. Configure the required object or objects.
 - IP object profiles
For more information, see [Configuring IP Object Profiles on page 75](#).
 - Service object profiles
For more information, see [Configuring Service Object Profiles on page 76](#).
 - Protocol filter profiles
For more information, see [Configuring Protocol Filter Profiles on page 77](#).
 - IPS profiles
For more information, see [Configuring IPS Profiles on page 97](#).
 - File Filter profiles
For more information, see [Configuring File Filter Profiles on page 100](#).
2. Click the device group you want to manage.
3. Click the [Policy Enforcement] tab.



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

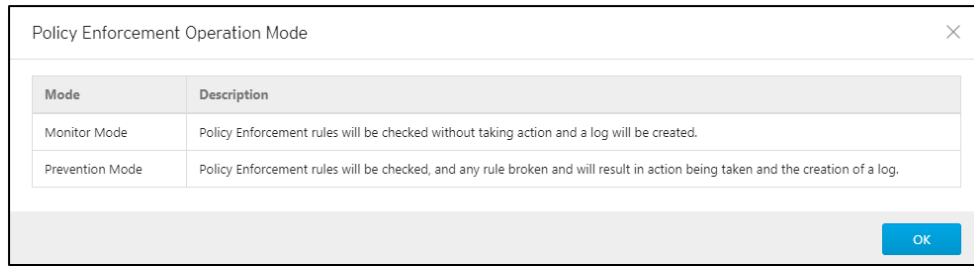
▼ Policy Enforcement General Settings

Enable Policy Enforcement

Policy Enforcement Operation Mode Monitor Mode Prevention Mode

Policy Enforcement Default Rule Action Accept Deny

5. Select a mode ([Monitor Mode], or [Prevention Mode]) for policy enforcement.



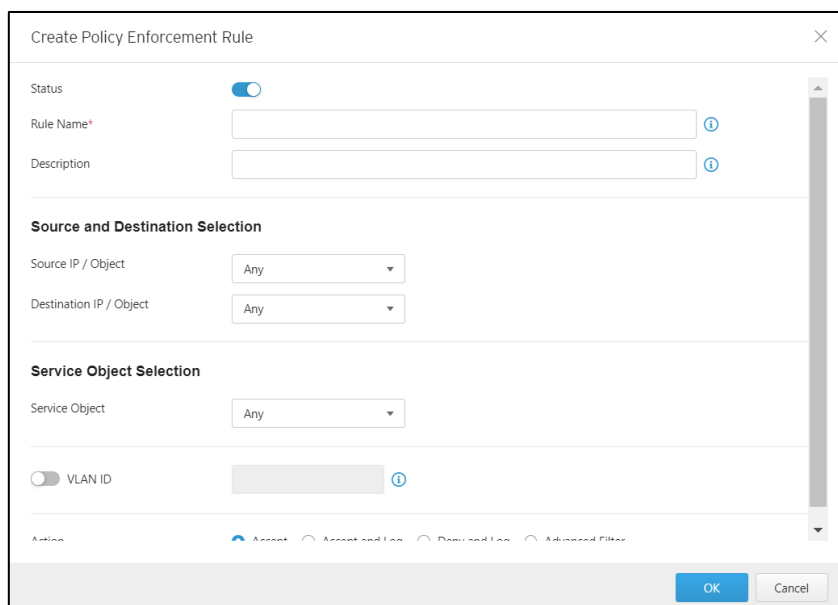
6. Under the [Policy Enforcement Default Rule Action] drop-down menu, select a default action for when no pattern is matched.

The following table summarizes the settings:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	<ul style="list-style-type: none"> ▪ Detects and monitors packets that violate a policy, but does not block network attacks. ▪ Generates logs.
	Prevention Mode	<ul style="list-style-type: none"> ▪ Blocks packets that violate a policy. ▪ Generates logs.
Offline Mode	Monitor and Log	<ul style="list-style-type: none"> ▪ Not supported.

Adding Policy Enforcement Rules

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



2. Use the toggle to enable or disable the policy rule.
3. Input a name for the rule.
4. Input a description for the rule.

5. Under the [Source IP / IP Object] drop-down menu, select one of the following for the source IP address(es):
 - Any
 - Single IP
 - IP Range
 - IP Subnet
 - Object

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

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

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

8. Under the [VLAN ID] , please enter the VLAN ID number. The number of maximum supported VLAN IDs is up to 5 IDs for each rule, and the VLAN ID Range is from 1 to 4094.
9. Under the [Action] drop-down menu, select one of the following:
 - a. **Accept:** Select this option to allow network traffic that matches this rule.
 - b. **Deny:** Select this option to block network traffic that matches this rule.
 - c. **Protocol Filter:** The node will further take actions based on the protocol filter:
 - Under the [Protocol Filter Profile] drop-down menu, select a protocol filter profile you have defined beforehand.
 - Under the [Protocol Filter Action] drop-down menu, select whether to allow or deny network traffic that matches the protocol filter.
 - Under the [IPS Profile] drop-down menu, select a protocol filter profile you have defined beforehand.

10. Click [Save] to save the configuration.

Managing Policy Enforcement Rules

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

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

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

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

Configuring Packet Capture

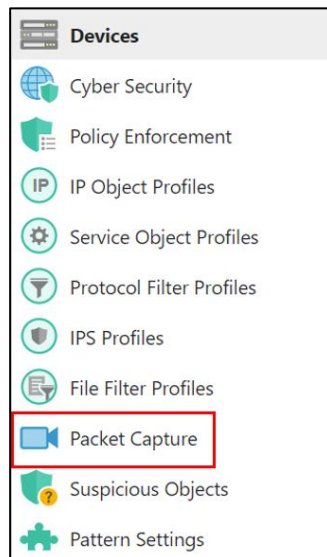
Packet Capture allows you to select one or multiple IPS rules to capture packets that meet the definitions. This feature can help users to quickly collect hit IPS rule packets as well as help support teams to quickly address false positive or false negative IPS rule enforcements.

Enabling Packet Capture

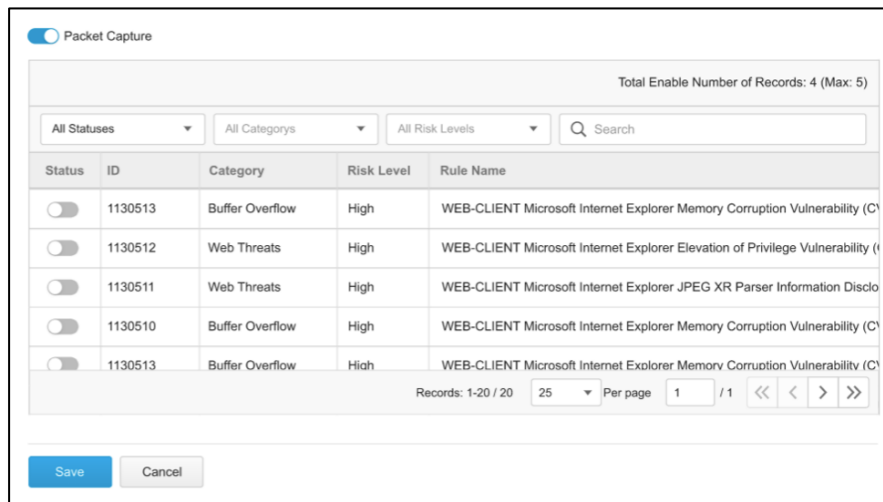
- Click the device group you want to manage.
- Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
- Ensure that [Packet Capture] is enabled, and click [Continue].
- Click the [Save] button to apply the settings.

Configuring Packet Capture

- Click the device group you want to manage.
- Click the [Packet Capture] tab.



3. Click [Enable] to enable IPS packet capture.



You can see an IPS rule list. From the list, select a rule to “Enable” for IPS packet capture. The IPS packet capture supports up to 20 rules being selected.

- The packet capture will collect selected IPS Rules. Once an IPS rule gets a hit, it will always collect the latest packet.

Configuring Suspicious Objects

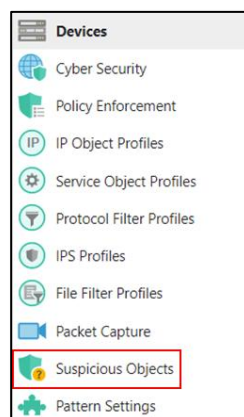
The Suspicious Object tab allows you to define the filter rules to pull suspicious objects from the global Suspicious Object Pool into a device group.

Enabling Suspicious Objects

1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that [Suspicious Object] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

Configuring Suspicious Object Filter

1. Click the device group you want to manage.
2. Click the [Suspicious Object] tab.



3. Click the gear button on the [Suspicious Object Filter] pane to configure the following settings:
 - Sources – the sources of the suspicious objects (SO), either “All Sources” or “Custom”. You may further specify the names of the SO sources when “Custom” is selected.
 - Approval Status – either “Approved Objects Only” or “Approved and New Objects”.
 - Types – “All Types”, “Node” or “Link”.
 - Risk Level – “All Risk Levels”, “High Only” or “High and Medium”.

Suspicious Object Filter ⚙️

Source	All Sources
Approval Status	Approved Objects Only
Type	All Types
Risk Level	All Risk Levels

4. Click the [Save] button to save the changes.

Configuring Suspicious Object Priority

1. Click the gear button on the [Suspicious Object Priority] pane to configure the priority of different sorting methods for the system to determine which suspicious objects should be kept first when the list has reached the upper limit. (For EdgeIPS™ LE, the upper limit is 512 objects.)

Suspicious Object Priority ⚙️

Sort by	Expiration date in descending order
Then by	Last updated time in descending order
Then by	Highest risk level first
Then by	Approval first

✕

Suspicious objects for EdgeIPS are limited to the first 512 objects in the list by following priority rule.

Sort by	Expiration date in descending order	^	v
Then by	Last updated time in descending order	^	v
Then by	Highest risk level first	^	v
Then by	Approval first	^	v

Save
Cancel

2. Click the [Save] button to save the changes.

Viewing the Suspicious Objects

The system will pull the suspicious objects from the global Suspicious Object Pool to this device group according to the given filter and display them in the table below the configuration panes. ODC will synchronize the suspicious object list to all devices in the group automatically.

The screenshot shows the 'Suspicious Object List' interface. It includes two configuration panes: 'Suspicious Object Filter' and 'Suspicious Object Priority'. Below these are filter dropdowns for 'All Types', 'All Sources', and 'All Risk Levels', along with a search bar. A table displays the object list with columns for ID, Type, Source, Object Content, Risk Level, Last Updated Time, and Expiration Time. The table contains three rows of data.

ID	Type	Source	Object Content	Risk Level	Last Updated Time	Expiration Time
72c6290cf9209bf46672fe66d42a02d1	Node	sssedf	IP=10.7.19.187	Medium	2022-01-26T11:13:41+08:00	2022-02-25T11:13:41+08:00
737ee2e2e56bb4ffe0ed035f1a1281d0	Node	sssedf	MAC=AA:BB:CC:DD:EE:FF	High	2022-01-12T13:53:12+08:00	Never expire
b0a8cdd56cd2295fd20af479075a4d1b	Node	sssedf	MAC=AA:BB:CC:DD:EE:BB	High	2022-01-12T13:53:12+08:00	Never expire

Configuring Pattern Settings

Under the [Node Management] tab, you can choose to deploy a specified DPI (Deep Packet Inspection) pattern to EdgeIPS™ LE nodes of the same device group.

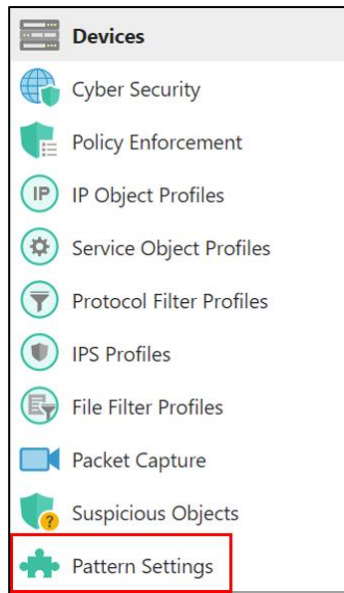
Enabling Pattern Settings

1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
An [Edit Settings] screen will appear.
3. Ensure that the [Pattern Setting] is enabled, and click [Continue].
4. Click the [Save] button to apply the settings.

A warning message box with a yellow background and a warning icon: "These settings will be applied immediately after you click the save button." It includes 'Save' and 'Cancel' buttons. Below the message is a breadcrumb navigation: "Node Management > EdgeIPS".

Configuring Pattern Settings

1. Click the device group you want to manage.
2. Click the [Pattern Settings] tab.



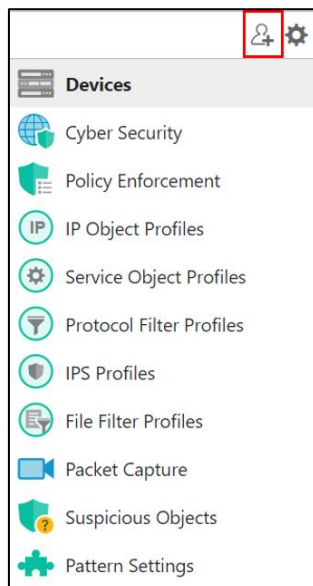
3. Select the DPI pattern to be deployed to the EdgeIPS™ LE nodes:
 - Latest: Always deploy the latest DPI pattern available on the OT Defense Console.
 - Fixed version: Deploy the fixed DPI version specified.

Sharing Management Permissions to Other User Accounts

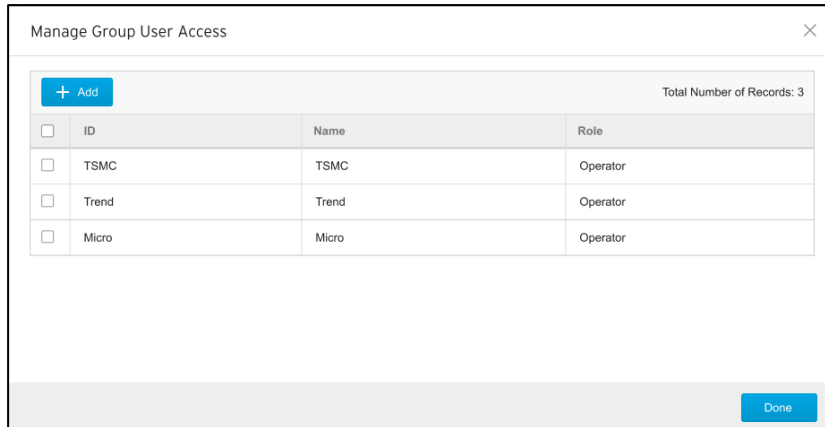
By default, the device group can only be created or managed by the [admin] account. However, you as the administrator can share management permissions to other users after a device group is created. See and [User Roles on page 130](#) for the details.

Procedure

1. Click the device group you want to manage.
2. Click the [Share with Others] button.



A [Manage Group User Access] screen will appear.



3. Add the user accounts with which you want to share management of the device group.

Object Profiles

Object profiles simplify policy management by storing configurations that can be used by the device group to which they belong.

You can configure the following types of object profiles in OT Defense Console:

- **IP Object Profiles:** Contain the IP addresses that you can apply to a policy rule.
- **Service Object Profiles:** Contain the service definitions that you can apply to a policy rule. TCP port range, UDP port range, ICMP, and custom protocol number are defined here.
- **Protocol Filter Profiles:** Contain more sophisticated and advanced protocol settings that you can apply to a policy rule. Details of ICS (Industrial Control System) protocols are defined here.
- **IPS Profiles:** Contain more sophisticated pattern rules that allow you to have granular control which can be applied to policy rules.
- **File Filter Profiles:** Contain the settings of file filter profiles that you can apply to a policy rule. Details of file filter by protocol are defined here.
- **Antivirus Profiles:** Streaming-based antivirus profiles provide an extra layer of protection under EdgeIPS Pro and scanning, optimizing memory utilization for large archive files by decompressing the files on the fly and scanning the PE and ELF format malware files.

Configuring IP Object Profiles

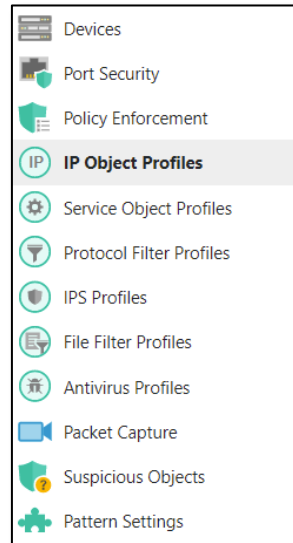
You can configure the IP address in an IP object profile, which can be applied to the device group to which they belong.


The types of IP address you can assign are:

- Single IP addresses
- IP ranges
- IP subnets

Procedure

1. Go to [Node Management] > [EdgeIPS], [EdgeFire], [EdgeIPS Pro] or [EdgeIPS LE].
2. Select the device group you want to manage.
3. Select [IP Object Profiles].



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

Configuring Service Object Profiles

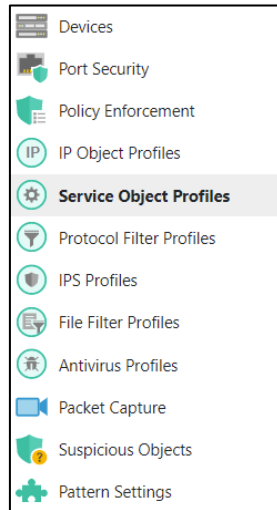
In a service object profile, you can define the following:


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

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

Procedure

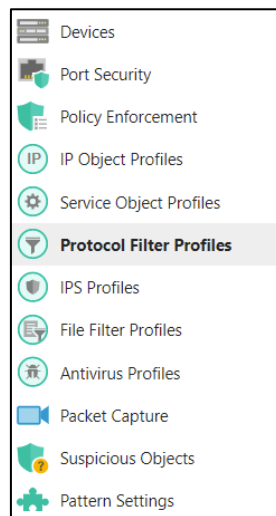
1. Go to [Node Management] > [EdgeIPS] or [EdgeFire].
2. Select the device group you want to manage.
3. Select [Service Object Profiles].



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

Configuring Protocol Filter Profiles

Protocol filter profiles contain more sophisticated and advanced protocol settings that you can apply to a policy rule.



The following can be configured in a protocol filter profile:

- **Details of ICS protocols, including:**

- Factory Automation

Modbus	SECS/GEM
CIP	TOYOPUC
S7COMM	OPC UA
S7COMM PLUS	OPC CLASSIC
PROFINET	GE SDI
SLMP	GE-SRTP
MELSOFT	HART-IP
FINS	

- Building Automation

- BACnet

- Healthcare

- DICOM
 - HL7

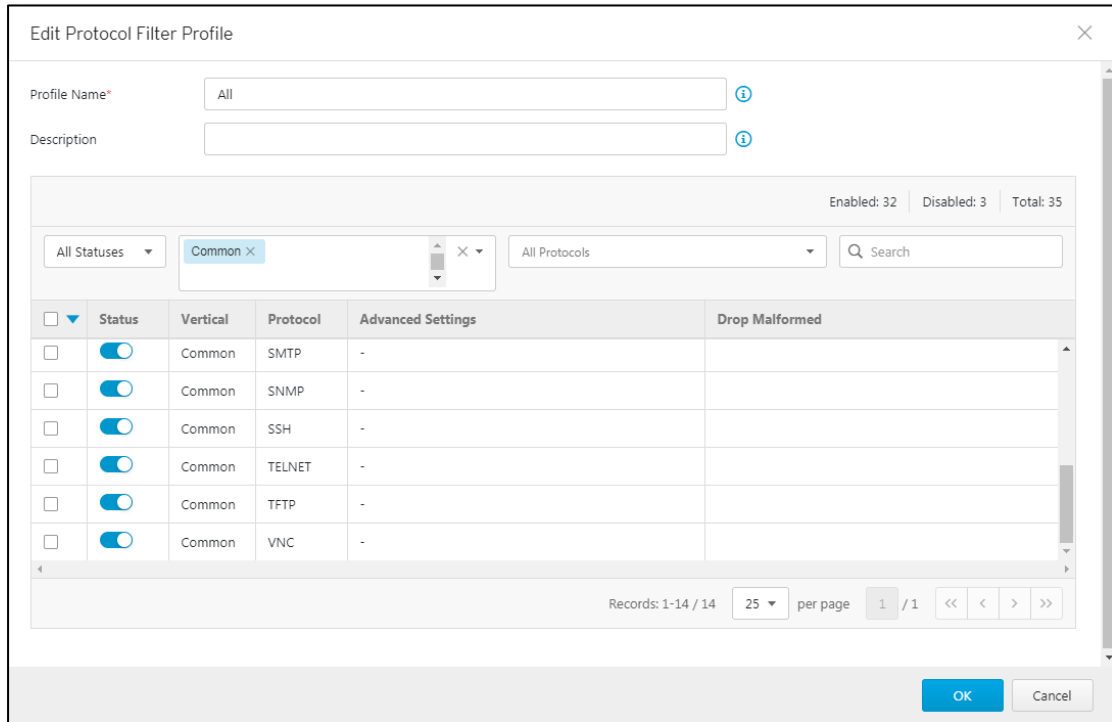
- Power and Electricity

- DNP3
 - IEC104
 - IEC61850-MMS

- General Protocols, including:

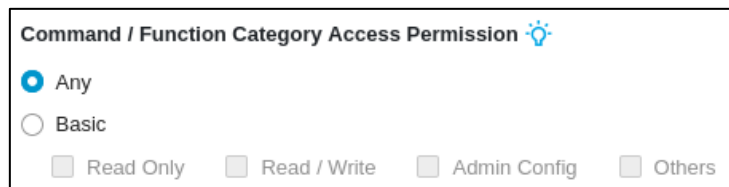
HTTP	SMTP
FTP	SNMP
SMB	SSH
RDP	TELNET
MQTT	TFTP
MSRPC	VNC
SIP	DNS

▪ The ICS protocols listed above are available for EdgeIPS, EdgeFire and EdgeIPS Pro.



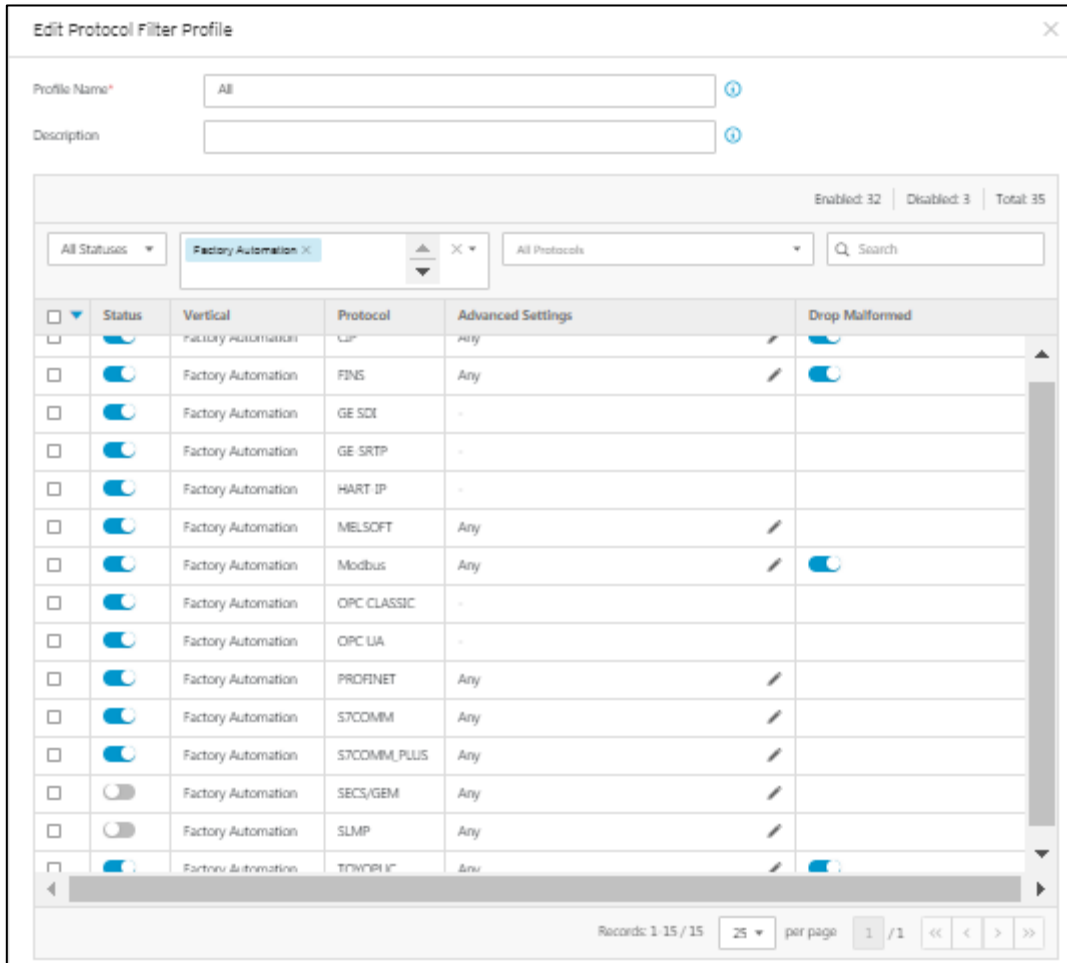
Specifying Commands Allowed in an ICS Protocol

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



Applying the Drop Malformed Option to an ICS Protocol

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



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

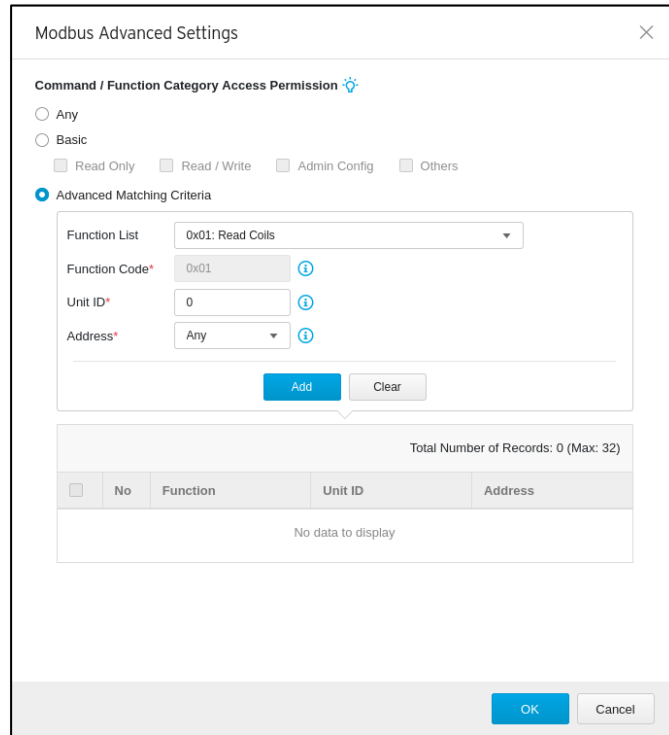
■ In ODC v1.1, Drop Malformed supports 4 protocols (Modbus, CIP, OMRON FINS and TOYOPUC).

Advanced Settings


List available Advanced settings of OT protocols

Advanced Settings for Modbus Protocol

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



Modbus Advanced Settings

Command / Function Category Access Permission 


Any


Basic


Read Only Read / Write Admin Config Others

Advanced Matching Criteria

Function List:

Function Code*: 

Unit ID*: 

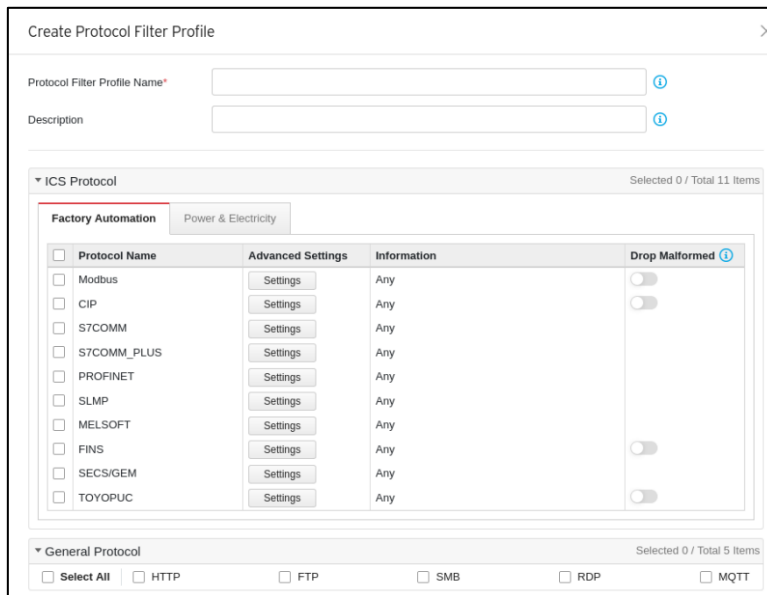
Address*: 

Total Number of Records: 0 (Max: 32)


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


Procedure

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




Create Protocol Filter Profile

Protocol Filter Profile Name* 

Description 

▼ ICS Protocol Selected 0 / Total 11 Items

Factory Automation Power & Electricity

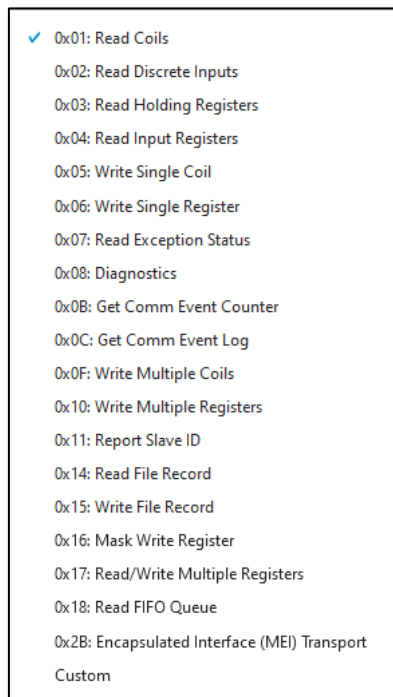
<input type="checkbox"/>	Protocol Name	Advanced Settings	Information	Drop Malformed 
<input type="checkbox"/>	Modbus	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	CIP	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	S7COMM	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	S7COMM_PLUS	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	PROFINET	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	SLMP	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	MELSOFT	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	FINS	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	SECS/GEM	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>
<input type="checkbox"/>	TOYOPUC	<input type="button" value="Settings"/>	Any	<input type="checkbox"/>

▼ General Protocol Selected 0 / Total 5 Items

Select All HTTP FTP SMB RDP MQTT

3. Type a profile name for the protocol filter.
4. Type a description.

5. On the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands in this protocol.
 - Basic - Multiple selections as follows:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - **Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected [Modbus], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [Modbus], and select [Advanced Matching Criteria].
 - Under the [Function list] drop-down menu, select a function of this protocol.

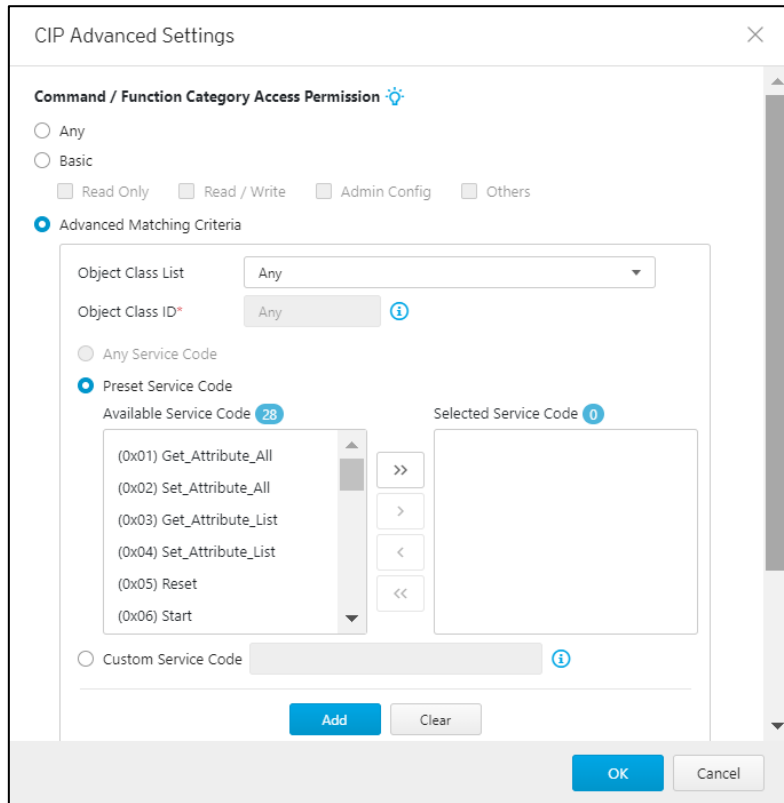


- If you want to specify a function code by yourself, then select [Custom] and input a function code in the [Function Code] field.
- Type a unit ID in the [Unit ID] field.
- Type the address or range of addresses against which the function will operate.
- Click [Add].
- Repeat the above steps if you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

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

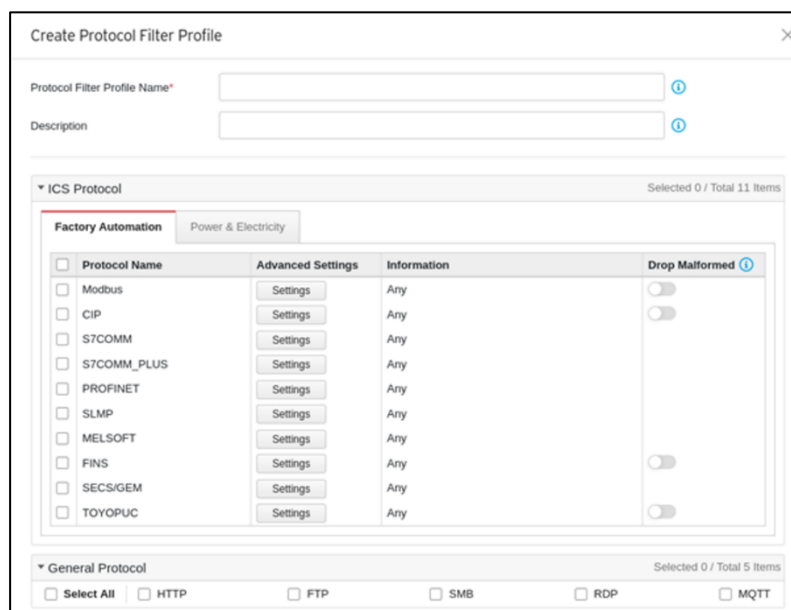
Advanced Settings for CIP Protocol

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



Procedure

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



3. Type a profile name for the protocol filter. Type a description.

In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

- a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands or function access for this protocol.
 - Basic - Multiple selections as follows:
 - Read Only: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - Read / Write: Read and write commands sent from HMI/EWS/SCADA to PLC.
 - Admin Config: Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - Others: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
- b. If you have selected [CIP], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [CIP], and select [Advanced Matching Criteria].
 - At the [Object Class List] drop-down menu, select a function of this protocol.

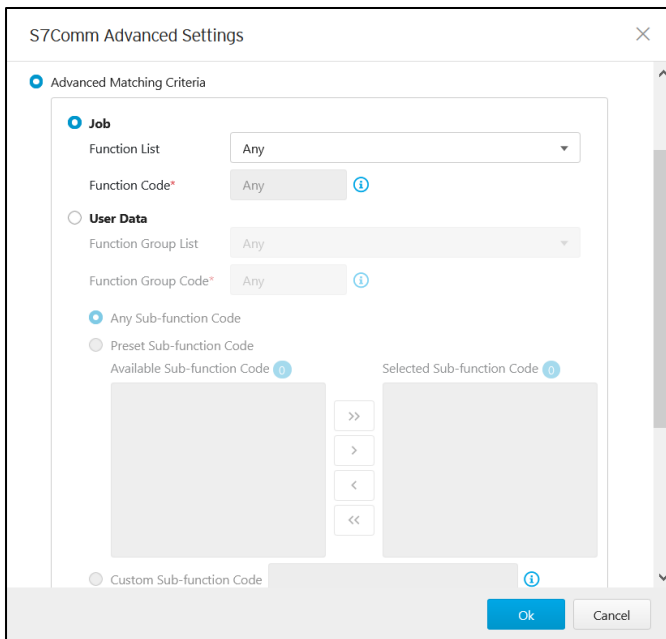
<ul style="list-style-type: none"> ✓ Any (0x0001) Identity (0x0002) Message Router (0x0003) DeviceNet (0x0004) Assembly (0x0005) Connection (0x0006) Connection Manage (0x0007) Register (0x0008) Discrete Input Point (0x0009) Discrete Output Point (0x000A) Analog Input Point (0x000B) Analog Output Point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

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

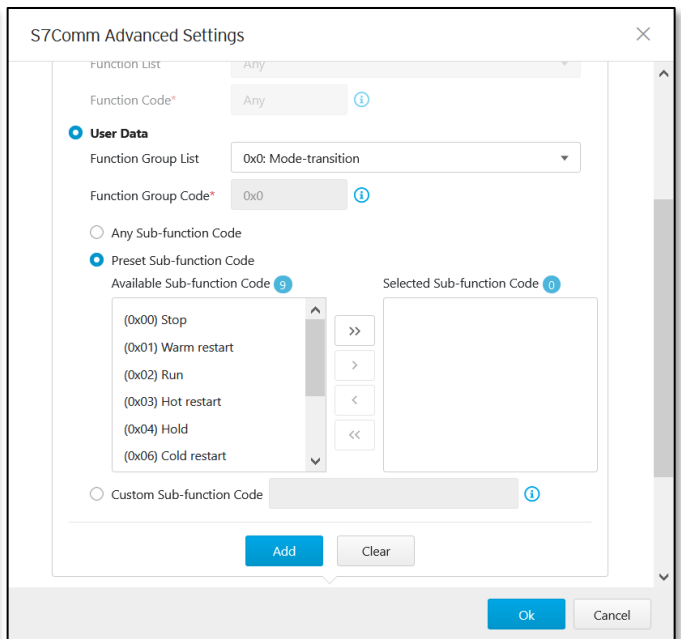
In the [General Protocol] pane, select the protocols you want to include in the protocol filter.
Click [OK].

Advanced Settings for S7Comm

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



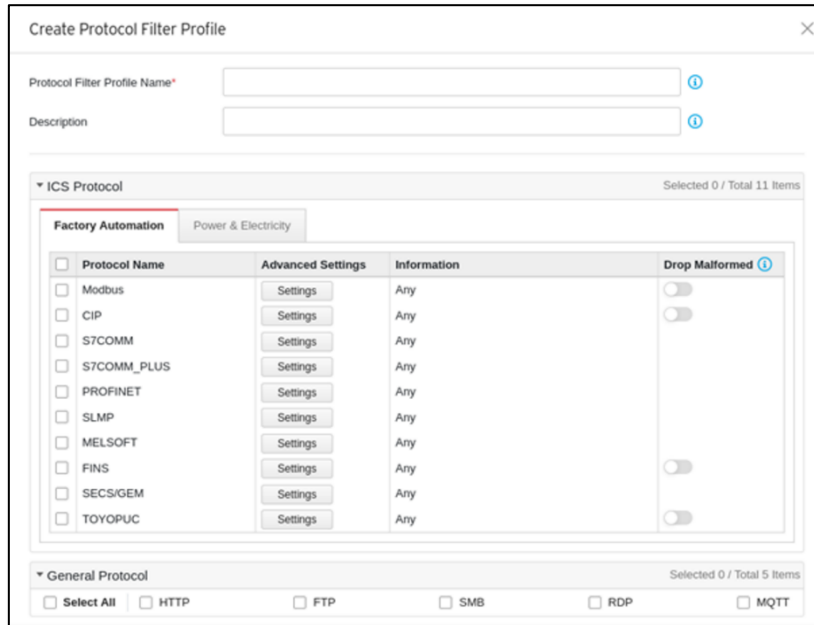
The screenshot shows the 'S7Comm Advanced Settings' dialog box with the 'Advanced Matching Criteria' section selected. It contains three radio button options: 'Job', 'User Data', and 'Any Sub-function Code'. The 'Job' option is selected. Under 'Job', there are fields for 'Function List' (set to 'Any'), 'Function Code*' (set to 'Any'), and 'Function Group Code*' (set to 'Any'). There are also fields for 'Available Sub-function Code' and 'Selected Sub-function Code' with navigation buttons (>>, >, <, <<). At the bottom, there are 'Ok' and 'Cancel' buttons.



The screenshot shows the 'S7Comm Advanced Settings' dialog box with the 'User Data' section selected. It contains fields for 'Function List' (set to 'Any'), 'Function Code*' (set to 'Any'), 'Function Group List' (set to '0x0: Mode-transition'), and 'Function Group Code*' (set to '0x0'). There are three radio button options: 'Any Sub-function Code', 'Preset Sub-function Code', and 'Custom Sub-function Code'. The 'Preset Sub-function Code' option is selected. Under 'Preset Sub-function Code', there are two lists: 'Available Sub-function Code' (containing (0x00) Stop, (0x01) Warm restart, (0x02) Run, (0x03) Hot restart, (0x04) Hold, (0x06) Cold restart) and 'Selected Sub-function Code'. Navigation buttons (>>, >, <, <<) are between the lists. At the bottom, there are 'Add' and 'Clear' buttons, and 'Ok' and 'Cancel' buttons.

Procedure

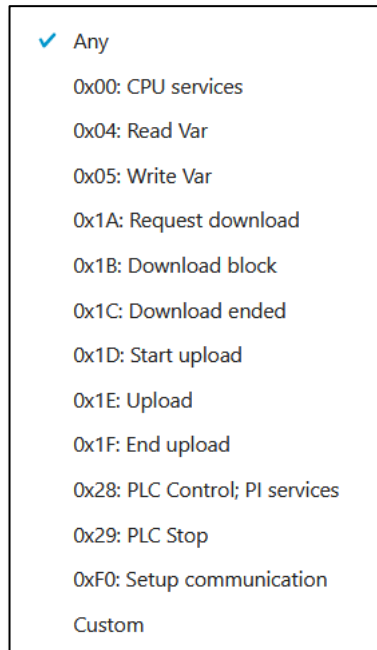
1. Go to [Object Profiles] > [Protocol Filter Profiles].
2. Click [Add] to add a protocol filter profile.
The [Create Protocol Filter Profile] screen will appear.



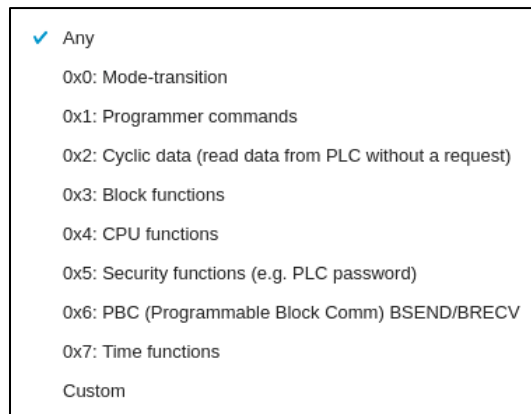
The screenshot shows the 'Create Protocol Filter Profile' window. It has two text input fields at the top: 'Protocol Filter Profile Name*' and 'Description'. Below these is a section for 'ICS Protocol' with a sub-header 'Factory Automation' and 'Power & Electricity'. A table lists protocols with checkboxes, 'Advanced Settings' buttons, and 'Information' columns. A 'Drop Malformed' toggle is on the right. At the bottom, a 'General Protocol' section has checkboxes for 'Select All', 'HTTP', 'FTP', 'SMB', 'RDP', and 'MQTT'.

Protocol Name	Advanced Settings	Information	Drop Malformed
<input type="checkbox"/> Modbus	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> CIP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7COMM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> S7COMM_PLUS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> PROFINET	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SLMP	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> MELSOFT	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> FINS	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> SECS/GEM	Settings	Any	<input type="checkbox"/>
<input type="checkbox"/> TOYOPUC	Settings	Any	<input type="checkbox"/>

3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands or function access for this protocol.
 - Basic - Multiple selections as follows:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - **Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected [S7Comm], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [S7Comm], and select [Advanced Matching Criteria].
 - If you want to specify one function code from the category [Job], then select the category [Job] and select a function from the [Function list] drop-down menu.



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

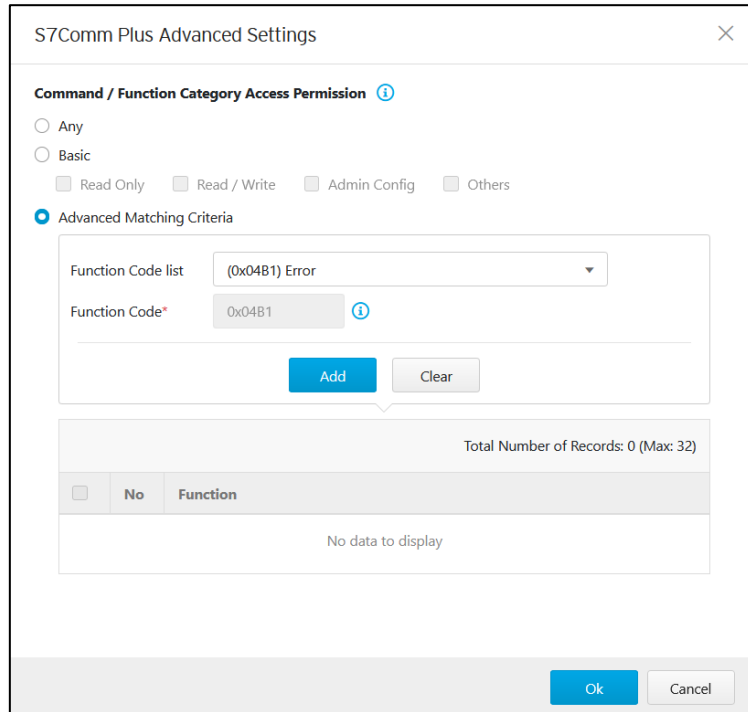


- If you want all the sub-function codes within the function group code you specified to be applied, then select [Any Sub-Function Code]
- If you want to specify one sub-function code or multiple sub-function codes, then select [Preset Sub-Function Code] and move the sub-function code(s) from the [Available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

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

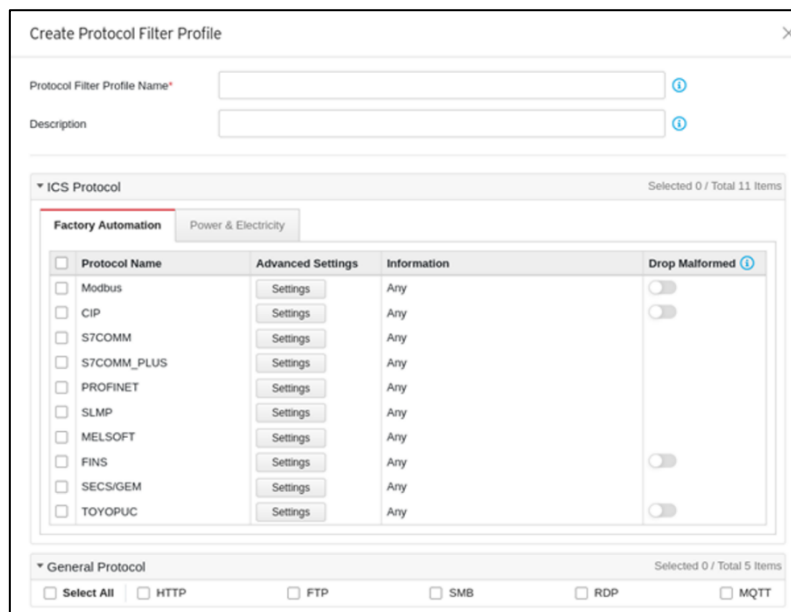
Advanced Settings for S7Comm Plus

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



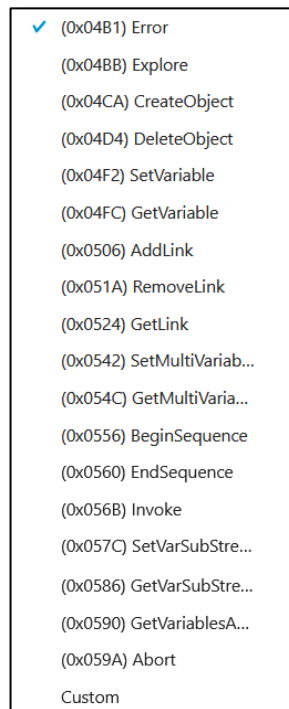
Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

- a. Click [Settings] next to a protocol, and select one of the following:
 - **Any** - Specify all available commands or function access privileges for this protocol.
 - **Basic** - Multiple selections as follows:
 - **Read Only**: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write**: Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config**: Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
- b. If you have selected [S7Comm Plus], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [S7Comm Plus], and select [Advanced Matching Criteria].
 - Under the [Function list] drop-down menu, select a function of this protocol.

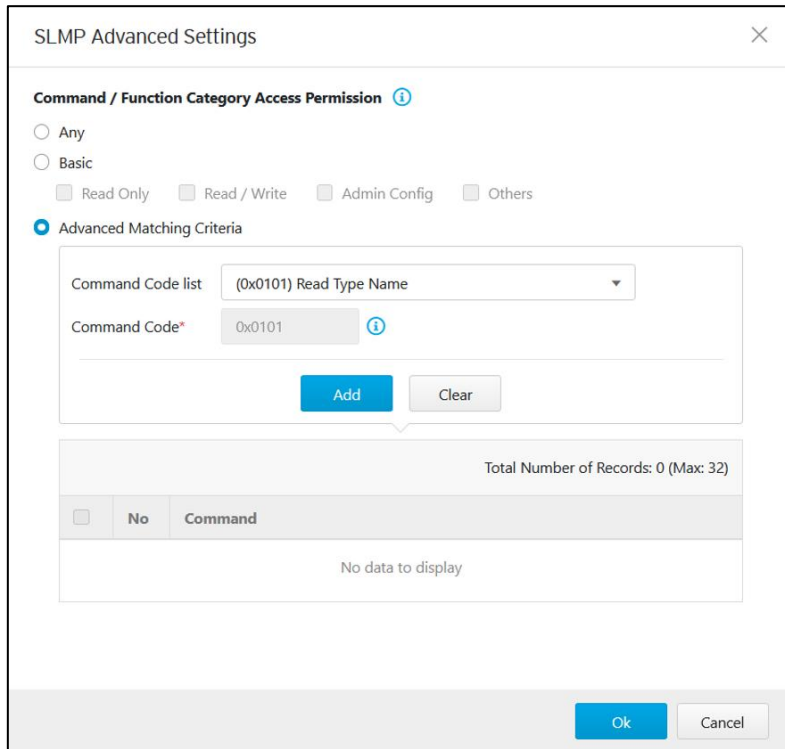


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

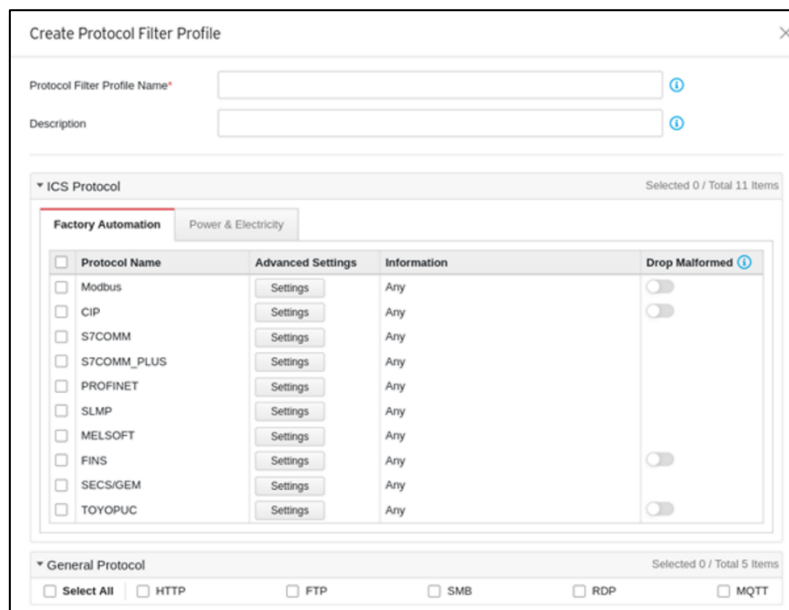
Advanced Settings for SLMP

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



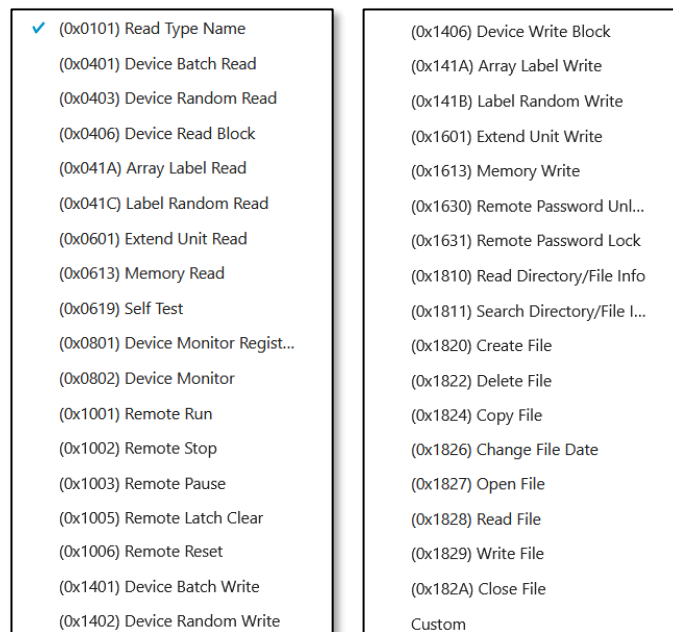
Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.

5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands or function access for this protocol.
 - Basic - Multiple selections as follows:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, Project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - **Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected [SLMP], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [SLMP], and select [Advanced Matching Criteria].
 - Under the [Command Code List] drop-down menu, select a function of this protocol.

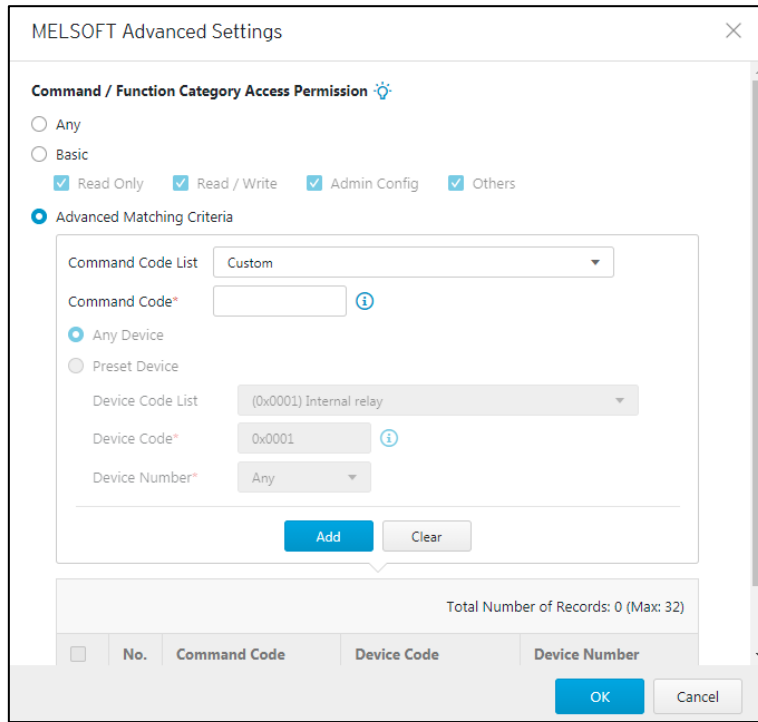


- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

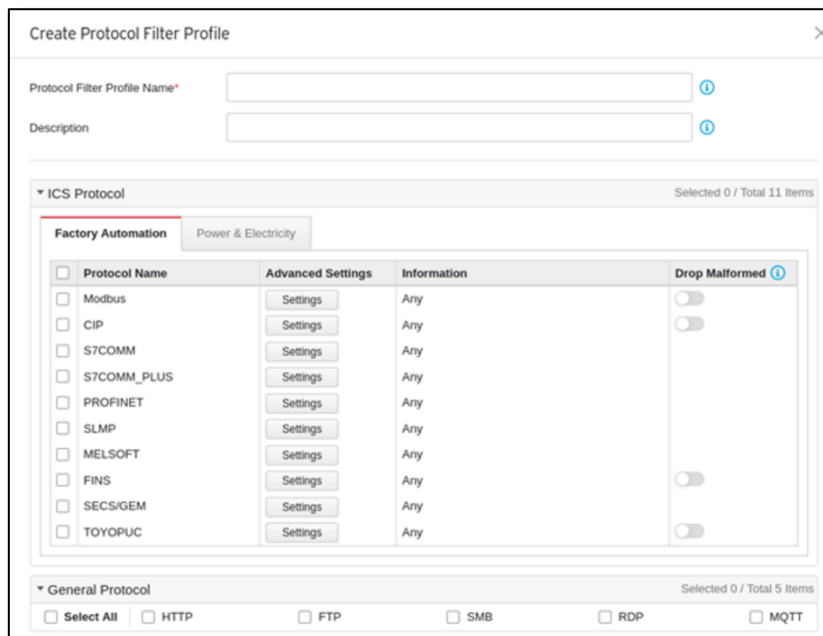
Advanced Settings for MELSOFT

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



Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.

5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands or function access for this protocol.
 - Basic - Multiple selections as follows:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration-relevant commands sent from EWS to PLC.
 - **Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected [MELSOFT], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [MELSOFT], and select [Advanced Matching Criteria].
 - Under the [Command Code List] drop-down menu, select a function of this protocol.

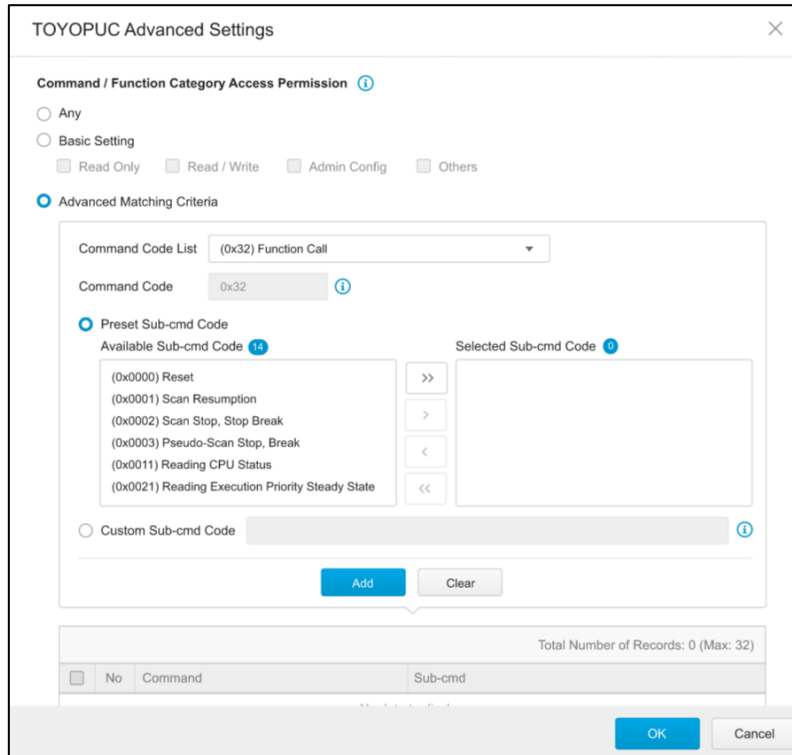
(0x0101) Read CPU Model Na...	(0x1401) Device Batch Write
(0x0114) Authentication	(0x1402) Device Random Write
(0x0121) Read CPU Model - R ...	(0x1640) Password Unlock
(0x0401) Device Batch Read	(0x1641) Password Lock
(0x0403) Device Random Read	(0x1810) Read DIR/File Info
(0x0801) Device Monitor Regs...	(0x1811) Search Directory File
(0x0802) Device Monitor	(0x1820) Create File
(0x0B05) Read Info - Q Series	(0x1826) Modify File Time
(0x0B11) Auto Search - Q Series	(0x1827) Open File
(0x0B20) Auto Search - R Series	(0x1828) Read File
(0x0B2A) Read Info - R Series	(0x1829) Write File
(0x1001) Remote RUN	(0x182A) Close File
(0x1002) Remote STOP	(0x1836) Write to Storage
(0x1003) Remote Pause	(0x1837) Close File SP
(0x1005) Remote Latch Clear	(0x1838) Delete a File
(0x1006) Remote RESET	Custom

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

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

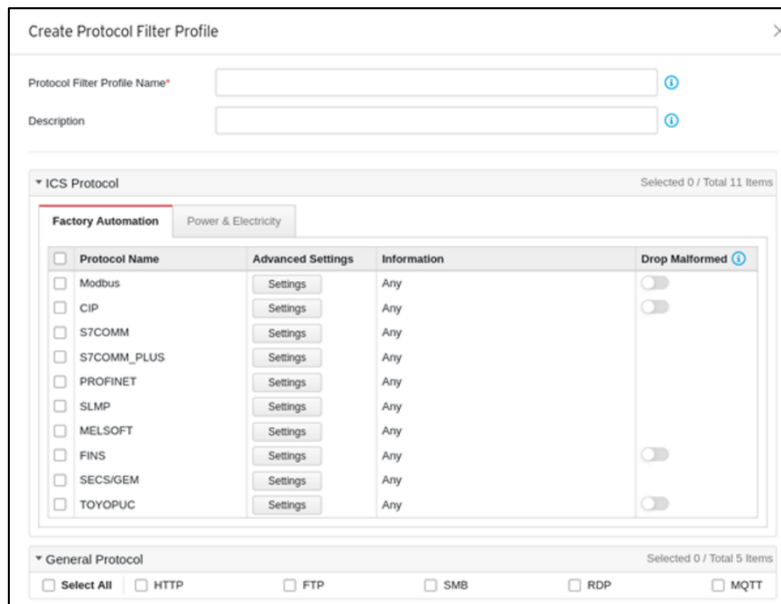
Advanced Settings for TOYOPUC

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



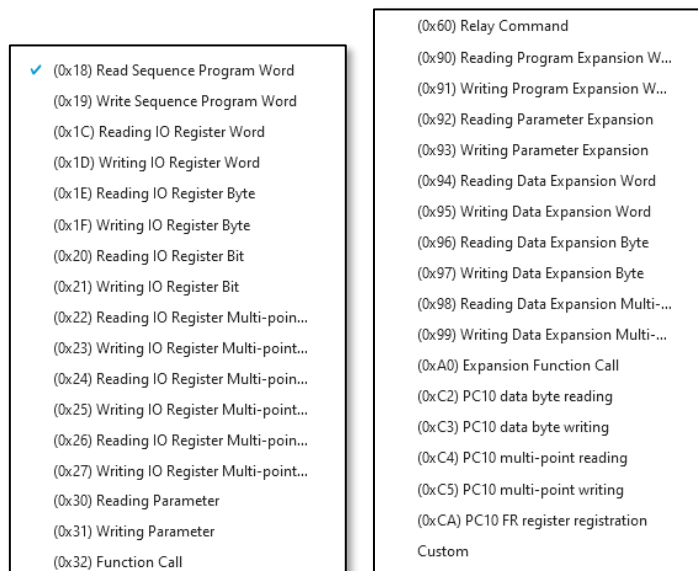
Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.

5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.
 - a. Click [Settings] next to a protocol, and select one of the following:
 - Any - Specify all available commands or function access for this protocol.
 - Basic - Multiple selections as follows:
 - **Read Only:** Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
 - **Read / Write:** Read and write commands sent from HMI/EWS/SCADA to PLC.
 - **Admin Config:** Firmware update commands sent from EWS to PLC, project update (i.e., PLC code download) commands sent from EWS to PLC, and commands relevant to administration configuration sent from EWS to PLC.
 - **Others:** Private commands, un-documented commands, or particular protocols provided by an ICS vendor.
 - b. If you have selected [TOYOPUC], you can optionally configure advanced settings for this protocol:
 - Click [Settings] next to [TOYOPUC], and select [Advanced Matching Criteria].
 - Under the [Command Code List] drop-down menu, select a function of this protocol.

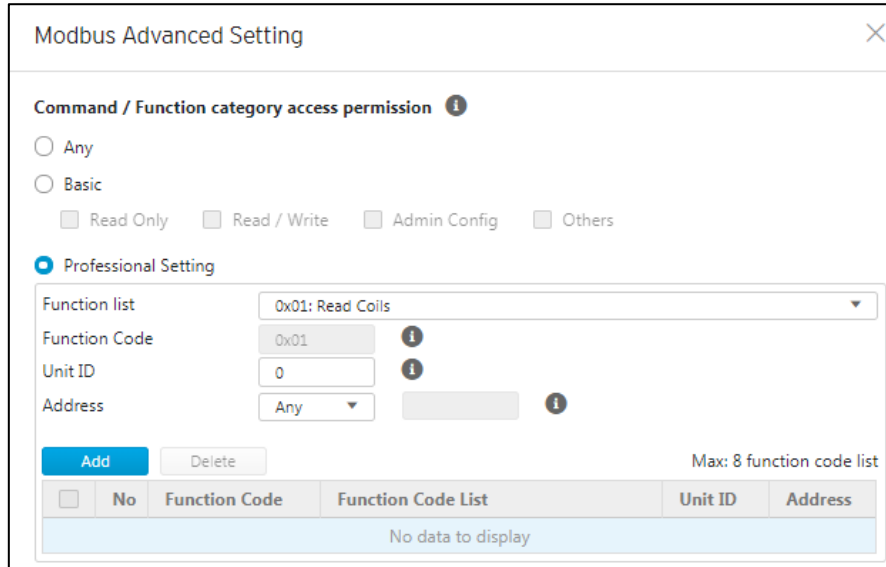


- If you want to specify one sub-command code or multiple sub-command codes, then select [Preset Sub-Cmd Code] and move the sub-function code(s) from the [Available Sub-Cmd Code] field to the [Selected Sub-Cmd Code] field.
 - If you want to specify a sub-command code by yourself, then select [Custom Sub-Cmd Code] and input a sub-command code in the [Custom Sub-Cmd Code] field.
 - Click [Add].
 - Repeat the above steps if you want to add more protocol definition entries.
 - Click [OK].
- Not all the command codes support the feature of [Preset Sub-cmd code] and [Custom Sub-cmd]. Only the command codes "(0x32) Function Call" and "(0xA0) Expansion Function Call" support them.

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

Advanced Settings for Modbus Protocol

The OT Defense Console features more detailed configurations for the Modbus ICS protocol. Through the [Professional Settings] pane, you can further specify the function code/function, Unit ID, and address or address range against which the function will operate.

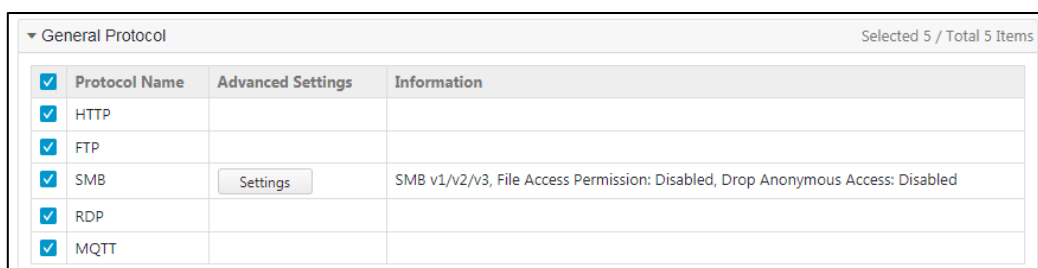


Procedure

1. Go to [Node Management] > [EdgeIPS] or [EdgeFire].
2. Select the device group you want to manage.
3. Select [Protocol Filter Profiles].

Advanced Settings for SMB

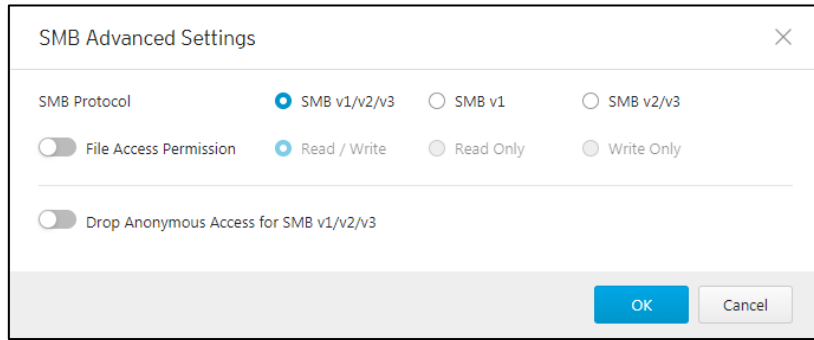
The device features more detailed configurations for the SMB protocol. Through the [Advanced Settings] pane, you can further specify the configuration settings.



General Protocol		Selected 5 / Total 5 Items	
Protocol Name	Advanced Settings	Information	
<input checked="" type="checkbox"/> HTTP			
<input checked="" type="checkbox"/> FTP			
<input checked="" type="checkbox"/> SMB	Settings	SMB v1/v2/v3, File Access Permission: Disabled, Drop Anonymous Access: Disabled	
<input checked="" type="checkbox"/> RDP			
<input checked="" type="checkbox"/> MQTT			

Procedure

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



3. Type a profile name for the protocol filter.
4. Type a description.
5. In the [ICS Protocol] pane, select the protocols you want to include in the protocol filter.

Click SMB [Settings] and configure the following:

- **SMB Protocol:** Specify SMB protocol version combination, includes SMBv1/v2/v3, SMBv1 and SMB v2/v3 all available commands or function access for this protocol.
- **File Access:** Allow user to select access permission behavior:
 - **Read / Write:** Read and write file access.
 - **Read Only:** File access for reading
 - **Write Only:** File access for writing.
- **Drop Anonymous Access for SMB v1/v2/v3:** Drop file access over SMB v1/v2/v3 for Anonymous accounts.

■ Starting from ODC v1.2, SMB Advanced setting is only available for EdgeIPS Pro.

Configuring IPS Profiles

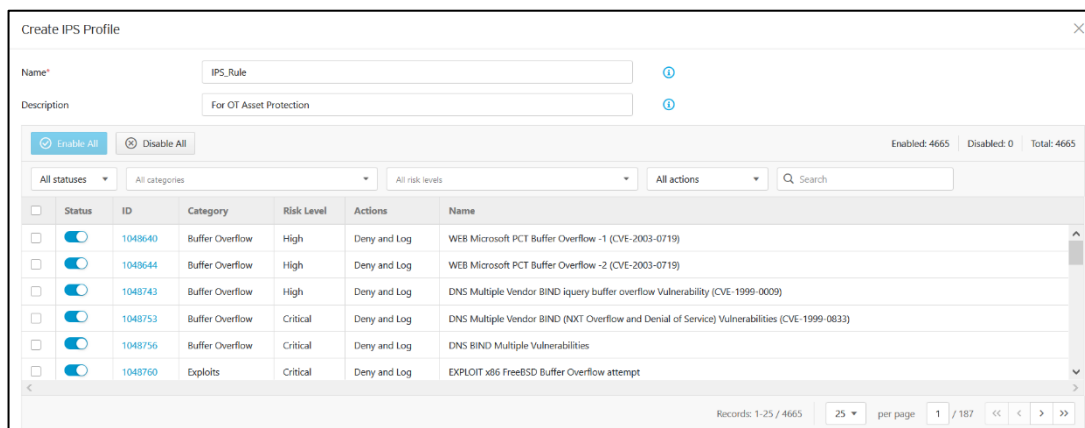
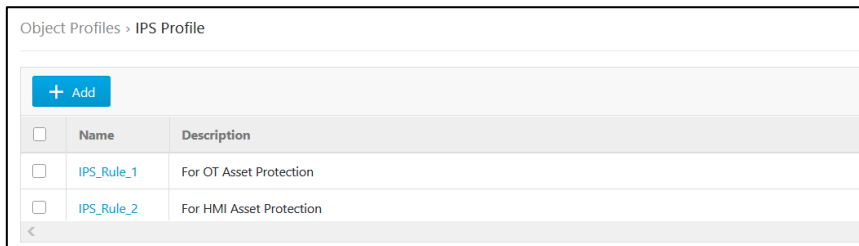
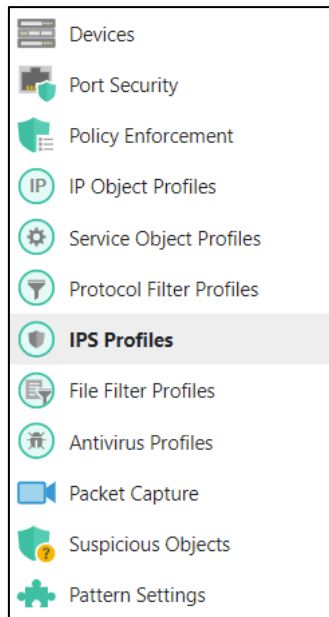
An IPS profile contains more sophisticated pattern rules that allow you to have granular control which can be applied to policy rules.

The following can be configured in an IPS profile:

- Details of the IPS protocol category, including:
 - File Vulnerabilities
 - Buffer Overflow
 - DoS Attacks
 - Exploits
 - Malware Traffic
 - Reconnaissance
 - Web Threats
 - ICS Threats
 - Flooding and Scan
 - Protocol Attack Protection
 - IP Spoofing
 - Others
 - Policy Violation
 - Misc.

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

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



Configuring a Pattern Rule for Granular Control

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

Status	ID	Category	Risk Level	Actions	Name
<input type="checkbox"/>	1133637	Exploits	Critical	Deny and Log	SMB Microsoft Windows MS17-010 SMB Remote Code Execution -3
<input type="checkbox"/>	1133638	Exploits	Critical	Deny and Log	SMB Microsoft Windows MS17-010 SMB Remote Code Execution -4
<input type="checkbox"/>	1133710	Buffer Overflow	High	Deny and Log	SMB Microsoft Windows SMB Server SMBv1 CVE-2017-0147 Information Disclosure -1
<input type="checkbox"/>	1133713	Buffer Overflow	Critical	Deny and Log	SMB Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption -1 (CVE-2017-0146)
<input type="checkbox"/>	1133812	Buffer Overflow	High	Deny and Log	SMB Microsoft Windows SMB Server SMBv1 CVE-2017-0144 Memory Corruption -1
<input checked="" type="checkbox"/>	1136717	Malware traffic	High	Deny and Log	Malware.Ransom.WannaCry

IPS Rule Details ✕

Status

ID 1136717

Name Malware.Ransom.WannaCry

Category Malware traffic

Risk Level High

Impact Critical data was encrypted and services were stopped.

Reference https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Actions Accept and Log Deny and Log

Keyword WannaCry

Procedure

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

Create IPS Profile ✕

Name*

Description

Enabled: 4665 Disabled: 0 Total: 4665

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

Records: 1-25 / 4665 25 per page 1 / 187

2. Type a profile name for the IPS profile.
3. Type a description.
4. Select a pattern rule you want to configure by clicking on the rule ID.

5. IPS rule details will show up. Select one of the following:
- **Status** - Specify the pattern rule to be enabled or disabled.
 - **Actions** - Multiple selections as follows:
 - **Accept and Log:** When the attack is detected by EdgeIPS Pro, the attack will be bypassed and logged for monitoring.
 - **Deny and Log:** When the attack is detected by EdgeIPS Pro, the attack will be bypassed and logged for monitoring.

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

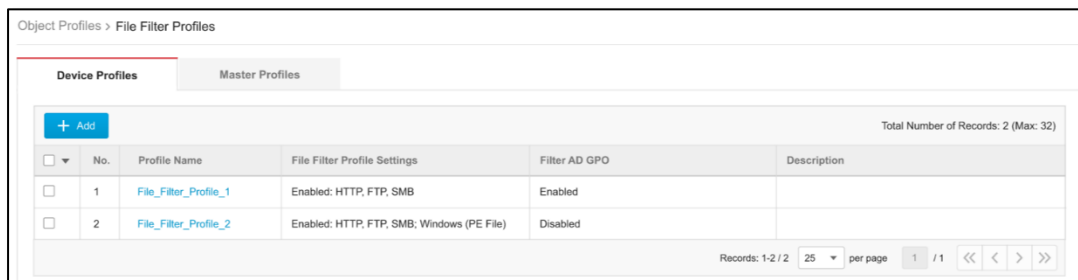
When you are finished configuring the pattern rule, press [Save].

Configuring File Filter Profiles

The File Filter Profile contains detailed access protocols, executable file type and Active Directory (AD) GPO dispatch settings, allowing you to create or edit profiles to apply to a policy rule.

In a profile, you can define the following:

- File Filter by Protocol
Including: HTTP, FTP and SMB
- Drop Executable File(s)
Including: Windows (PE files) and Linux (ELF file)
- Filter AD GPO
Enable or disable Drop Active Directory (AD) GPO



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

Procedure

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

Create File Filter Profile
✕

Profile Name* i

Description i

File Filter Profile Settings

File Filter by Protocol

Protocol* HTTP FTP SMB

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

Filter AD GPO

Drop Active Directory(AD) GPO dispatch

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

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

Configuring File Exclusions

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

Object Profiles > File Filter Profiles

File Exclusions

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

Total Number of File Exclusion(s): 3

[File Exclusion Settings](#) [Download CSV Template](#)

File Filter Profiles

[+ Add](#) Total Number of Records: 2 (Max: 256)

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

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

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

Procedure

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

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

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

File Exclusion Settings

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

[+ Add](#) [Import](#) Total Number of Records: 3 (Max: 2000)

Search

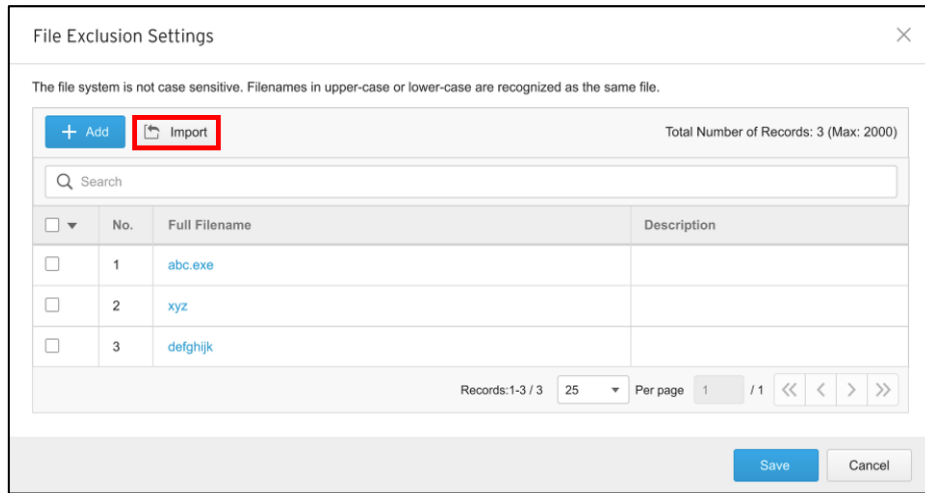
<input type="checkbox"/>	No.	Full Filename	Description
<input type="checkbox"/>	1	abc.exe	
<input type="checkbox"/>	2	xyz	
<input type="checkbox"/>	3	defghijk	

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

[Save](#) [Cancel](#)

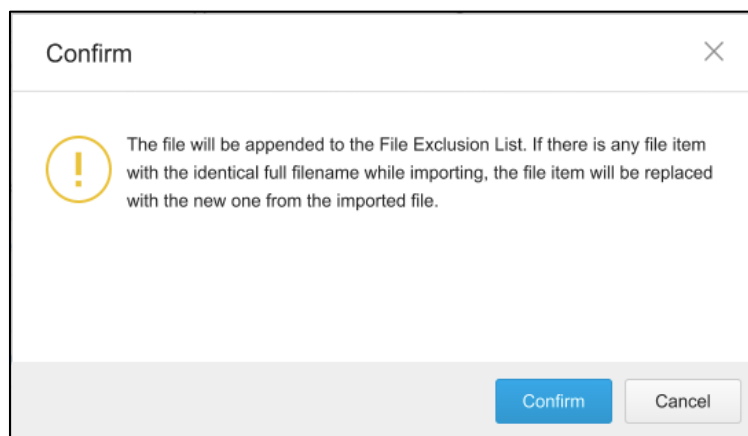
Scenario 2: Import an Edited CSV File with Multiple File Items (Steps 5 & 6)

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



- Note: You do not need to unzip zip/gz file(s) for scanning each compressed file, as the system can identify zip/gz file(s) and determine whether the filename list contains the file items for exclusions. Notice that zip/gz files larger than 100MB will be ignored.
- Note: The full filename format can be **Filename.File Extension** (e.g. abc.exe), or just **Filename** (e.g. abc).
- Note: Notice that the file system is not case sensitive. Filenames in uppercase or lowercase are identified as the same file. In addition, Whitespace character(s) cannot be included in the beginning and the end of a filename. Special characters (<, >, :, ", /, \, |, ? and *) are not allowed.
- Note: The maximum full filename length is 128 bytes with UTF-8. When the UTF-8 user input is based on English characters, the maximum full filename length is 128 characters. When the UTF-8 user input is based on non-English characters, the maximum full filename length may be reduced to 32 characters.

7. After you have completed the file exclusion settings by either of the methods, click [Save]. A Confirm window will appear. Click [Confirm].



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

Configuring Antivirus Profiles

EdgeIPS Pro series Antivirus is a streaming-based design. The Antivirus Profile can be configured to check HTTP, FTP protocol and it also includes advanced settings such as file size limitation setting and Compress file scanning, allowing you to create or edit profiles to apply to a policy rule.

- Antivirus features is only available on EdgeIPS Pro product line.

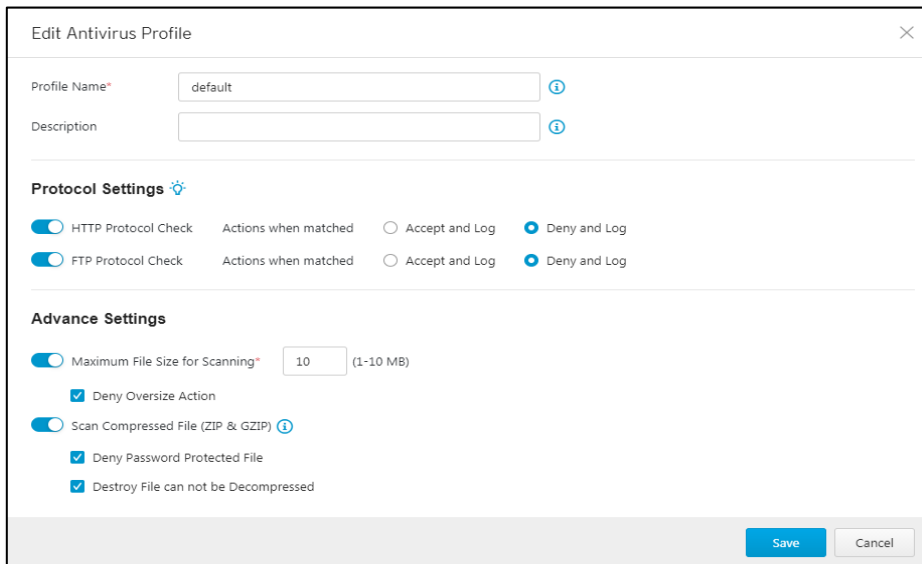
In a profile, you can define the following:

- File exceptions: User can import an SHA1-based exception list.
- Protocol settings for HTTP and FTP
Advanced settings includes
 1. Maximum file size
 2. Compressed file scan

Procedure

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

The [Create Antivirus Profile] screen will appear.



3. Type a name for the Antivirus Profile in the profile name field.
4. Type Description.
5. Under the [Antivirus Profile Settings], enable file filter by protocol
 - File Filter by Protocol, including: HTTP and FTP
 - Actions when matched, including: Accept and Log & Deny and Log
6. If you want to apply advanced settings, you can enable
 - Maximum File size for scanning: file size range is 1-10MB
 - Deny oversize action.
7. If you want to scan compressed file
 - Only supports ZIP and GZIP file formats
 - Two options are available, "Deny password protected file" and "Destroy file cannot be Decompressed".
8. Click [Save] to save profile.

Configuring File Exceptions

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

Object Profiles > Antivirus Profiles

File Exceptions

The system skips the antivirus file scanning based on the list in File Exception Settings. To import the list into File Exception Settings, please download the CSV template and fill in the SHA value(s) and the description(s).

Total Number of File Exception(s): 2

[File Exception Settings](#) [Download CSV Template](#)

Antivirus Profiles

[+ Add](#) Total Number of Records: 2 (Max: 256)

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

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

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

Procedure

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

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

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

File Exception Settings

[+ Add](#) [Import](#) Total Number of Records: 2 (Max: 2000)

Search

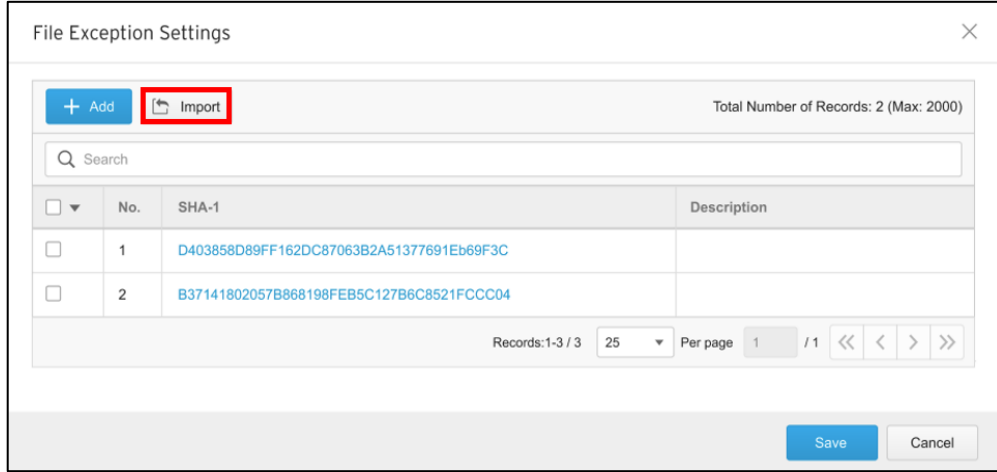
<input type="checkbox"/>	No.	SHA-1	Description
<input type="checkbox"/>	1	D403858D89FF162DC87063B2A51377691Eb69F3C	
<input type="checkbox"/>	2	B37141802057B868198FEB5C127B6C8521FCCC04	

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

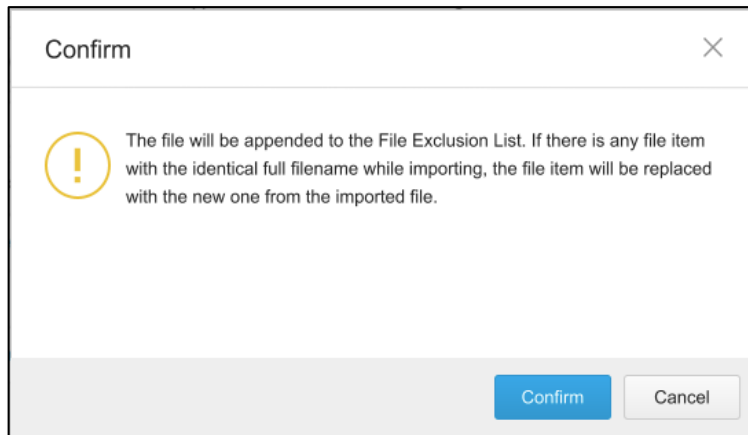
[Save](#) [Cancel](#)

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

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



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



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

Logs

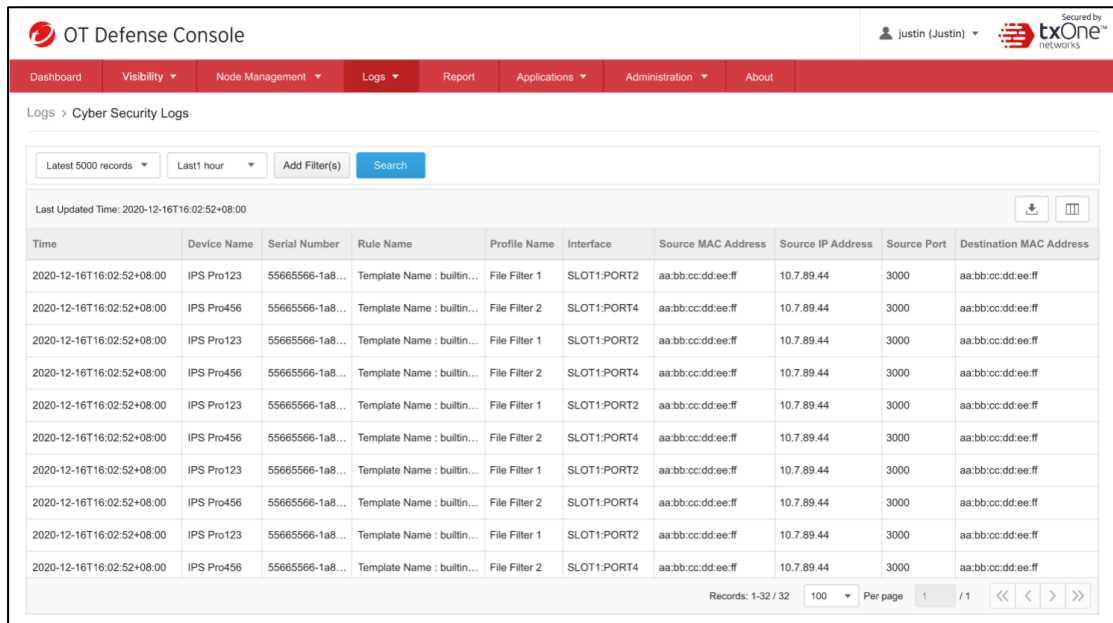
This chapter describes the system event logs and security detection logs you can view on the management console.

You can view the following logs on ODC:

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

Viewing Cyber Security Logs

The cyber security logs cover logs detected by both the intrusion prevention and denial of service prevention features.



OT Defense Console

Dashboard | Visibility | Node Management | **Logs** | Report | Applications | Administration | About

Logs > Cyber Security Logs

Latest 5000 records | Last 1 hour | Add Filter(s) | Search

Last Updated Time: 2020-12-16T16:02:52+08:00

Time	Device Name	Serial Number	Rule Name	Profile Name	Interface	Source MAC Address	Source IP Address	Source Port	Destination MAC Address
2020-12-16T16:02:52+08:00	IPS Pro123	55665566-1a8...	Template Name : builtin...	File Filter 1	SLOT1:PORT2	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro456	55665566-1a8...	Template Name : builtin...	File Filter 2	SLOT1:PORT4	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro123	55665566-1a8...	Template Name : builtin...	File Filter 1	SLOT1:PORT2	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro456	55665566-1a8...	Template Name : builtin...	File Filter 2	SLOT1:PORT4	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro123	55665566-1a8...	Template Name : builtin...	File Filter 1	SLOT1:PORT2	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro456	55665566-1a8...	Template Name : builtin...	File Filter 2	SLOT1:PORT4	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro123	55665566-1a8...	Template Name : builtin...	File Filter 1	SLOT1:PORT2	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro456	55665566-1a8...	Template Name : builtin...	File Filter 2	SLOT1:PORT4	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro123	55665566-1a8...	Template Name : builtin...	File Filter 1	SLOT1:PORT2	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff
2020-12-16T16:02:52+08:00	IPS Pro456	55665566-1a8...	Template Name : builtin...	File Filter 2	SLOT1:PORT4	aa:bb:cc:dd:ee:ff	10.7.89.44	3000	aa:bb:cc:dd:ee:ff

Records: 1-32 / 32 | 100 | Per page 1 | 1 | << < > >>

Procedure

1. Go to [Logs] > [Cyber Security Logs].
2. Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.

3. Select the number of search results from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, **Latest 5000 records**, and **Last 50000 records**.

4. Click [Add Filter(s)] button and the screen below will appear.

Select parameters for [Field] and [Operator] (is or is not) from the drop-down menu.

Options for [Field] are listed below:

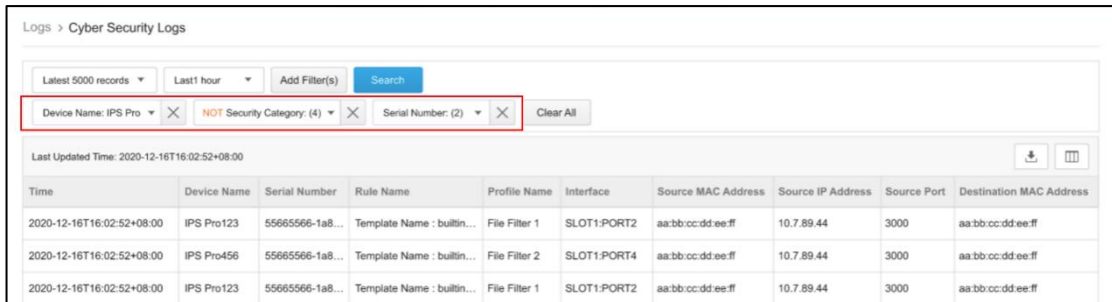
- Device Name
- Serial Number
- Rule Name
- Profile Name
- Event ID
- TID
- Security Category
- Security Severity
- Direction
- Interface
- Attacker
- Source MAC Address
- Source IP Address
- Source Port
- Destination MAC Address
- Destination IP Address
- Destination Port
- VLAN ID
- Ethernet Type
- IP Protocol Name
- Action

Input values in [Value] and press **enter** or type a comma (,) to input more values.

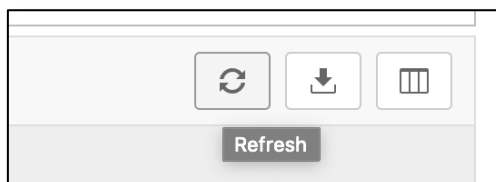
To add more filters, click .

- You can list up to 10 search values. If no value is input, the empty data will be searched.
- The maximum numbers of filters can be 10.

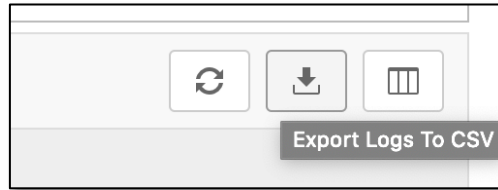
Then, click the [Apply] button. Afterwards, the filters that you just applied will be listed. Click [Search] button to query cyber security logs.



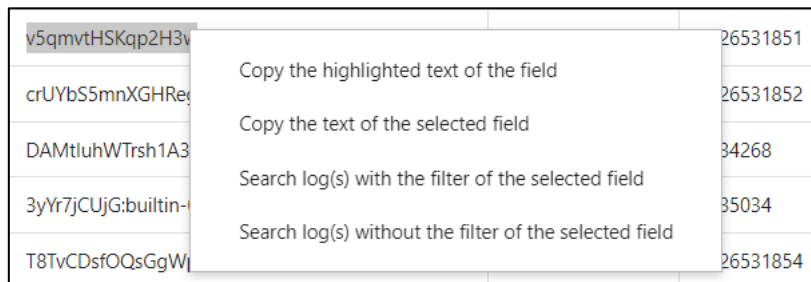
5. Click the [Refresh] button to search again.



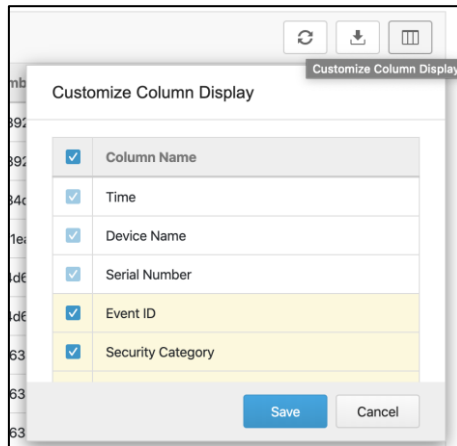
- Click the [Export Logs To CSV] button to export a CSV file of your current search results.



- Right click on a log entry and a menu screen will appear. You can take one of the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field



- To customize the data columns displayed, do the following:
 - Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
 - Select one or multiple table columns to display.
 - Click [Save].



The following table describes the cyber security log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Event ID	The ID of the matched signature
Security Category	The category of the matched signature
Security Severity	The severity level assigned to the matched signature

Field	Description
Direction	The name of the interface direction that EdgeFire was accessed from (This field is only for EdgeFire)
Interface	The interface information of the Edge series product
Attacker	Where the attacker is coming from
Security Rule Name	The name of the matched signature
Source MAC Address	The source MAC address of the connection
Source IP Address	The source IP address of the connection
Source Port	The source port of the connection
Destination MAC address	The destination MAC address of the connection
Destination IP Address	The destination IP address of the connection
Destination Port	The destination port of the connection
VLAN ID	The VLAN ID of the connection
Ethernet Type	The ethernet type of the connection
IP Protocol Name	The IP protocol name of the connection
Action	The action performed based on the policy settings
Count	The number of detected network packets within the detection period after the detection threshold was reached

Viewing Policy Enforcement Logs

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

Time	Device Name	Serial Number	Rule Name	Direction	Interface	Source MAC Address	Source IP Address	Source Port	Destination MAC Address	Destination IP Address	Destination Port	VLAN ID	IP Protocol Name	Action
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow
2020-09-24T16:15:23+08:00	EdgeIPS	TMG02190000016	smb	-	PORT2	12:22:64:07:05:15	100.7.5.21	28070	12:22:64:08:00:0a	100.8.0.10	445	N/A	TCP	Allow

Procedure

1. Go to [Logs] > [Policy Enforcement Logs].
2. You can take the following actions:

- Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
- Select the number of search result from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
- Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, and then click the [Search] button.
- Click the [Refresh] button to search again.
- Click the [Export Logs To CSV] button to export a CSV file of your current search results.
- Right-click on a field and the menu screen will appear. You can take one of the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the policy enforcement log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Rule Name	The name of the policy enforcement rule that was used to generate the log
Direction	The name of the interface direction that EdgeFire was accessed from(The field is only for EdgeFire)
Source MAC Address	The source MAC address of the connection
Source IP Address	The source IP address of the connection
Source Port	The source port, if the selected protocol is TCP/UDP The ICMP type, if the selected protocol is ICMP
Destination MAC address	The destination MAC address of the connection
Destination IP Address	The destination IP address of the connection
Destination Port	The destination port, if the selected protocol is TCP/UDP The ICMP code, if the selected protocol is ICMP
VLAN ID	The VLAN ID information
IP Protocol Name	The IP protocol name of the connection
Action	The action performed based on the policy settings

Viewing Protocol Filter Logs

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

Time	Device Name	Serial Number	Rule Name	Profile Name	Direction	Interface	Source MAC Address	Source IP Address	Source Port	Destination MAC Address	Destination IP Address	Destination Port	VLAN ID	Ethernet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT3	74e6e2e29375	10.132.149.50	59413	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT3	74e6e2e29375	10.132.149.50	59414	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	74e6e2e29375	10.132.149.50	59417	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT3	74e6e2e29375	10.132.149.50	59415	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	74e6e2e29375	10.132.149.50	59418	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	74e6e2e29375	10.132.149.50	59416	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	74e6e2e29375	10.132.149.50	59402	00:00:0c:9f:fd:10	10.76.96.74	10011	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	001c7f7d4fc9	10.76.96.24	54143	02:42:3e:63:25:2d	10.132.151.1	102	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT3	001c7f7d4fc9	10.76.96.24	54143	02:42:3e:63:25:2d	10.132.151.1	102	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	001c7f7d4fc9	10.76.96.24	54121	02:42:3e:63:25:2d	10.132.151.7	102	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT3	001c7f7d4fc9	10.76.96.24	54121	02:42:3e:63:25:2d	10.132.151.7	102	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	001c7f7d4fc9	10.76.96.24	54121	02:42:3e:63:25:2d	10.132.151.7	102	N/A	Internet
2020-09-24T16:20:16+08:00	EdgeIPS-Pro-VM	LTwillgivespocamoney	AllSPS_PF_Basic	All_Basic	-	SLOT1:PORT4	001c7f7d4fc9	10.76.96.24	54121	02:42:3e:63:25:2d	10.132.151.7	102	N/A	Internet

Procedure

- Go to [Logs] > [Protocol Filter Logs].
- You can take the following actions:
 - Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
 - Select the number of search result from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
 - Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, then click the [Search] button.
 - Click the [Refresh] button to search again.
 - Click the [Export Logs To CSV] button to export a CSV of your current search result.
 - Right-click on a field and the menu screen will appear. You can take the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

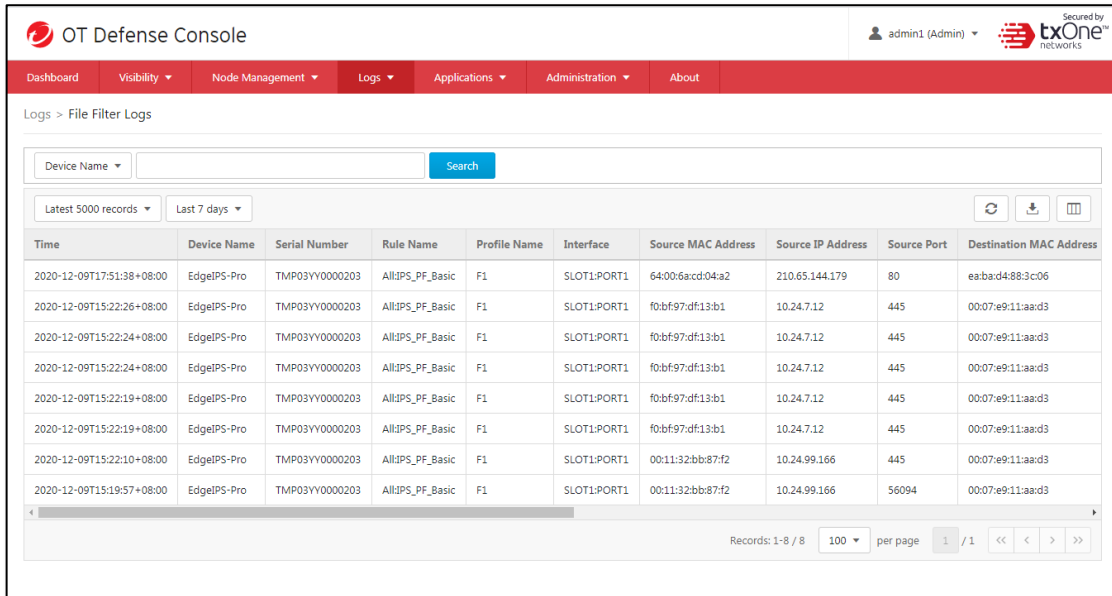
- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the protocol filter log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Rule Name	The name of the policy enforcement rule that was used to generate the log
Profile Name	The name of the protocol filter profile that was used to generate the log
Direction	The name of the interface direction that EdgeFire was accessed from (This field is only for EdgeFire)
Interface	The interface information of the Edge series product
Source MAC Address	The source MAC address of the connection
Source IP Address	The source IP address of the connection
Source Port	The source port, if the selected protocol is TCP/UDP The ICMP type, if the selected protocol is ICMP
Destination MAC address	The destination MAC address of the connection
Destination IP Address	The destination IP address of the connection
Destination Port	The destination port, if the selected protocol is TCP/UDP The ICMP code, if the selected protocol is ICMP
VLAN ID	The VLAN ID information
Ethernet Type	The Ethernet type of the connection
IP Protocol Name	The IP protocol name of the connection
L7 Protocol Name	The layer 7 protocol name of the connection -- the term 'layer 7' refers to the one defined in the OSI (Open Systems Interconnection) model
Cmd / Fun No	The command or the function number that triggered the log
Extra Information	Extra information provided with the log
Action	The action performed based on the policy settings
Count	The number of detected network packets

Viewing File Filter and Antivirus Logs

You can view details about system events on the OT Defense Console.



OT Defense Console

admin1 (Admin) | txOne networks

Dashboard | Visibility | Node Management | **Logs** | Applications | Administration | About

Logs > File Filter Logs

Device Name: Search

Latest 5000 records | Last 7 days

Time	Device Name	Serial Number	Rule Name	Profile Name	Interface	Source MAC Address	Source IP Address	Source Port	Destination MAC Address
2020-12-09T17:51:38+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	64:00:6a:cd:04:a2	210.65.144.179	80	ea:ba:d4:88:3c:06
2020-12-09T15:22:26+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	f0:bf:97:df:13:b1	10.24.7.12	445	00:07:e9:11:aad3
2020-12-09T15:22:24+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	f0:bf:97:df:13:b1	10.24.7.12	445	00:07:e9:11:aad3
2020-12-09T15:22:24+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	f0:bf:97:df:13:b1	10.24.7.12	445	00:07:e9:11:aad3
2020-12-09T15:22:19+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	f0:bf:97:df:13:b1	10.24.7.12	445	00:07:e9:11:aad3
2020-12-09T15:22:19+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	f0:bf:97:df:13:b1	10.24.7.12	445	00:07:e9:11:aad3
2020-12-09T15:22:10+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	00:11:32:bb:87:f2	10.24.99.166	445	00:07:e9:11:aad3
2020-12-09T15:19:57+08:00	EdgeIPS-Pro	TMP03YY0000203	AllIPS_PF_Basic	F1	SLOT1:PORT1	00:11:32:bb:87:f2	10.24.99.166	56094	00:07:e9:11:aad3

Records: 1-8 / 8 | 100 per page | 1 / 1

Procedure

- Go to [Logs] > [File Filter Logs].
- You can take the following actions:
 - Select a time period from the drop-down list, and a search will immediately be conducted. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
 - Select the number of search results from the drop-down list, and a search will immediately be conducted. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
 - Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, then click the [Search] button.
 - Click the [Refresh] button to search again.
 - Click the [Export Logs To CSV] button to export a CSV file of your current search results.
 - Right-click a field and the menu screen will appear. You can take the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

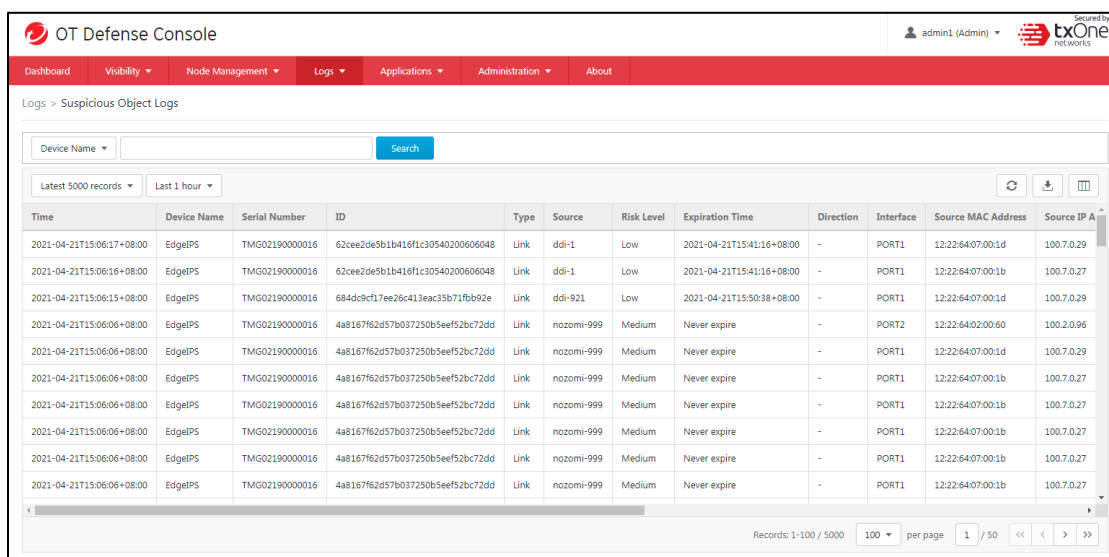
- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the file filter and antivirus log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Rule Name	The name of the policy enforcement rule that was used to generate the log
Profile Name	The name of the file filter profile or Antivirus filter profile that was used to generate the log
Interface	The interface information of the Edge Series product
Source MAC Address	The source MAC address of the connection
Source IP Address	The source IP address of the connection
Source Port	The source port, if the selected protocol is TCP/UDP The ICMP type, if the selected protocol is ICMP
Destination MAC address	The destination MAC address of the connection
Destination IP Address	The destination IP address of the connection
Destination Port	The destination port, if the selected protocol is TCP/UDP The ICMP code, if the selected protocol is ICMP
VLAN ID	The VLAN ID information
L7 Protocol Name	The layer 7 protocol name of the connection -- the term 'layer 7' refers to the one defined in the OSI (Open Systems Interconnection) model
Extra Information	Extra information provided with the log
Action	The action performed based on the policy settings

Viewing Suspicious Object Logs

You can view details about suspicious object log events on the OT Defense Console.



OT Defense Console

admin1 (Admin) | txOne networks

Dashboard | Visibility | Node Management | Logs | Applications | Administration | About

Logs > Suspicious Object Logs

Device Name: [] Search

Latest 5000 records | Last 1 hour

Time	Device Name	Serial Number	ID	Type	Source	Risk Level	Expiration Time	Direction	Interface	Source MAC Address	Source IP Address
2021-04-21T15:06:17+08:00	Edge1PS	TMG02190000016	62cee20e5b1b416f1c30540200606048	Link	ddi-1	Low	2021-04-21T15:41:16+08:00	-	PORT1	12:22:64:07:00:1d	100.7.0.29
2021-04-21T15:06:16+08:00	Edge1PS	TMG02190000016	62cee20e5b1b416f1c30540200606048	Link	ddi-1	Low	2021-04-21T15:41:16+08:00	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:15+08:00	Edge1PS	TMG02190000016	684dc9cf17ee26c413eac35b73fb92e	Link	ddi-921	Low	2021-04-21T15:50:38+08:00	-	PORT1	12:22:64:07:00:1d	100.7.0.29
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT2	12:22:64:02:00:60	100.2.0.96
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1d	100.7.0.29
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27
2021-04-21T15:06:06+08:00	Edge1PS	TMG02190000016	4a8167f62d57b037250b5eef52bc72dd	Link	nozomi-999	Medium	Never expire	-	PORT1	12:22:64:07:00:1b	100.7.0.27

Records: 1-100 / 5000 | 100 per page | 1 / 50

Procedure

1. Go to [Logs] > [Suspicious Object Logs].
2. You can take the following actions:
 - Select a time period from the drop-down list, and a search will immediately be conducted. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
 - Select the number of search results from the drop-down list, and a search will immediately be conducted. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
 - Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, then click the [Search] button.
 - Click the [Refresh] button to search again.
 - Click the [Export Logs To CSV] button to export a CSV file of your current search results.
 - Right-click a field and the menu screen will appear. You can take the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

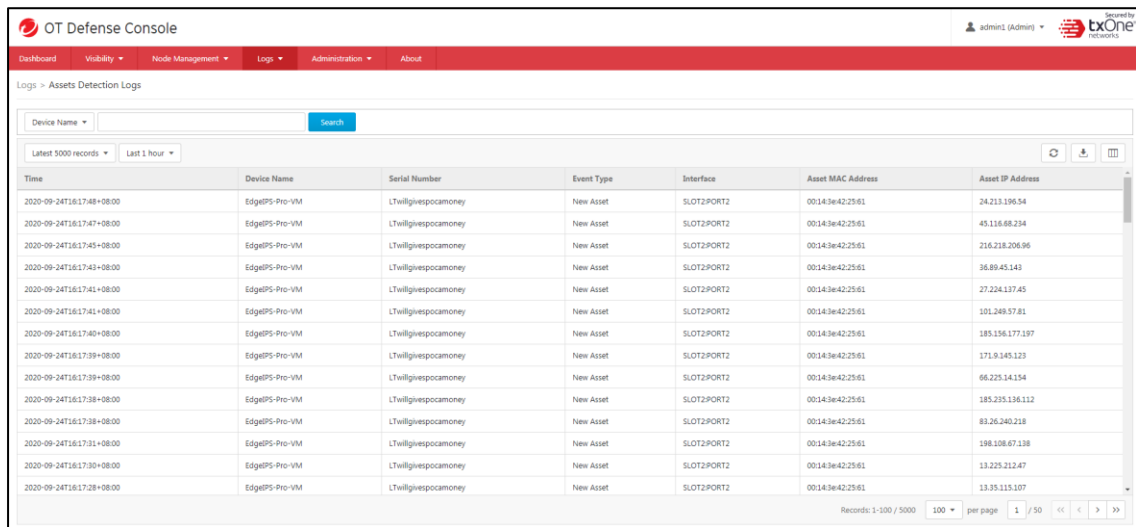
The following table describes the suspicious object log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
ID	The suspicious object ID generated by ODC
Type	The type includes Node and Link
Source	The SO source name information
Risk Level	The risk level is reported from SO source
Expiration date	The imported SO expiration date and time
Interface	The interface of the Edge device where the SO is detected
Source MAC Address	The source MAC address of the connection
Source IP Address	The source IP address of the connection
Source Port	The source port, if the selected protocol is TCP/UDP The ICMP type, if the selected protocol is ICMP
Destination MAC address	The destination MAC address of the connection
Destination IP Address	The destination IP address of the connection
Destination Port	The destination port, if the selected protocol is TCP/UDP The ICMP code, if the selected protocol is ICMP
VLAN ID	The VLAN ID information
Ethernet type	The Ethernet type of the connection
IP Protocol Name	The IP protocol name of the connection

Field	Description
Action	The action performed based on the policy settings, including 'Allow' and 'Deny'
Count	The event count

Viewing Asset Detection Logs

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



Time	Device Name	Serial Number	Event Type	Interface	Asset MAC Address	Asset IP Address
2020-09-24T16:17:48+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	24.213.196.54
2020-09-24T16:17:47+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	45.116.68.234
2020-09-24T16:17:45+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	216.218.206.96
2020-09-24T16:17:43+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	36.89.45.143
2020-09-24T16:17:41+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	27.224.137.45
2020-09-24T16:17:41+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	101.249.57.81
2020-09-24T16:17:40+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	185.156.177.197
2020-09-24T16:17:39+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	171.9.145.123
2020-09-24T16:17:39+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	66.225.14.154
2020-09-24T16:17:38+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	185.235.136.112
2020-09-24T16:17:38+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	83.26.240.218
2020-09-24T16:17:31+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	198.108.67.138
2020-09-24T16:17:30+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	13.225.212.47
2020-09-24T16:17:28+08:00	EdgePS-Pro-VM	LTwillgivespocamoney	New Asset	SLOT2:PORT2	0014:3e42:25:61	13.35.115.107

Procedure

- Go to [Logs] > [Asset Detection Logs].
- You can take the following actions:
 - Select a time period from the drop-down list and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
 - Select the number of search results from the drop-down list and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
 - Select a specific parameter from the drop-down list, type a value that you want to search in the text field, then click the [Search] button.
 - Click the [Refresh] button to search again.
 - Click the [Export Logs To CSV] button to export a CSV file of your current search results.
 - Right-click on a field and the menu screen will appear. You can take one of the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

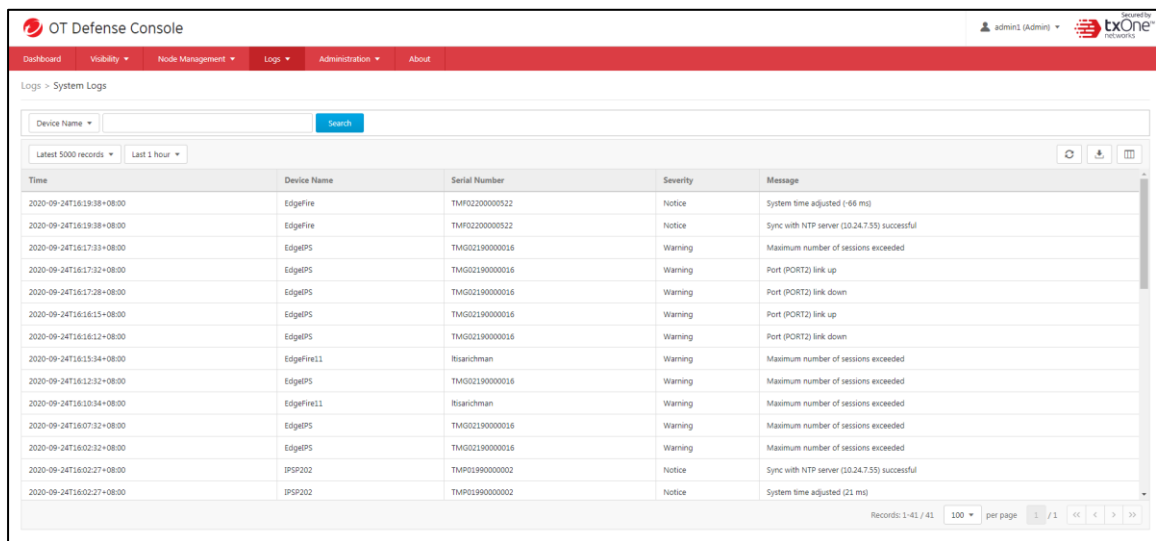
- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the asset detection log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Event Type	The log event description
Interface	The interface information of Edge series product
Asset MAC Address	The MAC address of the asset
Asset IP Address	The source IP address of the asset

Viewing System Logs

You can view details about system events on the OT Defense Console.



The screenshot displays the OT Defense Console interface. At the top, there is a navigation bar with 'Dashboard', 'Viability', 'Node Management', 'Logs', 'Administration', and 'About'. The 'Logs' section is active, showing 'System Logs'. Below the navigation, there is a search bar for 'Device Name' and a 'Search' button. The main content area shows a table of log entries with the following columns: Time, Device Name, Serial Number, Severity, and Message. The table contains 16 rows of log data, including events like 'System time adjusted (-46 ms)', 'Sync with NTP server (10.24.7.55) successful', 'Maximum number of sessions exceeded', and 'Port (PORT2) link up/down'. At the bottom right of the table, there is a pagination control showing 'Records: 1-42 / 41' and '100 per page'.

Procedure

1. Go to [Logs] > [System Logs].
2. You can take the following actions:

- Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
- Select the number of search results from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
- Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, then click the [Search] button.
- Click the [Refresh] button to search again.
- Click the [Export Logs To CSV] button to export a CSV file of your current search results.
- Right-click a field and the menu screen will appear. You can take the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

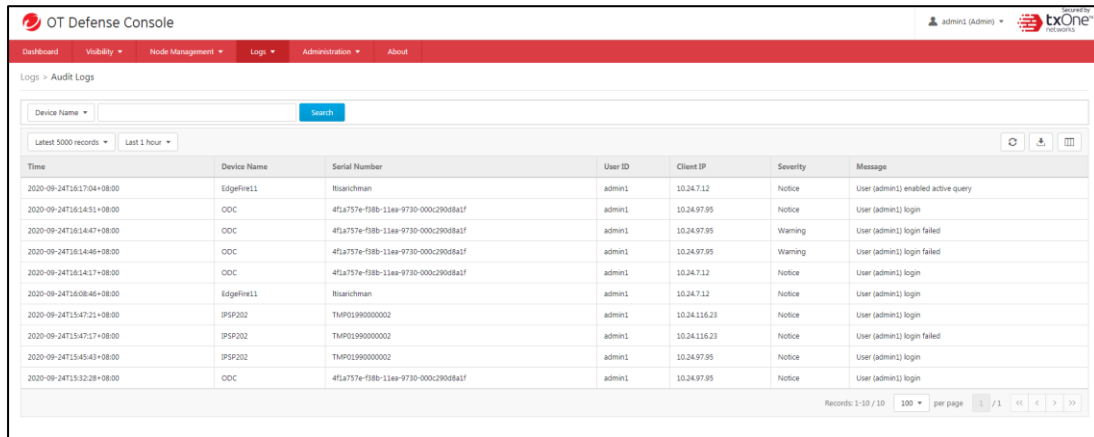
- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the system log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
Severity	The severity level of the log
Message	The log event description

Viewing Audit Logs

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



Time	Device Name	Serial Number	User ID	Client IP	Severity	Message
2020-09-24T16:17:04+08:00	EdgeFire11	Risarichman	admin1	10.24.7.12	Notice	User (admin1) enabled active query
2020-09-24T16:14:51+08:00	ODC	4f5a757e-f98b-11e9-9730-000c29088a1f	admin1	10.24.97.95	Notice	User (admin1) login
2020-09-24T16:14:47+08:00	ODC	4f5a757e-f98b-11e9-9730-000c29088a1f	admin1	10.24.97.95	Warning	User (admin1) login failed
2020-09-24T16:14:46+08:00	ODC	4f5a757e-f98b-11e9-9730-000c29088a1f	admin1	10.24.97.95	Warning	User (admin1) login failed
2020-09-24T16:14:17+08:00	ODC	4f5a757e-f98b-11e9-9730-000c29088a1f	admin1	10.24.7.12	Notice	User (admin1) login
2020-09-24T16:08:46+08:00	EdgeFire11	Risarichman	admin1	10.24.7.12	Notice	User (admin1) login
2020-09-24T15:47:21+08:00	IPSP202	TM901990000002	admin1	10.24.116.23	Notice	User (admin1) login
2020-09-24T15:47:17+08:00	IPSP202	TM901990000002	admin1	10.24.116.23	Notice	User (admin1) login failed
2020-09-24T15:45:43+08:00	IPSP202	TM901990000002	admin1	10.24.97.95	Notice	User (admin1) login
2020-09-24T15:32:38+08:00	ODC	4f5a757e-f98b-11e9-9730-000c29088a1f	admin1	10.24.97.95	Notice	User (admin1) login

Procedure

1. Go to [Logs] > [Audit Logs].
2. You can take the following actions:
 - Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
 - Select the number of search result from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.
 - Select a specific parameter from the drop-down list, type a value that you want to search for in the text field, and then click the [Search] button.
 - Click the [Refresh] button to search again.
 - Click the [Export Logs To CSV] button to export a CSV file of your current search results.
 - Right-click a field and the menu screen will appear. You can take one of the following actions:
 - Copy the highlighted text of the field
 - Copy text of the selected field
 - Search log(s) with the filter of the selected field
 - Search logs without the filter of the selected field

To customize the data columns displayed, do the following:

- Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
- Select one or multiple table columns to display.
- Click [Save].

The following table describes the audit log information.

Field	Description
Time	The time the log entry was created
Device Name	The host name of the node that generated the log
Serial Number	The serial number of the node
User ID	The user account used to execute the task
Client IP	The IP address of the host used to access the management console
Severity	The severity level of the logs
Message	The log event description

The Report Tab

This chapter describes how to use Report function. OT Defense Console provides report templates for easy access to threat information. Reports help you better understand complex threat scenarios, prioritize responses, and plan containment and mitigation.

The report feature allows users to create instant reports and schedule reports. The report content can be selected by different content. You can configure the following report features in OT defense console”.

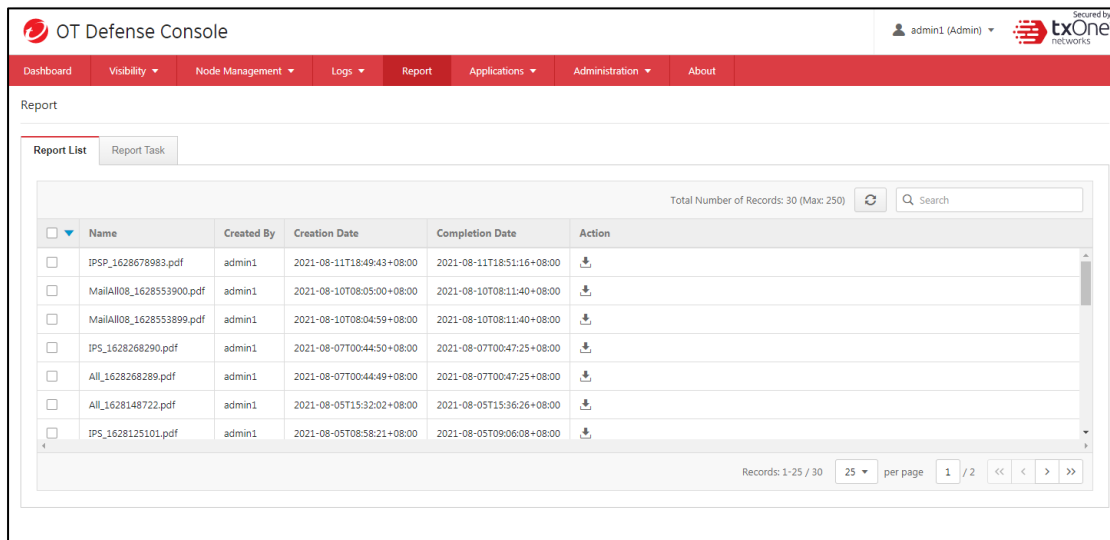
- **Report List:** Contains all generated report and can be downloaded manually or further deleted.
- **Report Task:** Allows you to use to create report task by scheduling or generating instant report according to the selected content.

Report List

Allows user to download the generated report manually.

Procedure

1. Go to [Report]
2. Click [Report List] to select generated Report file.

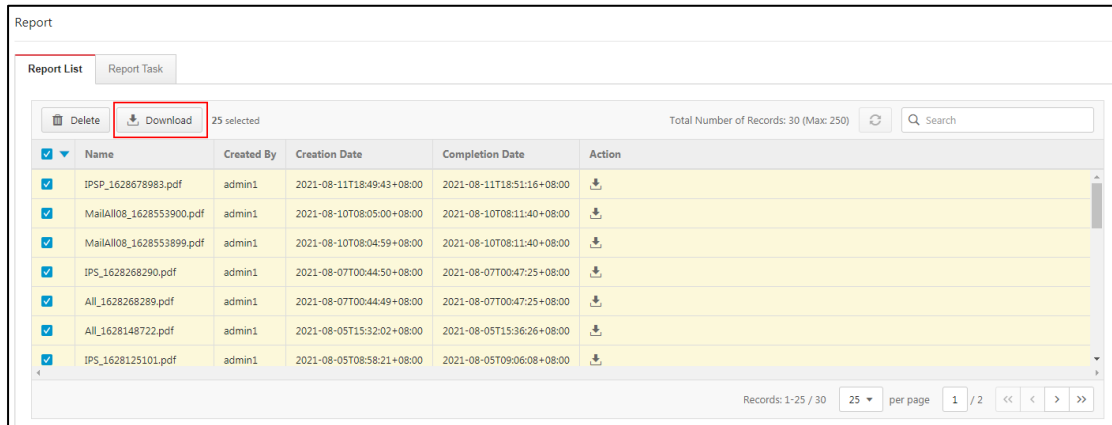


The screenshot shows the OT Defense Console interface. At the top, there is a navigation bar with tabs: Dashboard, Visibility, Node Management, Logs, Report, Applications, Administration, and About. The 'Report' tab is active. Below the navigation bar, there are two sub-tabs: 'Report List' (selected) and 'Report Task'. The main content area displays a table of generated reports. The table has columns for Name, Created By, Creation Date, Completion Date, and Action. There are 7 rows of data, each with a download icon in the Action column. At the bottom of the table, there is a pagination control showing 'Records: 1-25 / 30', '25' per page, and '1 / 2' pages.

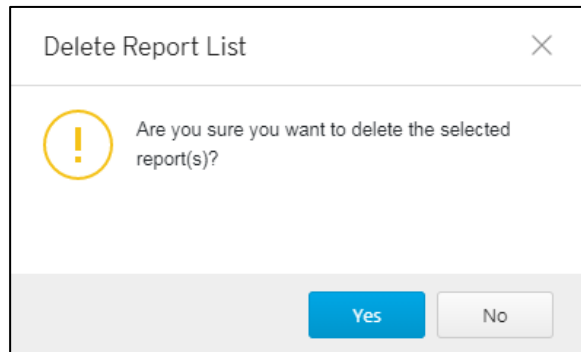
Name	Created By	Creation Date	Completion Date	Action
IPSP_1628678983.pdf	admin1	2021-08-11T18:49:43+08:00	2021-08-11T18:51:16+08:00	Download
MailAll08_1628553900.pdf	admin1	2021-08-10T08:05:00+08:00	2021-08-10T08:11:40+08:00	Download
MailAll08_1628553899.pdf	admin1	2021-08-10T08:04:59+08:00	2021-08-10T08:11:40+08:00	Download
IPS_1628268290.pdf	admin1	2021-08-07T00:44:50+08:00	2021-08-07T00:47:25+08:00	Download
All_1628268289.pdf	admin1	2021-08-07T00:44:49+08:00	2021-08-07T00:47:25+08:00	Download
All_1628148722.pdf	admin1	2021-08-05T15:32:02+08:00	2021-08-05T15:36:26+08:00	Download
IPS_1628125101.pdf	admin1	2021-08-05T08:58:21+08:00	2021-08-05T09:06:08+08:00	Download

3. You can click the download icon to download the generated report manually.

- You can use another way to select all generated report and click the download button to download all the selected report in one zip file to your desktop.



- If you would like to delete the generated reports, select one or multiple reports then click the [Delete] button.

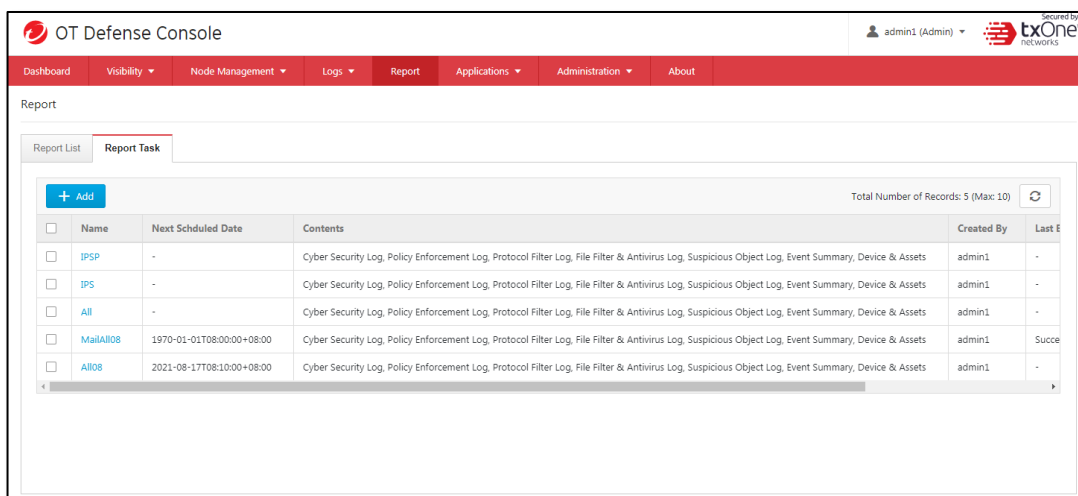


Report Task

Allows user to add report task by scheduling and editing what content will be generated.

Procedure

- Go to [Report]



- Click [Report Task] to select the generated Report file.

3. You can click [Add] button to create new Report task.

Field	Description
Name	Report task name
Description	Task description
Schedule	Provide weekly and montly scheduled reports
Time period	Available to select data source period and offer options including " Last 7 days", "Last 14 days" and "last 30 days"
Device type	Available to select device type by product line.
Content selection	Allows user to select different content source by event log type.

4. You can use another way to select all the generated report and click the download button to download all the selected report in one zip file to your desktop.
5. If you would like to delete the scheduled reports, select one or multiple reports then click the [Delete] button.

Report Sample

The generated report can be downloaded in PDG file format. A sample report is provided below.



ODC Report

Version: ODC_7617_15190264
 Platform: webportal
 Report Date: 2023-04-07 08:16:57-08:00
 Report Range: 001_200000

Copyright © 2023 Trend Micro Incorporated. All rights reserved. TM

1	Cyber Security	2
1.1	Cyber Security Severity	2
1.2	Top Cyber Security Events by Source IP	4
1.3	Cyber Security Severity Trends	2
1.4	Top 5 Cyber Security Events Category Trends	4
1.5	Top IPS Attack Event Categories	6
1.6	Top Cyber Security Events	7
1.7	Top Cyber Security Events by Destination IP	7
1.8	Top Cyber Security Events by Device	7
2	Devices	8
2.1	Device List	8
3	Protocol Filter	10
3.1	Top L7 Protocol Filter Events by Device	10
3.2	Top Protocol Filter Events by Destination IP	10
3.3	Top L7 Protocols	11
3.4	Top Protocol Filter Events by Source IP	11
3.5	Top L7 Protocols Event Trends	11
4	File Filter	13
4.1	Top File Filter Events by Source IP	13
4.2	Top File Filter Events by Destination IP	13
4.3	Top File Filter Events by Device	13
5	Policy Enforcement	14
5.1	Top Policy Enforcement Events by Source IP	14
5.2	Top Policy Enforcement Events by Destination IP	14
5.3	Top Policy Enforcement Events by Device	15



1. Cyber Security

1.1 Cyber Security Severity

This widget displays the numbers of the cyber security events by severity level in the selected device group(s) for the last 24 hours.

Level	Count
High	3702331
Medium	2312559
Critical	1471463

1.2 Top Cyber Security Events by Source IP

This widget displays the top 5 or 10 source IP addresses for cyber security events found in the selected device group(s) for the last 24 hours.

IP	Count
10.0.1.101	4039
10.0.1.126	3714
10.0.15.90	3545
10.0.15.142	3441
10.0.22.174	3027

1.3 Cyber Security Severity Trends

This widget displays the event trends for the top 5 or 10 cyber security severity levels found in the selected device group(s) for the last 24 hours.



ODC Report

Page 1 of 15

ODC Report

Page 2 of 15

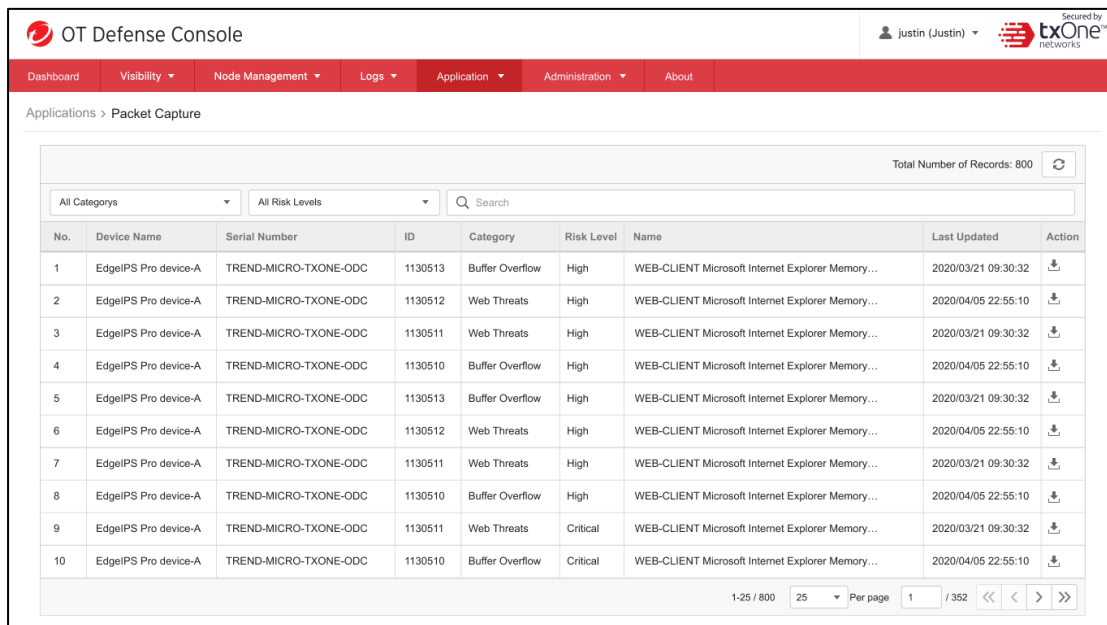
The Application Tab

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

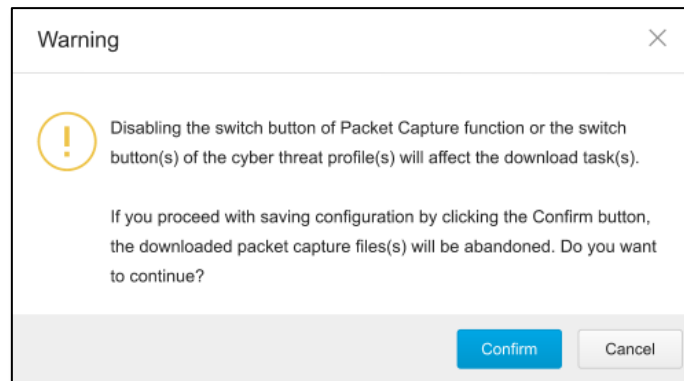
Packet Capture

Procedure

1. Go to [Application] > [Packet Capture].
2. Click [Download List] to select IPS rules and packets.



3. You can click the download icon to download the packet to your disk.
4. If you disable packet capture, all captured packets will be deleted, but before that it will show the following notification page.



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

Suspicious Object Pool

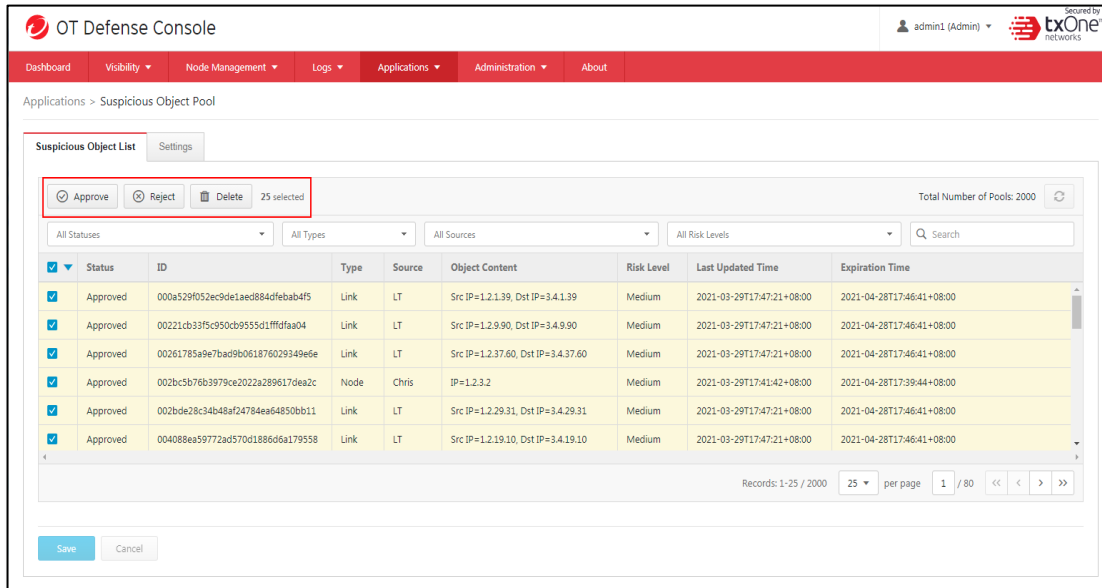
The Suspicious Objects (SO) are suspicious IP addresses (Node) or network connections (Link) to be blocked on the Edge devices. They are imported to ODC from external SO sources, such as Trend Micro Deep Discovery Inspector, via the Suspicious Object APIs.

The Suspicious Object Pool allows the administrator to review the imported suspicious objects and to configure how the system imports objects or ages them out of the pool.

Reviewing Imported Suspicious Objects

Procedure

1. Go to [Application] > [Suspicious Object Pool].
2. Click the [Suspicious Object List] tab.
3. Click the checkbox to select/deselect suspicious objects and choose a desired action, "Approve", "Reject" or "Delete", for the selected objects.
4. Click the [Save] button to save the changes.



The screenshot shows the 'Suspicious Object List' interface in the OT Defense Console. At the top, there are navigation tabs: Dashboard, Visibility, Node Management, Logs, Applications, Administration, and About. The current view is 'Applications > Suspicious Object Pool'. Below the navigation, there are tabs for 'Suspicious Object List' and 'Settings'. A toolbar contains 'Approve', 'Reject', and 'Delete' buttons, along with a '25 selected' indicator. Below the toolbar, there are filters for 'All Statuses', 'All Types', 'All Sources', and 'All Risk Levels', along with a search bar. The main area is a table with the following columns: Status, ID, Type, Source, Object Content, Risk Level, Last Updated Time, and Expiration Time. The table contains 6 rows of data, all with a status of 'Approved' and a risk level of 'Medium'. At the bottom of the table, there are pagination controls showing 'Records: 1-25 / 2000' and '25 per page'. Below the table, there are 'Save' and 'Cancel' buttons.

Status	ID	Type	Source	Object Content	Risk Level	Last Updated Time	Expiration Time
Approved	000a529f052e3de1aed884dfebab4f5	Link	LT	Src IP=1.2.1.39, Dst IP=3.4.1.39	Medium	2021-03-29T17:47:21+08:00	2021-04-28T17:46:41+08:00
Approved	00221cb33f5c950cb9555d1fff0fa04	Link	LT	Src IP=1.2.9.90, Dst IP=3.4.9.90	Medium	2021-03-29T17:47:21+08:00	2021-04-28T17:46:41+08:00
Approved	00261785a9e7bad9b061876029349e6e	Link	LT	Src IP=1.2.37.60, Dst IP=3.4.37.60	Medium	2021-03-29T17:47:21+08:00	2021-04-28T17:46:41+08:00
Approved	002bc5b76b3979ce2022a2896170ea2c	Node	Chris	IP=1.2.3.2	Medium	2021-03-29T17:41:42+08:00	2021-04-28T17:39:44+08:00
Approved	002bde28c34b48af24784ea64850bb11	Link	LT	Src IP=1.2.29.31, Dst IP=3.4.29.31	Medium	2021-03-29T17:47:21+08:00	2021-04-28T17:46:41+08:00
Approved	004088ea59772ad570d1886d6a179558	Link	LT	Src IP=1.2.19.10, Dst IP=3.4.19.10	Medium	2021-03-29T17:47:21+08:00	2021-04-28T17:46:41+08:00

- The suspicious object list is refreshed every 10 seconds by default, and can host up to 2000 suspicious objects.
- The rejected suspicious objects will remain on the list but will not be dispatched to the Edge device groups.
- The deleted suspicious objects will be removed from the list. They can appear as new objects if imported by the suspicious object source(s) again later.

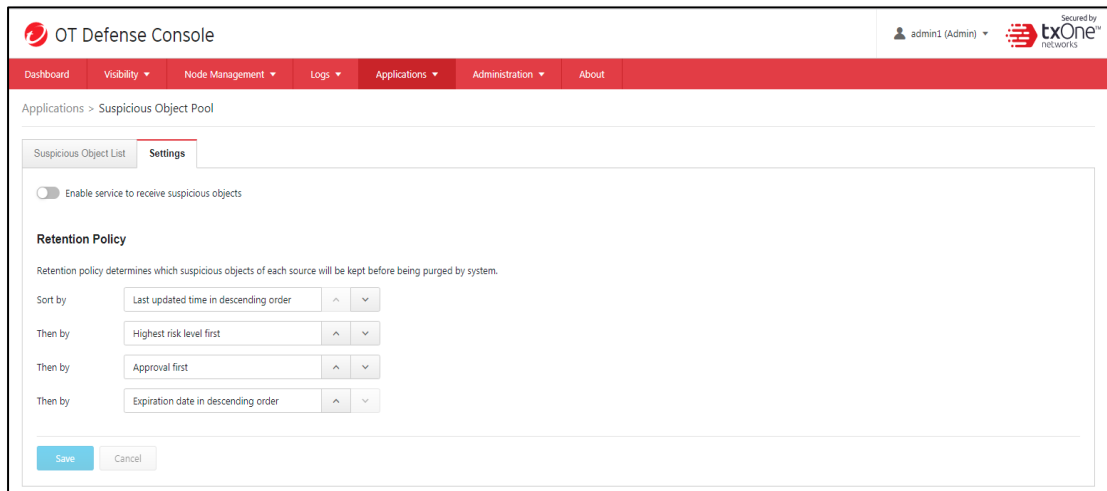
Configuring Suspicious Objects Import Settings

Procedure

1. Go to [Application] > [Suspicious Object Pool].
2. Click the [Settings] tab.

Here you can enable or disable receiving suspicious objects from external systems or adjust the retention policy. In the retention policy section, you can define the priority of different sorting methods for the system to determine which suspicious objects should be kept first when the list needs to be purged due to the upper limit of the suspicious object list.

3. Click the [Save] button to save the changes.



OT Defense Console

admin1 (Admin)

Secured by txOne networks

Dashboard Visibility Node Management Logs Applications Administration About

Applications > Suspicious Object Pool

Suspicious Object List Settings

Enable service to receive suspicious objects

Retention Policy

Retention policy determines which suspicious objects of each source will be kept before being purged by system.

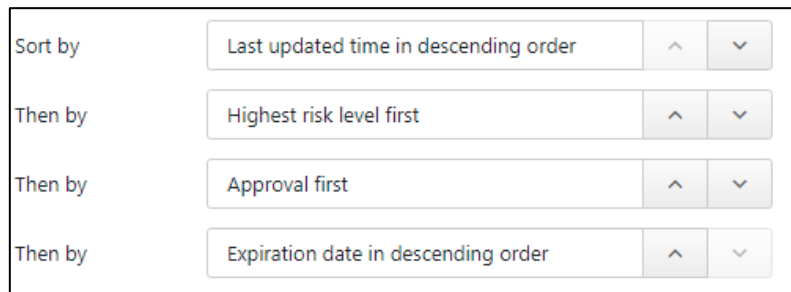
Sort by Last updated time in descending order

Then by Highest risk level first

Then by Approval first

Then by Expiration date in descending order

Save Cancel



Sort by Last updated time in descending order

Then by Highest risk level first

Then by Approval first

Then by Expiration date in descending order

Administration

This chapter describes the available administrative settings for ODC (Operational Technology Defense Console).

Account Management

- Log on to the management console using the administrator account to access the Accounts tab.

ODC 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 can log on to the management console using custom user accounts.

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

Task	Description
Add account	Click [Add] to create a new user account. For more information, see Account Input Format on page 132 .
Delete existing accounts	Select "pre-existing user accounts" and click "delete".
Edit existing accounts	Click the name of a pre-existing user account to view or modify the current account settings.
Configure Password Policy	Click [Password Policy] to adjust password restrictions. For more information, see Password Complexity on page 134 .
Login Protection	Click [Login Protection] configure Login protection.

User Roles

The following table describes the permissions matrix for user roles.

Administration Tab

Sub-Tab	Action	User Role				
		Master Admin	System Admin	Operator	Viewer	Auditor
Account Management	View	Yes	Yes	No	No	No
	Create Account	Yes	Yes	No	No	No
		-System Admin	- Operator			
		- Operator	-Viewer			
		-Viewer				

Sub-Tab	Action	User Role				
		Master Admin	System Admin	Operator	Viewer	Auditor
	Delete Account	Yes -System Admin - Operator -Viewer	Yes - Operator -Viewer	No	No	No
	Multi Accounts	No Only 1 Fixed Account	Yes	Yes	Yes	No Only 1 Fixed Account
System Time	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
Syslog	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
Updates	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
SSL Certificate	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
Log Purge	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
Backup/Restore	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No
License Control	View	Yes	Yes	No	No	No
	All operations	Yes	Yes	No	No	No

Dashboard, Visibility, and Log Tabs

Tab	Action	User Role			
		Admin	Operator	Viewer	Auditor
Dashboard	View	Yes	VG	VG	No
Visibility	View	Yes	VG	VG	No
Log (system, cyber security, policy enforcement, protocol filtering, asset detection)	View	Yes	VG	VG	No
Audit Log	View	Yes	No	No	Yes

- VG denotes that if the administrator has assigned/shared the device group permissions to/with the user account, then on the Dashboard/Visibility/Log tabs the user can view the information for that device group.

Node Management Tabs

Item	Action	User Role			
		Admin	Operator	Viewer	Auditor
Ungroup	View	Yes	Yes	No	No
	All Operations	Yes	No	No	No
Recycle Bin	View	Yes	Yes	No	No
	All Operations	Yes	No	No	No
Groups	View	Yes	Yes	No	No
	Device Operations (Move / Delete)	Yes	No	No	No
	Device Operations (Edit / Reboot)	Yes	Yes	No	No
	Edit Group Configuration	Yes	Yes	No	No
	Edit Permission Settings	Yes	No	No	No
	Group Operations (Add/Delete/Rename)	Yes	No	No	No
	Enable / Disable Device Group Configurations [Note]	Yes	Yes	No	No

■ 'Device group configurations' refers to cyber security, policy enforcement, and pattern settings.

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.

Type	Length	Format	Reserved Name
ID	1-32 characters	<ul style="list-style-type: none"> letters a-z, A-Z numbers 0-9 special characters: <ul style="list-style-type: none"> - periods [.] - underscores [_] leading and trailing characters are not special characters non-successive special characters 	<ul style="list-style-type: none"> admin administrator root auditor
Name	1-32 characters	<ul style="list-style-type: none"> letters a-z, A-Z numbers 0-9 special characters: <ul style="list-style-type: none"> - periods [.] - underscores [_] - space [] single spaces are not allowed 	

Type	Length	Format	Reserved Name
Description	0-64 characters	<ul style="list-style-type: none"> • letters a-z, A-Z • numbers 0-9 • special characters: <ul style="list-style-type: none"> - periods [.] - underscores [_] - space [] - parentheses [() []] - hyphen [-] 	

Adding a User Account

When you log on using the administrator account, you can create new user accounts for accessing the ODC system.

Procedure

1. Go to [Administration] > [Account Management].
2. Click [Add]. The Add User Account screen appears.

3. Configure the account settings.

Field	Description
ID	Type the user ID to log on to the management console.
Name	Type the alias name for this account used for display.
Full name	Type the name of the user for this account.
Password	Type the account password.
Confirm password	Type the account password again to confirm.
Role	Select a user role for this account. For more information, see and User Roles on page 130 .
Authentication source	Select authentication source from sources, including local and external authentication server.
Description	Type a description for this account.

4. Click [Save].

- When Authentication Source is selected as SAML SSO, the logon screen will shown with the extra option, [Use SAML SSO Log On].

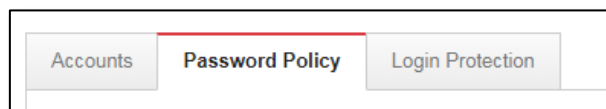
Changing Your Password

Procedure

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

Password Complexity

To improve password strength, the administrator can customize password policy in account management.



The available configuration options are shown as follows:

Administration > Account Management

Accounts
Password Policy
Login Protection

Password Complexity Settings

Minimum password length* (8 - 32)

Must not include user's account ID

Must not include user's account name

Must include at least one uppercase letter (A - Z)

Must include at least one lowercase letter (a - z)

Must include at least one number (0 - 9)

Must include at least one non-alphanumeric character (~!@#\$%^&*_-+=`\|000;'"<>.,?/)

Must not be the same as the last password

Password Expiration Settings

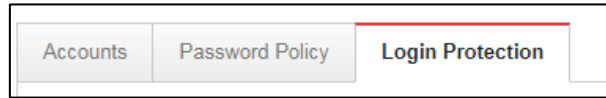
Set password expiration days

Days before passwords expire* (30 - 180 days)

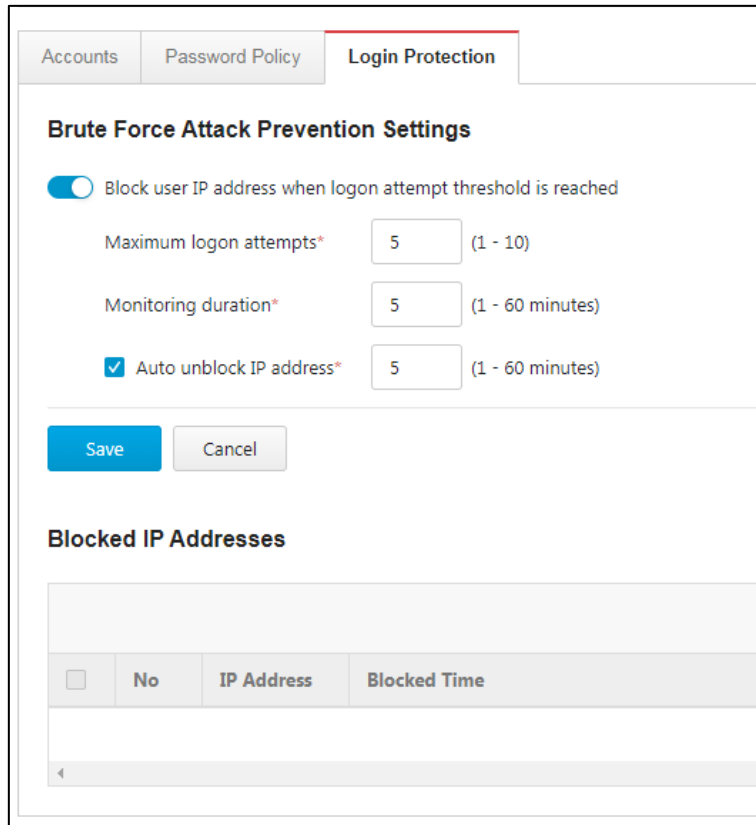
Days before a user is notified about expiration* (1 - 30 days)

Login Protection

To increase user login security, the administrator can configure Login Protection settings under account management.



The available configuration options are as follows:



Brute Force Attack Prevention Settings

Block user IP address when logon attempt threshold is reached

Maximum logon attempts* (1 - 10)

Monitoring duration* (1 - 60 minutes)

Auto unblock IP address* (1 - 60 minutes)

Blocked IP Addresses

<input type="checkbox"/>	No	IP Address	Blocked Time

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 Logon	Password Changed By Admin
Admin	Reset ID / Password	
Auditor	Reset ID / Password	Reset Password
Operator	Reset Password	Reset Password
Viewer	Reset Password	Reset Password

Auth Services

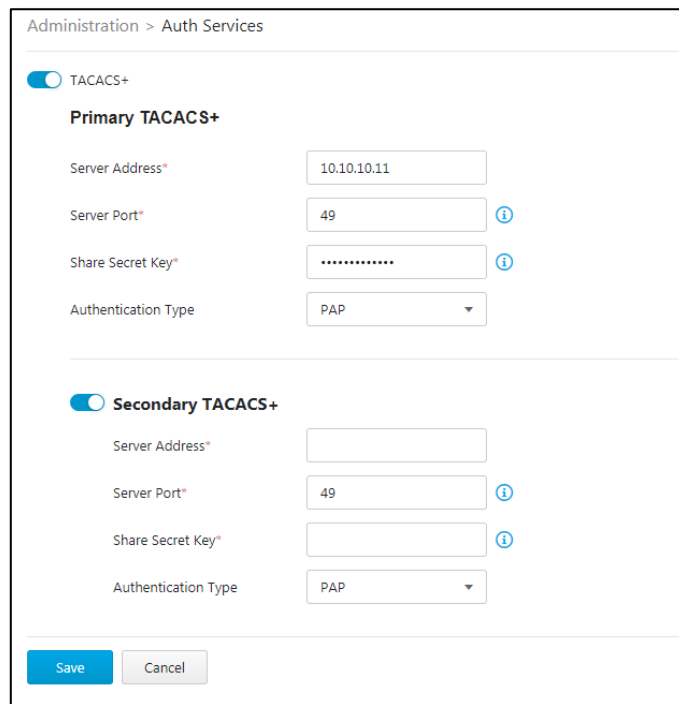
Under the [Auth Services] tab you may do the following:

- Configure the TACACS+ of the device.
- Configure SAML SSO of the device.

Configuring TACACS+

Procedure

1. Go to [Administration] > [TACACS+].
2. In the [TACACS] pane, provide the Primary and Secondary TACACS+ Servers for the device.



Administration > Auth Services

TACACS+

Primary TACACS+

Server Address*

Server Port* ⓘ

Share Secret Key* ⓘ

Authentication Type

Secondary TACACS+

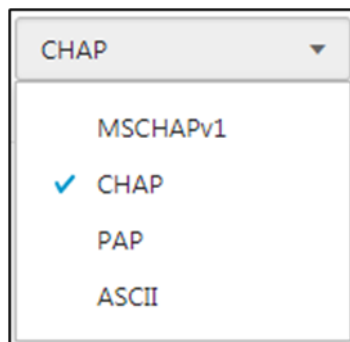
Server Address*

Server Port* ⓘ

Share Secret Key* ⓘ

Authentication Type

3. Enable Primary TACACS+ and configure the following settings.
 - Server address
 - Server port (default port: 49)
 - Share secret key (maximum 64 characters)
 - Authentication type – select one of the following options.



CHAP ▼

MSCHAPv1

✓ CHAP

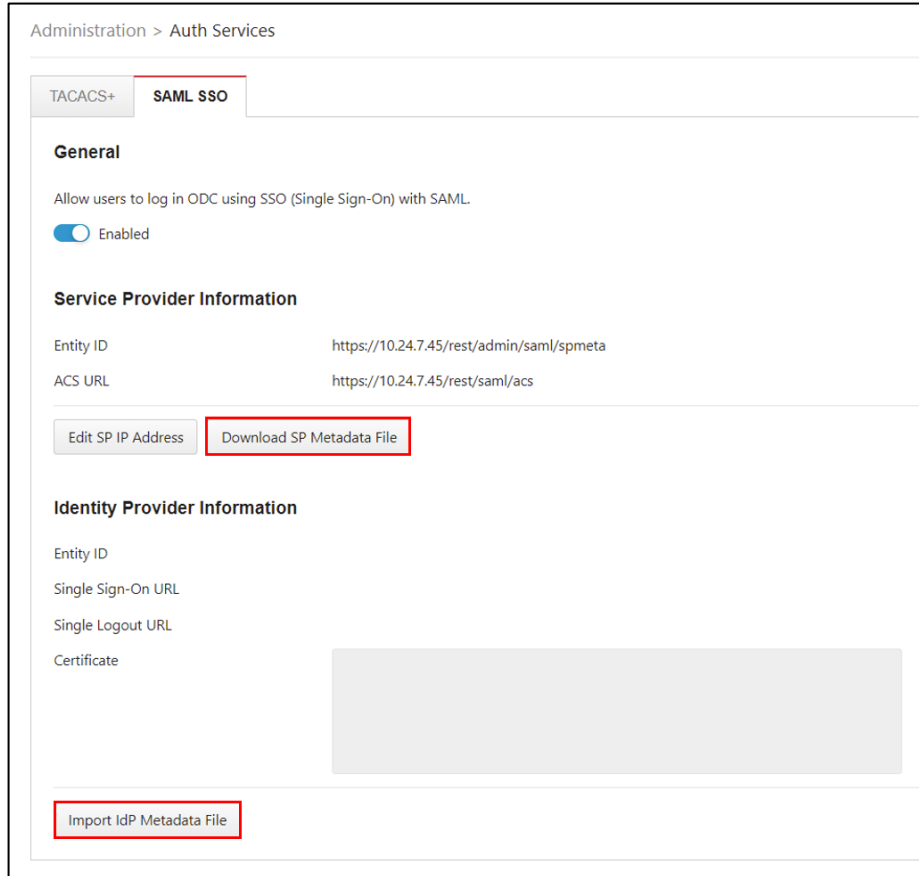
PAP

ASCII

- Enable secondary TACACS+ server if necessary.

Configuring SAML SSO

SAML SSO (Single Sign-On) allows users to log on to ODC™, the web management console service, after ODC metadata file is provided with the external identity provider. Metadata file indicates the data that provide information about the basic configuration data for authentication and authorization.



Procedure

1. Access the web user interface of the ODC management system.
2. Go to [Administration] > [Auth Services].
3. Click the [SAML SSO] tab.
4. Use the toggle to enable logging in to ODC with SAML SSO.
5. On the [Service Provider Information] pane, the following information will be automatically shown on the screen:
 - Entity ID
 - ACS URL
6. Click the [Download SP Metadata File] button to download ODC™ metadata file in XML format.



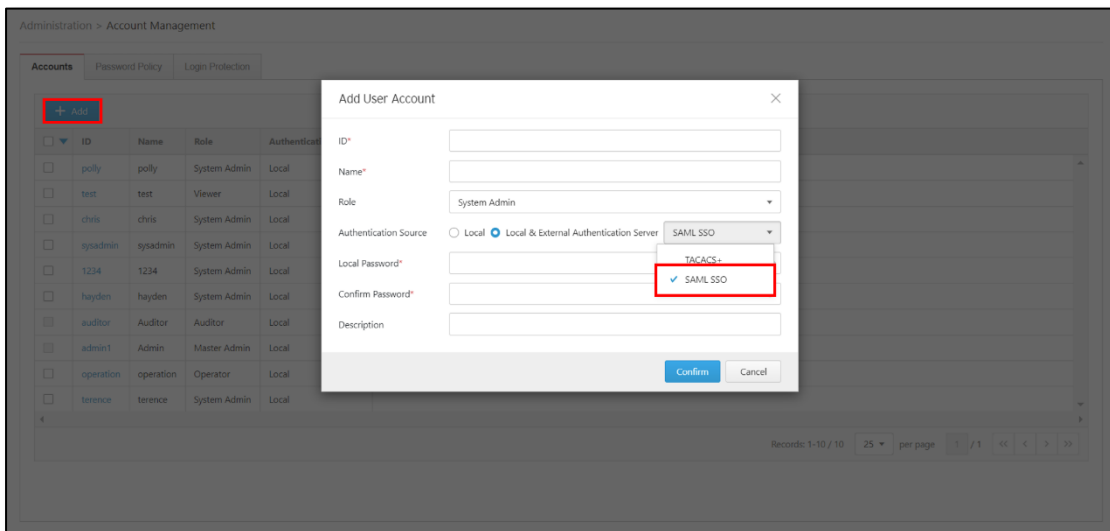
7. Go to the external Identity Provider server and import ODC™ metadata file. The integrated metadata file will be generated.

8. On 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
9. After confirming the information above, click [Import IdP Metadata File] to import the integrated authentication and authorization data to ODC™.

Adding User Account with Local and SAML SSO Authentication

Procedure

1. Access the web user interface of the ODC management system.
2. Go to [Administration] > [Account Management].
3. Under the [Accounts] tab, click [Add] to add a user account. Then the following pop-up window will appear.

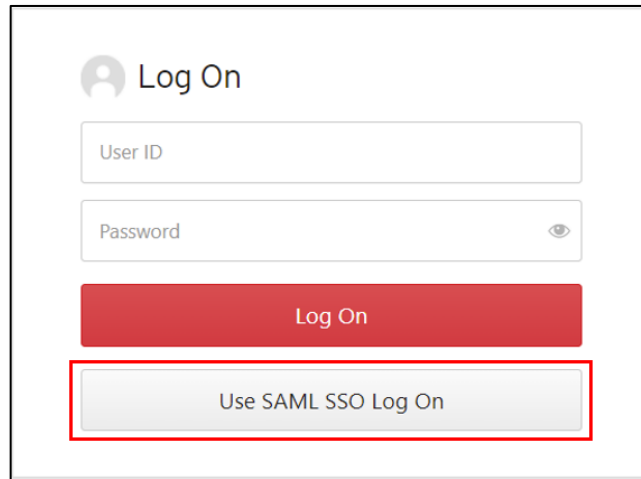


4. Configure the following user account settings.
 - ID: **Mail ID** only
 - Name: User name
 - Role: Select one role from the drop-down list, **System Admin**, **Viewer**, or **Auditor**.
 - Authentication Source: Use the radio button to select **Local & External Authentication Server**, and then select **SAML SSO** from the drop-down list.
 - Local Password: Refer to Admin (Master Admin or System Admin) configuration on **Password Policy**. Notice that the default minimum length of password is **8** characters.
 - Confirm Password: Enter the password again to ensure your input of password is correct.
 - Description

Logging on via SAML


Procedure

1. Access the web user interface of the ODC management system.
2. The following window will appear. Click [User SAML SSO Log On].



Log On

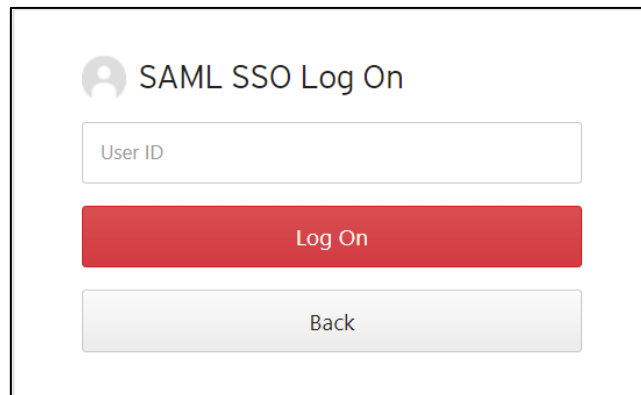
User ID

Password 

Log On

Use SAML SSO Log On

3. The following window will appear. Enter User ID in email format, then Click [Log On].



SAML SSO Log On

User ID

Log On

Back

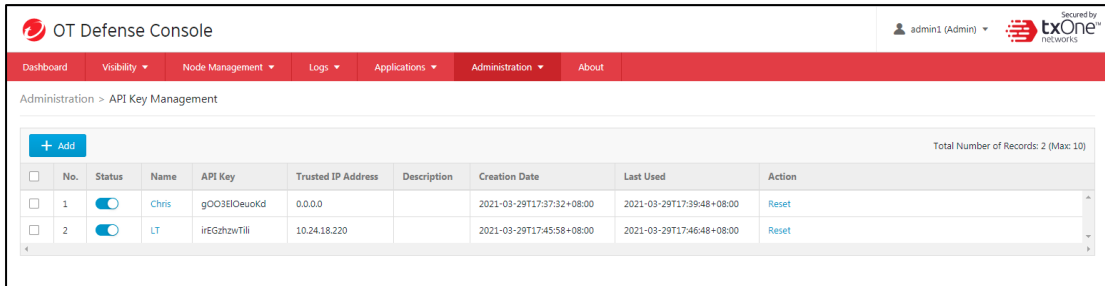
API Key Management

The API Key and API Secret are the software-level credentials for external systems to access ODC 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.

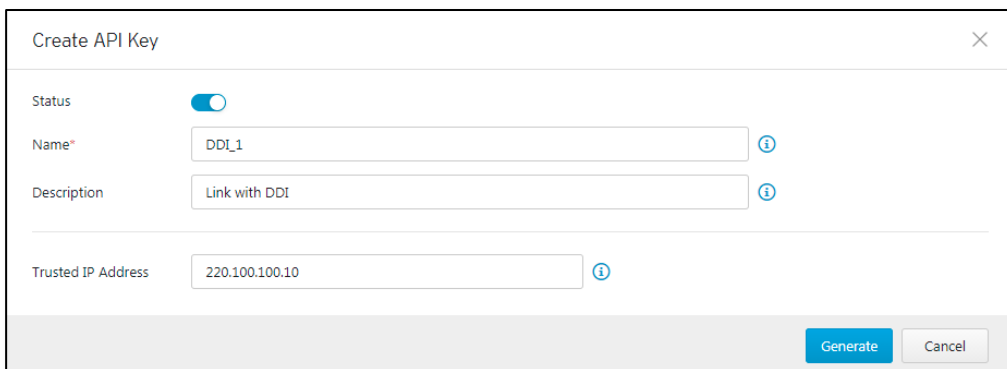
Adding API Key

Procedure

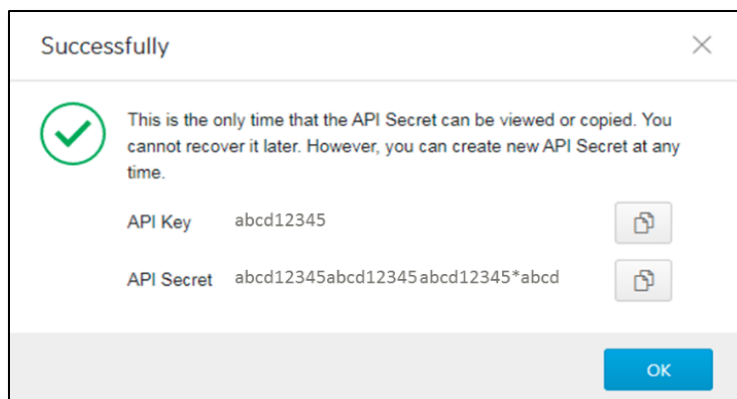
1. Go to [Administration] > [API Key Management].



2. Click the [Add] button to create a new API key.
 - Configure the name of the API client.
 - Provide an optional description of the API client.
 - Configure the "Trusted IP Address" of the API key. If it is configured, the system will reject API requests if the client's IP address does not match the given "Trusted IP Address".



3. A new API key and API secret will be generated and displayed on the screen. Click on the [Copy] button to copy the API key and API secret and paste them onto the API client.



Resetting API Key

Procedure

1. Go to [Administration] > [API Key Management].
2. Click the "Reset" action of the selected API key.
3. Click the "Confirm" button on the confirmation dialog. Please note that the old API secret will be invalidated then.
4. The system will generate a new API secret for the API key. Click the "Copy" button to copy the API key and API secret, then paste them into the API client.

Deleting API Key

Procedure

1. Go to [Administration] > [API Key Management].
2. Select the API key(s) to be deleted.
3. Click the "Delete" button.
4. Click the "Confirm" button on the confirmation dialog.

- As of ODC v1.3, a set of RESTful APIs is available for external systems to block the Node or Link type of suspicious objects (SO) on the Edge devices. The products and services supporting the SO integration are listed as follows.

Integrating Products/Services

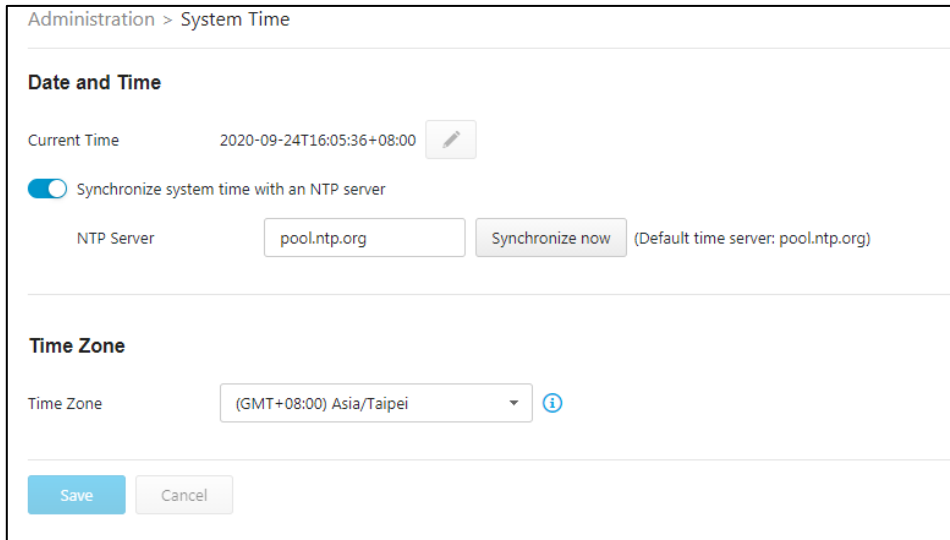
Product/Service	Version
Trend Micro Deep Discovery Inspector	V5.8

Configuring 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.

Procedure

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



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

■ The ODC system synchronizes the system time with its managed nodes.

Configuring Syslog Settings

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

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

Procedure

1. Go to [Administration] > [Syslog].
2. Click [Add] to create a syslog profile.

Administration > Syslog

Total Number of Records: 3 (Max: 32)

No.	Status	Name	Server Address	Port	Protocol	Format	Facility Level	Log Level	Log Output
1	Disabled	syslog_1	10.24.7.191	514	UDP	LEEF	local 0	INFO	CYBER_SECURITY_LOG, ASSET_LOG, SYSTEM_LOG, AUDIT_LOG, FILE_FILTER_LOG
2	Disabled	syslog_2	10.24.7.191	514	UDP	CEF	local 0	INFO	CYBER_SECURITY_LOG
3	Disabled	syslog_1(t)	10.24.7.191	514	UDP	LEEF	local 0	INFO	ASSET_LOG, SYSTEM_LOG, AUDIT_LOG, FILE_FILTER_LOG

3. A window will appear for syslog configuration.

Update Syslog Setting

Status:

Name*: 10.24.3.97

Description:

Server Address*: 10.24.7.18

Port*: 514

Protocol: TCP UDP

Format: CEF LEEF

Facility Level: local 0

Log Level: INFO

Log Output*: Available logs (5): Protocol Filter Log, File Filter Log, Assets Detection Log, System Log, Audit Log. Selected logs (3): Cyber Security Log, Policy Enforcement Log, Suspicious Object Log.

OK Cancel

4. Select [Send logs to a syslog server] to set the ODC system to send logs to a syslog server. Configure the following settings:

Field	Description
Server address	Type the IP address of the syslog server.
Port	Type the port number.
Format	Type of CEF and LEEF
Protocol	Select the protocol for the communication.

Field	Description
Facility level	Select a facility level to determine the source and priority of the logs.
Severity level	Select a syslog severity level. ODC system only sends logs with the selected severity level or higher to the syslog servers. For more information, see Syslog Severity Level Mapping Table on page 144 .

5. Select the types of logs to send.
6. Click [Save].

Syslog Severity Levels

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

Level	Severity	Description
0	Emergency	<ul style="list-style-type: none"> ▪ Complete system failure Take immediate action.
1	Alert	<ul style="list-style-type: none"> ▪ Primary system failure Take immediate action.
2	Critical	<ul style="list-style-type: none"> ▪ Urgent failures Take immediate action.
3	Error	<ul style="list-style-type: none"> ▪ Non-urgent failures Resolve issues quickly.
4	Warning	<ul style="list-style-type: none"> ▪ Error pending Take action to avoid errors.
5	Notice	<ul style="list-style-type: none"> ▪ Unusual events Immediate action is not required.
6	Informational	<ul style="list-style-type: none"> ▪ Normal operational messages useful for reporting, measuring throughput, and other purposes No action is required.
7	Debug	<ul style="list-style-type: none"> ▪ Useful information when debugging the application. ▪ Setting the debug level can generate a large amount of syslog traffic in a busy network. Use with caution.

Syslog Severity Level Mapping Table

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

Policy Enforcement / Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
		0 - Emergency
	Critical	1 - Alert
	High	2 - Critical

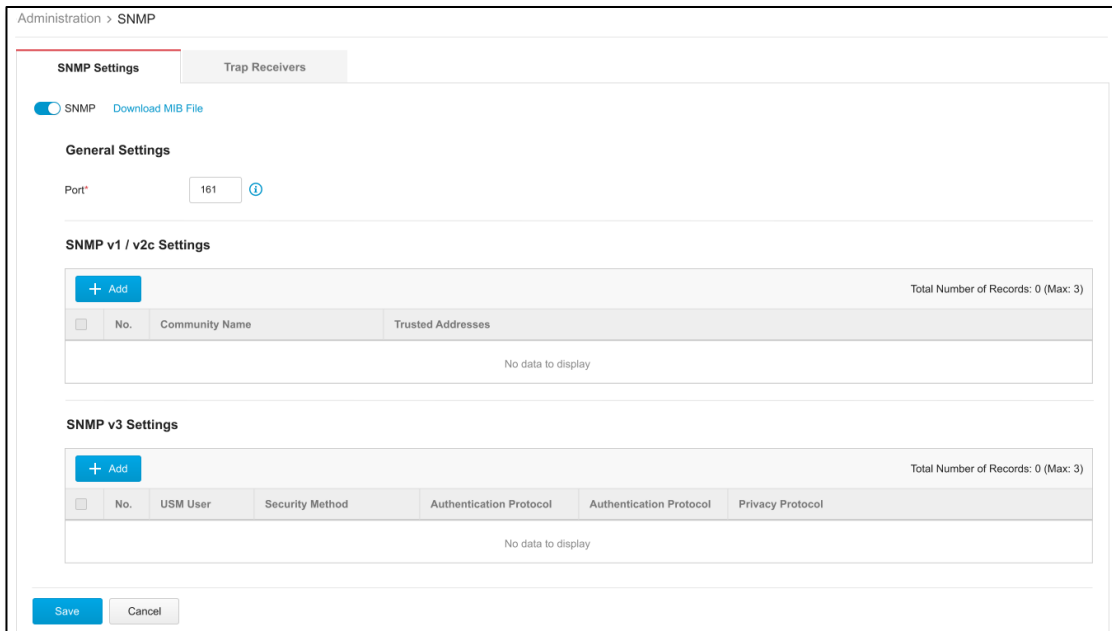
Policy Enforcement / Protocol Filter Action	Cyber Security Severity Level	Syslog Severity Level
		3 - Error
Deny	Medium	4 - Warning
	Low	5 - Notice
Allow	Information	6 - Information
		7 - Debug

The SNMP

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

Procedure

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

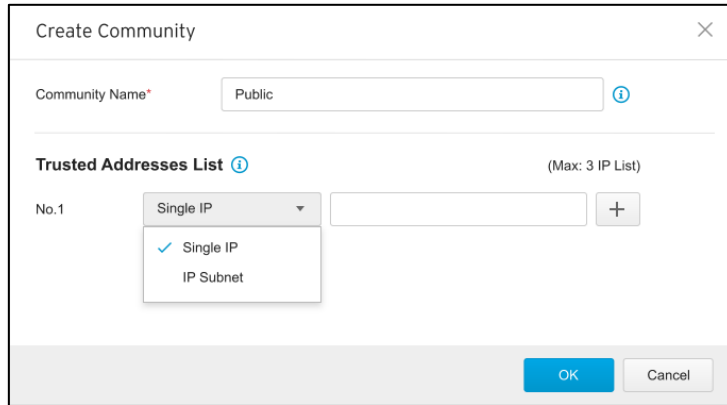


The screenshot shows the 'Administration > SNMP' configuration page. It features two tabs: 'SNMP Settings' (active) and 'Trap Receivers'. In the 'SNMP Settings' tab, there is a toggle switch for 'SNMP' which is currently turned on, and a 'Download MIB File' link. Below this is the 'General Settings' section with a 'Port*' field set to '161'. The 'SNMP v1 / v2c Settings' section contains an 'Add' button and a table with columns for 'No.', 'Community Name', and 'Trusted Addresses', currently showing 'No data to display'. The 'SNMP v3 Settings' section also has an 'Add' button and a table with columns for 'No.', 'USM User', 'Security Method', 'Authentication Protocol', and 'Privacy Protocol', also showing 'No data to display'. At the bottom, there are 'Save' and 'Cancel' buttons.

Configuring SNMP v1/v2c

Procedure

1. Go to [Administration] > [SNMP]
2. Click [Add] to create SNMP v1/v2 settings.

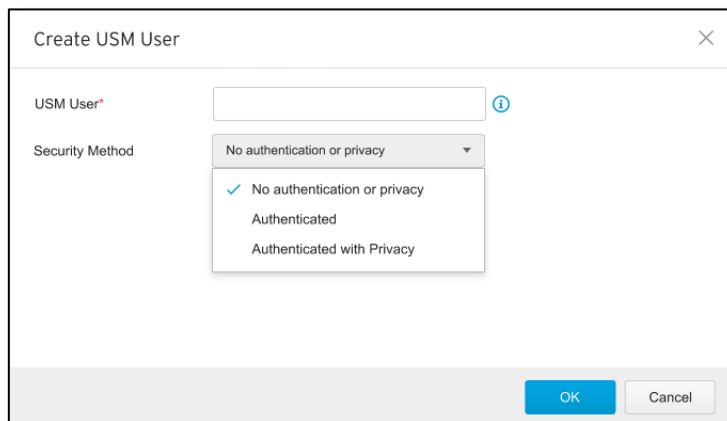


- a. Enter a Community name.
- b. Add a Trusted Address list from the two supported types, Single IP and IP Subnet.
- c. Click [OK] to create a new SNMP v1/v2c community.

Configuring SNMP v3

Procedure

1. Go to [Administration] > [SNMP]
2. Click [Add] to create SNMP v3 settings.



3. Fill in the USM user field.
4. Select [Security Method] – options include:
 - a. No authentication or privacy
 - b. Authenticated – including SHA and MD5, and you can select an appropriate authentication protocol and enter an Authentication Key
 - c. Authenticated with Privacy – including SHA and MD5, and you can select an appropriate authentication and a privacy protocol.
5. Click [OK] to create the new SNMPv3 USM User.

Configuring SNMP Trap Settings

Procedure

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

Administration > SNMP

SNMP Settings **Trap Receivers**

[+ Add](#) Total Number of Records: 2 (Max: 5)

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

[Save](#) [Cancel](#)

3. Click [Add] to create a new Trap Receiver.
 - Click [Status] to enable Trap Receiver.
 - Enter the desired Trap Receiver name under [Name].
 - Add a [Description] if necessary.
 - Select SNMP version – options include SNMP v1 and SNMP v2c
 - Enter [Server Address]
 - Enter [Server port] – default setting: port 162.
 - Select a message type – options include “Trap” and “Inform Request”.
 - Enter a Trap Community, default name: PUBLIC.
 - Trap Retry Time can be set to range from 1 to 10 times

✕

Create Trap Receiver

Status

Name* ⓘ

Description ⓘ

Version SNMP v1 SNMP v2c

Server Address*

Server Port* ⓘ

Message Type Trap InformRequest

Trap Community*

Trap Retry Times ▼

- Select Event Notification – possible notification triggers are as follows:

Event Notification*

- System Boot
- System Ready
- High CPU Usage i
- High Memory Usage
- Insufficient Storage Available
- Node Registered
- Node Deregistered
- Node Connected
- Node Disconnected

- When the CPU usage reached 70%, 80% or 95%, the system will send an event notification.
- When the memory usage reached 80%, the system will send an event notification.
- When the log storage reached 95%, the system will keep sending event notifications until the log storage is below 95%
- Please refer to Appendix D for the supported MIB objects.

Updates

Download and deploy components for EdgeIPS, EdgeFire and EdgeIPS Pro. Trend Micro frequently creates new component versions and performs regular updates to address the latest network threats.

Update components to immediately download the latest component updates from the Trend Micro ActiveUpdate server. The components will be deployed to security nodes based on the settings of the [Node Management] tab. For more information, see [Node Management on page 30](#).

- Updates for Device

Administration > Updates

Device System

Name	Latest Version	Release Date	Scheduled Update	Actions
Trend Micro EdgeIPS Pro DPI Pattern	TM_IPSP_200908_08	2020-09-08T09:58:06+08:00	Disabled	Update Now Import
Trend Micro DPI Pattern	TM_200922_12	2020-09-21T14:01:13+08:00	Disabled	Update Now Import
EdgeFire 1000 Series Firmware	IEF_T01_1.1.1	2020-09-10T20:17:42+08:00	Disabled	Update Now Import
EdgeIPS 100 Series Firmware	IPS_G02_1.1.7	2020-08-24T17:33:57+08:00	Disabled	Update Now Import
EdgeIPS Pro Series Firmware	IPSP_T01_1.0.19	2020-09-14T17:38:03+08:00	Disabled	Update Now Import

- Updates for the ODC System

Administration > Updates

Device **System**

Pattern

Version: SDP_200831_09

Release Date: 2020-08-31T10:03:45+08:00

Description: SDP_200831_09 testing sig

Firmware

Version: 1.1.7

Release Date: 2020-09-17T18:41:23+08:00

Description: 1.1.7

Device Update - Components

The following table describes the available components on the Updates tab.

Field	Description
Trend Micro DPI Pattern	Contains signatures to enable: <ul style="list-style-type: none"> ▪ Intrusion prevention Detects and prevents behaviors related to network intrusion attempts and targeted attacks at the network level.
Trend Micro EdgeIPS Pro DPI Pattern	For the EdgeIPS Pro series, these patterns contain signatures to enable: <ul style="list-style-type: none"> ▪ Intrusion prevention Detects and prevents behaviors related to network intrusion attempts and targeted attacks at the network level.
EdgeFire 1000 Series Firmware	EdgeFire™ firmware
EdgeIPS 100 Series Firmware	EdgeIPS™ firmware
EdgeIPS Pro Series Firmware	EdgeIPS™ Pro firmware

- The ODC system maintains various versions of components in its repository, which allows you to configure which version (a fixed version or the latest) to deploy to the managed nodes.

You can update the components using one of the following methods:

- Manual updates: You can manually update components in the ODC system.
 - Manual import of components: You can manually import components to the ODC system.
 - Scheduled updates: The ODC system automatically downloads the latest components from an update source based on a schedule.
-
- The updated components are deployed to managed nodes based on the settings of the [Node Management] tab.
 - Internet access is needed for ODC to perform manual updates and/or scheduled updates. Specifically, the ODC system will need to visit odc.cs.txone-networks.com and txone-component-prod.s3.amazonaws.com via HTTPS in order to check the update information and/or to download components.

Updating the Components Manually

You can manually update the components in the ODC system. When a component update is complete, ODC system deploys the updated components to managed nodes based on the settings under the [Node Management] tab.

Procedure

1. Go to [Administration] > [Updates].
2. For a component with a new version, click [Update Now] in the [Actions] column.
When the component update is complete, the value in the [Latest Version] and [Release Date] columns will be updated or, if it is already up-to-date, kept the same.

Importing a Component File

If you have a component file, you can manually import the file to the ODC system. The ODC system deploys the updated components to managed nodes based on the settings under the [Node Management] tab.

Procedure

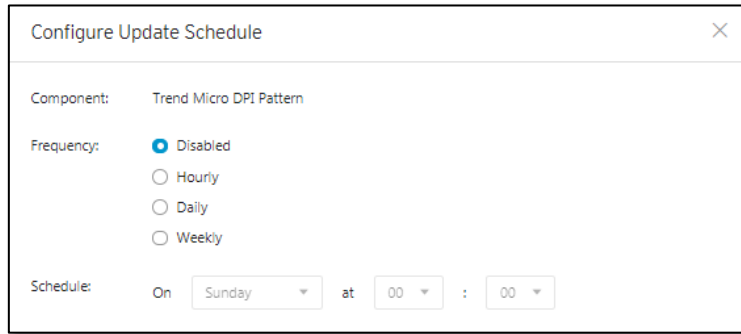
1. Go to [Administration] > [Updates].
2. Click [Import] for the component.
3. Select the component file.
4. Click [Open] to start the import process.

Scheduling Component Updates

Configure scheduled updates to receive protection against the latest threats from an updated firmware of the managed nodes. The ODC system deploys the updated components to managed nodes based on the settings under the [Node Management] tab.

Procedure

1. Go to [Administration] > [Updates].
2. Click the edit button under the [Schedule Update] field.



Configure Update Schedule

Component: Trend Micro DPI Pattern

Frequency: Disabled
 Hourly
 Daily
 Weekly

Schedule: On Sunday at 00 : 00

3. Specify the update interval.
4. Click [Save].

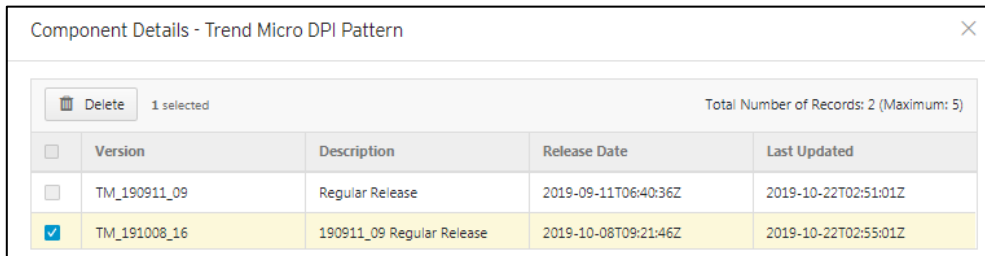
■ The ODC system features hourly, daily, and weekly scheduled updates.

Managing the Component Repository

All the imported or updated components are maintained in the component repository. You can view and manage the available components in the repository.

Procedure

1. Go to [Administration] > [Updates].
2. Click the update component.
 A [Component Details] window appears, which allows you to view the available components in the repository.



Component Details - Trend Micro DPI Pattern

Delete 1 selected Total Number of Records: 2 (Maximum: 5)

	Version	Description	Release Date	Last Updated
<input type="checkbox"/>	TM_190911_09	Regular Release	2019-09-11T06:40:36Z	2019-10-22T02:51:01Z
<input checked="" type="checkbox"/>	TM_191008_16	190911_09 Regular Release	2019-10-08T09:21:46Z	2019-10-22T02:55:01Z

3. (Optional) If you want to delete a component, select the component and click [Delete].
4. Click [OK].

ODC System Update - Components

The following table describes the available components on the Updates tab.

Field	Description
Pattern	Contains signatures to enable the following features: <ul style="list-style-type: none"> ▪ Self-protection ▪ Detects and prevents behaviors related to network intrusion attempts and targeted attacks to ODC's system
Firmware	ODC system component update

You can update the pattern and ODC system components using one of the following methods:

- Manually import: You can manually update components by importing an ODC system component or a pattern file.
- Manually check online for updates: Click the “Check for Updates” button to download current pattern and component updates to ODC.

Importing an SSL Certificate

The ODC system uses the HTTPS protocol to encrypt web traffic between the user’s web browser and the ODC web server. By default, the ODC web server uses an auto-generated, self-signed SSL certificate for the HTTPS connections. This chapter introduces how to change the SSL certificate.

Replacing an SSL certificate

1. Go to [Administration] > [SSL Certificate].
2. Click [Replace Certificate].
 - a. Next to the [Certificate] field, click to import your certificate file.
 - b. Next to the [Private Key] field, click to import the private key (PEM-encoded PKCS#1 format) for the certificate file.
 - c. Input the passphrase of the private key if the private key is encrypted.
 - d. Click [Import] and then [Restart].

Verifying an SSL certificate

After adding a new certificate to the ODC system, you can verify whether the certificate is effective.

1. Log in to the ODC system with the Chrome browser.
2. Go to Three Dots Menu > More Tools > Developer Tools.
3. Click on the [Security] Tab.
4. It will give you a Security Overview.
5. Under [Security Overview], click the [View certificate] button, and you will see the certificate details of the ODC system.

Removing the imported SSL certificate

You can optionally choose to remove the imported certificate:

1. Go to [Administration] > [SSL Certificate].
2. Click [Remove Certificate].
3. A [Remove Certificate] window will appear.
4. Click [Remove and Restart].

The default self-signed certificate will be used after the imported certificate is removed.

Log Purge

Use the [Log Purge] function for the following operations:

- Viewing the status of the logs stored in the ODC system
- Setting up purge criteria for automatic log purge
- Manually purging the logs that match a given condition

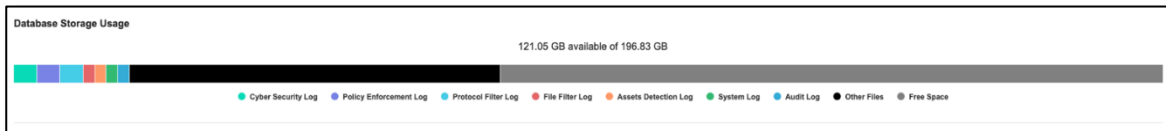
The ODC system maintains logs and reports in its appliance hard disk. You can purge the logs in the following ways:

- Automatic purge: The log can be automatically deleted based on a specified threshold number of log entries, a retention period for log data, or both.
- Manual log purge: The logs can be manually deleted based on a specified condition.

Viewing Database Storage Usage

Go to [Administration] > [Log Purge].

The [Database Storage Usage] pane shows the used and total size of database.



Configuring Automatic Log Purge

1. Go to [Administration] > [Log Purge].
2. Under the [Automatic Purge] pane, specify the automatic log purge criteria.
(The number shown under [keep at most xxxxx entries] is calculated based on the disk storage allocated to the ODC.)

Automatic Purge			
Purge Cyber Security Log	older than	no limit	and keep at most 10,000,000 entries
Purge Policy Enforcement Log	older than	no limit	and keep at most 10,000,000 entries
Purge Protocol Filter Log	older than	no limit	and keep at most 10,000,000 entries
Purge File Filter Log	older than	no limit	and keep at most 10,000,000 entries
Purge Assets Detection Log	older than	no limit	and keep at most 10,000,000 entries
Purge System Log	older than	no limit	and keep at most 10,000,000 entries
Purge Audit Log	older than	no limit	and keep at most 10,000,000 entries

3. Click [Save].

Manually Purging Logs

1. Go to [Administration] > [Log Purge].
2. Under the [Purge Now] pane, specify the criteria and click the [Purge Now] button.
The logs that meet the criteria will be purged immediately.

Purge Now			
Purge	--Select--	older than	no limit
			and keep at most 0 entries
			Purge Now

- The ODC system starts to clear the logs, beginning with the oldest, when the number of a log type reaches the maximum value.

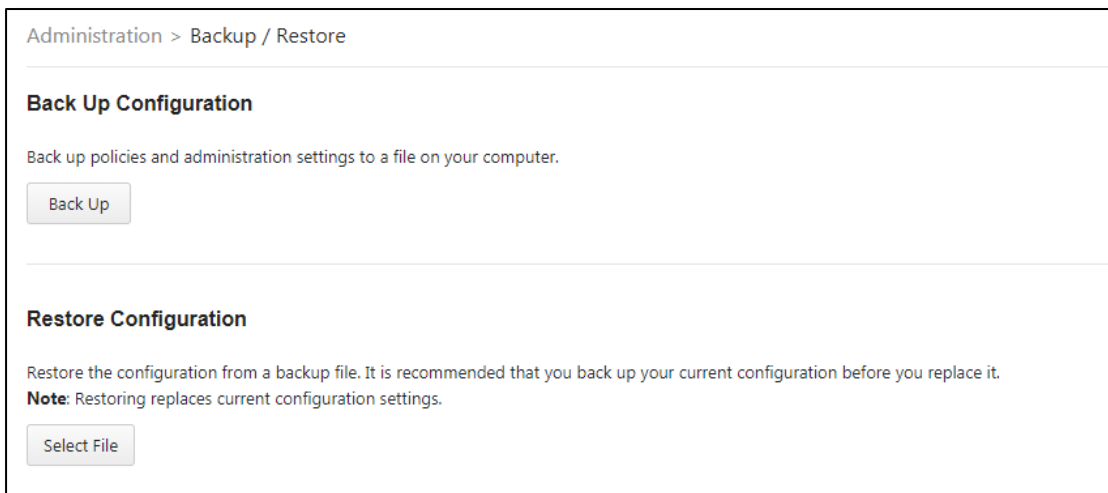
Back-Up / Restore

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

We recommend the following:

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

The following picture shows an example of license information.



Backing Up a Configuration

You can back up the following settings to a configuration file:

- Administration > Account Management
- Administration > Auth Service
- Administration > System Time
- Administration > Syslog
- Administration > SNMP
- Administration > Log Purge
- Administration > Updates (only schedule settings)
- Administration > Proxy
- Node Management > EdgeIPS
- Node Management > EdgeFire
- Node Management > EdgeIPS Pro

Procedure

1. Go to [Administration] > [Back Up / Restore].
2. Next to [Configuration Settings Backup], click [Export]. A [File Download] window will appear.
3. Click [Save] to save the configuration file to local storage.

Restoring a Configuration

Follow the steps to restore the configuration of ODC.

Procedure

1. Go to [Administration] > [Back Up / Restore].
2. Next to [Restore Configuration Settings], click [Choose File] or [Browse] and then locate the file.
3. Click [Restore].
4. All services will restart. It may take some time to restart services after applying imported settings and rules.

License

The [License] tab displays license information and accepts a valid license key to enable specific functions in ODC.

- Log on to the management console using the administrator account to access the License tab.

Introduction to the Licenses

Three license types are used for ODC:

- Node License
- EdgeFire Software License
- EdgeIPS Software License
- EdgeIPS Pro Software License

Node License - Determines the maximum number of nodes to be managed by ODC.

The following is an example of node license details for EdgeIPS™ Pro series.

Model Name	Node Count per Unit	Number of Module / Device	Total Node Count
EdgeIPS Pro-1048	12 nodes per module	2	24 nodes
EdgeIPS Pro-2096	12 nodes per module	4	48 nodes
EdgeIPS Pro-216	8 nodes per device	1	8 nodes
EdgeIPS Pro-2008	4 nodes per device	2	8 nodes

EdgeFire/EdgeIPS and EdgeIPS Pro Software License - The number of seats allowed in the license should be equal to or greater than the nodes managed by the ODC so that users can update pattern/firmware for the nodes via the ODC.

For EdgeFire/EdgeIPS Software License - The number of seats allowed in the license should be equal to or greater than the number of EdgeFire/EdgeIPS devices managed by the ODC.

For EdgeIPS Pro Software License - The number of seats allowed in the license should be equal to or greater than the total number of slots (module sets) of the EdgeIPS Pro devices managed by the ODC. If there are two EdgeIPS Pro devices managed by the ODC, and one has 1 slot and another has 2 slots, then the EdgeIPS Pro Software License needs to have at least 3 seats for the EdgeIPS Pro devices to be eligible for update services.

In ODC, only one **node license** is used at a time. Thus, when more than one **node license** is applied to the ODC, only the latest one will be kept in the ODC.

Multiple **EdgeFire/EdgeIPS and EdgeIPS Pro software licenses** can co-exist in an ODC. Thus, when multiple software licenses are applied to the ODC, all the licenses will be kept in the ODC.

The following picture shows an example of license information.

License Type	License Key	Seat	End Date	Remark
ODC Node License	H4DE-HEJ7-AZB2-FIF6	500	2020-11-15	
EdgeFire Software License	H6GP-GVR7-RTZF-KGMW	20	2020-12-17	
EdgeIPS Software License	GZAD-EDZW-IAZ6-KADA	50	2021-01-20	

Viewing Your Product License Information

Procedure

1. Go to [Administration] > [License]. The [License] tab will appear.
2. The following table describes the license information.

Field	Description
License Type	The type of the license key
License Key	The license key currently used
Seat	The number of nodes that can be managed by this ODC
End Date	The expiration date of the license key
Remark	Additional information for this license key

The following table describes further information for the [Remark] field.

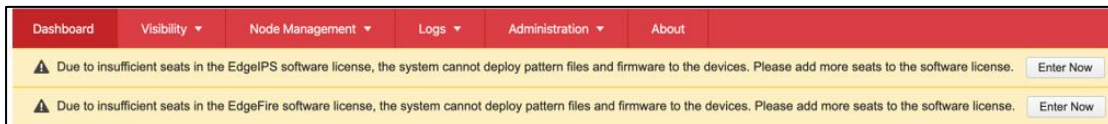
Message	Icon	Description
Expired license		The license has expired. It also has passed its grace period.
Void license		The license is invalid.
Will expire in X days		The license will expire in X days.
Not enough seats to support the EdgeFire Software License/EdgeIPS Software License license(s)		The message is self-explanatory. The number of node seats equals to the number of EdgeFire nodes plus the number of EdgeIPS nodes.

Alert Messages

When a license is going to expire or has expired, alert messages will pop-up when a user logs on to the web management console. If the logged in user is the `admin`, then the license key will be displayed on the screen. The license key will not be displayed if other users log in.

Message	Description
The license (xxx-xxx-xxx-xxx) expires in xx days. To continue using all features, please enter a new license key.	This message will pop up 30 days before the license expiration date.
The license (xxx-xxx-xxx-xxx) has expired. You will stop receiving product updates and technical support in xx days. To continue using all features, please enter a new license key.	The license has expired, but it is still in its grace period.
The license (xxx-xxx-xxx-xxx) has expired. To restore all features, please enter a new license key.	The license has expired, and also has passed its grace period.

When the EdgeIPS/EdgeFire software license seat number is not enough for current managed nodes, users will not be able to update the patterns and firmware for the nodes. Alert messages will also pop up on the web management console.



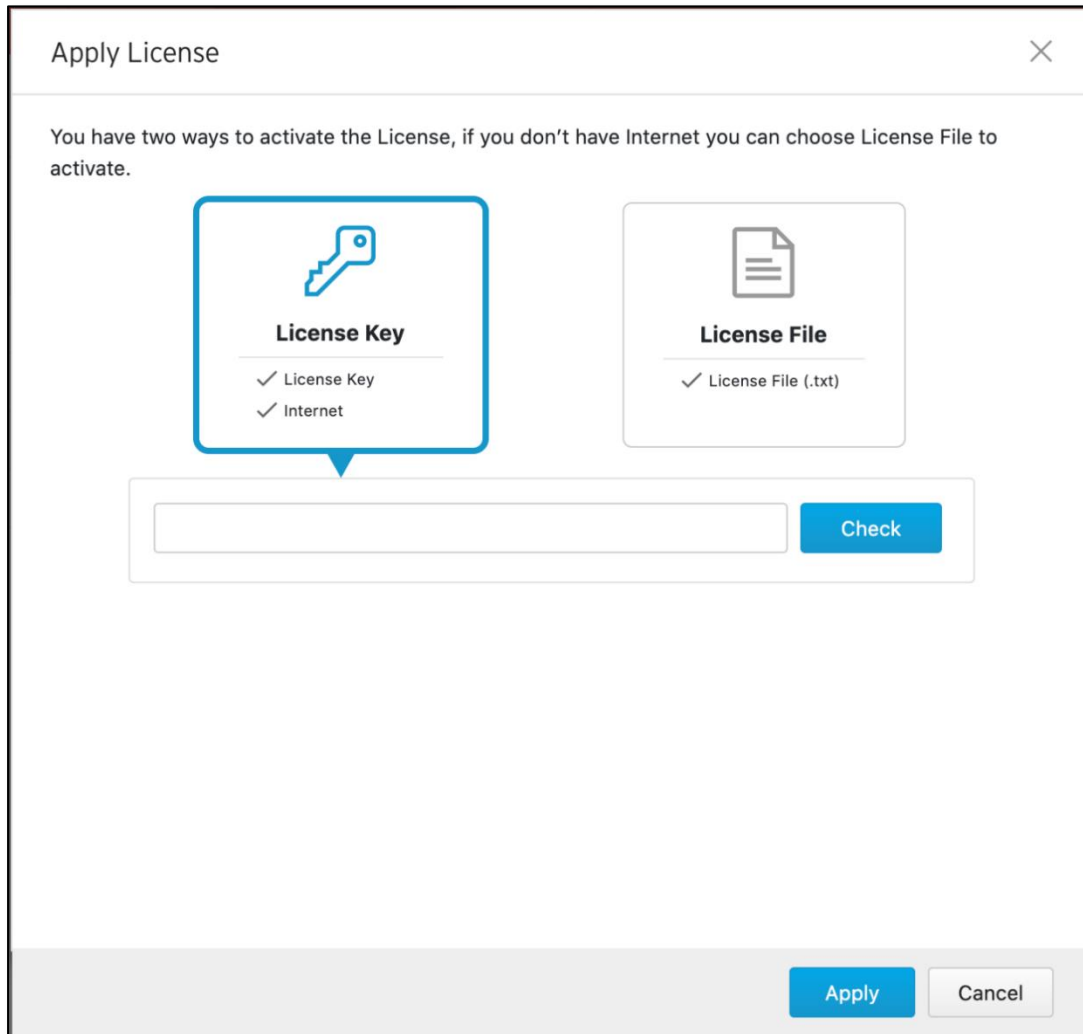
Activating or Renewing Your Product License

There are two ways to activate licenses: Apply License Key and Apply License File.

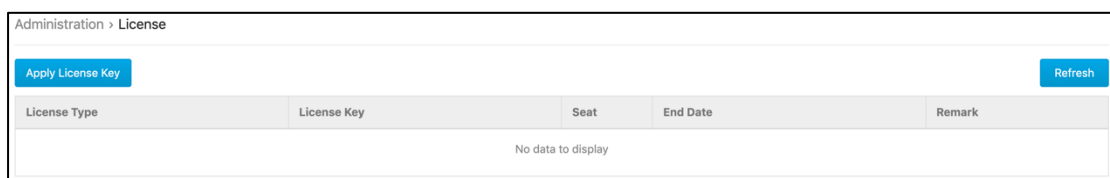
Procedure

By License Key

Apply License Key – The user can choose to apply license key if ODC has an active internet connection. The user needs to click the “Apply License Key” option from UI and then enter the license key.



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



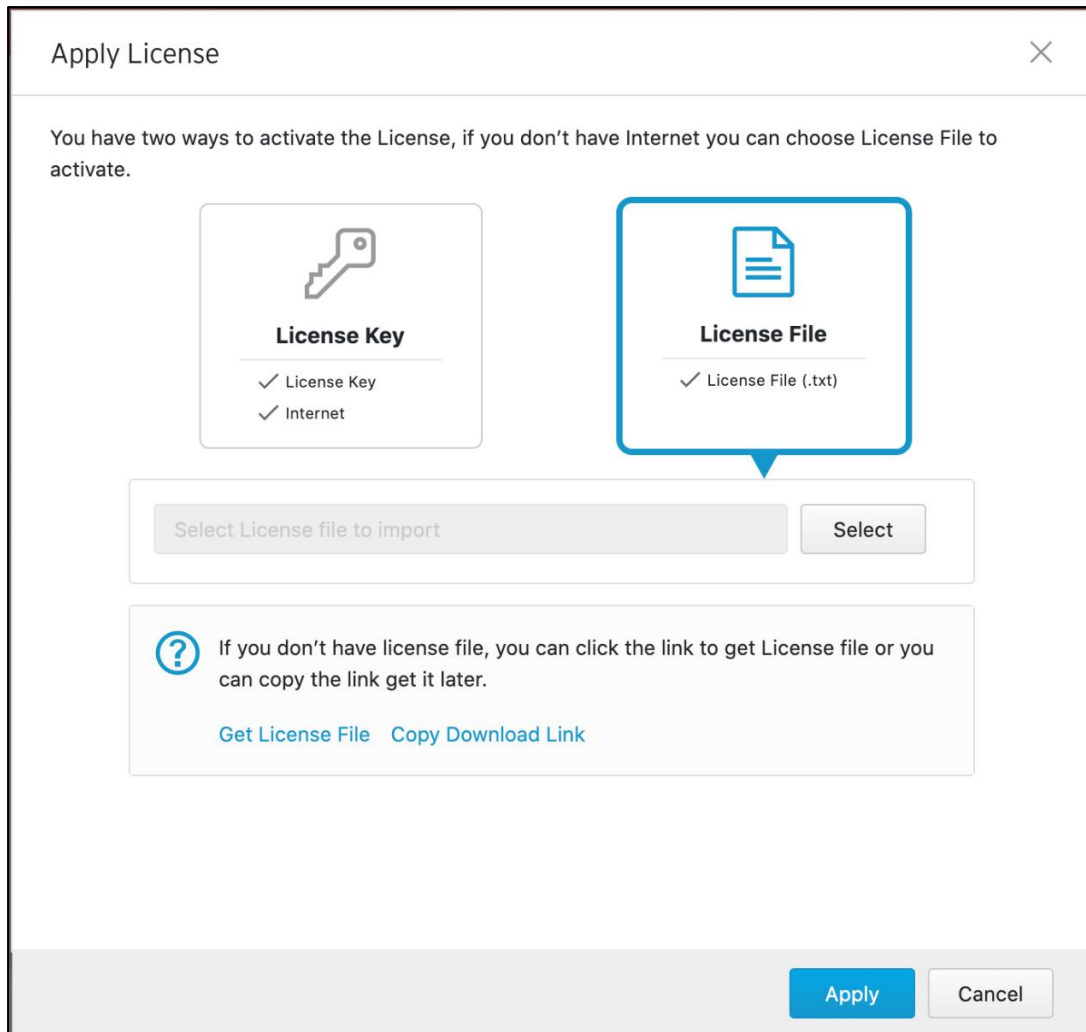
License Type	License Key	Seat	End Date	Remark
No data to display				

2. Click the [Apply License Key] button. The [Apply License Key] screen will display.
3. Enter a new license key.
4. Click [Check].
5. Verify the license information shown and click [OK].

- Internet access is needed for ODC when applying the license key this way. Specifically, the ODC system will need to visit odc.cs.txone-networks.com via HTTPS in order to register the license key and retrieve license information.

By License File

Apply License File – The user needs to apply a license file if ODC doesn't have an active internet connection. When the user clicks the "License File" option in the UI, two labels will be displayed, "Get License File" and "Copy Download Link".



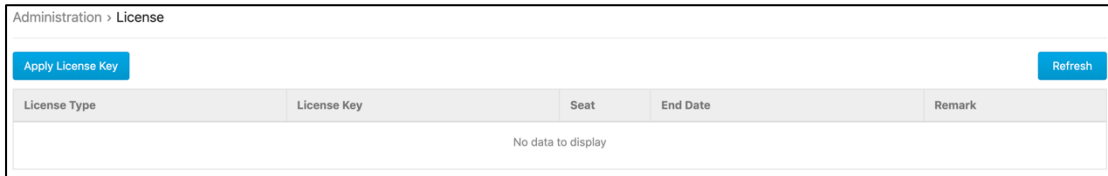
- If the user can connect to the Internet from the client, then they can click "Get License File" to connect to the Trend Micro backend server from a new browser window. He/she can enter the license key to download the license file. Once the license file is downloaded, the user can go back to "License File" on ODC UI, and then upload the license file.
- If the user cannot connect to the Internet from the client, he/she can choose to copy the download link, and open the link from the browser on a computer with an internet connection.
- The ODC serial number is provided in the download link. The license file generated by the download link is only valid when it is applied to the same ODC client from which the link was generated.

Manually Refreshing the License

If the privilege of your license is changed by Trend Micro at its backend license management server, e.g., the expiration date is extended or the seat number is increased, you can manually update your license at your web management console.

Procedure

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



2. Click the [Refresh] button.

- Internet access is needed for ODC when manually refreshing the license. Specifically, the ODC system will need to visit odc.cs.txone-networks.com via HTTPS in order to retrieve the license information.

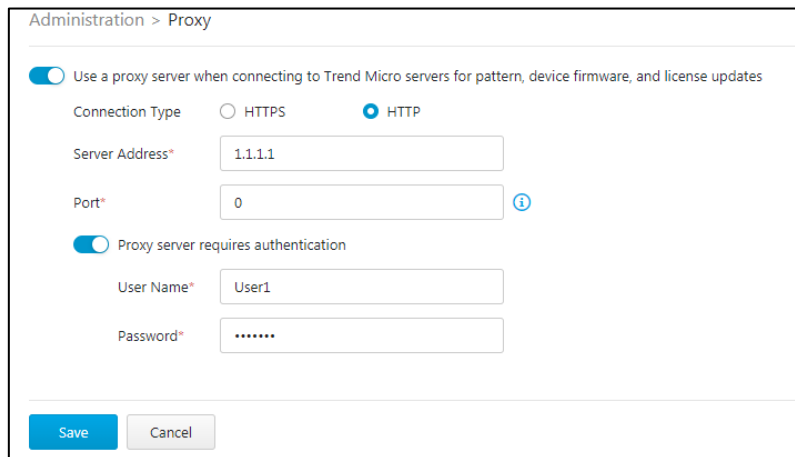
Proxy

If necessary, configure ODC to use a proxy server for component and license update.

Configuring Proxy Settings

Procedure

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



2. Click the button next to [Use a proxy server when connecting to the Trend Micro servers for pattern, device firmware, and license updates].
3. Specify the following details:
 - Server IP address of the proxy server
 - Port of the proxy server
4. If the server requires authentication, select [Proxy server requires authentication], and enter the required credentials.
5. Click Save.

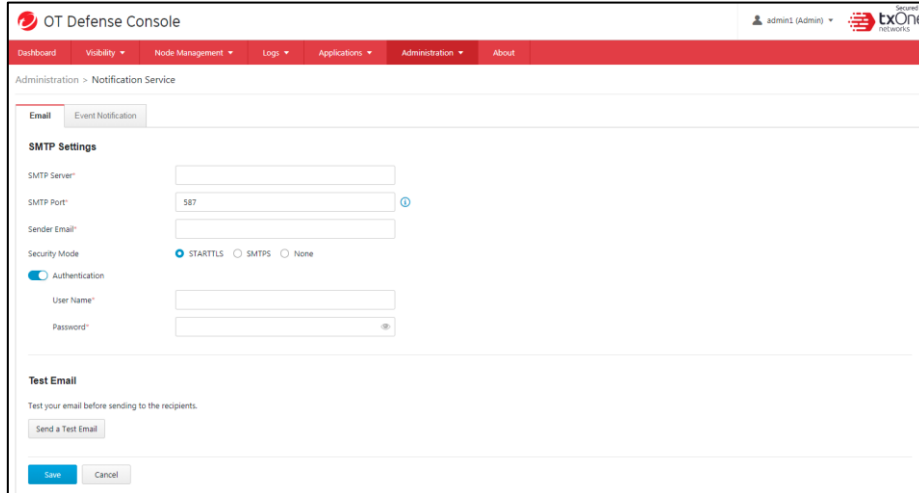
Notification Service

OT Defense Console can send email notifications for threshold-based network events.

Configuring Email

Procedure

1. Go to [Administration] > [Notification Service] > [Email].

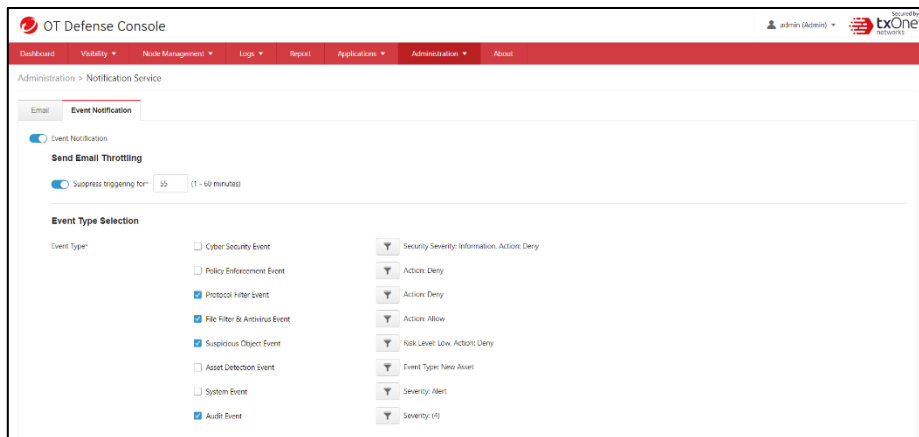



2. Configure the SMTP server IP address and SMTP port. (Default SMTP port is 587)
3. Configure the Sender Email. This email address will appear in the "From" field of the email notification.
4. Configure the Security Mode to secure SMTP. Available options are STARTTLS, SMTPS and None.
5. Configure the Authentication settings if it is needed.
6. Click the "Send a Test Email" button to test the given SMTP settings. The system will show a dialog for you to enter the recipient(s) of the test email.

Configuring Event Notification


Procedure


1. Go to [Administration] > [Notification Service]>[Event Notification]



2. Toggle "Event Notification" to switch this feature on or off.
3. You may enable the "Email Send Throttling" option and specify the time length, from 1 to 60 minutes, for the system to suppress email notification.
4. Select the event types to be included in the email notification and click  after each event to specify further configurations.
 - a. Cyber Security Event
 - b. Policy Enforcement Event
 - c. Protocol Filter Event
 - d. File Filter Event
 - e. Suspicious Object Event
 - f. Asset Detection Event
 - g. System Event
 - h. Audit Event
5. Configure the Email Template.

Email Template


To* 

Subject* 
32 Characters (Max: 75)

Message*

Hi System Owner,

 We detected new events and listed the summary below.
 {{HOST_INFO}}
 {{EVENT_COUNT}}


161 Characters (Max: 1024)

- a. Specify the email recipient(s) in the "To" field. Each recipient email address must be valid.
- b. Specify the subject of the email. The system variables `{{HOSTNAME}}` and `{{IP}}` can be used in the subject. The system will insert ODC's host name and IP address in place of `{{HOSTNAME}}` and `{{IP}}` when they are used in the subject field.
- c. Define the email body in the "Message" field. The system variables `{{HOST_INFO}}`, `{{EVENT_COUNT}}`, `{{EVENT_DURATION}}`, `{{EVENT_SUMMARY}}`, and `{{EVENT_DETAIL}}` can be used in the email body.

You may find the usage of these system variables and an example by clicking the light bulb icon (Message Reference) to the right of the "Message" field.

Example ×

Hi System Owner,

We detected new events and listed the summary below.

Web Console: <https://192.168.1.100>

Event Count: 2

Event Duration: 2021-01-22T10:00:01+08:00 to 2021-01-22T11:00:01+08:00

Event Summary:

Event Type	Numbers of Events
System Event	1
Policy Enforcement Event	1

Event Details: (Only display the latest 2 events)

System Event

Time	Device Name	Serial Number	Severity	Message
2021-01-22T10:00:02+08:00	System	ffffff-1a8d-11ea-baa4-123456789	Information	NTP server (10.10.1.1) synchronized

Policy Enforcement Event

Time	Device Name	Serial Number	Rule Name	Interface	Source IP Address	Destination IP Address	Action
2021-01-22T10:00:02+08:00	System	TMG01	Rule1	PORT2	10.0.9.47	10.0.9.47	Deny

OK

Technical Support

Learn about the following topics:

- [Troubleshooting Resources on page 164](#)
- [Contacting Trend Micro on page 165](#)
- [Other Resources on 165](#)

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal provides 24/7 online resources that contain the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select from the available products or click an appropriate button to search for solutions.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Contact Support and select the type of support needed.
A Trend Micro support engineer will investigate the case and respond in 24 hours or less.

<http://esupport.trendmicro.com/srf/SRFMain.aspx>
Tip: To submit a support case online, visit the following URL:

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro 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.

Go to <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> 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

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Expediting the 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

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.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<http://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the readme file to determine whether it is relevant to your environment. The readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any other Trend Micro document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Terms and Acronyms

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

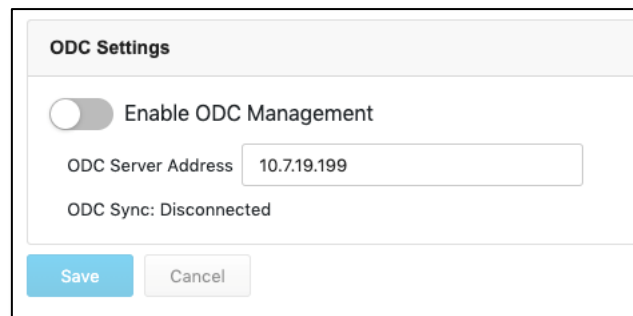
Term/Acronym	Definition
CEF	Common Event Format
LEEF	Log Event Extended Format
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Information Technology
ODC	Operational Technology Defense Console; OT Defense Console
OT	Operational Technology
OT Defense Console	Operational Technology Defense Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition

Setting Up Connection to ODC via EdgeFire, EdgeIPS or EdgeIPS Pro Web Console

A 'node' here refers to an Edge Series product that is managed by ODC. A managed node can be configured by ODC and send event logs to ODC. Here's how to enable the node to connect with ODC.

Procedure

1. Open the node's web console.
2. Enter your logon credentials (user name and password).
3. Use the default administrator logon credentials if it's the first-time login:
 - User name: `admin`
 - Password: `txone`
4. Go to [Administration] > [Sync Settings].



5. Specify the IPv4 address of ODC in [ODC Server Address].
6. Ensure that [Enable ODC Management] is enabled, and click [Save].

Introduction to the vShell

vShell is the ODC CLI (command line interface) tool that you can operate with commands to monitor status, troubleshoot, and configure settings.

First Time Using vShell

Signing in to vShell

When you want to open vShell, you can do the following:

1. Local machine

Remote machine over SSH

The default administrator credentials are:

- User: root
- Password: txone

Changing Default Password to Activate

When signing in to vShell for the first time, you will see the following WARNING messages.

```
Caution: please type the command ``oobe`` to activate vShell.  
Caution: please type the command ``oobe`` to activate vShell.  
Caution: please type the command ``oobe`` to activate vShell.  
Caution: please type the command ``oobe`` to activate vShell.  
Caution: please type the command ``oobe`` to activate vShell.
```

Please follow the steps below to activate the terminal:

```
$ oobe
```

Firstly, provide the default password:

```
Type current password:
```

Then, give a new password to change the default password:

```
Type the new password:
```

- The password field will only accept alphanumericals and some special characters: `!@#%^*+}:?~[]'./`
The password length should be 8-32 characters.

Confirm the new password:

```
Retype it:
```

After activating the vShell successfully, please log in again.

```
"Success! Please log in again."
```


How to Set Up a Network

Displaying the Network Settings

To see the details, you can enter something like:

```
$ iface ls
```

The part in the square brackets below shows the interface's configuration, and the part under the closed square brackets describes the current network settings running on the system.

```
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

Updating the Interface Settings

Using STATIC

Warning! The network interface name is "eth0", so any edits to the configuration of this interface could affect the system's ability to connect to the internet.

To use STATIC you need to change the network method and gateway, including the netmask:

```
$ iface update eth0 --method static --address 192.0.2.4 --gateway 192.0.2.254 -
netmask 255.255.255.0
```

Once the interface settings are changed, please restart the interface.

Settings are saved in the configuration file. Please note that the setting **eth0** does not take effect currently. Check it here:

```
$ iface ls
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "static",
    "Address": "192.0.2.4",
    "Netmask": "255.255.255.0",
    "Gateway": "192.0.2.254"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

After checking it, you need to restart eth0:

```
$ iface restart eth0
Restarted successfully! Please check the network status.
```

- Please check the status to ensure the interface boots up again successfully.

Using DHCP

Warning! The network interface name is "eth0", so any edits to the configuration of this interface could affect the system's ability to connect to the internet.

To use DHCP you need to change the network method:

```
$ iface update eth0 --method dhcp
Interface settings have been changed. Please restart the interface.
```

(OPTIONAL) Under the STATIC method an extra step is needed to remove the properties:

```
$ iface trim eth0 address
```

Interface settings have been changed. Please restart interface.

```
$ iface trim eth0 gateway
```

```
Interface settings have been changed. Please restart interface.
$ iface trim eth0 netmask
Interface settings have been changed. Please restart interface.
```

This is saved in the configuration file -- notice that the setting **eth0** will not take effect until it's restarted.

Here is one example of what a usable configuration might look like:

```
$ iface ls
[
  {
    "Name": "lo",
    "Family": "inet",
    "Method": "loopback"
  },
  {
    "Name": "eth0",
    "Family": "inet",
    "Method": "dhcp"
  }
]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:07:05:2c brd ff:ff:ff:ff:ff:ff
    inet 10.7.19.155/24 brd 10.7.19.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe07:52c/64 scope link
        valid_lft forever preferred_lft forever
```

After checking, you need to restart eth0:

```
$ iface restart eth0
Restarted successfully! Please check the network status.
```

■ Please retype `iface ls` to check that the interface has successfully come back up.

How to Set Up ACL (Access Control List)

The vShell access-list command allows you to restrict network access to the ODC services by three trust lists:

- SSH: When enabled, only the IP addresses on this list can access the SSH service (tcp:22) in the ODC system.
- Device: When enabled, only the IP addresses on this list can access the node management services, including the NTP service (udp:123), ODC command channel (tcp:7590) and ODC logging channel (tcp:9093).
- Web: When enabled, only the IP addresses on this list can access the dashboard service (tcp:443).

Querying the Status

To obtain the active statuses, port numbers and IPs/CIDRs on the trust list.

```
$ access-list ls

SSH(tcp:22)
Status: Disabled

Device(udp:123, tcp:7590)
Status: Enabled
1.1.1.1/32

Web(tcp:443)
Status: Disabled
```

Adding Clients to the Trust List

You can add client IPs or Classless Inter-Domain Routing (CIDR).

```
$ access-list append SSH 1.1.1.1
added! Please check the trust list.
$ access-list append SSH 1.1.1.0/24
1.1.1.0/24 added! Please check the trust list.
```

Deleting Clients from the Trust List

You can delete client IPs or Classless Inter-Domain Routing (CIDR).

```
$ access-list trim SSH 1.1.1.1
removed! Please check the trust list.
$ access-list removed SSH 1.1.1.0/24
1.1.1.0/24 removed! Please check the trust list.
```

Enabling/Disabling the ACL of modules

Warning! If you log in over SSH, enabling the SSH ACL will immediately force you out of your SSH session.

Warning! Before you enable the ACL, please add clients to the trust list. If clients are not added before ACL is enabled, all clients will be blocked from connecting. If clients are not added to the trust list before ACL is enabled, it will be necessary for the administrator to edit the trust list directly.

```
$ access-list up Device
Device enabled! Please check the trust list.
$ access-list down Device
Device disabled! Please check the trust list.
```

Shortcut Table

Tab	Auto-complete or choose the next suggestion on the list
Ctrl + A	Go to the head of the line (Home)
Ctrl + E	Go to the tail of the line (End)
Ctrl + D	Delete the character located at the cursor
Ctrl + L	Clear the screen

List of Command Prompt Commands

Summary

Command	Description
access-list	Manage the IP trust lists
env	Manage system environment variables
exit	Exit this shell
help	List all commands
iface	Manage the network interfaces
ping	Test the reachability of a host
poweroff	Shut down the machine immediately
reboot	Restart the machine immediately
resolv	Set up the domain name server
scp	Send files via scp
service	Manage the dashboard service
sftp	Send files via sftp
pwd	Change password
web	Change settings of web console
dx	Diagnose network connection
ssh	SSH to a device

access-list

Manage the IP trust lists.

SSH: Manage connections to the SSH server.

Device: Manage node connections.

Web: Manage dashboard user connections.

ls - List all IPs in the trust lists.

```
$ access-list ls
```

append - Append an IP/CIDR to the trust list.

```
$ access-list append Device 192.168.1.1
$ access-list append Device 192.168.0.0/16
```

trim - Delete an IP/CIDR from the trust list.

```
$ access-list trim Device 192.168.1.1
$ access-list trim Device 192.168.0.0/16
```

up - Enable an IP on the trust list.

```
$ access-list up Device
```

down - Disable an IP on the trust list.

```
$ access-list down Device
```

env

Manage system environment variables.

hostname - Assign /etc/hostname value

```
$ env hostname NAME
```

■ Length should be 1-64 characters.

exip - Assign /acus/external_ip value

```
$ env exip 192.168.1.1
$ env exip default
```

■ "default" is equal to the eth0 IP address.

ls - List the environment variables for this server.

```
$ env ls
Hostname:      my-dashboard-server
ID:           55365266-108d-11ea-bca4-080027171302
Web Version:  1.0.0
External IP:  Not Set
```

■ "Not Set" in External IP terms means the eth0 IP address.

exit

Exit this shell.

```
$ exit
```

help

List all commands

```
$ help
vShell, version v1.0.0
Command List:
access-list  Manage IP trust lists
env          Manage system environment variables
exit        Exit this shell
help        List all command usage
iface       Manage the network interfaces
ping        Test the reachability of a host
poweroff    Shut down the machine immediately
reboot      Restart the machine immediately
```

```
resolv      Manage the domain name server
scp         Send files via scp
service    Manage the dashboard service
sftp       Send files via sftp
```

Shortcut table:

```
Tab        Auto-complete or choose the next suggestion on the list
Ctrl + A   Go to the head of the line (Home)
Ctrl + E   Go to the tail of the line (End)
Ctrl + D   Delete the character located at the cursor
Ctrl + L   Clear the screen
```

iface

Manage the network interfaces.

FAQ for iface

Q: What should I do when the message displays "ifdown: interface INTERFACE_NAME not configured"?

A: Execute the command "iface up INTERFACE_NAME".

Q: What can I do to resume network service if all commands are unavailable?

A: Please reboot the machine and then restart the interface.

ls - List all the interfaces and display IP addresses in the trust list.

```
$ iface ls
```

add - Add the interface in /etc/network/interfaces, if the interface name is not yet there.

Options

--address

--netmask

--gateway

```
$ iface add INTERFACE METHOD [OPTIONS]
$ iface ls
[
{
  "Name": "lo",
  "Family": "inet",
  "Method": "loopback",
  "Address": "1.2.3.4",
},
{
  "Name": "eth0",
  "Family": "inet",
  "Method": "dhcp"
}
]
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:a0:4b:ec brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fea0:4bec/64 scope link
valid_lft forever preferred_lft forever

$ iface add eth1 static --address 192.168.1.3 --netmask 255.255.255.0 --gateway
192.168.1.1

$ iface up eth1
```

update - Update the existing interface in /etc/network/interfaces

Options

```
--method
--address
--netmask
--gateway
```

```
$ iface update INTERFACE [OPTIONS]
$ iface update eth0 --method dhcp
$ iface restart eth0
```

trim - Remove some options from the interface in /etc/network/interfaces

Options

```
--address
--netmask
--gateway
$ iface trim INTERFACE [OPTIONS]
$ iface trim eth0 gateway
$ iface restart eth0
```

rm - Remove the interface from /etc/network/interfaces and shut it down

```
$ iface rm INTERFACE
```

up - Activate the interface in /etc/network/interfaces

Options

```
--force
$ iface up INTERFACE
```



```
// You can force it up, if necessary
$ iface up eth0 --force
```

down - Deactivate the interface in /etc/network/interfaces

Options

```
--force

$ iface down INTERFACE

// You can force it down, if necessary
$ iface down eth0 --force
```

restart - Deactivate and then activate the interface in /etc/network/interfaces

Options

```
--force
$ iface restart INTERFACE
```

ping

Test the reachability of a host.

```
$ ping www.google.com
```

poweroff

Shut down the machine immediately.

```
$ poweroff
```

reboot

Restart the machine immediately.

```
$ reboot
```

resolv

Manage the DNS settings.

ls - List the DNS on the resolv.conf

```
$ resolv ls
```

add - Add the DNS to the /etc/resolvconf/resolv.conf.d/tail (This command is available only when resolv mode is set to 'custom')

```
$ resolv add NAMESERVER
```

mode - Set the DNS mode to either dhcp or custom. The DNS server(s) will be assigned by the DHCP server when resolv mode is set to 'dhcp'.

```
$ resolv mode dhcp
$ resolv mode custom
```

replace - Replace the DNS in the /etc/resolvconf/resolv.conf.d/tail (This command is available only when resolv mode is set to 'custom')

```
$ resolv replace OLD_NAMESERVER NEW_NAMESERVER
```

trim - Remove the DNS from the /etc/resolvconf/resolv.conf.d/tail (This command is available only when resolv mode is set to 'custom')

```
$ resolv trim NAMESERVER
```

scp

Send file via SCP.

dlog - The OS and service debug logs.

```
$ scp dlog USER IP DIRECTORY
$ scp dlog my-debugger 10.7.6.123 '~/Log\Folder\{1\}'
password:
$ scp dlog my-debugger 10.7.6.123 ~/Downloads
password:
```

service

Manage web services.

reload - Restart service if service configuration is changed

```
$ service reload
```

sftp

Send file via SFTP.

dlog - Show the OS and service debug logs.

```
$ scp dlog USER IP DIRECTORY
$ scp dlog my-debugger 10.7.6.123 '~/Log\Folder\{1\}'
password:
$ scp dlog my-debugger 10.7.6.123 ~/Downloads
password:
```

ssh

SSH to a device.

ssh - Connect to a device via SSH.

```
$ ssh Device-IP SSH-Port
$ ssh 10.7.19.150 22
user:root

TrendMicro
Welcome!

password:
```

pwd

Change password.

pwd - Change SSH password.

```
$ pwd
Type current password:
Type the new password:
```

dx

Diagnose network connection.

dx - Testing network connectivity to AU Server.

```
$ dx au --proxy http://192.168.0.1 --proxy-user user:password
```



web

Manage accounts on web console.

web – Manage accounts on web console.

```
$ web reset admin
```

Supported MIB Objects

The following tables list the MIB objects supported by the ODC v1.2. The TXOne private MIBs can be downloaded from the Web Console.

SNMP Queries

Object Label	OID	Description	MIB
sysDescr	1.3.6.1.2.1.1.1.0	A description of this device/agent.	SNMPv2-MIB
sysObjectID	1.3.6.1.2.1.1.2.0	The object ID of this device/agent.	SNMPv2-MIB
sysUpTime	1.3.6.1.2.1.1.3.0	The time (in hundredths of a second) since the device/agent was last re-initialized.	SNMPv2-MIB
sysName	1.3.6.1.2.1.1.5.0	The name of this device/agent.	SNMPv2-MIB
sysLocation	1.3.6.1.2.1.1.6.0	The physical location of this device/agent.	SNMPv2-MIB
ifNumber	1.3.6.1.2.1.2.1.0	The number of network interfaces	IF-MIB
ifTable	1.3.6.1.2.1.2.2	A list of interface entries. The number of entries is given by ifNumber.	IF-MIB
ifEntry	1.3.6.1.2.1.2.2.1	An entry containing management information applicable to a particular interface.	IF-MIB
ifIndex	1.3.6.1.2.1.2.2.1.1	A unique value, greater than zero, for each interface.	IF-MIB
ifDescr	1.3.6.1.2.1.2.2.1.2	A textual string containing information about the interface.	IF-MIB
ifType	1.3.6.1.2.1.2.2.1.3	The type of interface.	IF-MIB
ifMtu	1.3.6.1.2.1.2.2.1.4	The size of the largest packet which can be sent/received on the interface, specified in octets.	IF-MIB
ifSpeed	1.3.6.1.2.1.2.2.1.5	An estimate of the interface's current bandwidth in bits per second.	IF-MIB
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	The interface's MAC address.	IF-MIB
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	The desired state of the interface.	IF-MIB
ifOperStatus	1.3.6.1.2.1.2.2.1.8	The current operational state of the interface.	IF-MIB
ifLastChange	1.3.6.1.2.1.2.2.1.9	The value of sysUpTime at the time the interface entered its current operational state.	IF-MIB

SNMP Traps

Object Label	OID	Description	MIB
cmstCmsBoot	.1.3.6.1.4.1.55749.2.1.2.0.1	The system boot up	TXONE-CMS-MIB
cmstCmsReady	.1.3.6.1.4.1.55749.2.1.2.0.2	The services ready	TXONE-CMS-MIB
cmstCmsCpuUsageRising	.1.3.6.1.4.1.55749.2.1.2.0.11	The CPU usage over the high threshold (95%)	TXONE-CMS-MIB
cmstCmsMemUsageRising	.1.3.6.1.4.1.55749.2.1.2.0.13	The memory usage over the high threshold (95%)	TXONE-CMS-MIB
cmstCmsDiskUsageRising	.1.3.6.1.4.1.55749.2.1.2.0.15	The used disk space over the high threshold (95%)	TXONE-CMS-MIB
cmstNodeRegistered	.1.3.6.1.4.1.55749.2.1.2.0.101	A new node is added to the system	TXONE-CMS-MIB
cmstNodeDeregistered	.1.3.6.1.4.1.55749.2.1.2.0.102	An existing node is removed from the system	TXONE-CMS-MIB
cmstNodeConnected	.1.3.6.1.4.1.55749.2.1.2.0.103	A node connected to the system	TXONE-CMS-MIB
cmstNodeDisconnected	.1.3.6.1.4.1.55749.2.1.2.0.104	A node disconnected from the system	TXONE-CMS-MIB