Operational Technology Defense Console

Administrator's Guide

2020-02-14

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

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

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

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

Table of Contents

About OT Defense Console

Introduction

Operational Technology Defense Console (OT 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

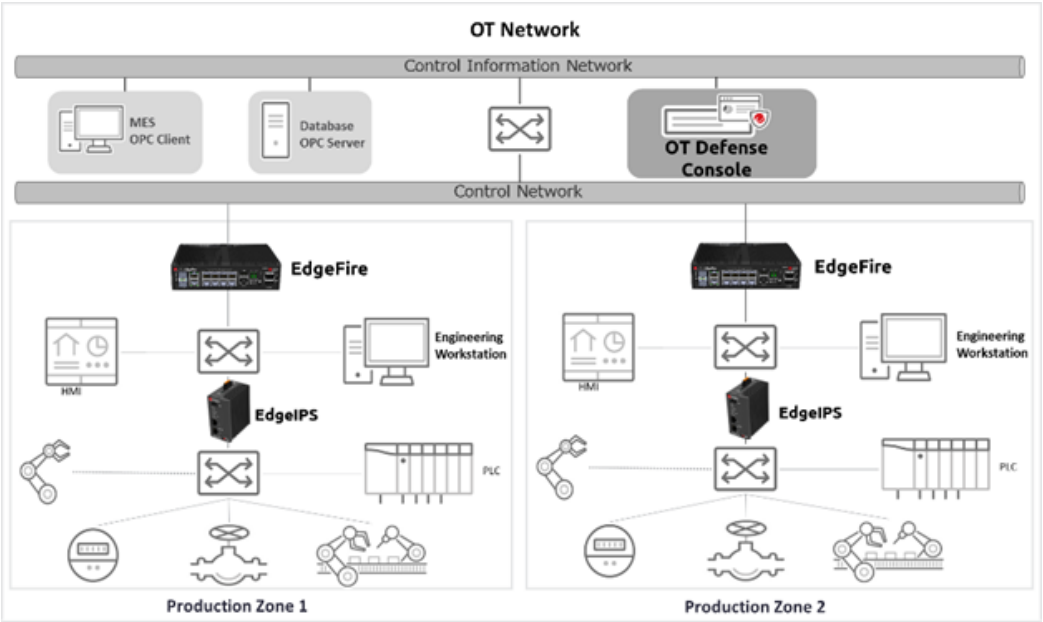


Figure 1. TXOne Networks security solutions for OT networks

Main Functions

EdgeIPS(tm) and EdgeFire(tm) are the security devices managed by the OT Defense Console. 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 Siemens, Mitsubishi, Schneider Electric, ABB, Rockwell, Omron, and Emerson. In addition to allowing OT and IT security system administrators to work together, this feature also allows the flexibility to deploy defense measures in appropriate network segments and seamlessly connects them to existing factory networks.

Policy Enforcement for Mission-Critical Machines

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

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

Getting Started

This chapter describes 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 8*.
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 65*.
4. Configure the system time.
   For more information, see *Configuring System Time on page 55*.
5. [Optional] Configure the Syslog settings.
   For more information, see *Configuring Syslog Settings on page 56*.
6. Update the components.
   For more information, see *Updates on page 59*.
7. Create the device groups for the EdgeIPS™ and EdgeFire™ devices.
   For more information, see *Group Management on page 24*.
8. Assigning policies to the device groups.
   For more information, see *Node Management on page 22* and *Object Profiles on page 36*.
9. Creating user accounts and sharing device group management permissions to the user accounts.
   For more information, see *Account Management on page 51* and *Sharing Management Permissions to Other User Accounts on page 34*.

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.

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

Procedure

1. In a web browser, type the address of the 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.

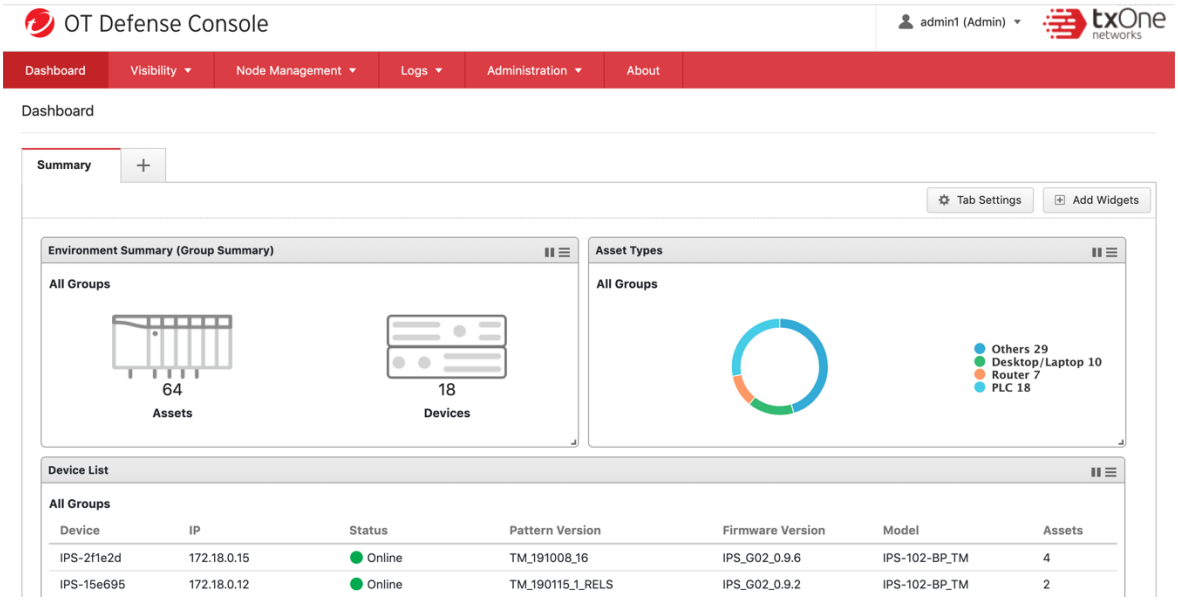
Note: The first time you log on, you must change the default login name and password before you can access the management console.

Note: 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

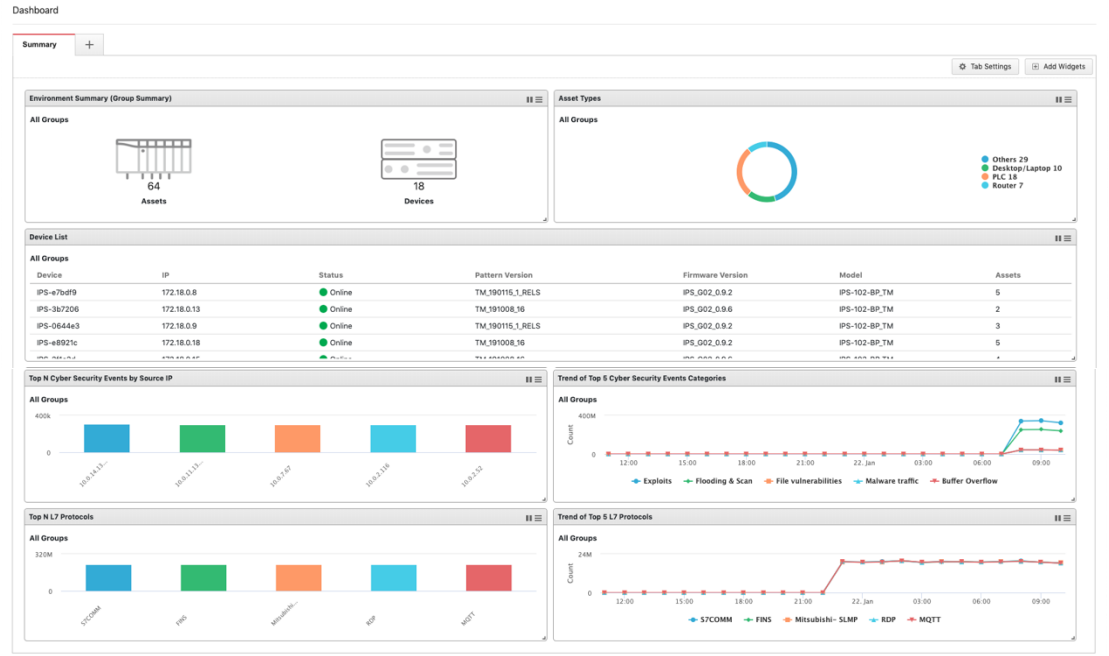
b. Click [Confirm].
   You will be automatically logged out of the system. The Log On screen will appear.

c. Log on again using your new credentials.



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], [Trends of Top 5 L7 Protocols]



Note: 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 34* and *User Roles on page 51*.

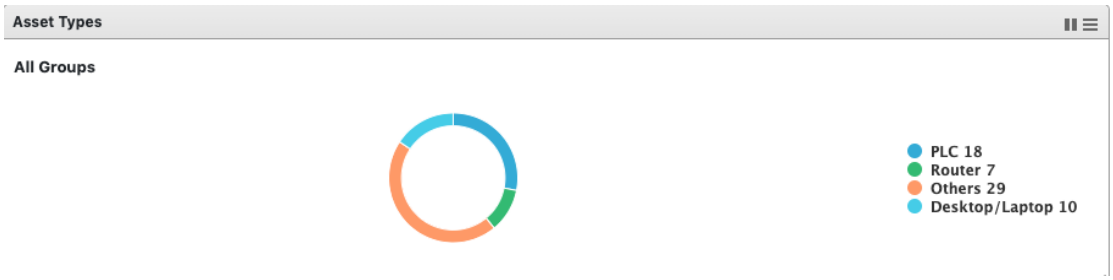
Note: The six widgets Top N Cyber Security Events by Source IP, Top N Cyber Security Events by Destination IP, Top N Protocol Filter Events by Source IP, Top N Protocol Filter Events by Destination IP, Top N Policy Enforcement Events by Source IP and Top N Policy Enforcement Events by Destination IP 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 > Assets Type

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



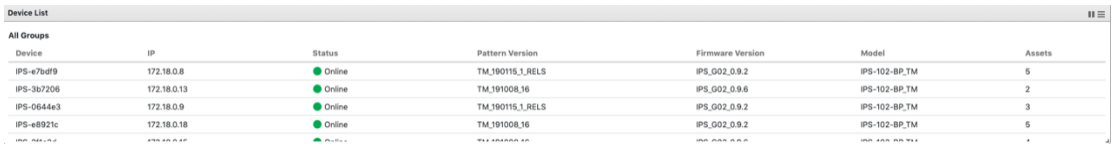
Assets > Environment Summary (Group Summary)

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.

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.

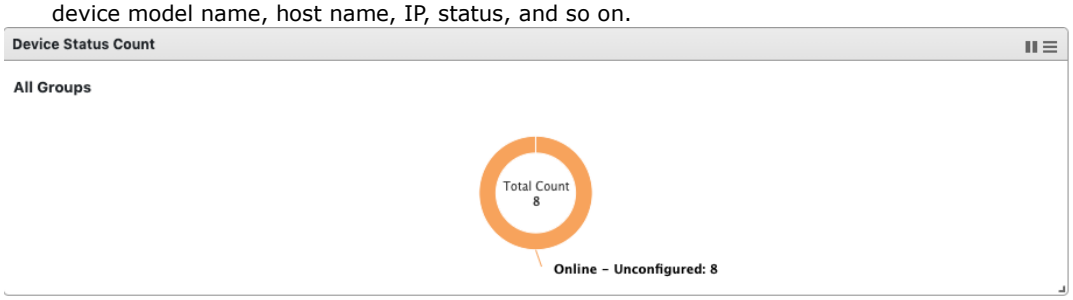


Item	Description
Device	Name of the device
IP	IP address of the device
Status	Status (online or offline) of the device
Pattern Version	Pattern version of the device
Firmware Version	The Firmware version of device
Model	The model name of device
Assets	The number of assets that are managed by the device

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.

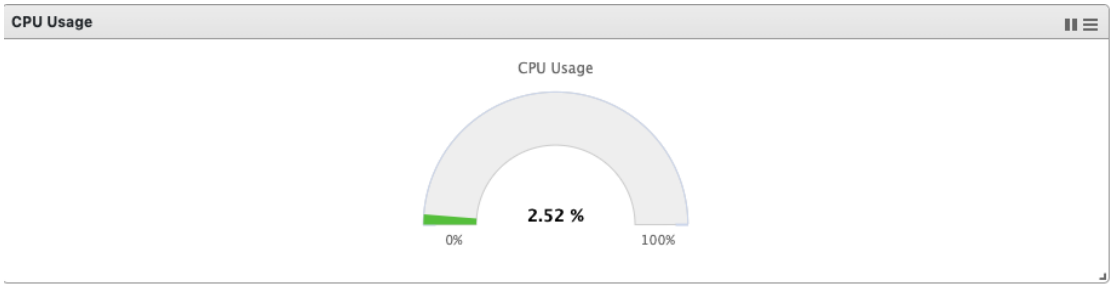


License > Node License Usage

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

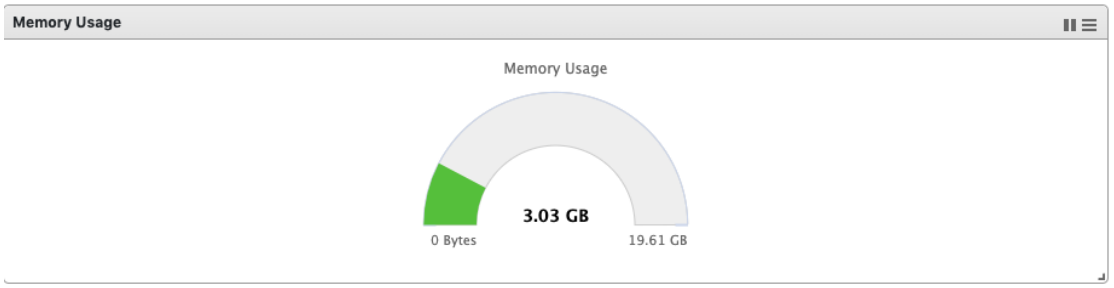
System > CPU Usage

Show the ODC CPU Usage.



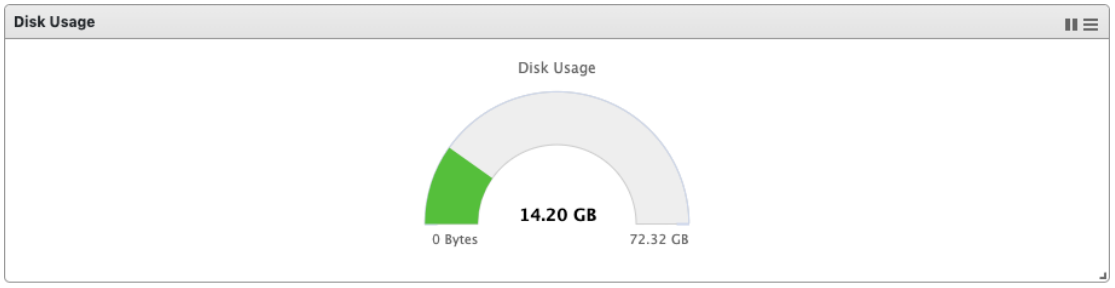
System > Memory Usage

Show the ODC Memory Usage.



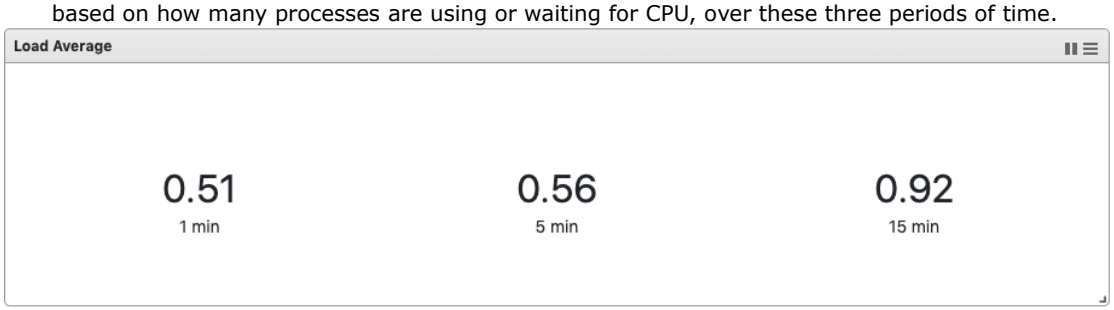
System > Disk Usage

Show the ODC Disk Usage.



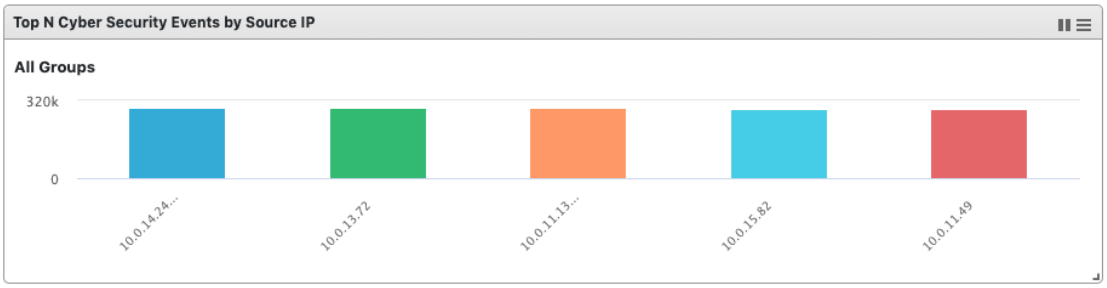
System > Load Average

Show the ODC 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.



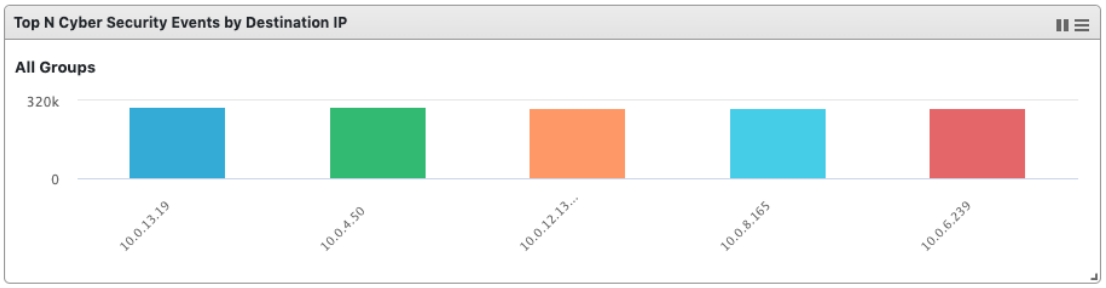
Cyber Security > Top N Cyber Security Events by Source IP

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)



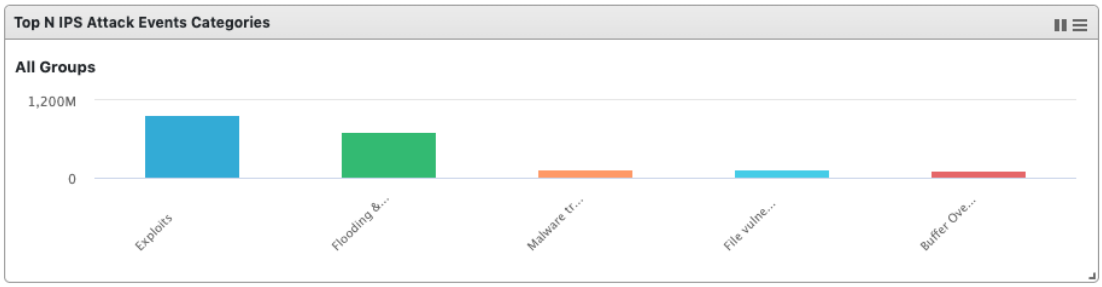
Cyber Security > Top N Cyber Security Events by Destination IP

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)



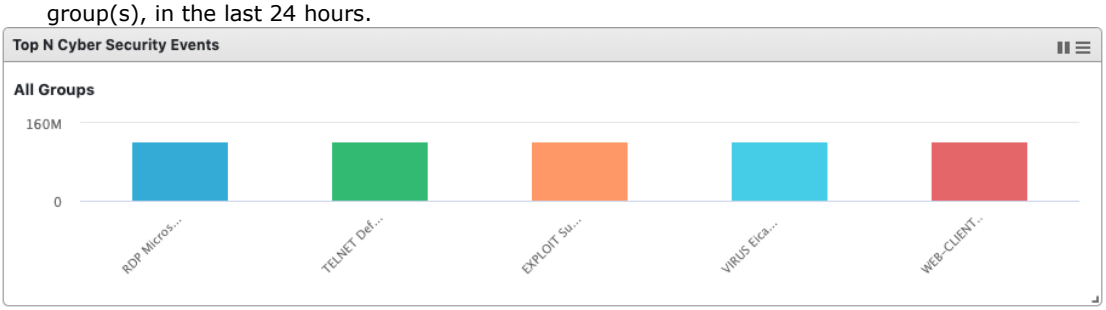
Cyber Security > Top N IPS Attack Events Categories

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.



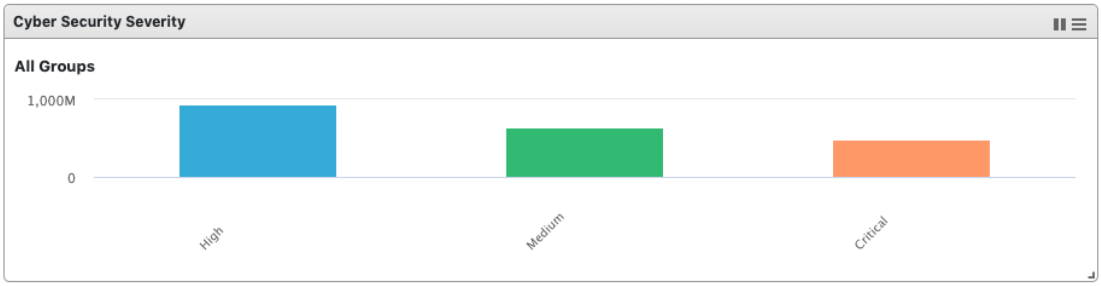
Cyber Security > Top N Cyber Security Events

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



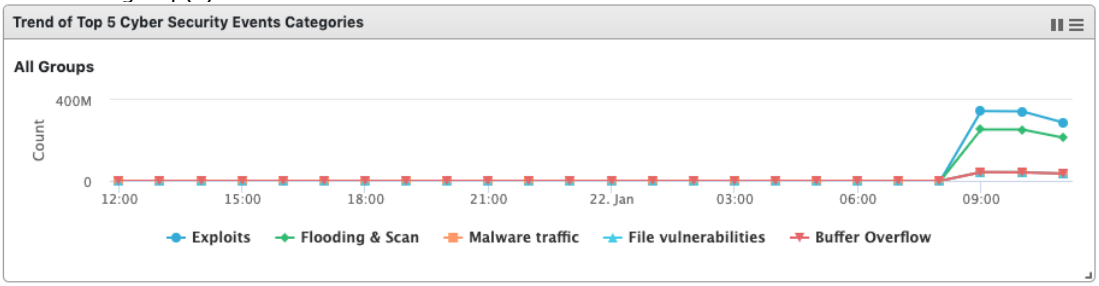
Cyber Security > Top N Cyber Security Severity

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



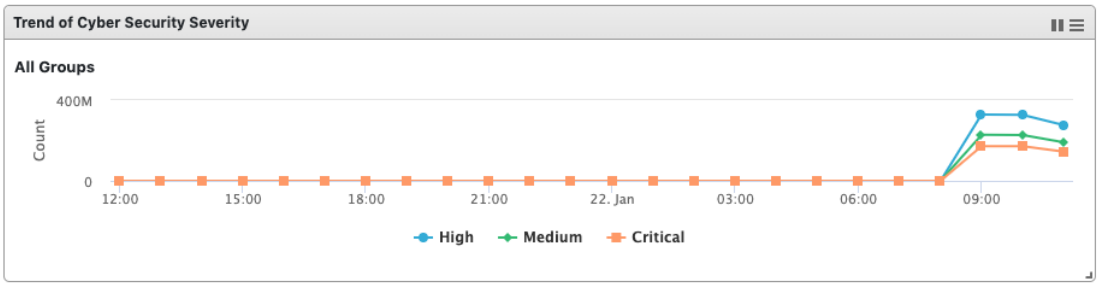
Cyber Security > Trends of Top N Cyber Security Events Categories

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



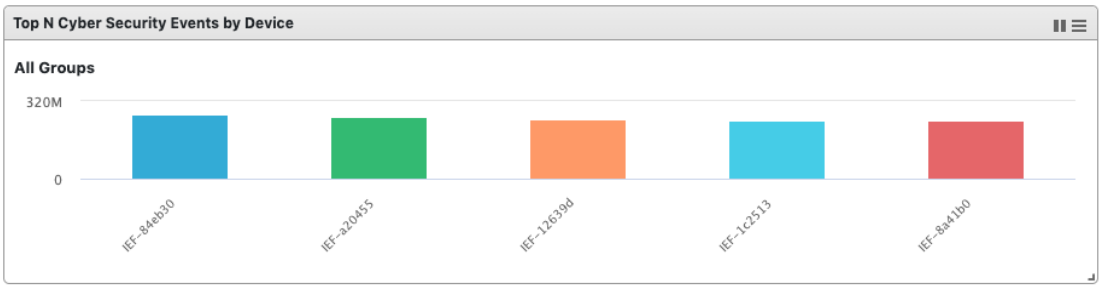
Cyber Security > Trends of Top N Cyber Security Severity

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



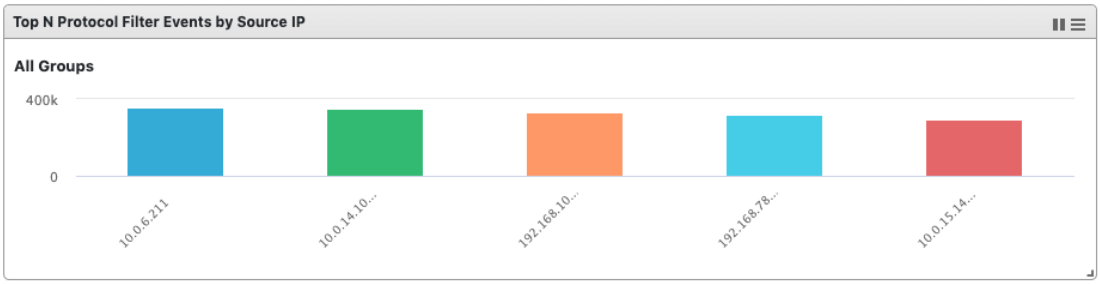
Cyber Security > Top N Cyber Security by Device

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.



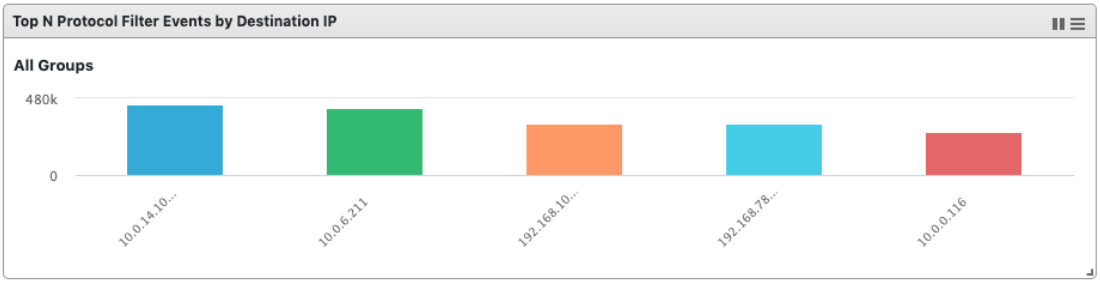
Protocol Filter > Top N Protocol Filter Events by Source IP

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)



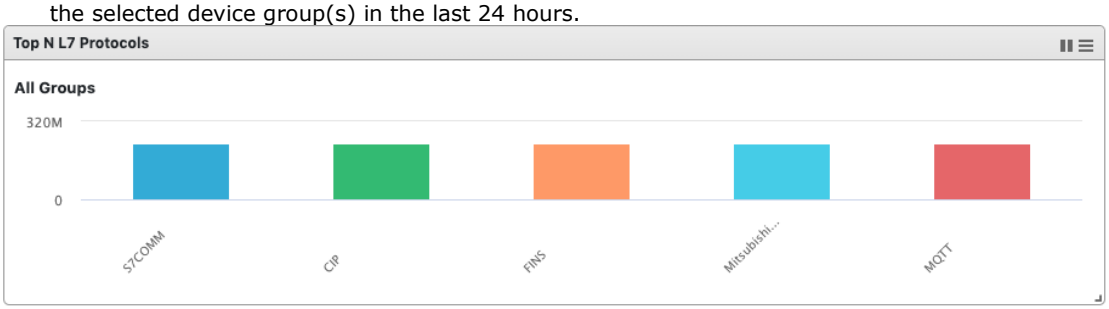
Protocol Filter > Top N Protocol Filter Events by Destination IP

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)



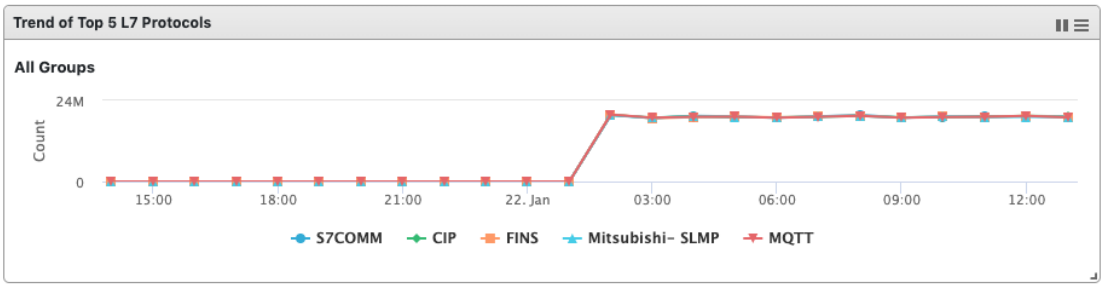
Protocol Filter > Top N L7 Protocols

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.



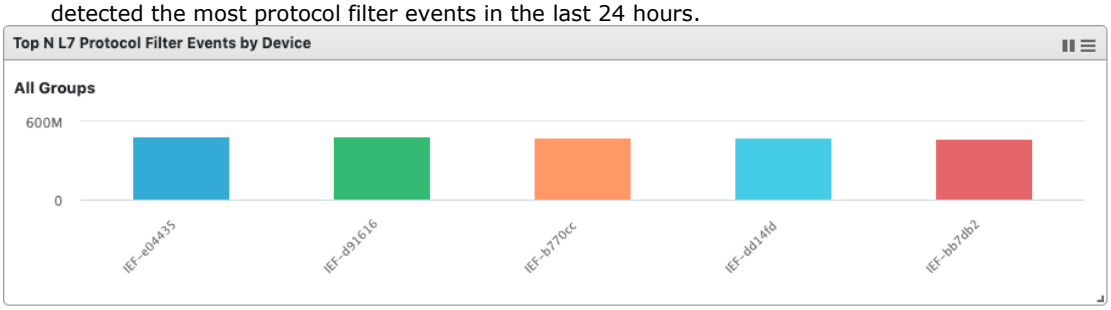
Protocol Filter > Trends of Top 5 L7 Protocols

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.



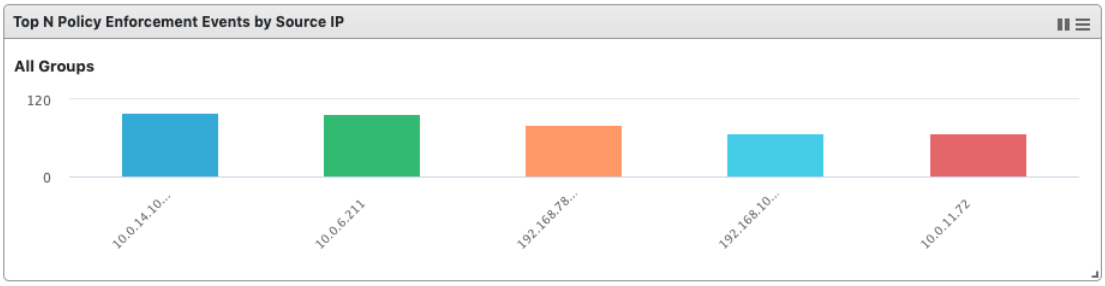
Protocol Filter > Top N L7 Protocol by Device

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.



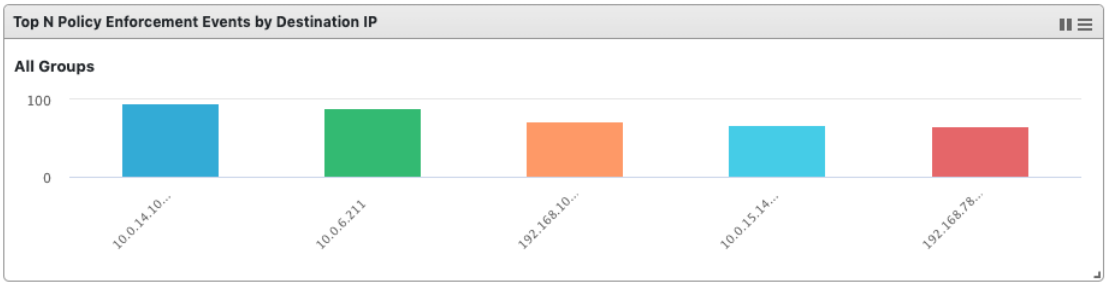
Policy Enforcement > Top N Policy Enforcement Events by Source IP

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)



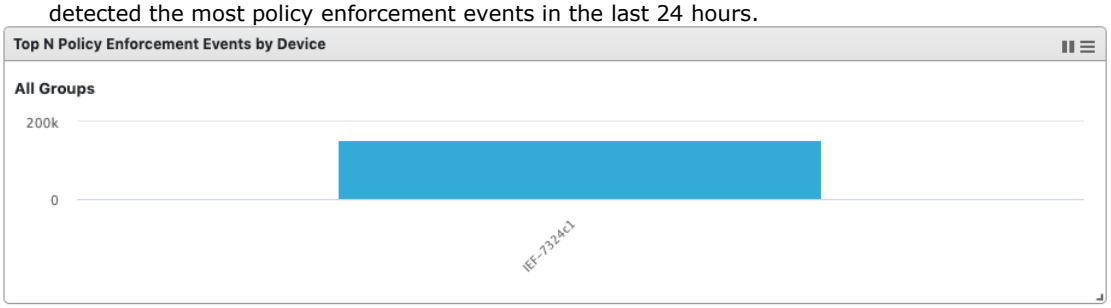
Policy Enforcement > Top N Policy Enforcement Events by Destination IP

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.



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

3. Click [Add Widgets].
4. Select one or more widgets by checking the check box. You can browse different categories of widgets by clicking different category names. The max amount of widgets for a tab is set to 10.
5. 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 right-bottom 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 the  button.

Widget Setting

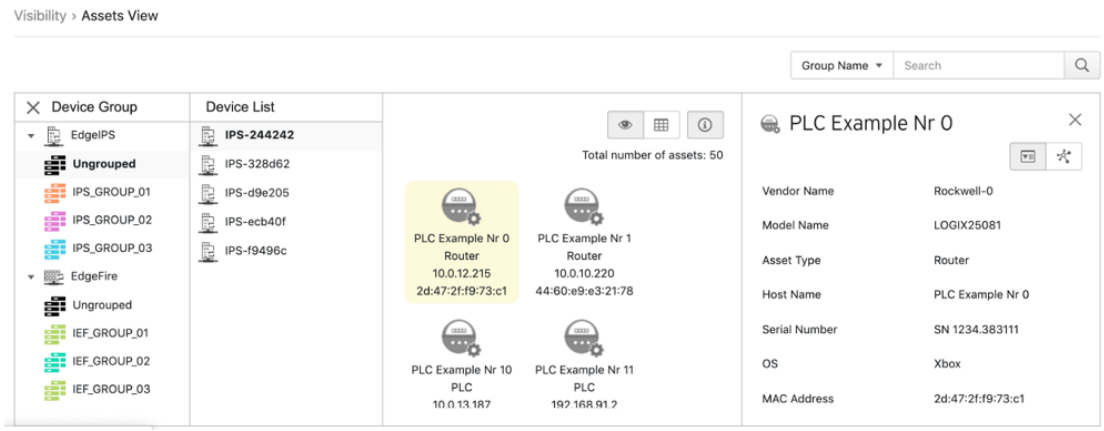
1. Click [Widget Settings], and the following setting options will be shown in a popup dialog.

Setting	Procedure
Widget Name	Edit the widget name in the input box. The widget name will display on the title of the widget in the Dashboard.
Auto Refresh Settings	Click the dropdown button on the right of the option name to select a different frequency of data refresh such as [Every 30 second] or [Every 1 minute]. You can choose [Manual Refresh] if the widget don't need to refresh automatically.
Top Statistics (selected widget only)	Click 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.
Chart Type (selected widget only)	Click on different chart icons for different chart types on the widget, such as bar chart or pie chart.
Device Type (selected widget only)	Click on the device type, EdgeFire/EdgeIPS, to get the corresponding group list. Select group by clicking group name on the [Groups] panel or deselect the group by click the group name on the [Selected Groups] panel.

2. When done configuring the settings, click [OK] to save them.

The Visibility Tab

The [Visibility] tab give you an overview of asset visibility of your managed assets. This tab provides you with timely and accurate information about the assets that are managed by EdgeIPS and EdgeFire



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

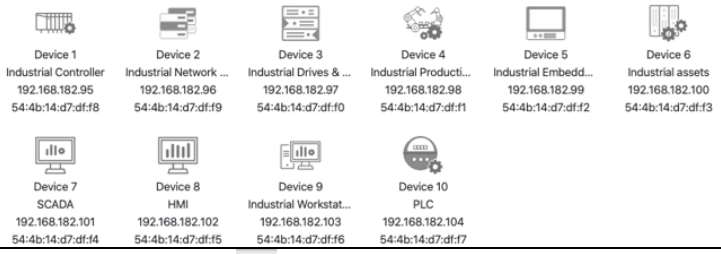
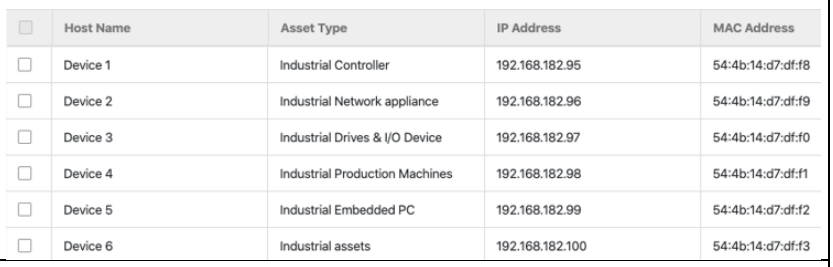
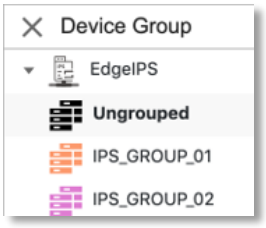
Note: The term **asset** in this chapter refers to the devices or hosts that are protected by Edge series solutions.

Note: 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 34* and *User Roles on page 51*.

Common Tasks

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

Task	Action
To search an asset	Specify the fields you want to search, input the search string, and click the [Search] button.  Possible options from the drop-down list: ▪ Group Name ▪ Device Serial Number ▪ Asset Serial Number ▪ Asset MAC Address ▪ Asset IP Address ▪ Asset Vendor Name ▪ Asset Model Name ▪ Asset Hostname ▪ Asset OS Name

To list devices/assets as icons	Click the Grid View button. 
To list devices in a table list	Click the Table View button. 
To fold up a device group	Click the X button to fold up the device group. 

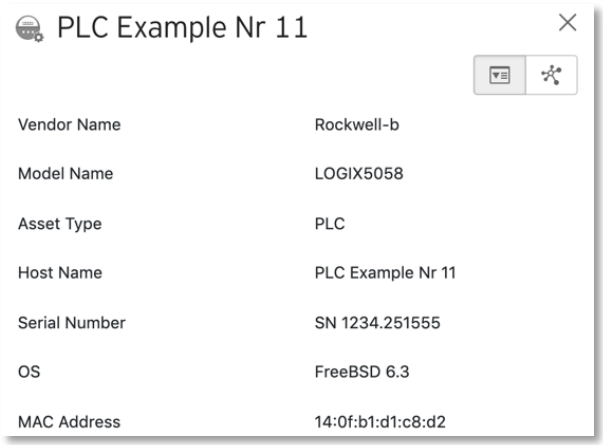
Displaying Asset Information

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:

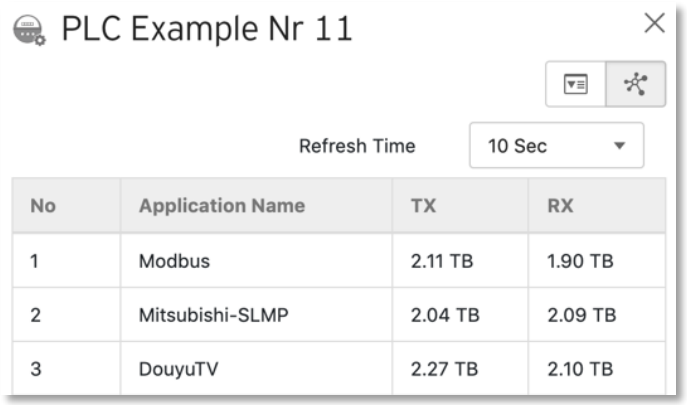


Field	Description	Example
Vendor Name	The vendor name of the asset.	Rockwell Automation/Allen-Bradley
Model Name	The model name of the asset.	1756-L61/B LOGIX5561
Asset Type	The asset type of the asset.	Industrial Controller
Host Name	The name of the asset.	Rockwell
Serial Number	The serial number of the asset.	7079450
OS	The system OS of the asset	Linux 2.6
MAC Address	The MAC address of the asset.	00:0c:29:da:14:1c
IP Address	The IP address of the asset.	10.24.254.94
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

Note: EdgeIPS and EdgeFire 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:



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.

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

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

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 node can be managed by the OT Defense Console:

- EdgeIPS™
- EdgeFire™

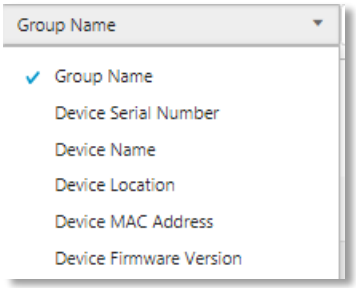
Note: The term **node** here refers to the TXOne Networks security devices that have been registered to the OT Defense Console.

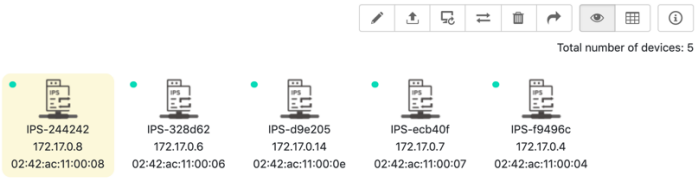
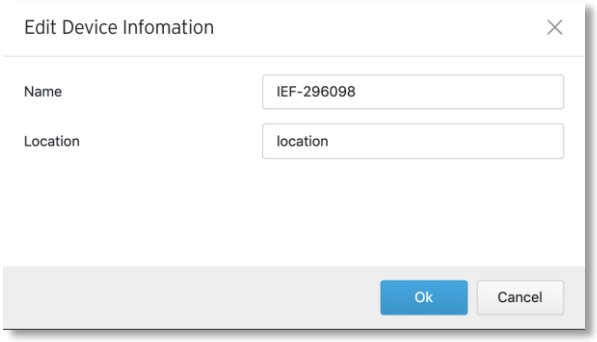
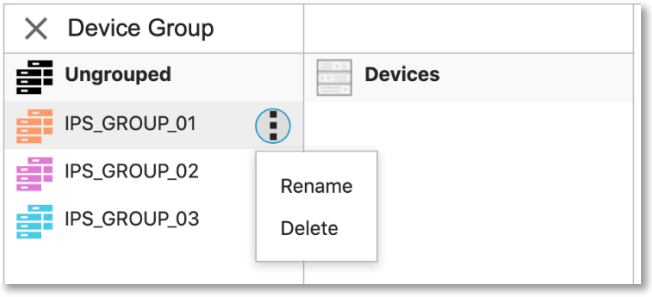
Note: The maximum number of supported managed nodes is dependent on the ODC model (physical appliance) or the resources allocated to the ODC (virtual appliance). See the datasheet for the details.

Note: 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 34* and *User Roles on page 51*.

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, 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.

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 more nodes. You can make changes to the nodes via the top-right buttons. 
To edit a device when in table view	Select the device and click the edit button at the top-right corner. 
To rename/delete a group	Hover over the group icon, click the button of the group, and select the desired action: 

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.

The security policy configurations that can be shared are:

- Security operation mode
- Cyber security policies
- Policy enforcement
- Pattern settings

Note: Security operation mode is supported by EdgeIPS only.

Go to [Node Management] > [EdgeIPS] or [Node Management] > [EdgeFire] to start managing your device groups.

Creating a New Device Group

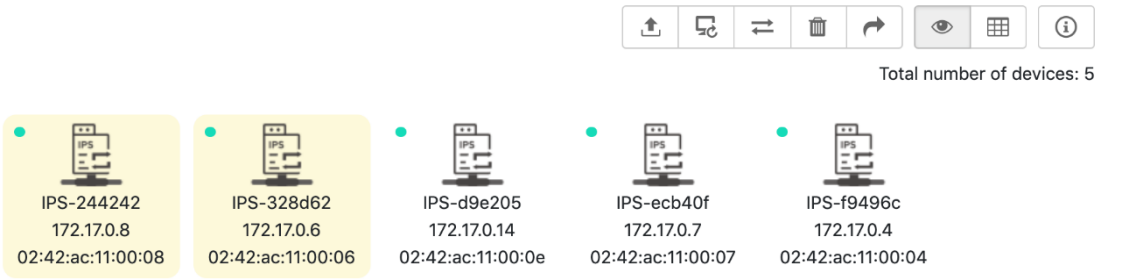
1. Under the [Device Group] panel, click ⊕.
2. Provide a name for the group and click [Confirm].
   - Length: 1~32
   - Only a-z / A-Z / 0-9, underline "_", hyphen "-", parentheses " ()" , and dot "." are supported in group names.

Renaming or Deleting a Device Group

1. Hover over the group icon and click the ⋮ button for the group.
2. Select the desired action.

Moving a Node into a Group

1. Select one or more 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 the node will be moved to.



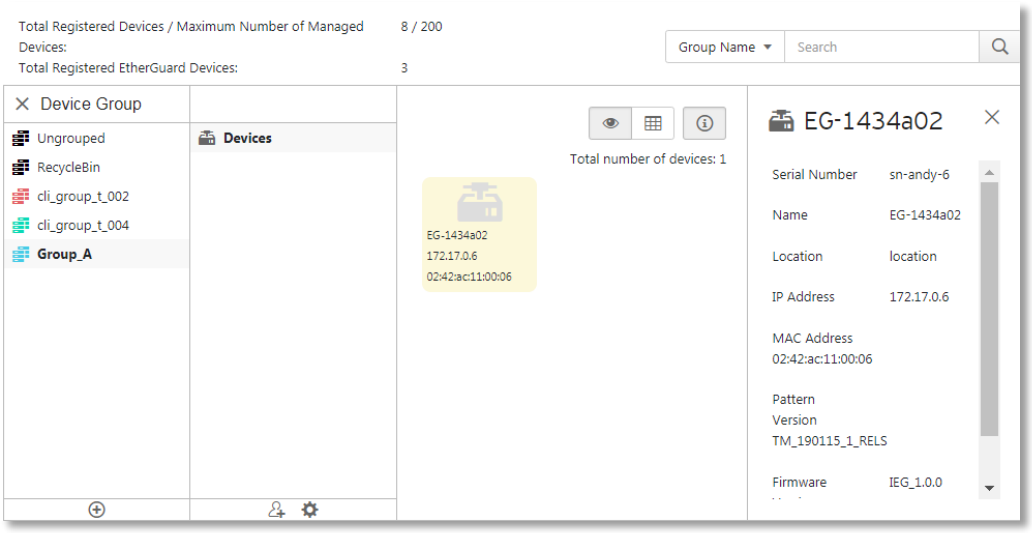
Managing EdgeIPS™ Devices

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.

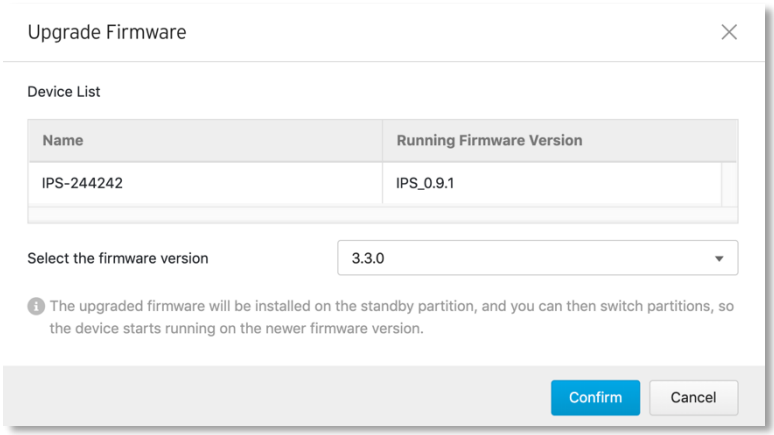


See *Common Tasks on page 22* for general tasks that can be performed under this tab.

Upgrading the Firmware

Procedure when in Table View

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



Procedure when in Grid View

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

Note: Only firmware versions the same as or newer than the [Running Firmware Version] can be upgraded. After the new firmware is uploaded to the node, the ' 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.

Note: 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 more nodes.
2. Click the button.

Procedure When in Grid View

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

Configuring Security Operation Mode

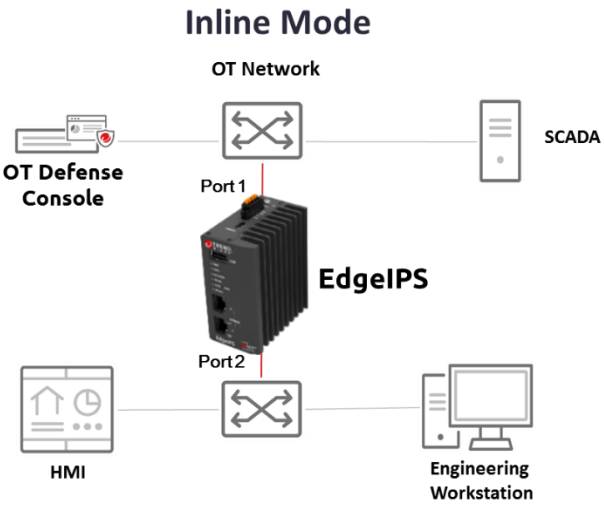
EdgeIPS™ offers two operation modes:

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

The following sections describe these two modes in detail.

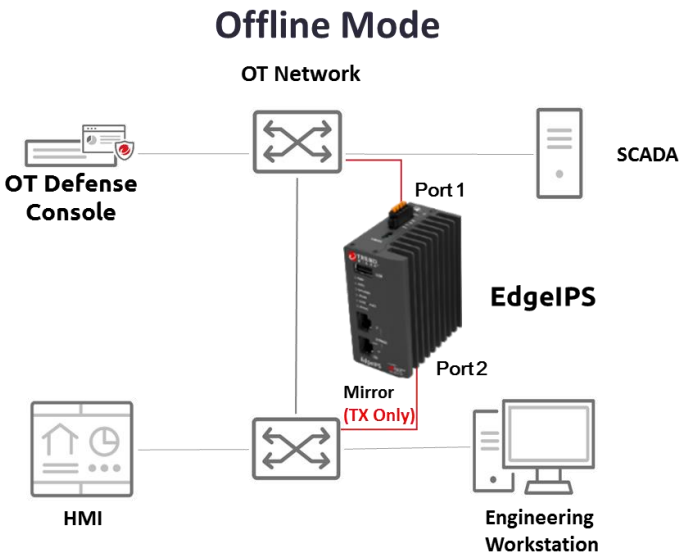
Inline Mode

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



Offline Mode

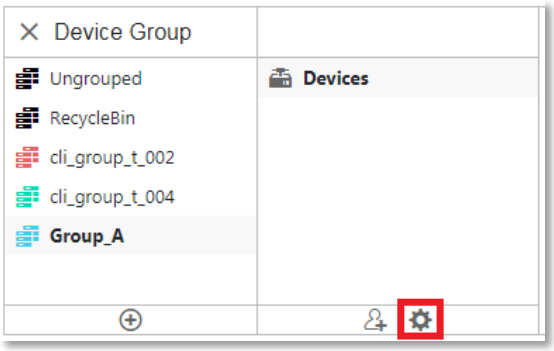
Data packets are mirrored from a switch to **port 2** of the EdgeIPS, which keeps detecting and monitoring, as well as outputting detection logs if threat events are detected.



Note:	The mirror port of the switch mirrors TX only to the **port 2** of the EdgeIPS.
Note:	**Port 1** of the EdgeIPS functions as the management port, which connects to another switch, allowing the EdgeIPS to be managed by ODC.

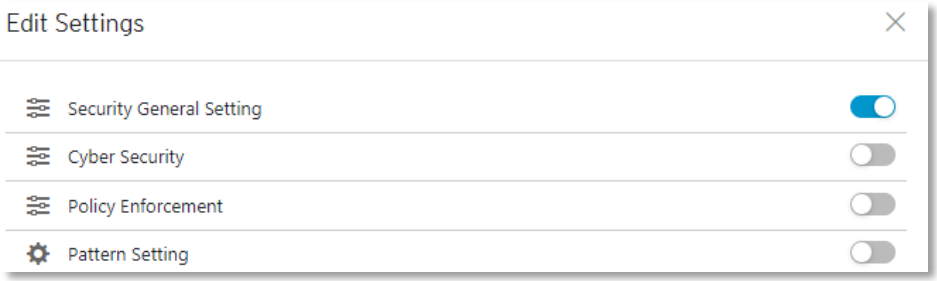
Enabling Security General Setting

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



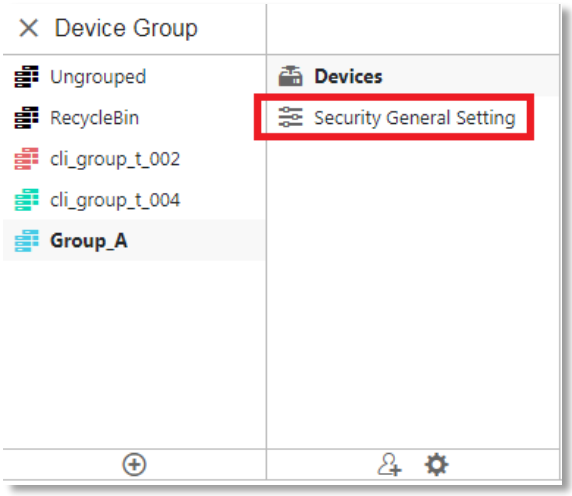
An [Edit Settings] screen will appear.

3. Ensure that the [Security General Settings] are enabled, and click [Continue].

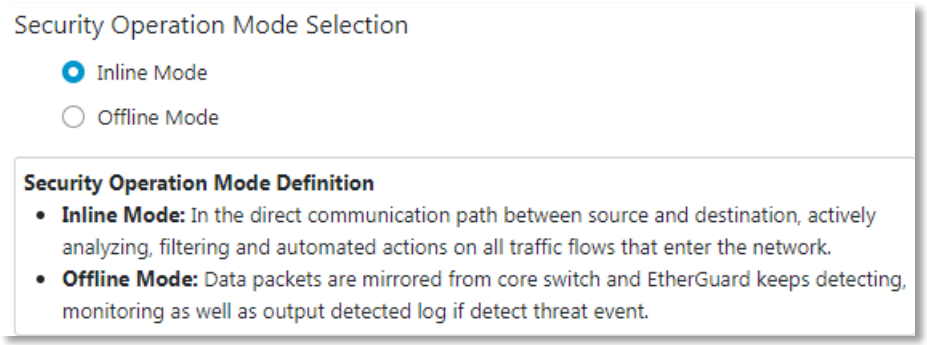


Configuring Security Operation Mode

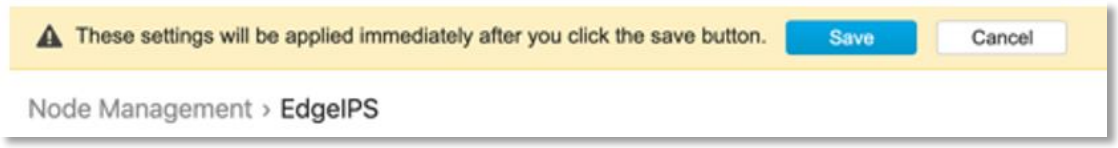
1. Click the [Security General Settings] tab for the device group.



2. Choose a desired operation mode for this device group.



3. Click the [Save] button to apply the settings.



Configuring Cyber Security

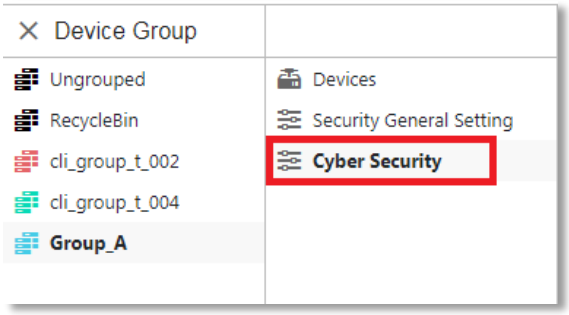
EdgeIPS features cyber security, which covers both intrusion prevention and denial of service attack prevention. The signature rules of intrusion prevention are called the 'Trend Micro DPI Pattern'. This pattern is provided by Trend Micro and can be regularly updated through ODC.

Enabling Cyber Security

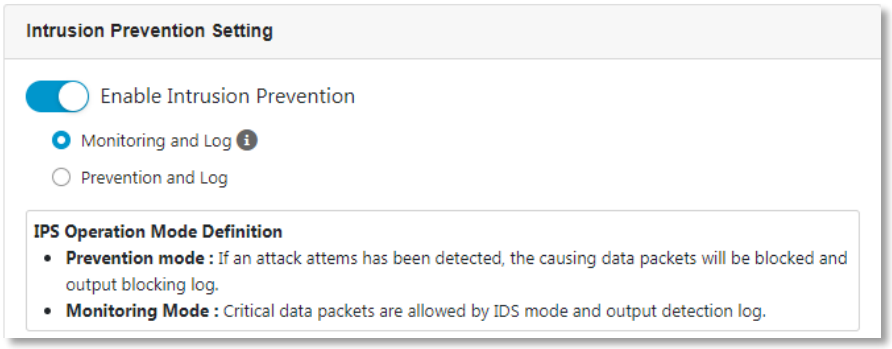
1. Click the device group you want to manage.
2. Click the [Edit Settings] button.
   An [Edit Settings] screen will appear.
3. Ensure that [Cyber Security] is enabled, and click [Continue].

Configuring Cyber Security - Intrusion Prevention

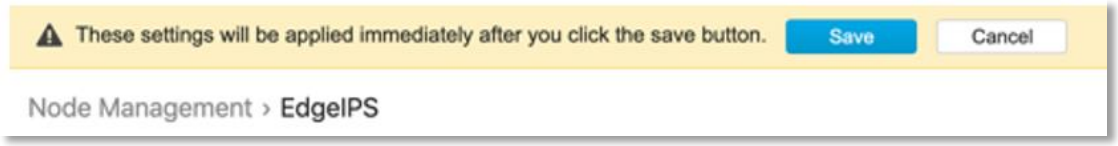
1. Click the [Cyber Security] tab for the device group.



2. Use the toggle to enable or disable the intrusion prevention feature.



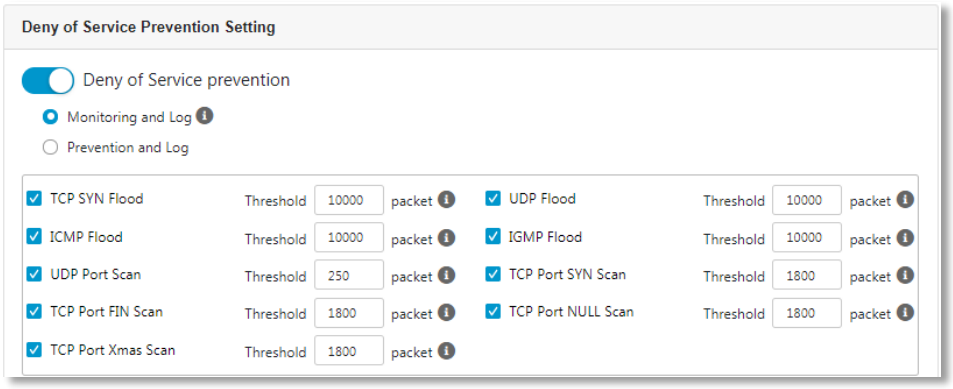
3. Select an action ([Monitor and Log] or [Prevent and Log]) for the intrusion prevention feature.
4. Click the [Save] button to apply the settings.



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



4. Select an action ([Monitor and Log] or [Prevent and Log]) for the feature.
5. You can optionally configure the thresholds of the denial of service rules.

Note: Flood/Scan Attack Protection rules 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:

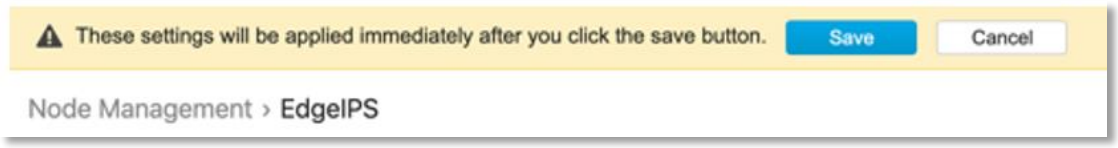
Mode (Security General Setting)	Action Settings	Action Performed
Inline Mode	Monitor and Log	▪ Detects and monitors network attacks, but does not block network attacks. ▪ Generates logs.
	Prevent and Log	▪ Blocks network attacks. ▪ Generates logs.
Offline Mode	Monitor and Log	▪ Passively detects and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

Configuring Policy Enforcement

Policy enforcement allows you to define a custom protocol that matches to an industrial or IT protocol, and then Allow-list or Block-list protocols in your network environment.

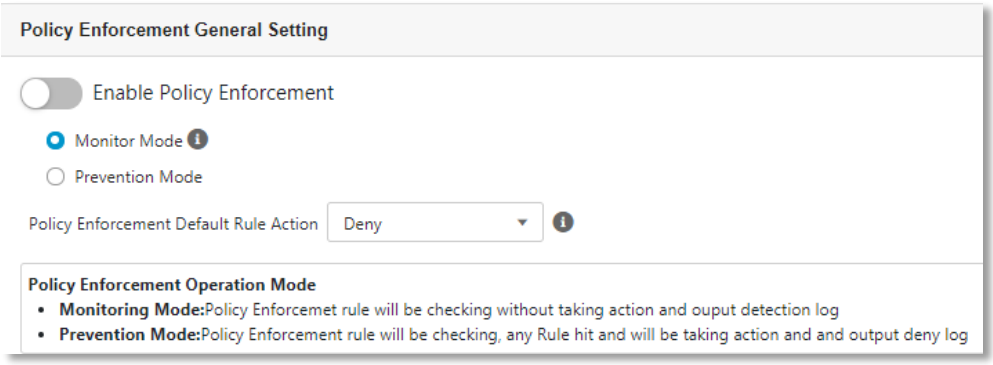
Enabling Policy Enforcement

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 or objects.
   - IP object profiles
     For more information, see *Configuring IP Object Profile on page 36*.
   - Service object profiles
     For more information, see *Configuring Service Object Profile on page 37*.
   - Protocol filter profiles
     For more information, see *Configuring Protocol Filter Profile on page 37*.
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.



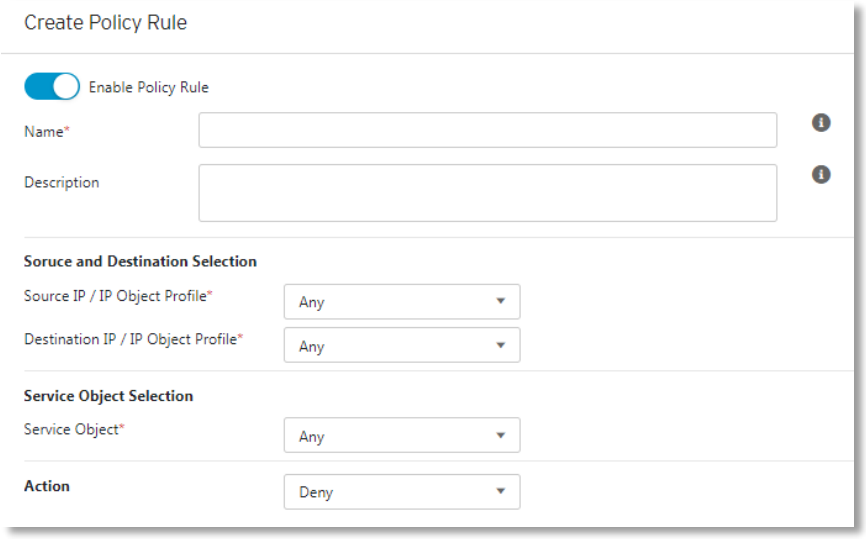
5. Select a mode ([Monitoring Mode], or [Prevention Mode]) for policy enforcement.
6. Under the [Policy Enforcement Default Rule Action] drop-down menu, select a default action for when no pattern is matched.

The following table summarizes the settings:

Mode (Security General Setting)	Mode (Policy Enforcement)	Action Performed
Inline Mode	Monitor Mode	▪ Detects and monitors packets that violate a policy, but does not block network attacks. ▪ Generates logs.
	Prevention Mode	▪ Blocks packets that violate a policy. ▪ Generates logs.
Offline Mode	Monitor and Log	▪ 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 descriptive name for the rule.
4. Input a description for the rule.
5. 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
   - Object

Note: 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 Profile] 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 either one of the following for the layer 4 criteria:
   - TCP
     You can further specify the port range for this protocol.
   - UDP
     You can further specify the port range for this protocol.
   - ICMP
     You can further specify the type and code for this protocol.
   - Custom
     You can further specify the protocol number for this protocol. The term protocol number refers to the one defined in the internet protocol suite.
   - Service Object

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

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

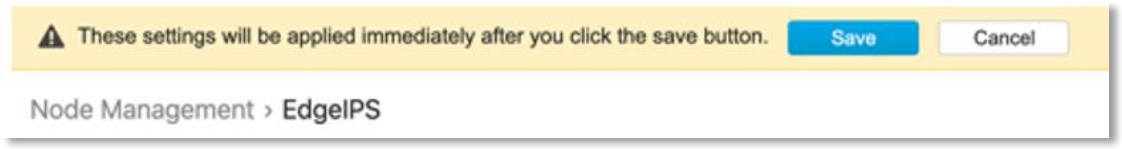
Note: When more than one policy enforcement rule is matched, EdgeIPS™ takes the action of the rule with the highest priority, and ignores the rest of the rules. The rules are listed on the table of the UI tab ordered by priority, with the highest priority rule listed on the first row of the table.

Configuring Pattern Setting

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

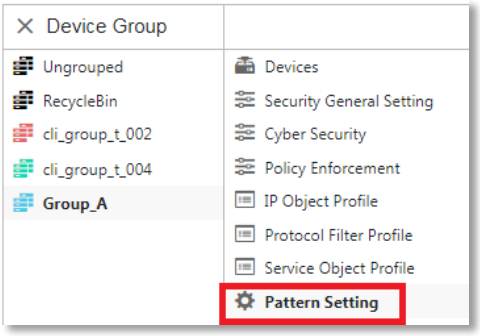
Enabling Pattern Setting

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.



Configuring Pattern Settings

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



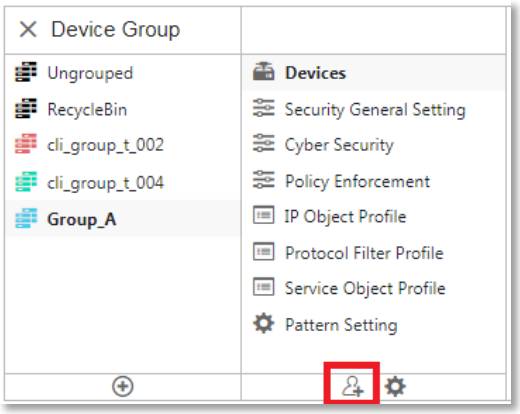
3. Select the DPI pattern to be deployed to the EdgeIPS™ nodes:
   - Latest: Always deploy the latest DPI pattern available on the OT Defense Console.
   - Fixed version: Deploy the fixed DPI version specified.

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 *User Roles on page 51* for the details.

Sharing Management Permissions

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



A [Share with Others] 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 *22* for general tasks that can be performed on this tab.

Note: The rest of the configurations are the same as those of managing EdgeIPS™ devices. Please see *Managing EdgeIPS™ Devices on page 24* for more details.

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

Configuring IP Object Profile

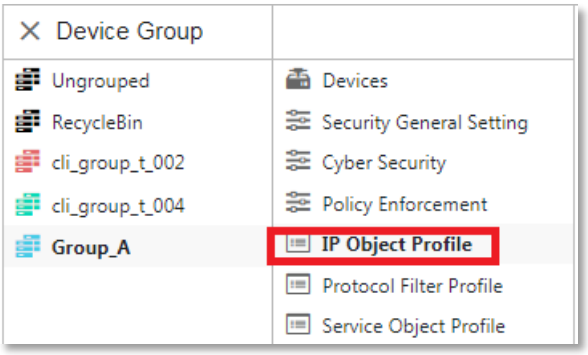
You can configure the IP address in an IP object profile, which can be applied to the device group to which they belong.

The types of IP address you can assign are:

- Single IP addresses
- IP ranges
- IP subnets

Procedure

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



4. Click [Add].
5. Type a descriptive 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.
9. Click [OK].

Configuring Service Object Profiles

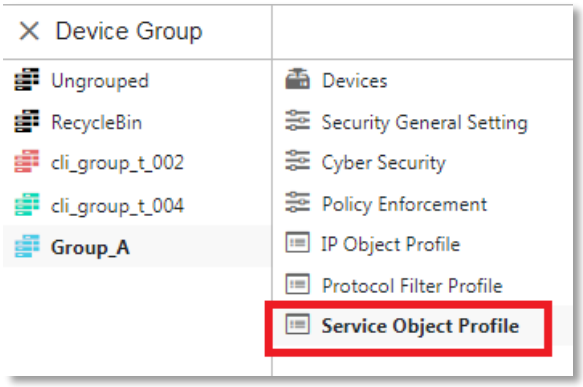
In a service object profile, you can define the following:

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

Note: 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 Profile].



4. Click [Add].
5. Type a descriptive 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.
9. Click [OK].

Configuring Protocol Filter Profile

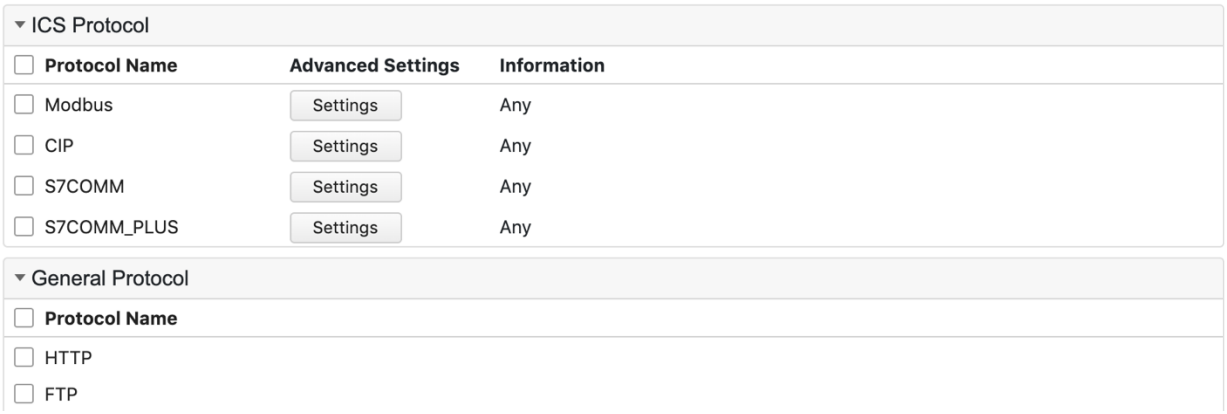
A protocol filter profile contains more sophisticated and advanced protocol settings that you can apply to a policy rule.

The following can be configured in a protocol filter profile:

- Details of ICS protocols, including:
  - Modbus
  - CIP
  - S7COMM
  - S7COMM_PLUS
  - PROFINET

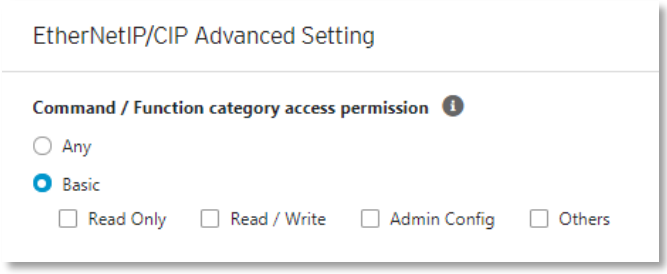
- SLMP
- FINS

- General Protocol, including:
  - HTTP
  - FTP
  - SMB
  - RDP
  - MQTT



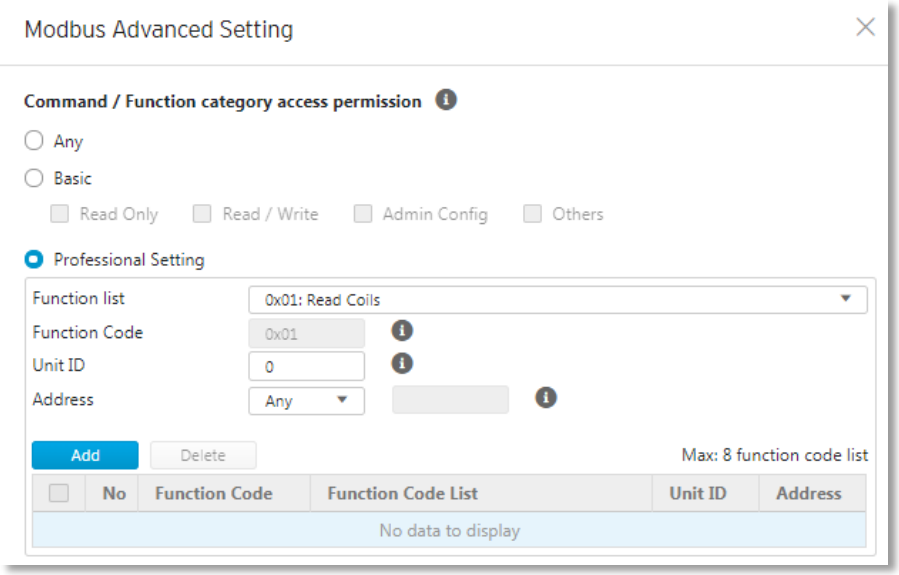
Specifying Commands Allowed in an ICS Protocol

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



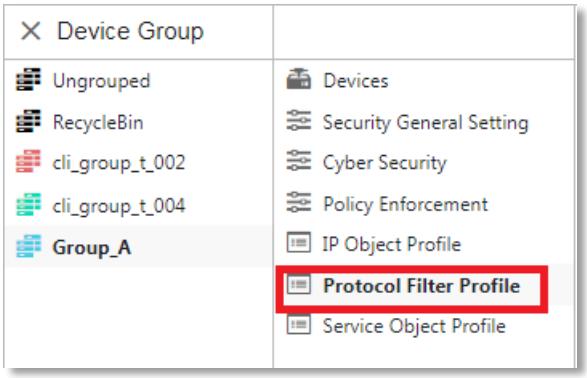
Advanced Settings for Modbus Protocol

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

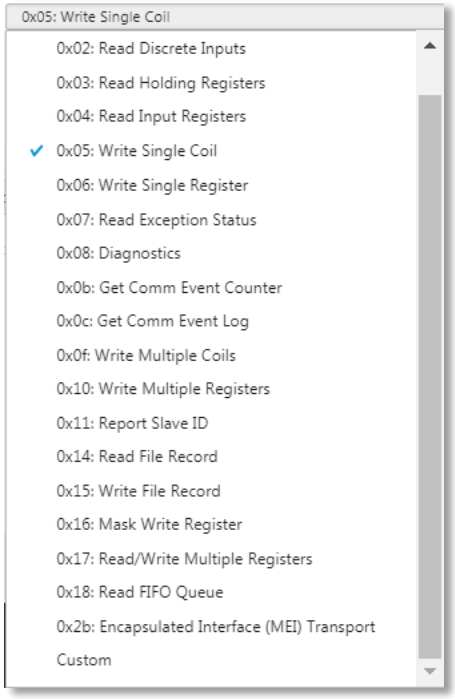
1. Go to [Node Management] > [EdgeIPS] or [EdgeFire].
2. Select the device group you want to manage.
3. Select [Protocol Filter Profile].



4. Click [Add].
5. Type a descriptive name.
6. Type a description.
7. 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 accesses in this protocol.
      - **Basic** - Multiple selections of the following:
        - **Read Only**: Read commands sent from HMI (Human-Machine Interface) / EWS (Engineering Work Station) / SCADA (Supervisory Control and Data Acquisition) to PLC (Programmable Logic Controller).
        - **Read / Write**: Read and write commands sent from HMI/EWS/SCADA to PLC.
        - **Admin Config**: Firmware update commands sent from EWS to PLC, project update (i.e., PLC code download) commands sent from EWS to PLC, and administration configuration relevant commands sent from EWS to PLC.
        - **Others**: Private commands, un-documented commands, or particular protocols provided by an ICS vendor.

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

- Click [Settings] next to [Modbus], and select [Professional Settings].
- At the [Function List] drop-down menu, select a function for 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 address range against which the function will operate.
- Click [Add].
- Repeat the above steps if you want to add more protocol definition entries.
- Click [OK].

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

Logs

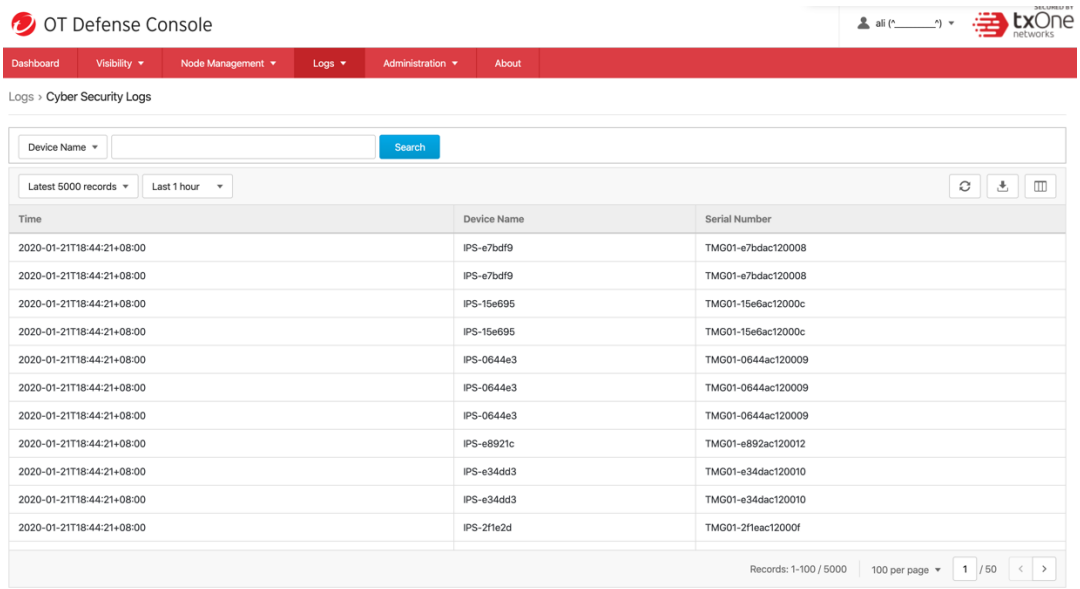
This chapter describes the system event logs and security detection logs you can view on the management console.

You can view the following logs on ODC:

- **Cyber security logs**
- **Protocol filter logs**
- **System logs**
- **Audit logs**
- **Asset detection logs**
- **Policy enforcement logs**

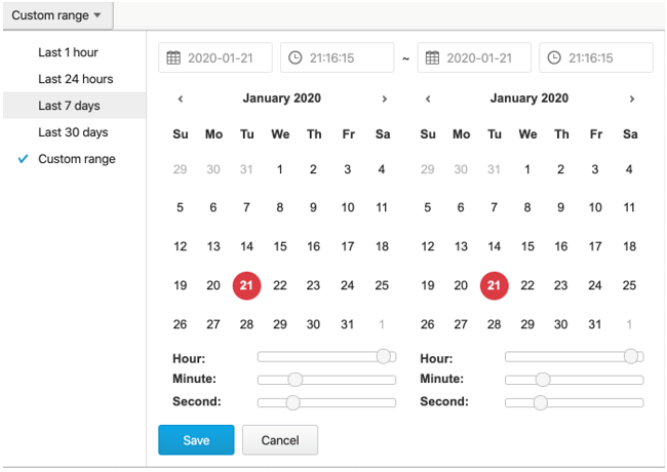
Viewing Cyber Security Logs

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

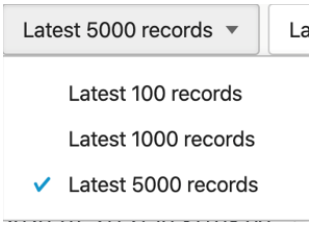


Procedure

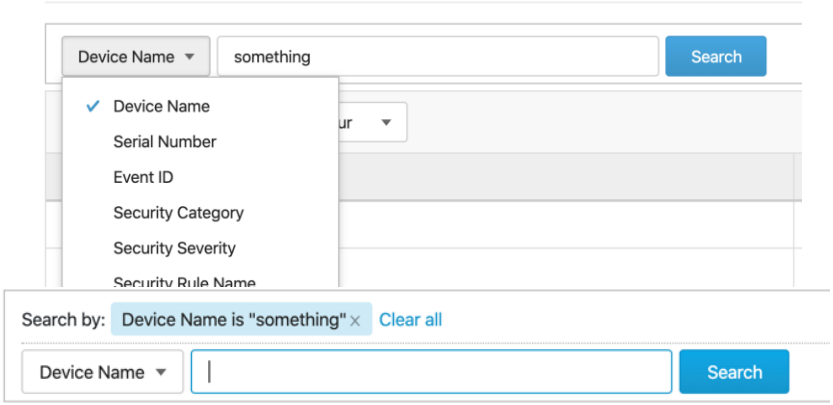
1. Go to [Logs] > [Cyber Security Logs].
2. You can take the following actions:
   - Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.



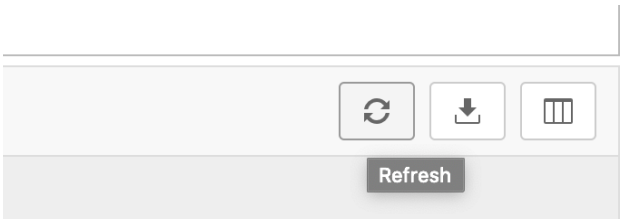
- Select the number of search results from the drop-down list, and it will search immediately. The options include **Latest 100 records**, **Latest 1000 records**, and **Latest 5000 records**.



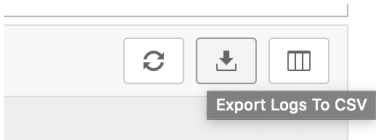
- Select a specific parameter from the drop-down list, type a value that you want to search in the input field, then click the [Search] button.

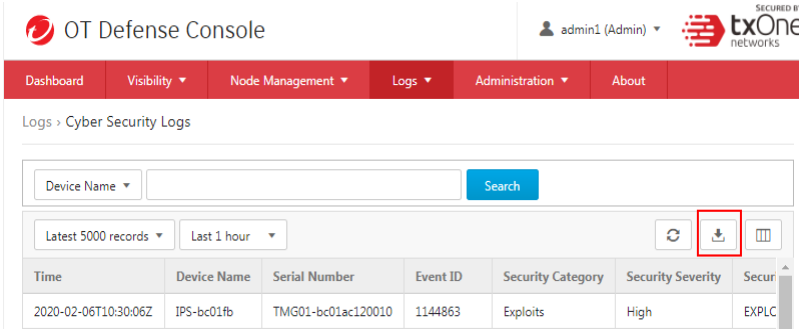


- Click the [Refresh] button to search again.

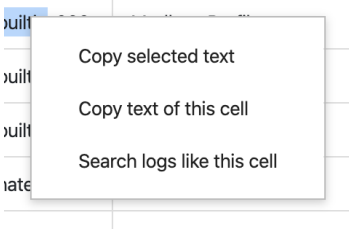


- Click the [Export Logs To CSV] button to export a CSV file of your current search result.

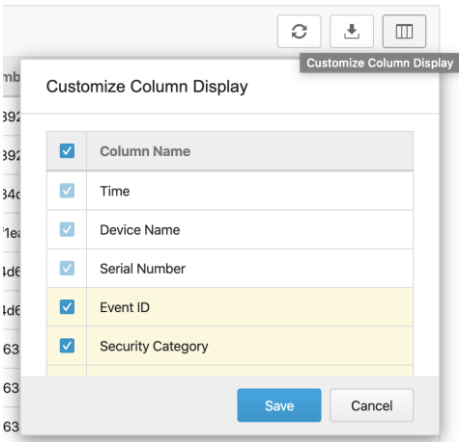




- Right click on a cell and the menu screen will appear. You can take one of the following actions:
  - Copy selected text
  - Copy text of this cell
  - Search logs for this cell's text



- 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 more table columns to display.
  - Click [Save].



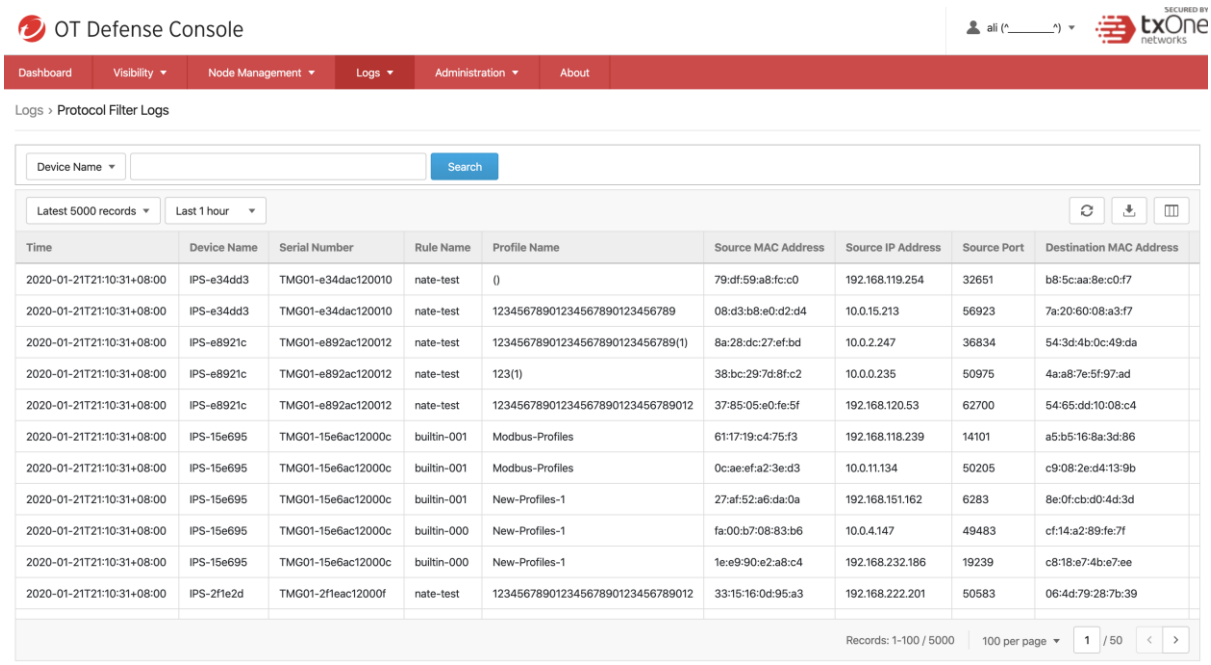
The following table describes the log's fields.

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.
Security Rule Name	The name of the matched signature.
Source MAC Address	The source MAC address of the connection.

Field	Description
Source IP Address	The source IP address of the connection.
Source Port	The source port of the connection.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port of the connection.
VLAN ID	The VLAN ID of the connection.
Ethernet Type	The ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.
Count	The number of detected network packets within the detection period after the detection threshold is reached.

Viewing 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.



Procedure

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

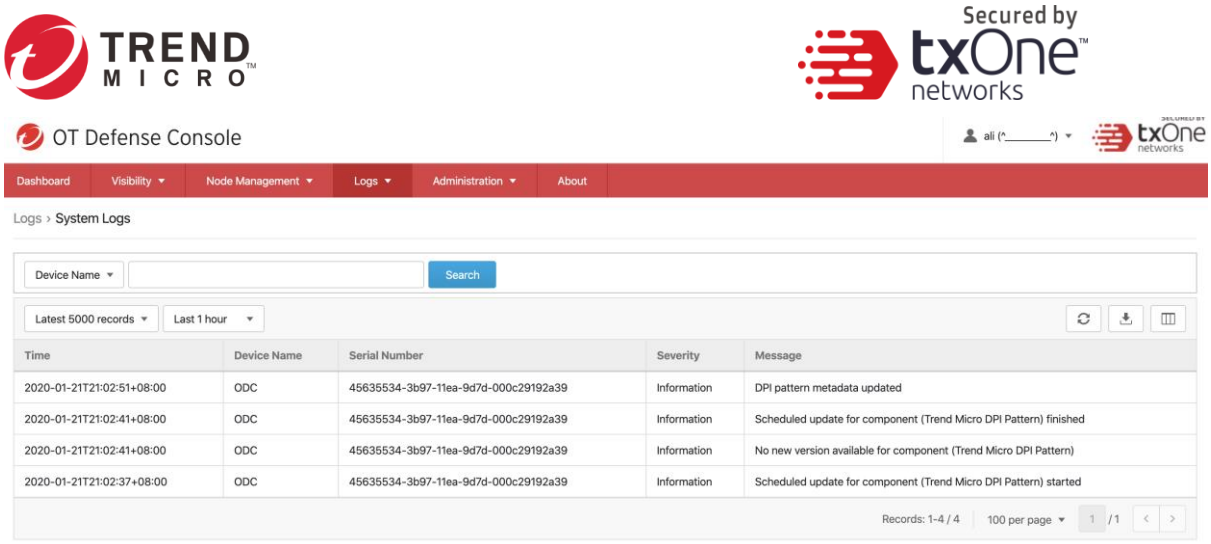
- Right-click on a cell and the menu screen will appear. You can take the following actions:
  - Copy selected text
  - Copy text of this cell
  - Search logs for this cell's text
- To customize the data columns displayed, do the following:
  - Click the settings icon [Customize Column Display] on the top right-hand corner of the information table. The [Customize Column Display] screen will appear.
  - Select one or more table columns to display.
  - Click [Save].

The following table describes the log's fields.

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.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port, if protocol is selected TCP/UDP. The ICMP type, if protocol is selected ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if protocol is selected TCP/UDP. The ICMP code, if protocol is selected ICMP.
Ethernet Type	The Ethernet type of the connection.
IP Protocol Name	The IP protocol name of the connection.
L7 Protocol Name	The layer 7 protocol name of the connection. The term layer 7 refers to the one defined in the OSI (Open Systems Interconnection) model.
Cmd / Fun No	The command or 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 System Logs

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



Procedure

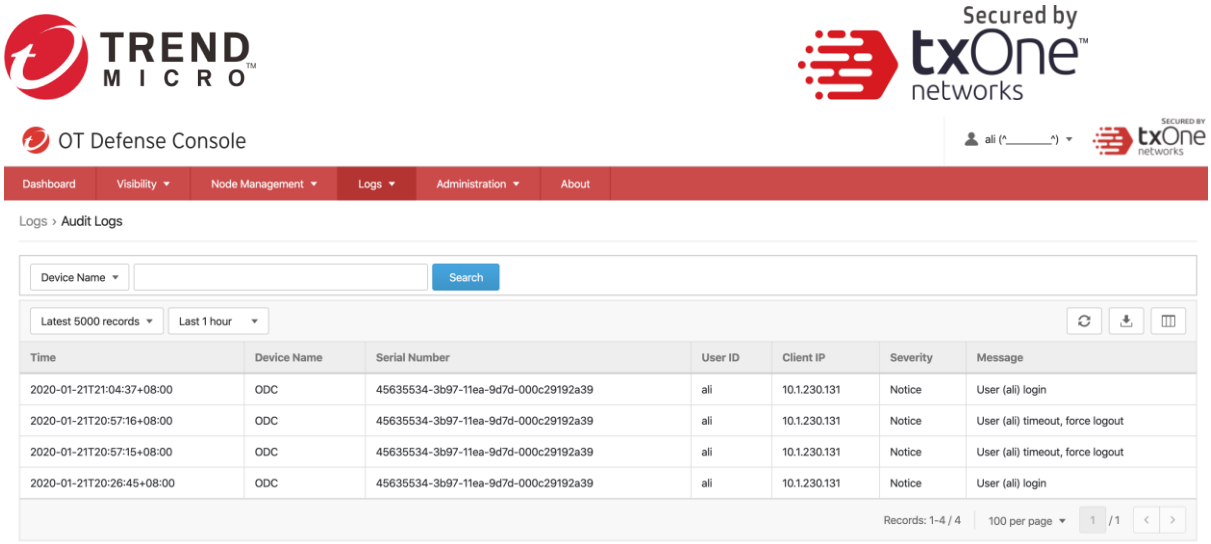
1. Go to [Logs] > [System Logs].
2. And you can take the following actions:
   - Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
   - Select the number of search 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 result.
   - Right-click a cell and the menu screen will appear. You can take the following actions:
     - Copy selected text
     - Copy text of this cell
     - Search logs for this cell's text
   - 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 more table columns to display.
     - Click [Save].

The following table describes the log's fields.

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.



Procedure

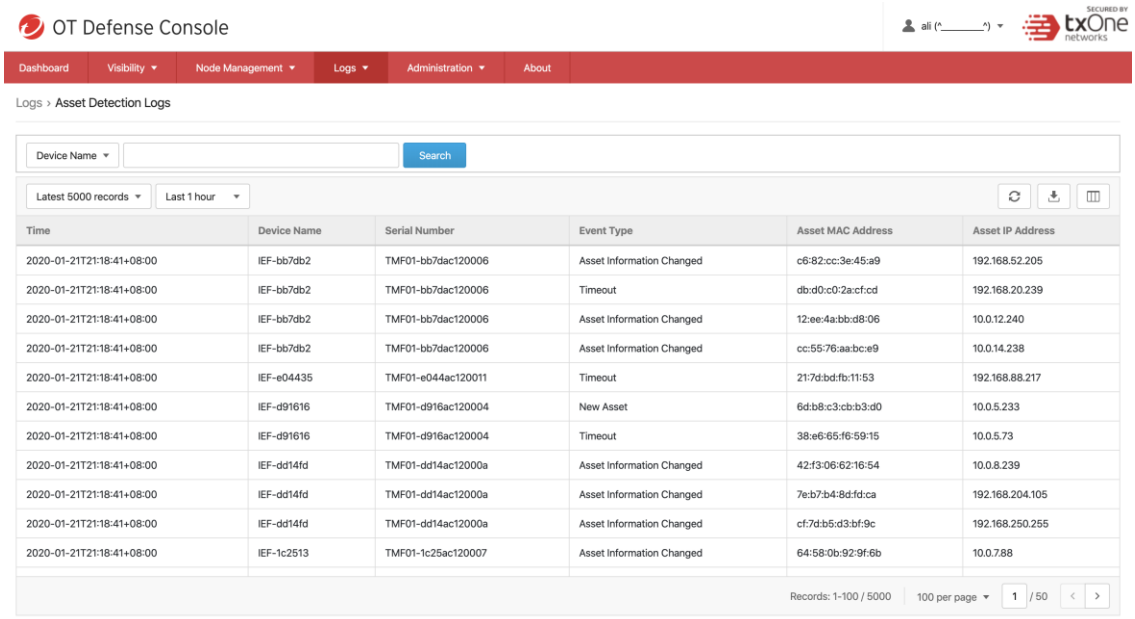
1. Go to [Logs] > [Audit Logs].
2. And you can do one of actions in the following actions
   - Select a time period from the drop-down list, and it will search immediately. The options include **Last 1 hour**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom range**.
   - Select the 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 file of your current search result.
   - Right-click a cell and the menu screen will appear. You can take one of the following actions:
     - Copy selected text
     - Copy text of this cell
     - Search logs for this cell's text
   - 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 more table columns to display.
     - Click [Save].

The following table describes the log's fields.

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.

Viewing Asset Detection Logs

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



Procedure

1. Go to [Logs] > [Asset Detection 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 something value that you want to search in the input text, 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 result.
   - Right-click on a cell and the menu screen will appear. You can take one of the following actions:
     - Copy selected text
     - Copy text of this cell
     - Search logs for this cell's text
   - 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 more table columns to display.
     - Click [Save].

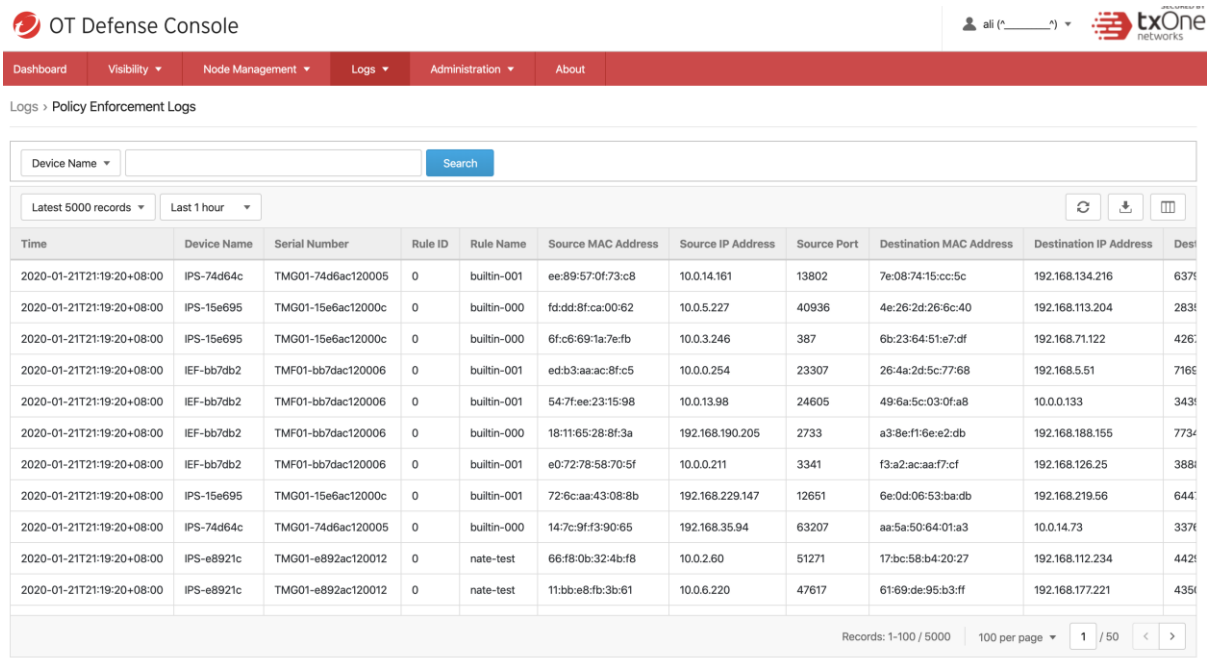
The following table describes the log's fields.

Field	Description
Time	The time the log entry was created.
Device Name	The host name of the node that generated the log.

Field	Description
Serial Number	The serial number of the node.
Event Type	The log event description.
Asset MAC Address	The MAC address of the asset.
Asset IP Address	The source IP address of the asset.

Viewing Policy Enforcement Logs

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



Procedure

1. Go to [Logs] > [Policy Enforcement Logs].
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 input text, 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 result.
   - Right-click on a cell and the menu screen will appear. You can take one of the following actions:
     - Copy selected text
     - Copy text of this cell
     - Search logs for this cell's text
   - 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 more table columns to display.
- Click [Save].

The following table describes the log's fields.

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.
Source MAC Address	The source MAC address of the connection.
Source IP Address	The source IP address of the connection.
Source Port	The source port, if protocol is selected TCP/UDP. The ICMP type, if protocol is selected ICMP.
Destination MAC address	The destination MAC address of the connection.
Destination IP Address	The destination IP address of the connection.
Destination Port	The destination port, if protocol is selected TCP/UDP. The ICMP code, if protocol is selected ICMP.
IP Protocol Name	The IP protocol name of the connection.
Action	The action performed based on the policy settings.

Administration

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

Account Management

Note: Log onto 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 log on to the management console using custom user accounts.

The following table outlines the tasks available on the <Account Management> tab.

Task	Description
Add account	Click [Add] to create a new user account. For more information, see *Account Input Format on page 53*.
Delete existing accounts	Select preexisting user accounts and click Delete.
Edit existing accounts	Click the name of a preexisting user account to view or modify the current account settings.
Configure Password Policy	Click [Password Policy] to adjust password restrictions. For more information, see Password Complexity on page 54.

User Roles

The following table describes the permissions matrix for user roles.

Administration Tab

		User Roles			
Sub-Tab	**Action**	**Admin**	**Operator**	**Viewer**	**Auditor**
Account Management	View	Yes	No	No	No
	All operations	Yes	No	No	No
System Time	View	Yes	No	No	No
	All operations	Yes	No	No	No
Syslog	View	Yes	No	No	No
	All operations	Yes	No	No	No
Updates	View	Yes	No	No	No
	All operations	Yes	No	No	No

SSL Certificate	View	Yes	No	No	No
	All operations	Yes	No	No	No
Log Purge	View	Yes	No	No	No
	All operations	Yes	No	No	No
Backup/Restore	View	Yes	No	No	No
	All operations	Yes	No	No	No
License Control	View	Yes	No	No	No
	All operations	Yes	No	No	No

Dashboard, Visibility, and Log Tabs

		User Roles			
Tab	**Action**	**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

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

Node Management Tabs

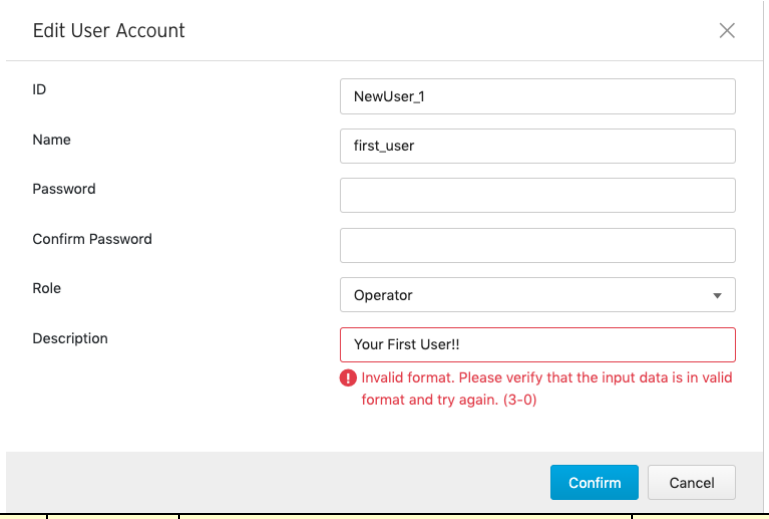
		User Roles			
Item	**Action**	**Admin**	**Operator**	**Viewer**	**Auditor**
Ungroup	View	Yes	Yes	No	No
	All Operations	Yes	No	No	No
Recycle Bin	View	Yes	Yes	No	No
	All Operations	Yes	No	No	No
Groups	View	Yes	Yes	No	No
	Device Operations (Move / Delete)	Yes	No	No	No
	Device Operations (Edit / Reboot)	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

Note: 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	• letters a-z, A-Z • numbers 0-9 • special characters: - periods [.] - underscores [_] • leading and trailing characters are not special characters • non-successive special characters	• admin • administrator • root • auditor
Name	1-32	• letters a-z, A-Z • numbers 0-9 • special characters: - periods [.] - underscores [_] - space [ ] • single spaces are not allowed	
Description	0-64	• letters a-z, A-Z • numbers 0-9 • special characters: - 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 *User Roles on page 51*.
Description	Type the description details for this account.

4. Click [Save].

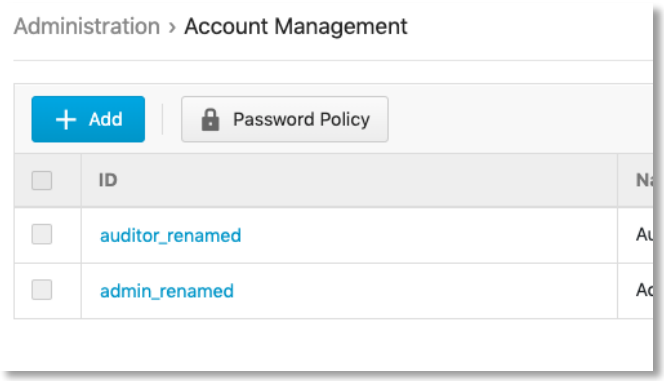
Changing Your Password

Procedure

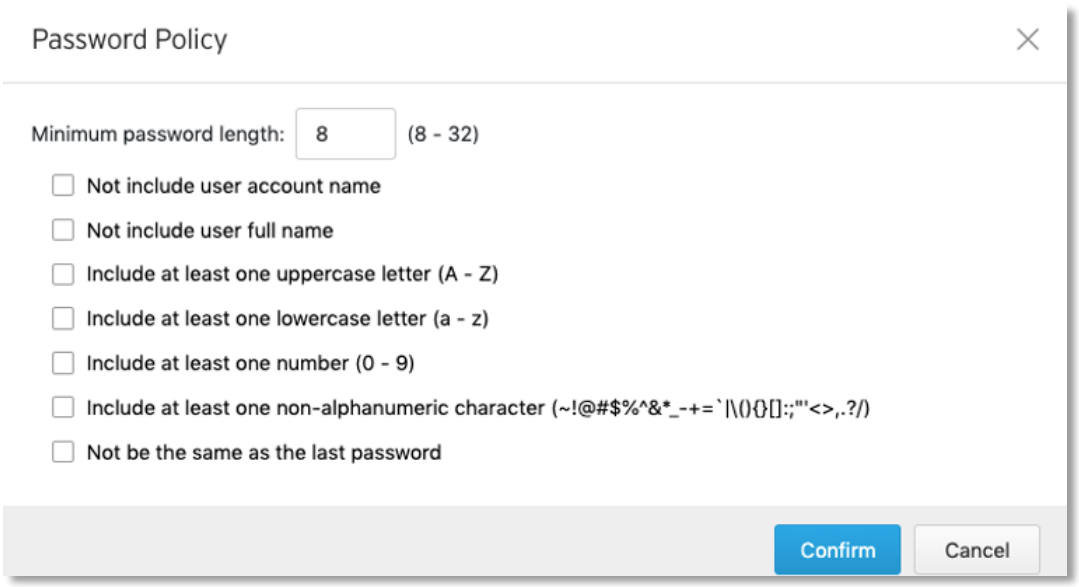
1. On the management console banner, click your account name.
2. Click [Change Password].
   The Change Password screen will appear.
3. Specify the password settings.
   - Old password
   - New password
   - Confirm password
4. Click [Save].

Password Complexity

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



The available configuration options show as the following:



ID/Password Reset

In some specific situations, for security reasons, users are required to reset their ID or password in their next log on session.

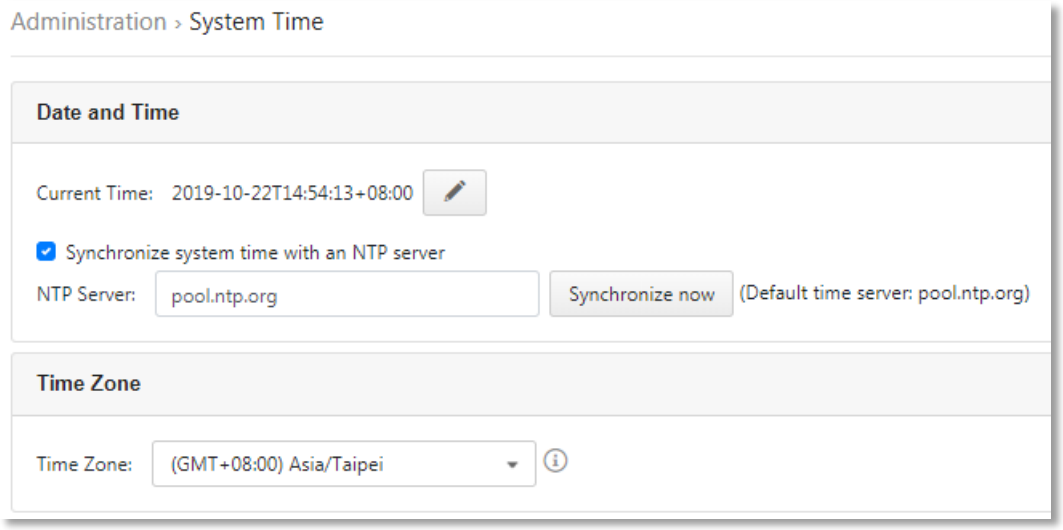
	Scenario	
User Roles	**First Time Log on**	**Password Changed By Admin**
Admin	Reset ID / Password	
Auditor	Reset ID / Password	Reset Password
Operator	Reset Password	Reset Password
Viewer	Reset Password	Reset Password

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

Note: The ODC system synchronizes the system time with its managed nodes.

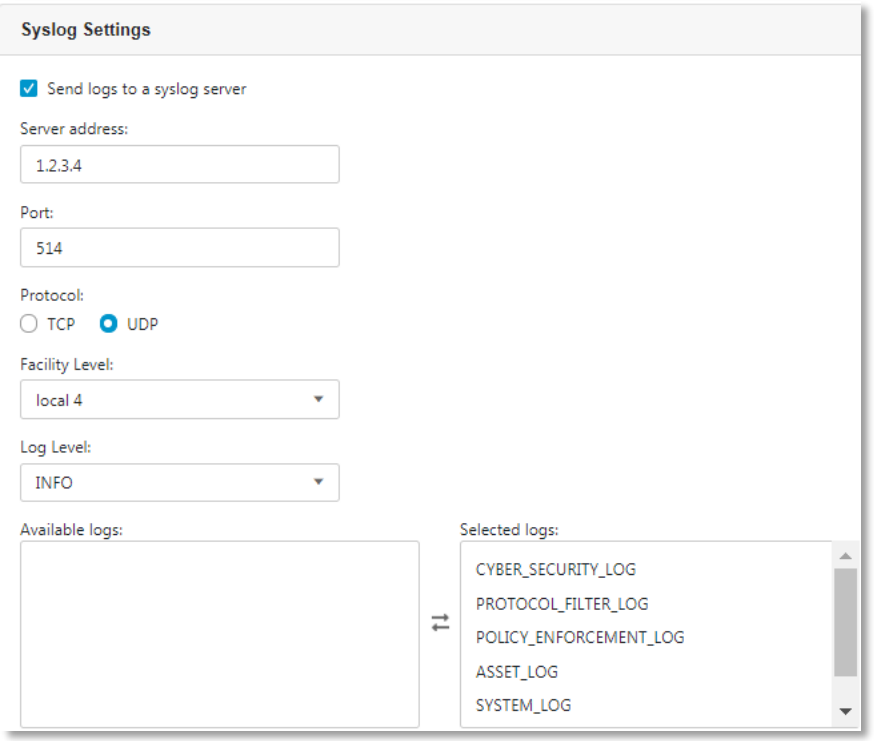
Configuring Syslog Settings

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

Field	Description
Server address	Type the IP address of the syslog server.
Port	Type the port number.
Protocol	Select the protocol for the communication.
Facility level	Select a facility level to determine the source and priority of the logs.
Severity level	Select a syslog severity level. 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 58*.

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

Syslog Severity Levels

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

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

Syslog Severity Level Mapping Table

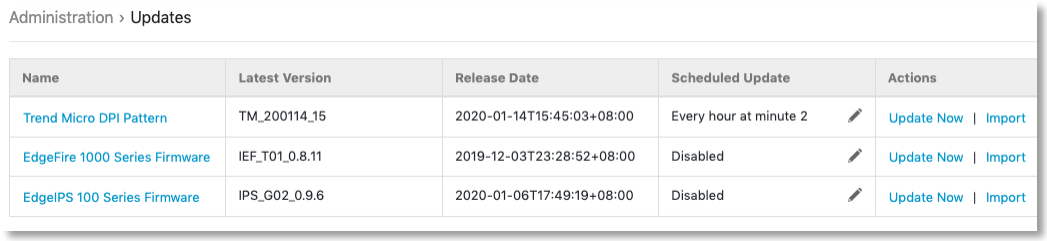
The following table summarizes the logs of Policy Enforcement/Protocol Filter/Cyber Security and their equivalent Syslog severity levels.

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

Updates

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

Update components to immediately download the 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 22*.



Components

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

Field	Description
Trend Micro DPI Pattern	Contains signatures to enable the following features: ▪ Intrusion prevention Detects and prevents behaviors related to network intrusion attempts and targeted attack at the network level.
EdgeFire 1000 Series Firmware	EdgeFire™ firmware
EdgeIPS 100 Series Firmware	EdgeIPS™ firmware

Note: 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 on the ODC system.
- Manual import of components: You can manually import components on the ODC system.
- Scheduled updates: The ODC system automatically downloads the latest components from an update source based on a schedule.

Note: The updated components are deployed to managed nodes based on the settings of the [Node Management] tab.

Note: 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 on the ODC system. When a component update is complete, ODC system deploys the updated components to managed nodes based on the settings of the [Node Management] screens.

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 [Latest Version] and [Release Date] column will be updated or keep the same if it is already up-to-date.

Importing a Component File

If you are provided 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 of the [Node Management] screens.

Procedure

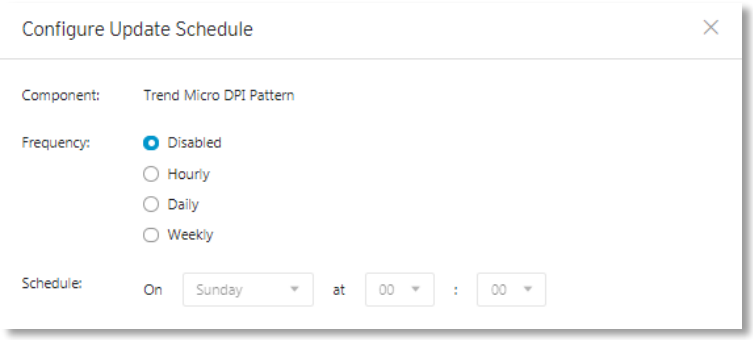
1. Go to [Administration] > [Updates].
2. Click [Import] for the component.
3. Select the component file.
4. Click [Open] to start the import process.

Scheduling Component Updates

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

Procedure

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



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

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

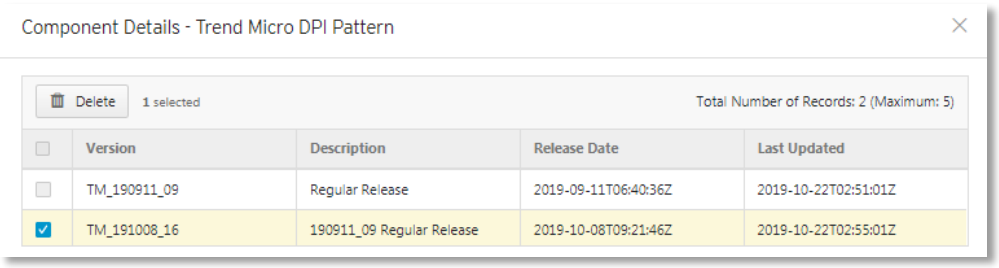
Managing the Component Repository

All the imported or updated components are maintained on the component repository. You can

view and manage the available components on 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 on the repository.



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

Importing an SSL Certificate

The ODC system uses the HTTPS protocol to encrypt web traffic between the user's web browser and the web management console. The HTTPS protocol uses an SSL certificate signed by TXOne. 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 for the certificate file.
   c. Input the passphrase if the certificate requires one.
   d. Click [Import] and then [Restart].

Verifying an SSL certificate

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

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

Removing the Built-In Certificate

You can optionally choose to remove the built-in certificate:

1. Go to [Administration] > [SSL Certificate].
2. Click [Remove Certificate].
   A [Remove Certificate] window will appear.
3. Click [Remove and Restart].
   A self-signed certificate will be used after the built-in certificate is removed.

Log Purge

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

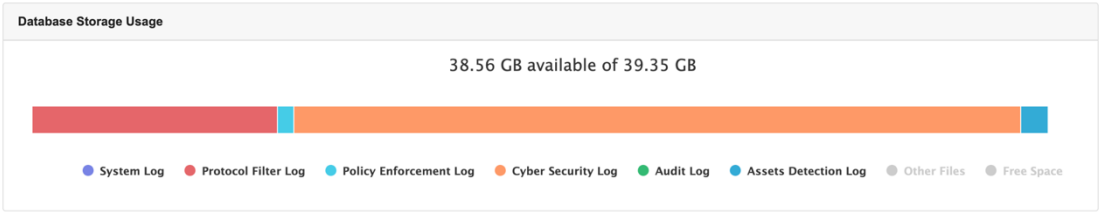
- Viewing the status of the logs stored in the ODC system
- Setting up purge criteria for automatic log purge
- Manually purging the logs that match a given condition

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

1. Go to [Administration] > [Log Purge].
   The [Database Storage Usage] pane shows the used and total size of database.



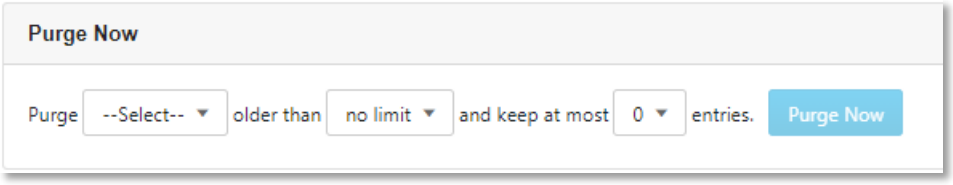
Configuring Automatic Log Purge

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.)

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.



Note: 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.

Backing Up a Configuration

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

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

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].

All services will restart. It can 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.

Note: Log onto the management console using the administrator account o access the License tab.

Introduction to the Licenses

Three license types are used for ODC:

- Node License
- EdgeFire Software License
- EdgeIPS Software License

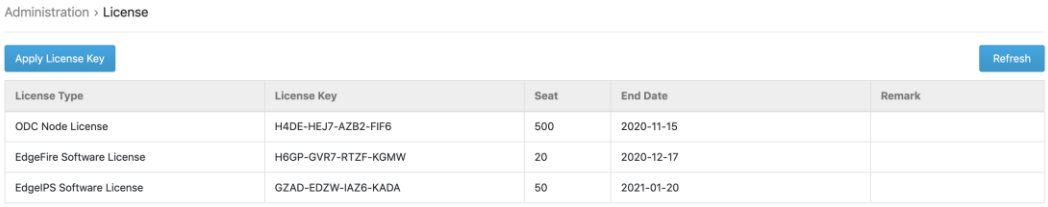
Node license - Determines the maximum number of nodes to be managed by ODC.

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

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 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.



Viewing Your Product License Information

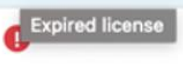
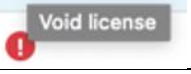
Procedure

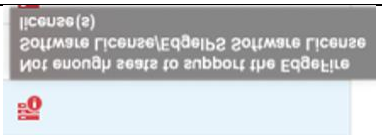
1. Go to [Administration] > [License].
   The [License] tab will appear.

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.

Message	Icon	Description
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.

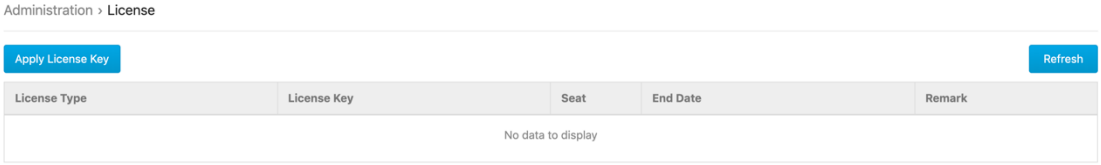
Message	Description
The license (xxx-xxx-xxx-xxx) expires in xx days. To continue using all features, specify a new license key.	30 days before the license expiration date, this message will pop up.
The license (xxx-xxx-xxx-xxx) has expired. You will stop receiving product updates and technical support in xx days. To continue using all features, specify 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, specify a valid 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 nodes managed, the nodes will not able to update their patterns and firmware. Alert messages will also pop up on the web management console.

Activating or Renewing Your Product License

Procedure

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



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].

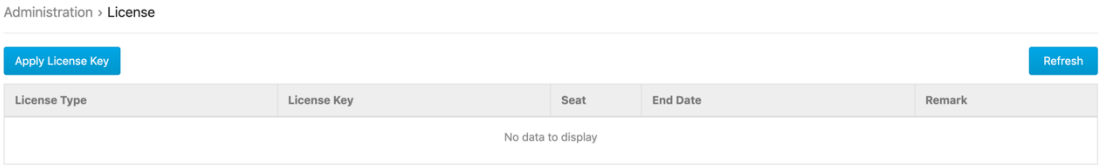
Note: Internet access is needed for ODC when applying the license key. Specifically, the ODC system will need to visit odc.cs.txone-networks.com via HTTPS in order to register the license key and retrieve the license information.

Manually Refresh 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 via a single button.

Procedure

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



2. Click the [Refresh] button.

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

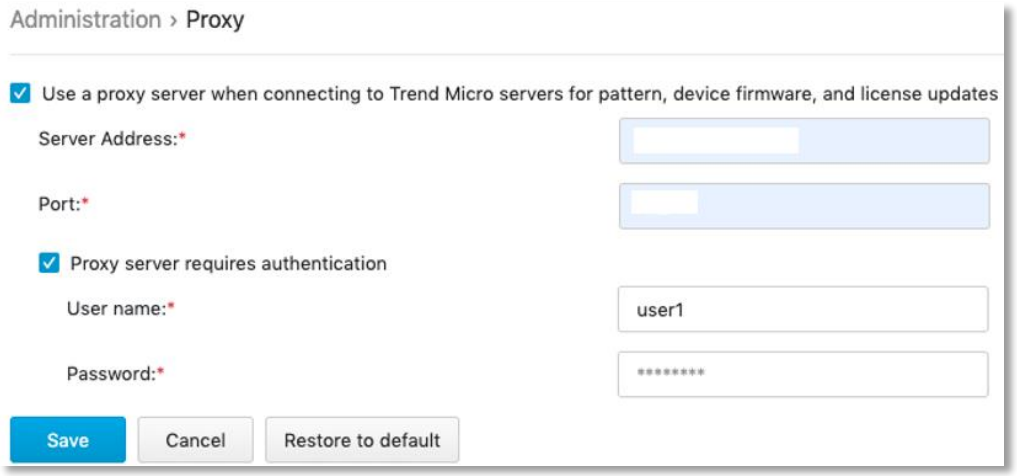
Proxy

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

Configuring Proxy Settings

Procedure

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



2. Click [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.

Technical Support

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

The Trend Micro Support Portal is a 24-7 online resource that contains 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 the 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.

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

A Trend Micro support engineer will investigate the case and respond in 24 hours or less.

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

Speeding Up the Support Call

To improve problem resolution, have the following information 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

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

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 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
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 ODC's Connection via EdgeFire or EdgeIPS' Web Console

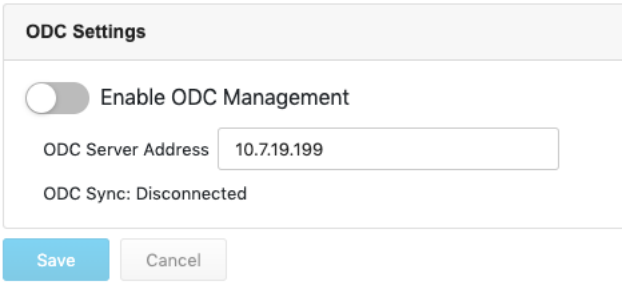
A node is an entity of Edge Series product that is managed by the ODC. A managed node can be configured by ODC and send event logs to ODC. Enable the node to connect with ODC.

Procedure

1. Open the node's web console.
2. Enter your logon credentials (user name and password).

   Use the default administrator logon credentials if it's first time logging in:

   - User name: `admin`
   - Password: `txone`
3. Go to [Administration] > [Sync Settings].



4. Specify the IP v4 address of ODC in [ODC Server Address].
5. 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 into vShell

When you want to open vShell, you can do so as follows:

1. Local machine
2. Remote machine over SSH

The default administrator credentials are:

- User: root
- Password: txone

Change Default Password to Activate

First signing in to vShell, you will see the WARNING messages.

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

Note: The password field will only accept alphanumericals with some additional characters: !@#%^* +}:?~[]'./

Note: Note: The length is between 8 and 32 characters.

```
Type the new password:
```

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
```

Below, the part in the square brackets 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
```

Update 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.

```
This saved in the configuration file, noticed that the setting eth0 does not
take effect currently, so just check it:
$ 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:

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

```
$ iface restart eth0
Successfully restart! Please check the network status
```

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 are changed. Please restart interface
```

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

```
$ iface trim eth0 address

Interface settings are changed. Please restart interface
$ iface trim eth0 gateway
Interface settings are changed. Please restart interface
$ iface trim eth0 netmask
Interface settings are 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:

Note: Please retype `iface ls` to check that the interface has successfully come back up.

```
$ iface restart eth0
Successfully restart! Please check the network status
```

How to Set Up ACL

vShell provides the Allowlisting to block all clients who are not on the Allowlist.

Three modules to limit:

- SSH: Manage SSH server connection privileges.
- Device: Manage EdgeIPS or EdgeFire connection privileges.
- Web: Manage users’ dashboard connection privileges.

Querying the Status

Obtain the active status, the port number and IP/CIDR in the Allowlist.

$ access-list ls

```
SSH(tcp:22)
Status: Disabled
Network
```

```
Device(udp:123, tcp:7590, tcp:9093)
Status: Enabled
Network
1.1.1.1/32

Web(tcp:443)
Status: Disabled
Network
```

Adding Clients to the Allowlist

You can add client IPs or Classless Inter-Domain Routing (CIDR).

```
$ access-list append SSH 1.1.1.1
added! Please check the Allowlist
$ access-list append SSH 1.1.1.0/24
1.1.1.0/24 added! Please check the Allowlist
```

Deleting Clients from the Allowlist

You can delete client IPs or Classless Inter-Domain Routing (CIDR).

```
$ access-list trim SSH 1.1.1.1
removed! Please check the Allowlist
$ access-list removed SSH 1.1.1.0/24
1.1.1.0/24 removed! Please check the Allowlist
```

Enable/Disable 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 Allowlist. If clients are not added before ACL is enabled, all clients will be blocked from connecting. If clients are not added to the Allowlist before ACL is enabled, it will be necessary for the administrator to edit the Allowlist directly.

```
$ access-list up Device
Device enabled! Please check the Allowlist
$ access-list down Device
Device disabled! Please check the Allowlist
```

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

Commands	Description
access-list	Manage the IP Allowlists.
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.

access-list

Manage the IP Allowlists.

SSH: Manage the connections to the SSH server granting.
Device: Manage the IPS or IEF connections granting.
Web: Manage the dashboard user connections granting.

ls - List all ip in the Allowlists.

```
$ access-list ls
```

append - Append an IP/CIDR to the Allowlist.

```
$ access-list append Device 192.168.1.1
$ access-list append Device 192.168.0.0/16
```

trim - Delete an IP/CIDR from the Allowlist.

```
$ access-list trim Device 192.168.1.1
$ access-list trim Device 192.168.0.0/16
```

up - Be enabled to Allowlist ip address.

```
$ access-list up Device
```

down - Be disabled to Allowlist ip address.

```
$ access-list down Device
```

env

Manage system environment variables.

hostname - Assign /etc/hostname value

Note: Note: Length should be between 1 and 64.

```
$ env hostname NAME
```

exip - Assign /acus/external_ip value

Note: Note: “default” is equal to the eth0 IP address.

```
$ env exip 192.168.1.1
$ env exip default
```

ls - List the environment variable in this server.

Note: Note: “Not Set” of the External IP term means the eth0 IP address.

```
$ env ls
Hostname:       my-dashboard-server
ID:             55365266-108d-11ea-bca4-080027171302
Web Version:    1.0.0
External IP:    Not Set
```

exit

Exit this shell.

```
$ exit
```

help

List all commands

```
$ help
vShell, version v1.0.0
The commands provided in:
access-list     Manage the IP Allowlists
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: Please 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 addr`.

```
$ iface ls
```

add - Add the interface in /etc/network/interfaces, if the interface name is not repeated

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 and shut down the interface from /etc/network/interfaces

```
$ iface rm INTERFACE
```

up - Activate the interface in /etc/network/interfaces

Options

--force

```
$ iface up INTERFACE

// you can force it up, if needed
$ iface up eth0 --force
```

down - Deactivate the interface in /etc/network/interfaces

Options

--force

```
$ iface down INTERFACE

// you can force it down, if needed
$ iface down eth0 --force
```

restart - Deactivate and then active 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

```
$ resolv add NAMESERVER
```

replace - Replace the dns in the /etc/resolvconf/resolv.conf.d/tail

```
$ resolv replace OLD_NAMESERVER NEW_NAMESERVER
```

trim - Remove the dns from the /etc/resolvconf/resolv.conf.d/tail

```
$ 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 - 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:
```