

User's Guide

TRENDNET®



12-Port Gigabit PoE+ Smart Surveillance Switch 18-Port Gigabit PoE+ Smart Surveillance Switch

TPE-3012LS / TPE-3018LS

Contents

Product Overview	1
Package Contents	1
Features	2
Product Hardware Features.....	3
Application Diagram	6
Switch Installation	7
Desktop Hardware Installation	7
Rack Mount Hardware Installation.....	7
Basic Installation	8
Connect additional devices to your switch.....	10
Access your switch management page.....	11
Saving configuration and switch between web modes	11
Saving configuration changes to NV-RAM.....	11
Switching between Standard and Surveillance Mode web interfaces	12
Surveillance Mode Web Interface.....	13
Dashboard	13
Status	13
Overview	14
Port Info	15
IP Camera Info	15
NVR Info.....	16
PoE Info.....	16
PoE Scheduling.....	17
Time	19
Clock Settings.....	19
SNTP Settings	19
Surveillance Settings.....	21

IP Settings	21
SNMP Host Settings	21
Log Server	22
Password Settings.....	23
Mail Alert.....	23
PD Alive Check.....	24
ONVIF.....	25
Discovering and authorizing ONVIF compliant devices	25
Applying IP address settings to ONVIF authorized devices	26
Changing the ONVIF device administrator password.....	28
Creating new ONVIF users in the ONVIF device	29
Upgrade ONVIF device firmware.....	30
E-map Management	31
Tools	33
View Firmware Information.....	33
Firmware Upgrade and Backup	33
Backup/Restore switch Configuration	35
Reset switch to factory default.....	36
Reboot switch	36
Standard Mode Web Interface	37
Status.....	37
View your switch system information	37
System Information	37
View your switch logging messages	38
View your switch port status information	39
View link aggregation status.....	41
View the MAC address table	41
Network.....	42
Set your IPv4 settings	42
Set your IPv6 settings	43
Set the switch date and time.....	45
Set the web management idle timeout.....	46
Port.....	47

Configure your switch ports and view port status.....	47	Spanning Tree (STP, RSTP, MSTP).....	77
Enable long-range PoE mode on PoE ports	48	Configure Spanning Tree Protocol settings	77
Configure Error Disabled port state.....	49	Configure Spanning Tree Protocol Port settings.....	79
Configure Trunk/Link Aggregation settings	50	Configure Spanning Tree Protocol MST settings (MSTP).....	80
Configure port power savings.....	52	Configure Spanning Tree Protocol MST Port settings (MSTP).....	82
Enable jumbo frame support.....	53	View your Spanning Tree Protocol Instance Statistics Information (MSTP)	83
ONVIF.....	54	LLDP (Link-Layer Discovery Protocol)	83
Discovering and authorizing ONVIF compliant devices	54	Configure LLDP settings	83
Applying IP address settings to ONVIF authorized devices.....	55	Configure LLDP Port Settings	84
Changing the ONVIF device administrator password	56	View LLDP Packet View Detail	85
Creating new ONVIF users in the ONVIF device	57	View LLDP Local Information	86
Upgrade ONVIF device firmware	58	View LLDP Neighbors.....	87
PoE (Power over Ethernet).....	59	View LLDP Statistics Counters.....	87
Enable or disable PoE.....	59	View LLDP Neighbor Information	89
PoE Scheduling.....	60	Multicast.....	90
PD Alive Check	61	Configure unknown multicast and multicast forwarding method	90
VLAN	62	Add static multicast group addresses.....	91
Add, modify, and remove VLANs	62	Add multicast router ports	92
Modify VLAN Port Membership.....	64	Configure IGMP snooping settings	93
Modify VLAN port settings.....	65	Configure IGMP snooping settings for IPv4 multicast traffic.....	93
Voice VLAN	66	Configure multicast querier settings	95
Create a Voice VLAN	67	View IGMP snooping statistics.....	96
Configure Voice VLAN OUI settings	69	Configure MLD snooping settings.....	97
MAC VLAN.....	70	Configure MLD snooping settings for IPv6 multicast traffic.	97
Create MAC-based VLAN groups	70	View MLD snooping statistics.....	99
Configure MAC VLAN group binding.....	71	Configure MVR settings	100
Surveillance VLAN	72	Configure MVR port settings	101
Create a Surveillance VLAN.....	73	Configure MVR Group Address Table	102
Configure Surveillance VLAN OUI settings.....	74	Security.....	103
MAC Address Table.....	75	Configure RADIUS settings.....	103
View the switch MAC address table	75	Configure RADIUS network authentication settings.....	105
Add static MAC address entries.....	75	Configure RADIUS network port settings	107
Add MAC Addresses used in filtering.....	76	View authenticated sessions	109
		Configure Management Access	110
		Configure Management ACL/ACE (Access Control Lists/Access Control Entries)	112
		

Create new access control list	112
Configure Port Security	114
Configure Protected Ports	115
Configure Storm Control	116
Denial of Service (DoS)	117
DHCP Snooping	119
View DHCP Snooping Statistics	120
Configure DHCP Option 82 settings	121
Configure DHCP Option 82 Circuit ID settings	123
Configure IP Source Guard	124
Configure IP Source Guard IMPV Binding	125
Save DHCP Snooping Database	126
ACL	127
Configure MAC ACL	127
Configure MAC ACE	128
Configure IPv4 ACL	130
Configure IPv4 ACE	131
Configure ACL Port Binding	134
QoS	136
Configure QoS Global Settings	136
Configure Queue Scheduling	137
Configure CoS Mapping	138
Configure IP Precedence Mapping	139
Configure Rate Limiting per port	140
Diagnostics	142
Configure Logging	142
Configure Remote Logging/Syslog Server	143
Configure Port Mirroring	144
Ping Test	145
Ping Watchdog	146
Traceroute	147
Copper Test	147
Fiber Module	148
UDLD	149
View UDLD Neighbors	151
Management	152
Modify admin password and create new users	152
Upgrade switch firmware	153
Backup/Restore switch Configuration	154
Save switch configuration to NV-RAM / Restore to default	156
SNMP	157
Configure the SNMP View Table	157
Configure the SNMP Group Table	158
Configure the SNMP Community Table	159
Configure the SNMP Users	160
Set the SNMP Engine ID	162
Configure the SNMP Trap Management	163
Configure the SNMP Notification	164
RMON	165
View RMON Statistics	165
Configure RMON History Table	167
Configure RMON Event Table	168
Configure RMON Alarm Table	169
Create Schedules	171
Technical Specifications	172
Troubleshooting	177
Appendix	178

Product Overview



TPE-3012LS



TPE-3018LS

Package Contents

In addition to your switch, the package includes:

- Quick Installation Guide
- Power cord (1.5m/5 ft.)
- Rackmount kit

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's Gigabit PoE+ Smart Surveillance Switch series is designed to simplify the installation and management of surveillance networks, especially for integrators and installers. These ONVIF switches are optimized for the surveillance industry; surveillance mode provides a graphical dashboard interface with detailed information about the switch and each connected PoE device. Connect ONVIF compliant IP cameras and NVRs for more advanced capabilities such as changing device IP settings, and to view individual IP camera video within the switch GUI. The Smart Surveillance Switches are also PoE self-healing switches featuring PoE device auto-recovery and power scheduling.

Installers and integrators can save on equipment costs and reduce installation time with TRENDnet's Gigabit PoE+ Smart Surveillance Switches by delivering up to 30W per port of PoE power and data over existing Ethernet cables. Available PoE port controls include enabling and disabling PoE, PD alive check, and power scheduling. PD alive check is an automated PoE self-healing switch feature that attempts to recover an unresponsive PoE device connected to the switch. If a PoE device such as a PoE camera becomes unresponsive to pings, the ONVIF compliant switch will auto-reboot the PoE port in an attempt to recover the device.

These PoE+ ONVIF switches feature a 4-digit LED display showing total PoE power, available power, and power-per-port. They also support long distance PoE+ networking up to 656 ft./200m away at speeds up to 10Mbps. TRENDnet's Gigabit PoE+ Smart Surveillance Switches also feature SFP slots to support long-distance fiber networking applications.

Advanced managed switch features include LACP to group ports to increase bandwidth between switches, VLANs for segmenting and isolating virtual LAN groups, QoS for traffic prioritization, port bandwidth controls, and SNMP monitoring, making this ONVIF switch a powerful SMB network solution. Improve voice performance by isolating and prioritizing VoIP traffic from normal data traffic with the easy-to-use voice VLAN feature.

Hardware Design

Provides gigabit PoE+ ports, SFP slots for fiber connectivity, and a 1U 19" rackmount design with brackets included

PoE Power

Each PoE+ managed ONVIF switch supplies up to 30W of power per port and data over a single Ethernet cable to PoE devices

Surveillance Mode

ONVIF switches are optimized for the surveillance industry, providing a graphical dashboard interface with useful information about the switch and each connected device

Troubleshooting

Real-time traffic comparison charts, error group charts, and a convenient cable diagnostic test aid in rapid troubleshooting.

Long Range PoE+

Long distance PoE+ networking up to 656 ft./200m away at speeds up to 10Mbps

4-Digit PoE LED Display

4-digit 7-segment LED display to view total power, available power, and power-per-port

IPv6 Ready

ONVIF switches support IPv6 configuration and IPv6 neighbor discovery

Traffic Management

Managed switch features include: Link aggregation, 802.1Q VLAN, Voice VLAN, Surveillance VLAN, RSTP, MSTP, Loopback Detection, QoS, and port bandwidth management

Troubleshooting

A convenient cable diagnostic test and traffic statistics aid in network troubleshooting

Monitoring

RMON, SNMP, and Port Mirroring support administrator monitoring solutions

Product Hardware Features

TPE-3012LS

Rear View



AC Power Connector

- **AC Power Connector** – Connect the AC power cord to the connector and the other side into a power outlet. (Input: 100~240VAC, 50/60Hz)

Front View



4-Digit Display Reset Button Diagnostic LEDs PoE+ Gigabit Ports Gigabit Ports SFP Slots

- **4-Digit 7-Segment Display** - Displays total power, available power, and power consumption per port using the toggle button.
- **Reset Button** – Press and hold this button for 10 seconds and release to reset the switch to factory defaults.
- **PoE+ Gigabit Ports (1-8)** – Connect PoE and non-PoE network devices.
- **Gigabit Ports (9-10)** – Connect non-PoE devices or uplinks.
- **SFP Slots (11-12)** – Supports optional 100BASE-SX/LX mini-GBIC modules.

• **Diagnostic LED Indicators**

SYS LED

On	:	The device is receiving power.
Blinking	:	The device is booting up.
Off	:	The device powered off or not receiving power.

PoE Alert

On	:	When reaching near the max PoE power budget provided 100W or above, the LED will turn on to indicate that PoE power consumption is near max. budget available.
Off	:	When the PoE power provided is below the 100W PoE power budget.

PoE+ Gigabit Ports (1-8)

On	:	When the Link/ACT LED lights on, the respective port is successfully connected to an Ethernet network.
Green/Amber	:	Green indicates the link is connected at 1000Mbps. Amber indicates the link is connected at 10/100Mbps.
Blinking	:	When the Link/ACT LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	:	No link.

PoE (Power over Ethernet)

Green	:	When the PoE powered device (PD) is connected and the port supplies power normally.
Off	:	No PoE powered device (PD) connected or unplugged the PoE output port.

Gigabit Ports (9-10)

On	:	When the Link/ACT LED lights on, the respective port is successfully connected to an Ethernet network.
Green/Amber	:	Green indicates the link is connected at 1000Mbps. Amber indicates the link is connected at

	10/100Mbps.
Blinking	: When the Link/ACT LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	: No link.

SFP Slots (11-12)

Green on	: When the mini-GBIC Green LED lights on, the respective port is inserted mini-GBIC Gigabit module.
Green blinking	: When the mini-GBIC Green LED is blinking, the port is transmitting or receiving data on the Gigabit network.
Amber on	: When the mini-GBIC Amber LED lights on, the respective port is inserted mini-GBIC 100Mbps module.
Amber blinking	: When the mini-GBIC Amber LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	: No link

TPE-3018LS

Rear View



AC Power Connector

- **AC Power Connector** – Connect the AC power cord to the connector and the other side into a power outlet. (Input: 100~240VAC, 50/60Hz)

Front View



4-Digit Display

Reset Button

Diagnostic LEDs

PoE+ Gigabit Ports

Gigabit Ports

SFP Slots

- **4-Digit 7-Segment Display** - Displays total power, available power, and power consumption per port using the toggle button.
- **Reset Button** – Press and hold this button for 10 seconds and release to reset the switch to factory defaults.
- **PoE+ Gigabit Ports (1-16)** – Connect PoE and non-PoE network devices.
- **Gigabit Ports (17-18)** – Connect non-PoE devices or uplinks. Disabled if SFP slots 17F or 18F are used.
- **SFP Slots Shared (17F-18F)** – Supports optional 1000BASE-SX/LX mini-GBIC modules.

- Diagnostic LED Indicators

SYS LED

On	: The device is receiving power.
Blinking	: The device is booting up.
Off	: The device powered off or not receiving power.

PoE Alert

On	: When reaching near the max PoE power budget provided 200W or above, the LED will turn on to indicate that PoE power consumption is near max. budget available.
Off	: When the PoE power provided is below the 200W PoE power budget.

PoE+ Gigabit Ports (1-16)

On	: When the Link/ACT LED lights on, the respective port is successfully connected to an Ethernet network.
Green/Amber	Green indicates the link is connected at 1000Mbps. Amber indicates the link is connected at 10/100Mbps.
Blinking	: When the Link/ACT LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	: No link.

PoE (Power over Ethernet)

Green	: When the PoE powered device (PD) is connected and the port supplies power normally.
Off	: No PoE powered device (PD) connected or unplugged the PoE output port.

Gigabit Ports (17-18)

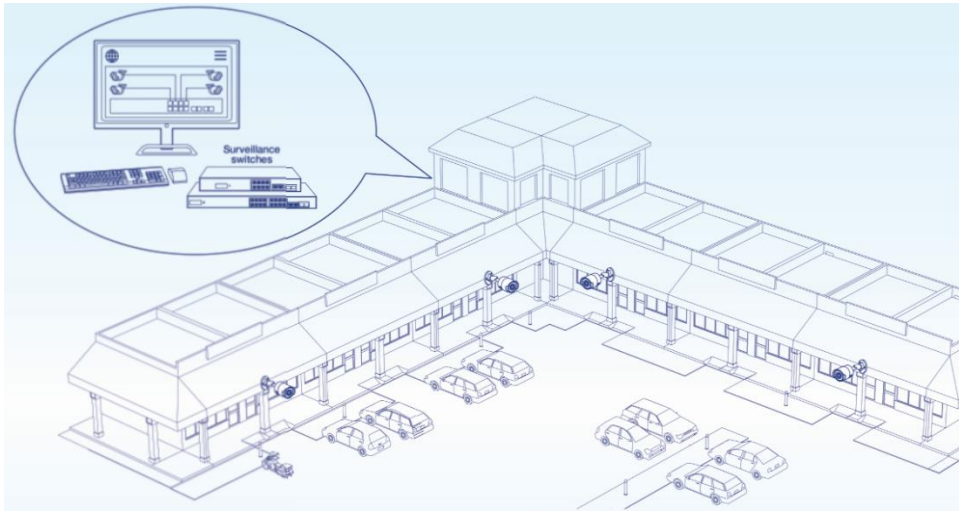
On	: When the Link/ACT LED lights on, the respective port is successfully connected to an Ethernet network.
Green/Amber	Green indicates the link is connected at 1000Mbps. Amber indicates the link is connected at

	: 10/100Mbps.
Blinking	: When the Link/ACT LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	: No link.

SFP Slots Shared (17F-18F)

Green on	: When the mini-GBIC Green LED lights on, the respective port is inserted mini-GBIC Gigabit module.
Green blinking	: When the mini-GBIC Green LED is blinking, the port is transmitting or receiving data on the Gigabit network.
Amber on	: When the mini-GBIC Amber LED lights on, the respective port is inserted mini-GBIC 100Mbps module.
Amber blinking	: When the mini-GBIC Amber LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	: No link

Application Diagram



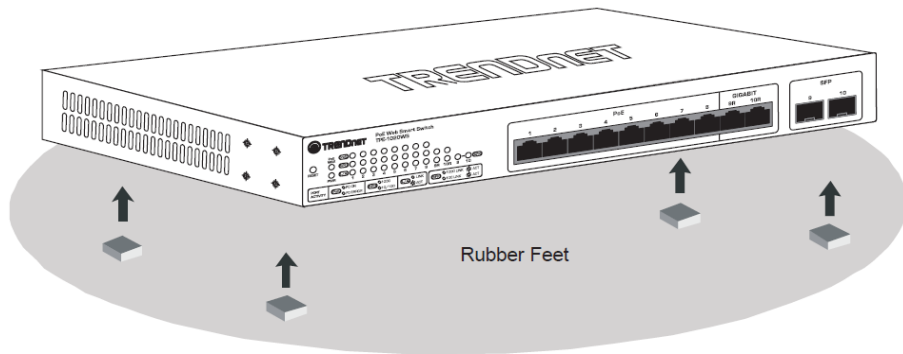
The Gigabit PoE+ Surveillance Switches are installed and providing PoE/PoE+ and data connectivity to the PoE surveillance IP cameras. The surveillance switches also offer additional management features via the ONVIF protocol and other self-healing features such as PD alive check to automatically recover PoE devices or reboot the switch if the PoE devices are unresponsive. The switches connect to your network through the non-PoE Gigabit Ethernet uplink port or SFP fiber to a switch that is connected to your network.

Switch Installation

Desktop Hardware Installation

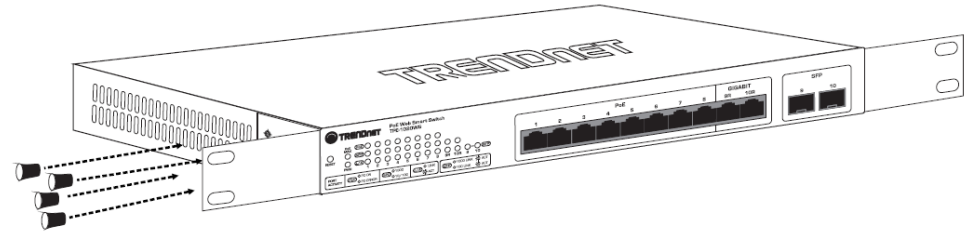
The site where you install the hub stack may greatly affect its performance. When installing, consider the following pointers:

- Install the Switch in a fairly cool and dry place.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Switch on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of each device. The rubber feet cushion the hub and protect the hub case from scratching.

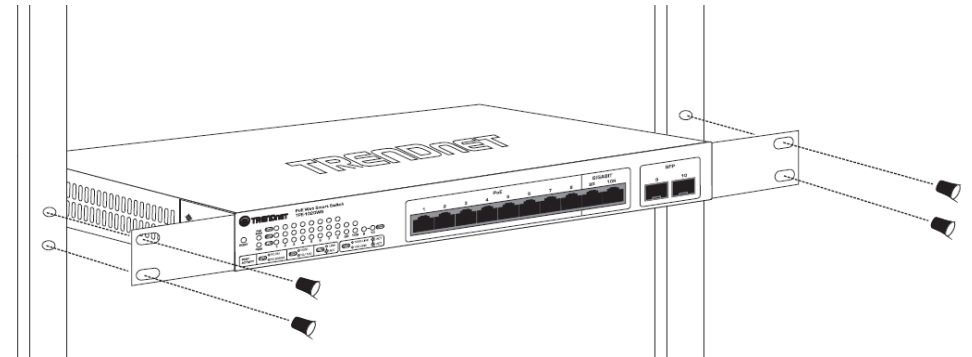


Rack Mount Hardware Installation

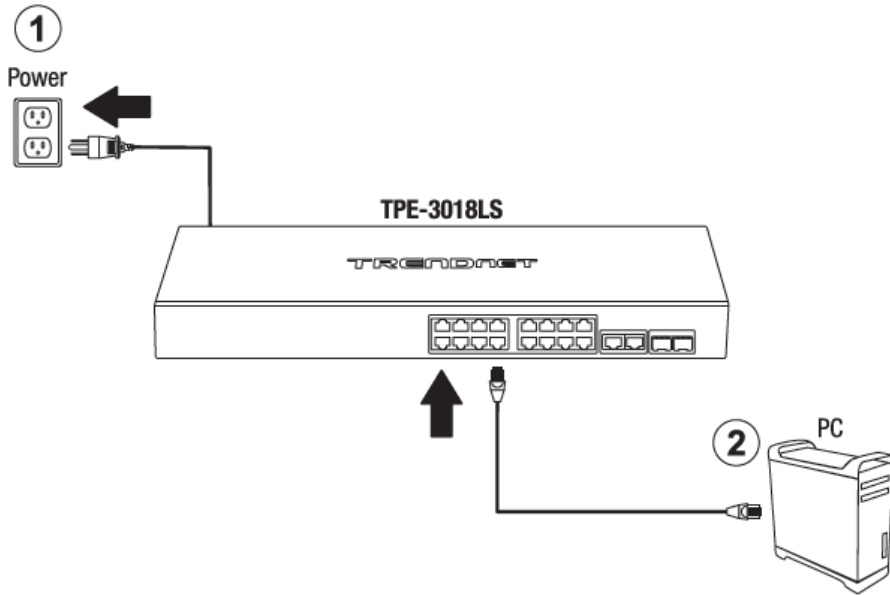
The switch can be mounted in an EIA standard-size, 19-inch rack, which can be placed in a wiring closet with other equipment. Attach the mounting brackets at the switch's front panel (one on each side), and secure them with the provided screws.



Then, use screws provided with the equipment rack to mount each switch in the rack.



Basic Installation



. Assign a static IP address to your computer's network adapter in the subnet of 192.168.10.x (e.g. 192.168.10.25) and a subnet mask of 255.255.255.0.

4. Open your web browser, and type the IP address of the switch in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.



5. Enter the User Name and Password, and then click **Login**. By default:

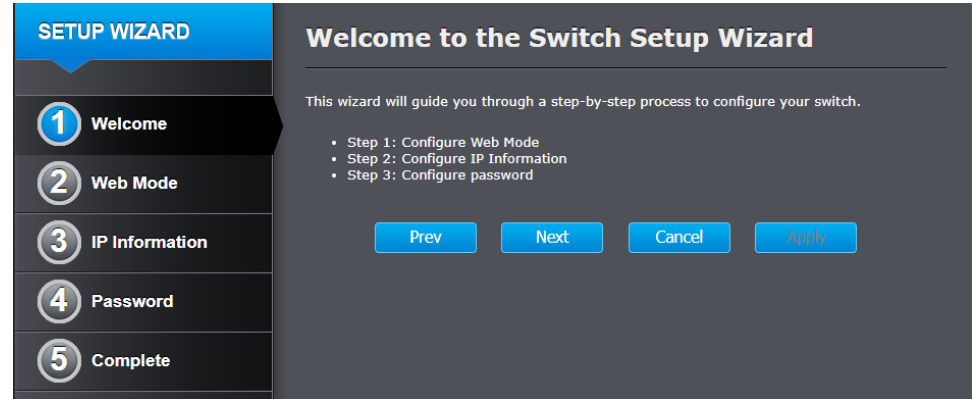
User Name: **admin**

Password: **admin**

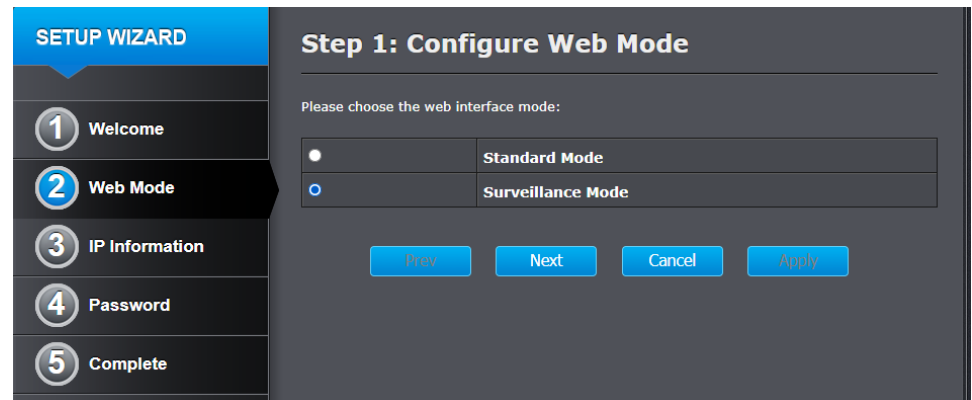
Note: User name and password are case sensitive.

Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="....."/>
<input type="button" value="LOGIN"/>	

6. On the Setup Wizard page, click **Next**.



7. For the web interface mode, select **Surveillance Mode** and click **Next**.



8. For the IP address information, configure the switch to match the requirements of your network by entering the appropriate IP Address, Subnet Mask, and Default Gateway settings, then click **Next**.

Note: You may need to modify the static IP address settings of your computer's network adapter to IP address settings within your subnet to regain access to the switch.

SETUP WIZARD

Step 2: Configure IP Information

The wizard will help to complete settings for IP address, Netmask, and Gateway.

Static DHCP

IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1

Prev Next Cancel Apply

9. Create a new administrator password for management access to the switch by entering a new password in the fields provided, then click **Next**.

SETUP WIZARD

Step 3: Configure password

Set up the password for authorized access.

Password	<input type="password"/>
Verify Password	<input type="password"/>

Prev Next Cancel Apply

10. On the final setup wizard page, you can check the “Ignore the wizard next time” option to prevent the setup wizard prompt from appearing at the next login to the web management interface, then click **Apply**.

SETUP WIZARD

Setup Complete!

The Switch Setup Wizard is complete. Click the Apply button to save and apply your settings.

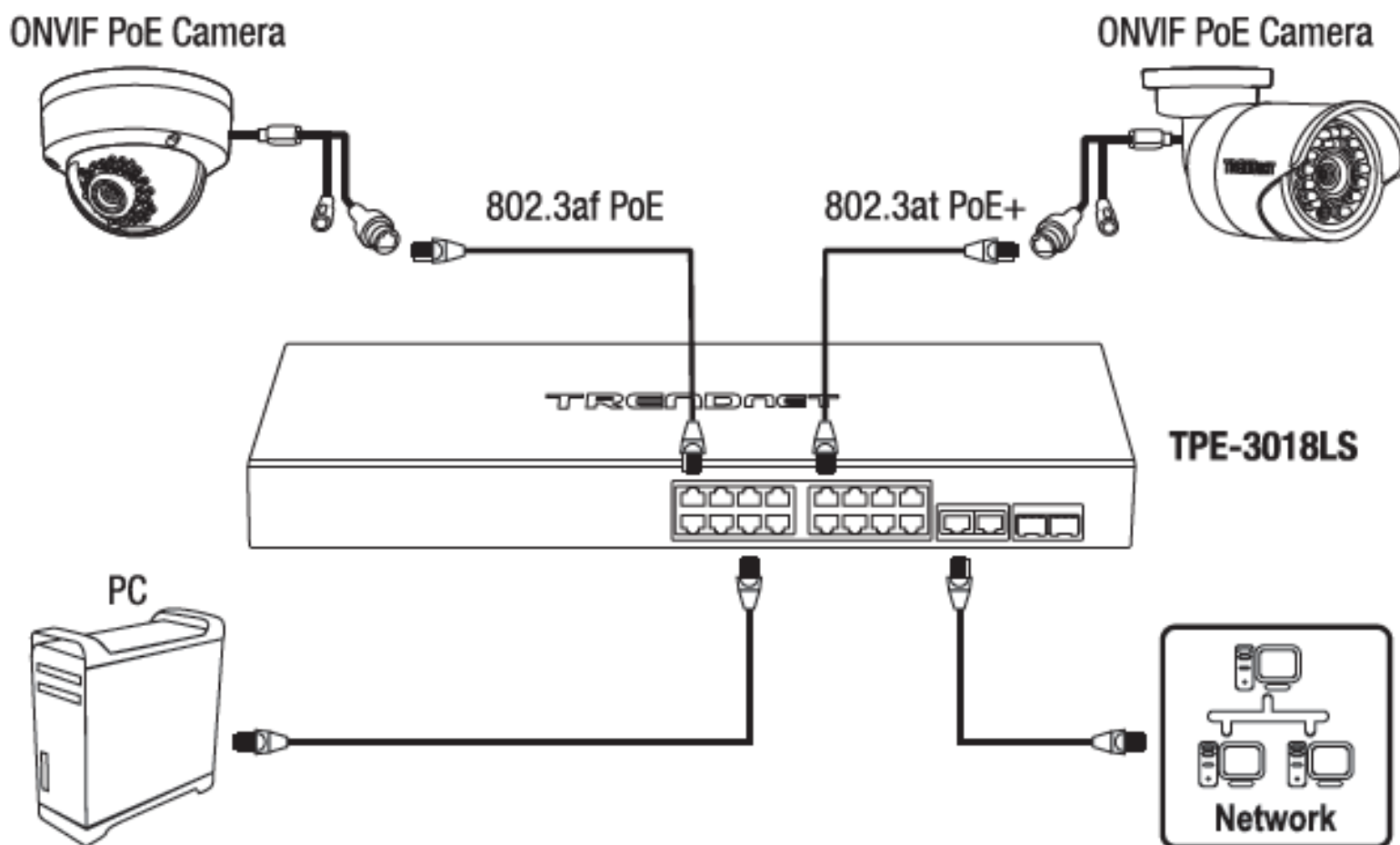
Ignore the wizard next time

Prev Next Cancel Apply

Connect additional devices to your switch

You can connect additional computers or other network devices PoE (Power over Ethernet) or non-PoE devices to your switch using Ethernet cables to connect them to one of the available PoE+ Gigabit Ports (TPE-3012LS PoE+ ports 1-8 / TPE-3018LS PoE+ ports 1-16) or Gigabit ports (TPE-3012LS Gigabit ports 9-10 / TPE-3018LS Gigabit ports 17-18). Check the status of the LED indicators on the front panel of your switch to ensure the physical cable connection from your computer or device.

Note: If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured properly within the network subnet your switch is connected. The switch model may be different than the one shown in the example below.



Access your switch management page

Note: Your switch default management IP address <http://192.168.10.200> is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.

1. Open your web browser and go to the IP address <http://192.168.10.200>. Your switch will prompt you for a user name and password.



2. Enter the user name and password. By default:

User Name: **admin**

Password: **admin**

Note: User Name and Password are case sensitive.

Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••"/>
<input type="button" value="LOGIN"/>	

Saving configuration and switch between web modes

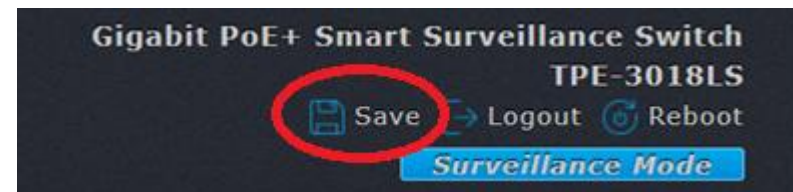
Saving configuration changes to NV-RAM

After applying configuration changes in the switch management, the configuration changes must be saved to startup configuration or NV-RAM (non-volatile random access memory) to keep configuration changes after the device reboots. If changes are not saved to NV-RAM, they will be lost after device reboots. After applying configuration changes, please make sure to commit changes to NV-RAM one of the sections below.

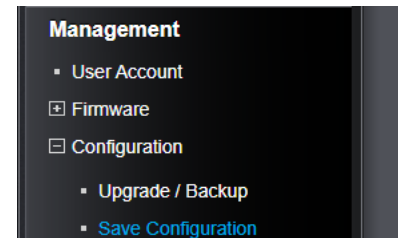
Standard Mode GUI

Click **Save** at the top right to commit changes to NV-RAM.

Note: You can also click **Logout** to log out of the switch management page, **Reboot** to initiate a switch reboot, **Surveillance Mode** to switch to the **Surveillance Mode GUI** switch management.



You can also click **Management**, click on **Configuration**, and click on **Save Configuration**.



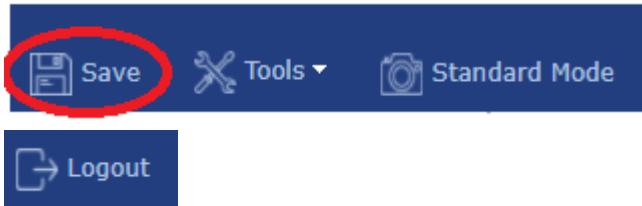
In the main window, click **Apply** with the Running config as the source and Startup config as the destination to save changes to NV-RAM.

Source File	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration
Destination File	<input checked="" type="radio"/> Startup Configuration
<input type="button" value="Apply"/> <input type="button" value="Restore Factory Default"/>	

Surveillance Mode GUI

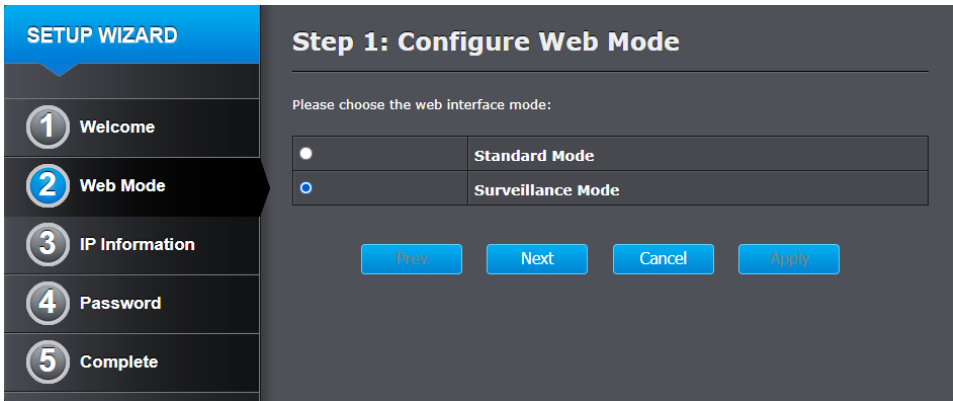
Click **Save** at the top left to commit changes to NV-RAM.

Note: You can also click **Standard Mode** to switch to the **Standard Mode GUI** switch management. Click **Logout** to logout at the top right of the switch management page.

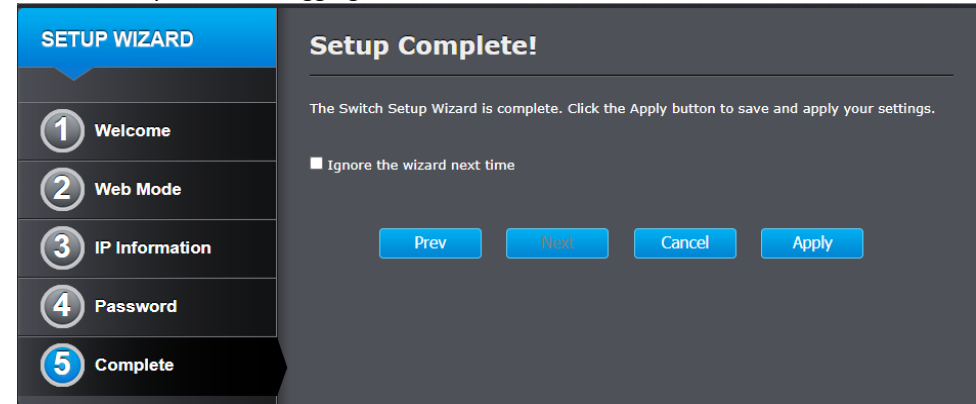


Switching between Standard and Surveillance Mode web interfaces

In the initial Setup Wizard, you can configure which GUI mode will load by default after logging into the switch management page. By default, the Standard mode GUI is configured.

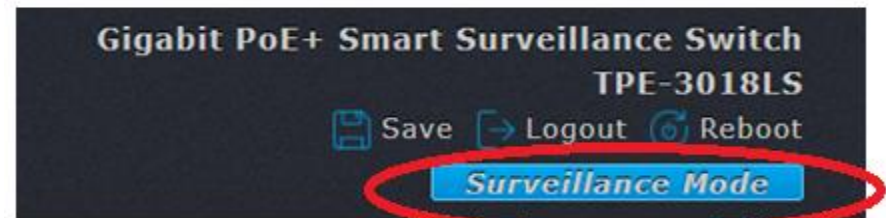


By selecting the “Ignore the wizard next time” at the last step of the setup wizard, the setup wizard will no longer appear after log and the web interface mode set will automatically load after logging in.

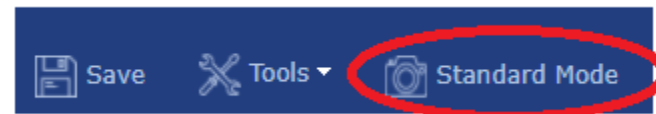


You can manually switch between web interface modes using the buttons noted below.

Standard Mode GUI



Surveillance Mode GUI



Surveillance Mode Web Interface

The surveillance mode interface provides a simplified graphical interface including only the most commonly used features. To access all the switch features, please use the standard mode web interface.

Dashboard

The Surveillance Mode Web Interface dashboard will provide an overview of which ports are used, total PoE budget, total PoE power consumed, and the devices connected. Additionally, you can easily turn PoE on or off in the Overview page.

Status

Status

The status page will display switch system information such as model number, hardware version, IP address settings, MAC and firmware version. Additionally, this page will provide the total PoE budget power utilization/consumption and total currently aggregated receive and transmit bandwidth per port.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Switch Model Number** in the top left and click the **Status** tab.
3. Review the information below.

Switch

- **Device Type** – Displays the model name of the switch.
- **System Name** – Displays the currently assigned system name.
- **Hardware Version** – Displays the switch hardware version
- **Serial Number** – Display the switch serial number.

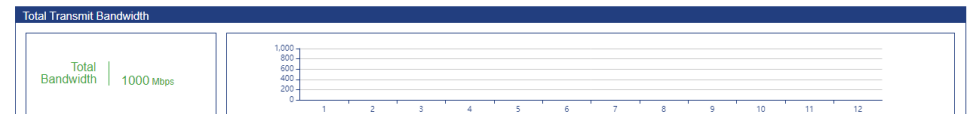
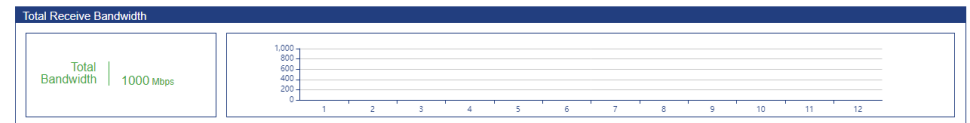
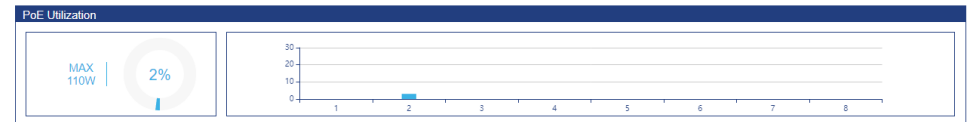
Web

- **IP Address** – Displays the currently assigned IPv4 address.
- **Mask** – Displays the currently assigned IPv4 subnet mask.
- **Gateway** – Displays the currently assigned IPv4 default gateway.
- **MAC Address** – Displays the switch MAC address.

Info

- **Boot PROM Version** – Displays the switch current boot loader version.
- **Firmware Version** – Displays the switch current firmware version.
- **System Time** – Displays the switch device date and time.
- **Using Time** – Displays the switch uptime running continuous operation without reboot or interruptions.

SWITCH		WEB		INFO	
Device Type	TPE-3012LS	IP Address	192.168.10.220	Boot PROM Version	2.1.3.46351
System Name	Switch	Mask	255.255.255.0	Firmware Version	1.01.28
Hardware Version	1.0	Gateway	192.168.10.1	System Time	2000-01-11 06:31:45 UTC-8
Serial Number	N/A	MAC Address	3C:8C:F8:F9:D0:4A	Using Time	10 day,6 hr,31 min and 45 sec.



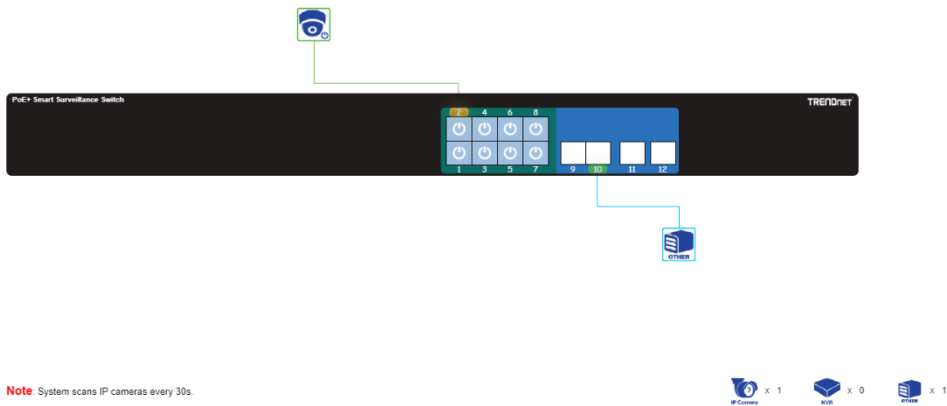
Note: Port numbers will be indicated at the bottom of the display charts. Hovering over your mouse cursor over the chart will provide more detail.

Overview

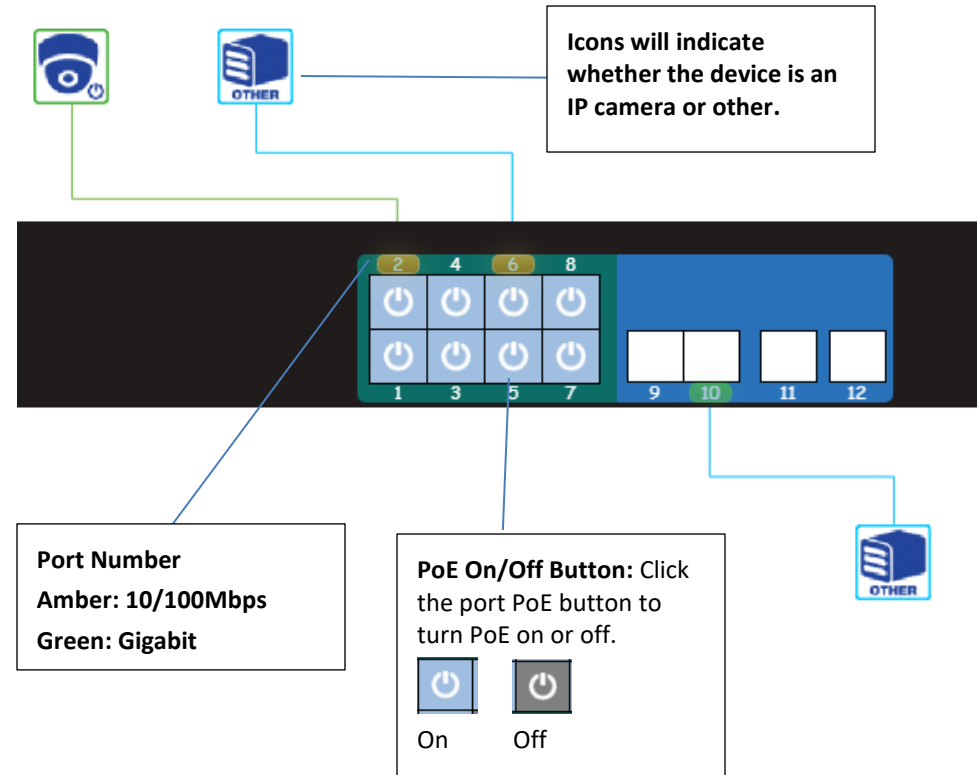
Overview

The overview page will provide a display of the front panel and icons representing connected devices or links. Additionally, this page will display specifically if IP cameras are connected or other links and also display the data link speed the devices are connected. PoE can also be enabled or displayed on each port.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **TPE-3012LS** or **TPE-3018LS** (depending on the switch model) in the top left and click the **Overview** tab.



Note: System scans IP cameras every 30s.



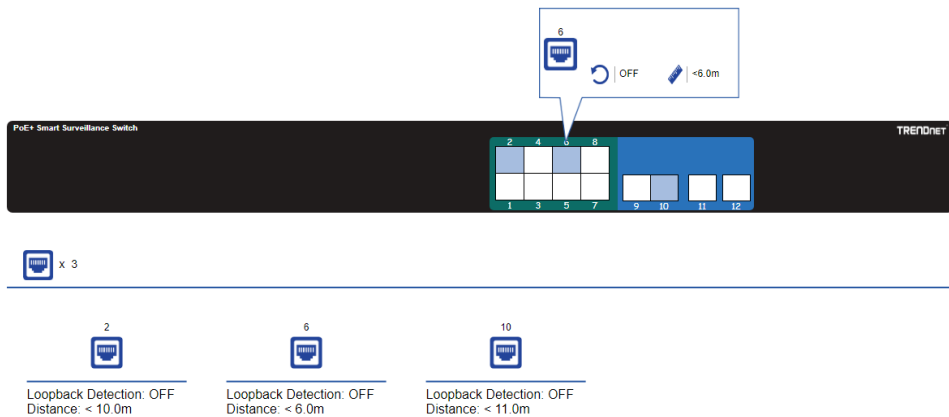
Note: The switch will scan for connected device every 30 seconds. Additionally, the green colored ports on the front indicate which ports are PoE and blue which ports are data ports only.

Port Info

Port Info

The port info. page which indicate which ports are connected, the approximated distance between the switch and the connected device, the loopback detection status.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **TPE-3012LS** or **TPE-3018LS** (depending on the switch model) in the top left and click the **Port Info** tab.

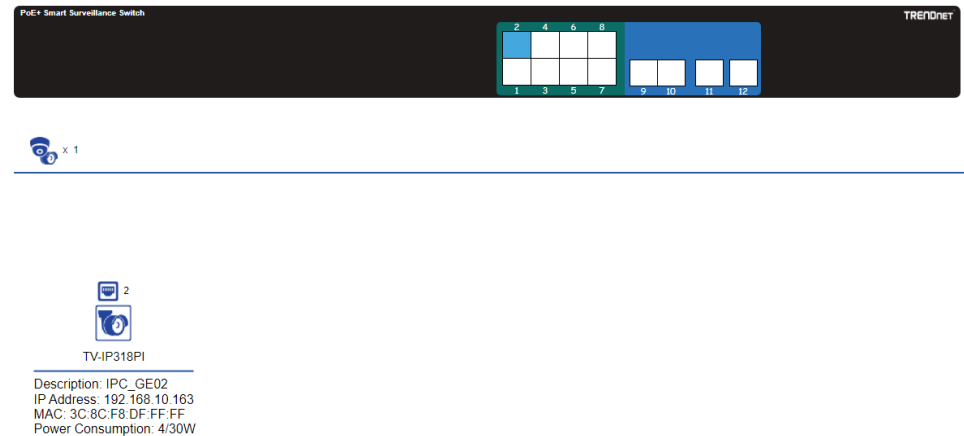


IP Camera Info

IP Camera Info

The IP Camera Info page will display which ports are specifically connected to IP cameras and additional info. about the IP cameras such as the detected model number, IP address, MAC address, and PoE power consumption for each connected IP camera.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **TPE-3012LS** or **TPE-3018LS** (depending on the switch model) in the top left and click the **IP Camera Info** tab.

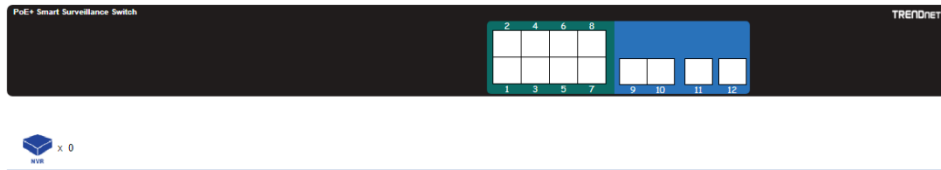


NVR Info

NVR Info

The NVR Info page will display which ports are specifically connected to NVRs and additional info. about the NVRs such as the detected model number, IP address, MAC address, and PoE power consumption for each connected NVR.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **TPE-3012LS** or **TPE-3018LS** (depending on the switch model) in the top left and click the **NVR Info** tab.

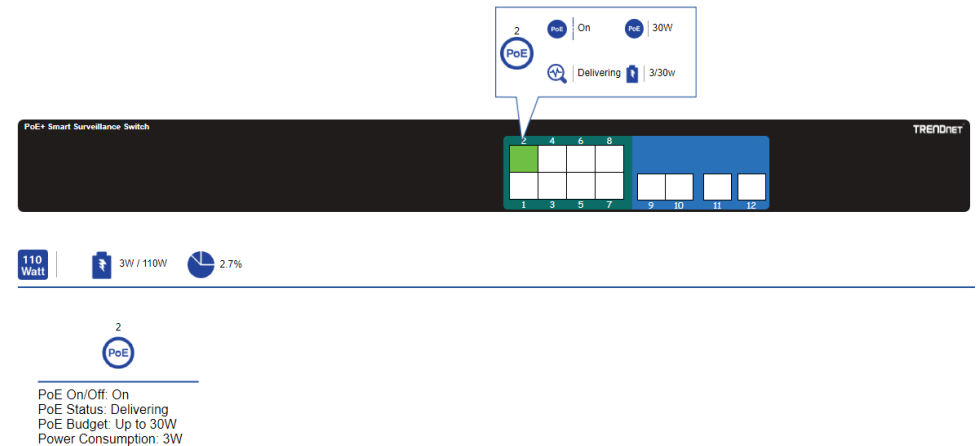


PoE Info

PoE Info

The PoE Info page will display which ports are delivery PoE power to the connected devices, total PoE power budget, total PoE power consumed, and power consumption for each connected device.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **TPE-3012LS** or **TPE-3018LS** (depending on the switch model) in the top left and click the **PoE Info** tab.



PoE Scheduling

PoE Scheduling

This page will allow you to configure schedules when PoE should be enabled or disabled for each port. Please make sure to configure the time and date settings under Time before configuring PoE scheduling.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **PoE Scheduling**.
3. Create schedules under the **Time Range** tab and apply the PoE scheduling configuration under the **Scheduling** tab. Review the settings below.

Time Range

Click **Add** to create a new schedule.

Item	Description
Range Name	Select Range name.
Days	Select a valid time for this schedule.
Start Time	Input the Start Time.
End Time	Input the End Time.

☐
Range Name

Add
Edit
Delete

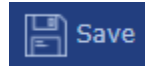
Range Name	Name_Default
Date	<input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun From <input style="width: 80px;" type="text" value="01:00"/> to <input style="width: 80px;" type="text" value="23:00"/>

Apply
Close

4. After completing your configuration changes, click **Apply**.



5. Click **Save** in the top left menu to save configuration to NV-RAM.



Scheduling

Under the **Schedule Status** setting, click the drop-down list and **Enable** to enable PoE Scheduling.

Item	Description
Nominal Power	Maximum supply power.
Consuming Power	Current consumed power.
Remaining Power	Remaining available power.
Schedule Status	Schedule status global switch.
Name	PoE Schedule Name.
Port List	The ports provide power in designated schedule index.
Schedule Status	The current schedule status.

Nominal Power	110 W
Consuming Power	3 W
Remaining Power	107 W
Schedule Status	Disable ▾

Apply

Select an entry to to configure PoE port scheduling and click **Edit**.

<input type="checkbox"/>	Index	Name	Port List	Schedule Status
<input checked="" type="checkbox"/>	1	None		Disable

Edit

Item	Description
Index	The serial number of schedule list.
Schedule Status	Schedule Status <ul style="list-style-type: none"> Checked: Schedule status is enabled. Unchecked: Schedule status is disabled.
Name	Enter the PoE schedule name.
Port List	Select the port provide power.

Index	1 ▾
Schedule Status	<input checked="" type="checkbox"/> Enable
Name	None ▾
Port List	<div style="text-align: center;"> </div>

Apply

Close

4. After completing your configuration changes, click **Apply**.

Apply

5. Click **Save** in the top left menu to save configuration to NV-RAM.

Save

Time

Time

This section will allow users to configure time and date settings.

Clock Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Time** and click on **Clock Settings**.
3. The date and time and can be manually entered and configured in the options provided.

Clock Setting

Manual Time	
Date	<input type="text" value="2000-01-11"/> YYYY-MM-DD
Time	<input type="text" value="11:36:14"/> HH:MM:SS
Time Zone	<input type="text" value="UTC -8:00"/> ▼
Current Time	2000-01-11 11:36:14 UTC-8

Apply

4. After completing your configuration changes, click **Apply**.

Apply

5. Click **Save** in the top left menu to save configuration to NV-RAM.

 **Save**

SNTP Settings

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Time** and click on **SNTP SETTINGS**.
3. Review the settings below.

Item	Description
Source	Select the time source. <ul style="list-style-type: none"> • SNTP: Time sync from NTP server. • From Computer: Time set from browser host.
Time Zone	Select a time zone difference from listing district.
SNTP	
Address Type	Select the address type of NTP server. This is enabled when time source is SNTP.
Server Address	Input IPv4 address or hostname for NTP server. This is enabled when time source is SNTP.
Server Port	Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.
Manual Time	
Date	Input manual date. This is enabled when time source is manual.
Time	Input manual time. This is enabled when time source is manual.
Daylight Saving Time	

Type	<p>Select the mode of daylight saving time.</p> <ul style="list-style-type: none"> • Disable: Disable daylight saving time. • Recurring: Using recurring mode of daylight saving time. • Non-Recurring: Using non-recurring mode of daylight saving time. • USA: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. • European: Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October.
Offset	Specify the adjust offset of daylight saving time.
Recurring From	Specify the starting time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Non-recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Non recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Non-Recurring" mode.

SNTP Settings

SNTP Server Settings	
Source	Manual Time
SNTP State	Disabled ▾
Address Type	<input type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	<input type="text"/>
Server Port	<input type="text" value="123"/> (1 - 65535, default 123)
Daylight Saving Time	
Type	<input type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input checked="" type="radio"/> USA <input type="radio"/> Europe
Offset	<input type="text" value="60"/> Min (1 - 1440, default 60)
Recurring	From: Day <input type="text" value="Sun"/> Week <input type="text" value="2"/> Month <input type="text" value="Mar"/> Time <input type="text" value="02:00"/>
	To: Day <input type="text" value="Sun"/> Week <input type="text" value="First"/> Month <input type="text" value="Nov"/> Time <input type="text" value="02:00"/>
Non-recurring	From: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
	To: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
Operational Status	
Current Time	2000-01-11 11:39:30 UTC-8

Apply

4. After completing your configuration changes, click **Apply**.

Apply

5. Click **Save** in the top left menu to save configuration to NV-RAM.

Save

Surveillance Settings

Surveillance Settings

This section will allow users to configure switch settings such as switch IPv4 address settings, DNS server settings, SNMPT host settings, syslog server, and admin password.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **Surveillance Settings**.

IP Settings

After you have completed configuration, click **Apply** and click **Save**.

Note: After changing IP address settings, you may need to log into the switch with the new IP address settings. Please also make sure to click **Save**.

- **Address Type:** Select **Static** to manually specify your IP address settings or **Dynamic** to allow your switch to obtain IP address settings automatically from a DHCP server on your network.
- **IP Address:** Enter the new switch IP address. (e.g. 192.168.200.200)
- **Subnet Mask:** Enter the new switch subnet mask. (e.g. 255.255.255.0)
- **Default Gateway:** Enter the default gateway IP address. (e.g. 192.168.200.1 or typically your router/gateway to the Internet).
- **DNS Server 1:** Enter the primary IPv4 DNS server address.
- **DNS Server 2:** Enter the secondary IPv4 DNS server address.

IP Settings	
Address Type	Static ▾
IP Address	192.168.10.220
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server 1	168.95.1.1
DNS Server 2	168.95.192.1

Apply

SNMP Host Settings

After you have completed configuration, click **Add**, **Apply**, and click **Save**.

Item	Description
Address Type	Notify recipients host address type.
Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP notification version <ul style="list-style-type: none"> • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none"> • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.
Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name <ul style="list-style-type: none"> • No Security: Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.

Server Port	Recipients server UDP port number, if "use default" checked the value is 162, else user configure.
Timeout	Specify the SNMP informs timeout, if "use default" checked the value is 15, else user configure.
Retry	Specify the SNMP informs retry count, if "use default" checked the value is 3, else user configure.

SNMP Host Settings

Server Address

Version SNMPv1
 SNMPv2
 SNMPv3

Type Trap
 Inform

Community / User

Security Level No Security
 Authentication
 Authentication and Privacy

Server Port Use Default
 (1 - 65535, default 162)

Timeout Use Default
 Sec (1 - 300, default 15)

Retry Use Default
 (1 - 255, default 3)

	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								
<input type="button" value="Add"/>	<input type="button" value="Delete"/>		<input type="button" value="Edit"/>	<input type="button" value="Apply"/>				

Log Server

This section will allow users to configure an external remote log server or syslog server. After you have completed configuration, click **Add**, **Apply**, and click **Save**.

Item	Description
Server Address	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0,local1, local2, local3, local4, local5, local6, and local7.
Severity	<p>The minimum severity.</p> <ul style="list-style-type: none"> • Emergence: System is not usable. • Alert: Immediate action is needed. • Critical: System is in the critical condition. • Error: System is in error condition
	<p>has occurred.</p> <ul style="list-style-type: none"> • Informational: Device information. • Debug: Provides detailed information about an event.

Log Server	
Server Address	<input type="text"/>
Server Port	<input type="text" value="514"/> (1 - 65535, default 514)
Facility	<input type="text" value="Local 7"/> ▾
Minimum Severity	<input type="text" value="Notice"/> ▾
Note: Emergency, Alert, Critical, Error, Warning, Notice	

■	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found					
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Apply"/>					

Password Settings

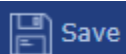
This section will allow users to change the admin password to log into the switch management interface.

After you have completed configuration, click **Apply** and click **Save**.

Password Settings	
Password	<input type="text"/>
Confirm Password	<input type="text"/>

4. After completing your configuration changes, click **Apply**.

5. Click **Save** in the top left menu to save configuration to NV-RAM.



Mail Alert

Mail Alert

This section will allow users to configure email alert notification for PD alive check and Ping Watchdog.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **Mail Alert**.

3. Review the settings below.

- **State:** Select **Enable** to enable the email notification/alerts.
- **SMTP Server:** Enter the SMTP server domain name or IP address.
Note: Please make sure the switch IP address default gateway and DNS server address settings are set correctly for domain name resolution.
- **SMTP Port:** Enter the SMTP port number used by the SMTP email server.
- **User Name:** Enter the user name or email account user name.
- **Password:** Enter the password for the email account.
- **State:** Select **Enable** to enable the email notification/alerts.
- **Sender:** Enter a sender email address.
- **Receiver:** Enter the receiving email address.
- **Alert Type:** Select the alert type to send notifications.
 - **PD Alive:** If selecting this option, email notifications will be sent when PD alive check is activated.
 - **Ping Watchdog:** If selecting this option, email notifications will be sent ping watchdog is activated.
- **Send Test:** Use this to verify your SMTP email configuration settings are configured correctly and email notification is working properly.

Mail Alert

IP Settings	
State	Disable ▾
SMTP Server	<input type="text"/>
SMTP Port	<input type="text" value="0"/>
User Name	<input type="text"/>
Password	<input type="text"/>
State	Disable ▾
Sender	<input type="text"/>
Receiver	<input type="text"/>
Alert Type	<input type="checkbox"/> PD alive check <input type="checkbox"/> Ping Watchdog

Apply

Send Test

4. After completing your configuration changes, click **Apply**.

Apply

5. Click **Save** in the top left menu to save configuration to NV-RAM.

Save

PD Alive Check

PD Alive Check

This section will allow users configure PD alive check which as feature that allows the switch to run a connectivity check on PoE device by pinging the IP address and automatically turn PoE on and off if connectivity fails to the PoE device in attempt to restore the PoE device to normal operation.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **PD Alive Check**.
3. Check the PoE port with the PoE device connected to you would like to configure for PD alive check and click **Edit**.

PD Alive Check Table

Entry	Port	Mode	ping PD IP Address	Interval Time	Retry Count	Action	Reboot Time	Connect Sta	
<input checked="" type="checkbox"/>	1	GE1	Disable	0.0.0.0	30	2	None	90	Off

Edit

4. Check the **Enable** option for Status to enable PD alive check on the selected port. Enter the IP Address for the PoE device under the **ping PD IP Address** (ex: 192.168.10.107)

Review the additional settings below.

- **Interval Time** – Enter the time in seconds each time the switch will check for a ping response from the PoE device. (Range: 10 – 300)
- **Retry Count** – In the case that a ping response fails, enter the number of times the switch will retry for a ping response before disabling and re-enabling the PoE port. (Range: 1-5)
- **Action** – An option must be selected for PD alive check to function.
 - **None** – If the ping response fails according to the time parameters set, no action will be taken.

- **PD Reboot** – If the ping response fails according to the time parameters set, the switch will disable and re-enable the PoE port attempting to automatically recover the connected PoE device.
- **Reboot&Alarm** - If the ping response fails according to the time parameters set, the switch will disable and re-enable the PoE port attempting to automatically recover the connected PoE device and also send out an email notification is configured.
- **Alarm** - If the ping response fails according to the time parameters set, the switch will only send out an email notification if configured.
- **Reboot Time** - If the ping response fails according to the time parameters set, enter the time in seconds from the time the PoE port is disabled to the time the PoE port is re-enabled. (Range: 30-180)

Port List	GE1	
Status	<input checked="" type="checkbox"/> Enable	
ping PD IP Address	<input type="text" value="0.0.0.0"/>	
Interval Time	<input type="text" value="30"/>	Sec (10 - 300, default 30)
Retry Count	<input type="text" value="2"/>	(1 - 5, default 2)
Action	None <input type="button" value="v"/>	
Reboot Time	<input type="text" value="90"/>	Sec (30 - 180, default 90)

4. After completing your configuration changes, click **Apply**.

5. Click **Save** in the top left menu to save configuration to NV-RAM.

ONVIF

This section will allow you to configure the ONVIF features available on the switch such as ONVIF device discovery and authorization. Apply configuration settings to ONVIF compliant IP cameras such as IP address settings, changing passwords, create users, and firmware upgrades. The switch is capable of discovering and applying configuration settings to ONVIF compliant devices connected to the same IP address subnet. The Surveillance Mode User Interface may provide more graphical-based tools in monitoring your devices and applying configuration settings.

Discovering and authorizing ONVIF compliant devices

ONVIF > IPC Discover

After the surveillance switch has discovered the ONVIF compliant device, the devices must be authorized with the surveillance switch to apply configuration changes to the ONVIF devices.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **IPC Discover**. The will list will display a list of the discovered ONVIF compliant IP cameras found on your network. The list will also display the IP address, MAC address, and port the device is connected. If the device or devices are connected to another switch in your network, the list will display the connected port as the uplink port from your surveillance switch to your network.



IPC Discover

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	unAuth

3. Before the surveillance switch can apply any configuration settings to your ONVIF compliant IP cameras, you must authorize by entering the ONVIF administrator credentials for each device.

Note: The IP camera administrator user name and password must be configured on the IP cameras first before they can be used with the surveillance switch. Some IP cameras may not have configuration options specific to ONVIF but may still comply with ONVIF. In this case, the IP camera management access user name and password may be the same as the ONVIF administrator user name and password.

4. To authorize an ONVIF compliant IP camera, check the IP camera in the list and click **Auth**.

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	unAuth

Edit **Auth** **Account**

5. Under the IPC Authorization section, enter the ONVIF administrator user name and password in the fields provided and click **Apply**. A success message will appear indicating that the IP camera has been successfully authorized. Under the Status column next to the device, the status will change from unAuth to Auth.

Note: If you are unable to successfully authorize the IP camera, please double check your ONVIF administrator credentials. You can also try to reboot the IP camera.

IPC authorization

Device Name	IPC_GE02
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

Apply **Close**



<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	Auth

Applying IP address settings to ONVIF authorized devices

ONVIF > IPC Discover

After ONVIF compliant devices have been discovered and successfully authorized, you can apply IP address configuration settings to these devices from the surveillance switch interface.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **IPC Discover**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Edit**.



IPC Discover

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	Auth

Edit **Auth** **Account**

4. Under the IPC Device Info Edit section, you can view additional device information, modify the Device Name and IP address configuration.

Basic info	
Device Name	IPC_GE02
MAC Address	3C:8C:F8:DF:FF:FF
Manufacturer	TRENDnet
Model Name	TV-IP318PI
SN	TV-IP318PI20170926AAWR837164107
HardwareId	88
Firmware Version	V5.5.3 build 191123

5. Scroll down the window to view or modify the device IP address configuration.

IP info	
Address Type	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
IPv4 Address	192.168.10.163
Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1
Token	eth0
Time info	
Date	2020-11-11
Time	23:47:34

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.

Apply



Note: After the configuration changes have been successfully applied, the device will appear in the list with the updated information.

Changing the ONVIF device administrator password

ONVIF > Device Authentication

After ONVIF compliant devices have been discovered and successfully authorized, you can change the ONVIF administrator password of the ONVIF compliant devices.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **IPC Discover**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Account**.



<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	Auth

4. Under the **IP Camera List** section below, a list of the current user accounts of the ONVIF device will be listed. To modify the ONVIF administrator password, check the device in the list with User Level admin and click **Edit**.

Privilege

<input type="checkbox"/>	Device Name	User name	User Level	Port ID	MAC Address
<input type="checkbox"/>	IPC_GE02	admin	admin	GE2	3C:8C:F8:DF:FF:FF

5. Scroll down to the **Edit User Account** section and you can enter in the administrator password settings in the password fields provided.

Note: Please note that the ONVIF user password typically requires eight characters for accounts.

Username	admin
Password	<input type="password"/>
Confirm Password	<input type="password"/>
User Level	<input checked="" type="radio"/> Admin <input type="radio"/> operator <input type="radio"/> User

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.



Creating new ONVIF users in the ONVIF device

ONVIF > Device Authentication

After ONVIF compliant devices have been discovered and successfully authorized, you create new ONVIF users to those devices if supported.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **Device Authentication**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Account**.



<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE02	192.168.10.163	3C:8C:F8:DF:FF:FF	GE2	Auth

[Edit](#) [Auth](#) [Account](#)

4. Under the **IP Camera List** section below, a list of the current user accounts of the ONVIF device will be listed. To create a new ONVIF user for the device, check the device in the list and click **Add**.

Privilege

<input type="checkbox"/>	Device Name	User name	User Level	Port ID	MAC Address
<input type="checkbox"/>	IPC_GE02	admin	admin	GE2	3C:8C:F8:DF:FF:FF

[Add](#) [Edit](#) [Delete](#)

5. Scroll down to the **Add User Account** section and enter the new account user name and password in the fields provided. For the User Level, select Operator or User.
Note: Please note that the ONVIF user password typically requires eight characters for accounts.

Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
User Level	<input checked="" type="radio"/> Admin <input type="radio"/> operator <input type="radio"/> User

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.

[Apply](#)



Upgrade ONVIF device firmware

ONVIF > Device FW Upgrade

After ONVIF compliant devices have been discovered and successfully authorized, you can upgrade the firmware of the ONVIF device from the surveillance switch interface.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **FW Upgrade**.
3. Depending on your web browser at the top, for the **Filename**, click **Browse** or **Choose File** and navigate to the folder on your computer where the unzipped firmware file for the ONVIF device is located and select it. Then click **Apply** to upload the firmware file to the surveillance switch.

Filename	empty
Filename	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>

4. After the firmware file has been successfully uploaded, a success message will appear indicating that the firmware file was successfully uploaded. Click **Done**.
5. The firmware file name will now appear under Filename.
6. In the IP Camera List, check the device you would like to upgrade with the previously loaded firmware file, then click **Upgrade**.

Note: If you have multiple devices of the same model that use the same firmware file, you can upgrade multiple devices of the same model by checking multiple devices in the list before clicking Upgrade.

<input type="checkbox"/>	Port ID	Brand	Model	Firmware Version	Status
<input checked="" type="checkbox"/>	GE2	TRENDnet	TV-IP318PI	V5.5.3 build 191123	stand by

The Status will change to uploading indicating that the firmware of the ONVIF device is upgrading.

If the firmware upgrade was successful, the Status will indicate that upgrade was successful.

Note: After the ONVIF device has successfully upgraded firmware and reboots, you may need to re-authorize the ONVIF device again under Discovery > IP Camera.

E-map Management

ONVIF > E-Map Management

This section will allow users to upload images of floorplans where IP camera can be placed on as a visual reference to the IP cameras physical locations.

Uploading E-Map Floorplan Images

ONVIF > E-Map Management > Image Upload

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **ONVIF**, click on **E-Map Management**, and click on **Image Upload**.
3. Click **Add** to upload a new floor plan image. Click **Browse** or **Choose File** and navigate to the location of the floorplan image to upload from your local drive, then click **Apply** to start the upload.



Image Upload

<input type="checkbox"/>	Name	Bind Num
0 results found.		

Add **Delete**

Image Upload Add

Filename

Apply **Close**

Note: Images are automatically scaled when uploaded. The image formats are JPG and PNG. Maximum file size for images is 1.5MB. The recommended resolution for images is 1024 x 768 pixels.

4. The file name of the image will be displayed after it has been successfully uploaded.

Binding E-Map Images with Location Name

ONVIF > E-Map Management > Image Settings

This section will allow users to set a location to a specific map image.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **ONVIF**, click on **E-Map Management**, and click on **Image Settings**.
3. Select an entry and click **Edit**.
 - **Location Name:** Enter a location name for the image.
 - **Map Image:** Click the drop-down list to select an uploaded floorplan image to assign. Click **Apply**.



Image Setting

<input type="checkbox"/>	Entry	Location name	Map Image
<input checked="" type="checkbox"/>	1		empty
<input type="checkbox"/>	2		empty
<input type="checkbox"/>	3		empty
<input type="checkbox"/>	4		empty

Edit

Image Setting Edit

Entry

Location name

Map Image

Apply **Close**

4. The location name and assigned floorplan image filename will appear in the entry.

Image Setting

<input type="checkbox"/>	Entry	Location name	Map Image
<input type="checkbox"/>	1	Office	office-floorplansample.jpg
<input type="checkbox"/>	2		empty
<input type="checkbox"/>	3		empty
<input type="checkbox"/>	4		empty

[Edit](#)

E-Map View

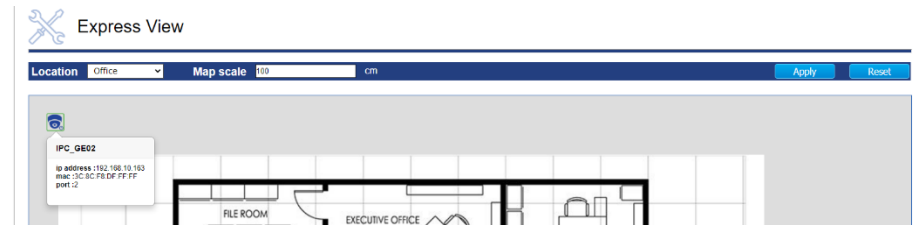
ONVIF > E-Map Management > E-Map View

This section will allow users to place IP cameras onto the uploaded image floorplans for visual reference to IP camera installed locations.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF**, click on **E-Map Management**, and click on **E-Map View**.
3. Review the settings.
 - **Location:** The drop-down list will contain a list of uploaded image floorplans that have been uploaded and already binded to a location name.
 - **Map Scale:** Scaling adjustment for reference to the physical of objects in the uploaded floorplan image.

IP Cameras will be available in the left size of the e-map. Using your mouse, drag and drop the IP cameras to the locations on the floorplan image for reference to the physical locations. Click **Apply**.

Note: Clicking **Reset** will reset the e-map to default and remove all IP cameras from the floorplan moved back to the top left of the e-map.



4. After completing your configuration changes, click **Apply**.

[Apply](#)

5. Click **Save** in the top left menu to save configuration to NV-RAM.

[Save](#)

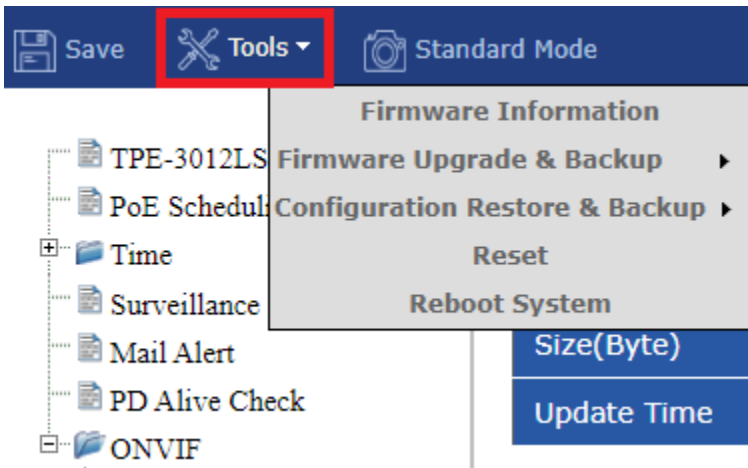
Tools

The tools menu will allow users to view firmware information, upgrade and backup switch firmware, backup and restore switch configuration, reboot, and reset switch to factory defaults.

View Firmware Information

Tools > Firmware Information

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. In the top left menu, click on **Tools** and click on **Firmware Information**.



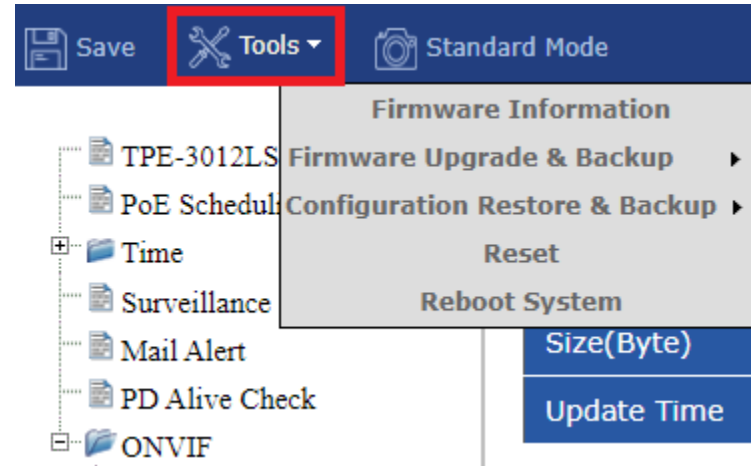
Firmware Information

Version	1.01.28
Size(Byte)	8168864
Update Time	Oct 14 2020 - 11:16:11

Firmware Upgrade and Backup

Tools > Firmware Upgrade & Backup

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. In the top left menu, click on **Tools** and click on **Firmware Upgrade & Backup**.
 - **Upgrade from HTTP/TFTP** – This section will allow you to upgrade the switch firmware by HTTP or TFTP protocol methods.
 - **Backup from HTTP/TFTP** - This section will allow you to backup the switch firmware by HTTP or TFTP protocol methods.



HTTP

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT. • Backup: Backup firmware image from DUT to remote host.

Method	Firmware upgrade / backup method. <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware. • HTTP: Using WEB browser to upgrade/backup firmware.
Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.

Firmware Upgrade/Backup

Action	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
Method	<input checked="" type="radio"/> TFTP <input type="radio"/> HTTP
Filename	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>

TFTP

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware. • HTTP: Using WEB browser to upgrade/backup firmware.

Address Type	Specify TFTP server address type <ul style="list-style-type: none"> • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

Firmware Upgrade/Backup

Action	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
Method	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
Address Type	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Filename	<input type="text"/>

Backup/Restore switch Configuration

Tools > Configuration Backup & Restore

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. In the top left menu, click on **Tools** and click on **Configuration Backup & Restore**.
 - **Restore from HTTP/TFTP** – This section will allow you to restore the switch configuration by HTTP or TFTP protocol methods.
 - **Backup from HTTP/TFTP** - This section will allow you to backup the switch configuration by HTTP or TFTP protocol methods.

HTTP

Item	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> • Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file
Filename	Use browser to upgrade configuration, you should select configuration file on your host PC.

Configuration Restore/Backup

Action	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
Method	<input checked="" type="radio"/> TFTP <input type="radio"/> HTTP
Configuration	<input type="radio"/> Running Configuration <input checked="" type="radio"/> Startup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
Filename	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>

Apply

TFTP

Item	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> • Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file

Address Type	Specify TFTP server address type <ul style="list-style-type: none"> • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address
Server Address	Specify TFTP server address address
Filename	File name saved on remote TFTP server

Configuration Restore/Backup

Action	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
Method	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
Configuration	<input type="radio"/> Running Configuration <input checked="" type="radio"/> Startup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
Address Type	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Filename	<input type="text"/>

Apply

Reset switch to factory default

Tools > Reset

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. In the top left menu, click on **Tools** and click on **Reset**.

Note: Clicking Restore Factory Default will reset all switch configuration settings to factory defaults.

Reset

Warning: The Switch will be reset to its factory defaults including IP address.

Restore Factory Default

Reboot switch

Tools > Reboot

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. In the top left menu, click on **Tools** and click on **Reboot**.

Note: Any configuration change that not been save to NV-RAM using the



Reboot

Warning: Reboot the system and unsaved changes in the configuration will be lost.

Reboot

Standard Mode Web Interface

Status

View your switch system information

Status > System Information

You may want to check the general system information of your switch such as firmware version, boot loader information, system time/date, MAC address, system uptime, administration information, IPv4 information. This section explains how to assign a name, location, and contact information for the switch. This information helps in identifying each specific switch among other switches in the same local area network. Entering this information is optional.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Status** and click on **System Information**.

System Information

- **Model** – Displays the model name of the switch.
- **System Name** – Displays the currently assigned system name.
- **System Location** – Displays the currently assigned system location.
- **System Contact** – Displays the currently assigned system contact.

Note: Clicking **Edit** at the top will allow you to modify the System Name, Location, and Contact information.

System Information		Edit
Model	TPE-3018LS	
System Name	Switch	
System Location	Default	
System Contact	Default	

- **MAC Address:** Displays the switch system MAC address.
- **IPv4 Address** – Displays the current IPv4 address assigned to your switch.
- **System Uptime** – The duration your switch has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Current Time** – Displays the current system time and date settings of the switch.

MAC Address	3C:8C:F8:F9:D0:57
IPv4 Address	192.168.10.200
System Uptime	0 day, 1 hr, 55 min and 17 sec
Current Time	2000-01-01 01:55:17 UTC-8

- **Loader Version** – The current boot loader version your switch is running.
- **Loader Date** – The current boot loader version date your switch is running.
- **Firmware Version** - The current software or firmware version your switch is running.
- **Firmware Date** – The current software or firmware version date your switch is running.

Loader Version	2.1.3.46351
Loader Date	Mar 18 2020 - 20:49:44
Firmware Version	1.01.25
Firmware Date	Mar 18 2020 - 20:50:25

- **Telnet** - Displays the current state of Telnet management access to the switch.
- **SSH** – Displays the current state of SSH management access to the switch.
- **HTTP** – Displays the current state of HTTP management access to the switch. By default, HTTP management access is enabled.
- **HTTPS** – Displays the current state of HTTPS management access to the switch.
- **SNMP** – Displays the current state of SNMP management access to the switch.

Telnet	Disabled
SSH	Disabled
HTTP	Enabled
HTTPS	Disabled
SNMP	Disabled

- **Consuming Power** – Displays the current PoE power consumption utilized by PoE devices connected to the switch.

Consuming Power	15
-----------------	----

View your switch logging messages

Status > Logging Message

You may want to check your switch logging messages for switch troubleshooting or verification on functionality.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Status** and click on **Logging Message**.
3. Review the settings.
 - **Viewing** – Click the drop-down list to view logging messages in RAM or Flash memory.
 - **Showing** – Click the drop-down list to select how log entries to be displayed per page.

Note: You can search the logging messages by keyword using the field below.

Logging Message Table			
Viewing RAM ▾			
Showing All ▾ entries		Showing 1 to 25 of 25 entries	
<input type="text"/>			
Log ID	Time	Severity	Description
1	Jan 01 2000 01:49:45	notice	New http connection for user admin, source 192.168.10.135 ACCEPTED
2	Jan 01 2000 01:32:40	notice	New http connection for user admin, source 192.168.10.135 ACCEPTED
3	Jan 01 2000 00:01:17	notice	GigabitEthernet8 link up

View your switch port status information

Status > Port > Statistics

You may want to view port statistics information, error disabled state, or bandwidth utilization information per port.

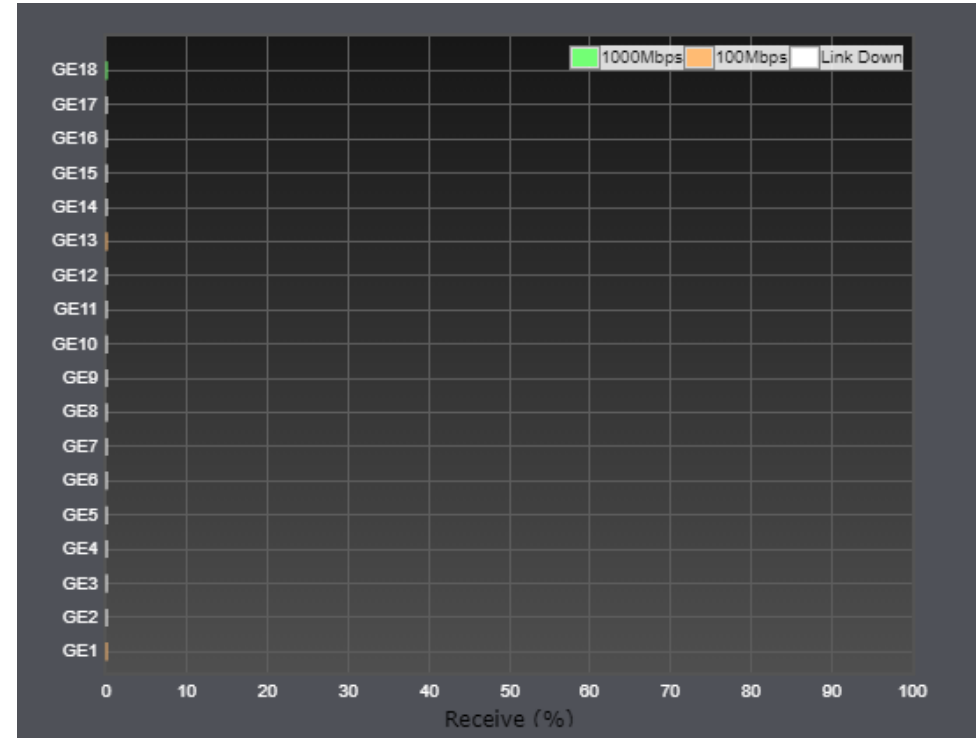
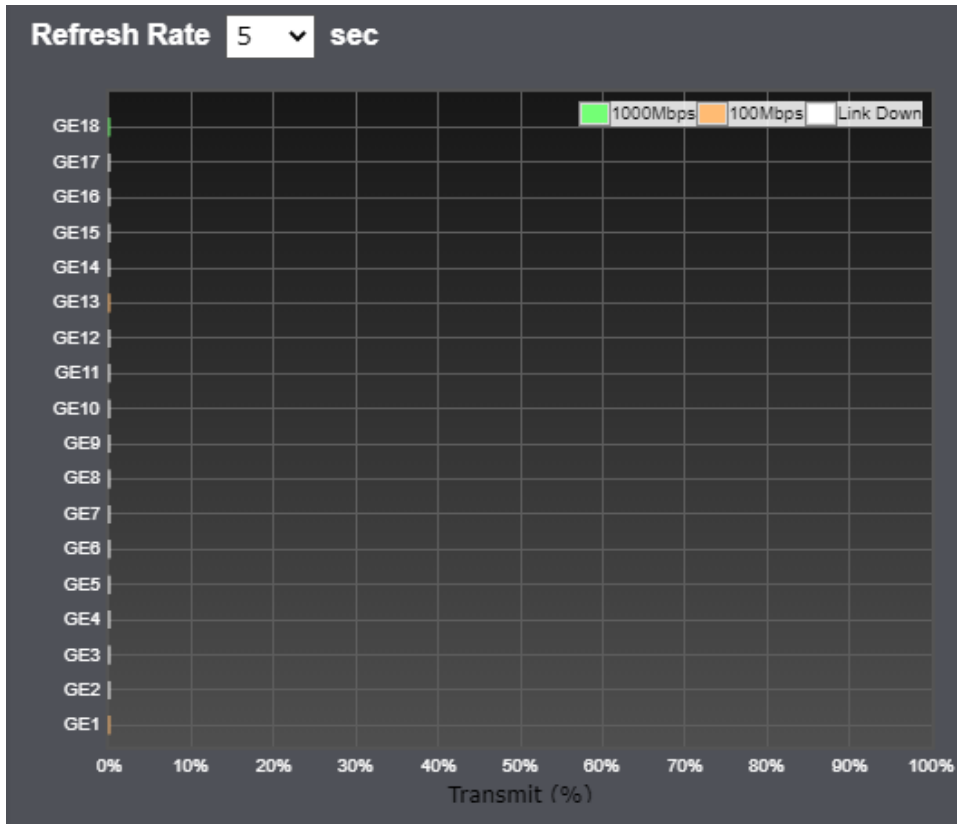
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Status** and click on **Port**.
3. Review the settings.
 - **Statistics** – This section displays the statistics and frame type counters for each switch port interface. Click the drop-down list to select which switch port to view the current statistics, (ex: GE10 means Gigabit Ethernet port number 10). You can filter which statistics to view by selecting **All**, **Interface**, **Etherlike**, **RMON**. The **Refresh Rate** option allows you to select the interval that the statistical data is updated. Click **Clear** to clear all statistics and reset the counters.

Port	GE1 ▾
MIB Counter	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Etherlike <input type="radio"/> RMON
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec
<input type="button" value="Clear"/>	
Interface	
ifInOctets	0

- **Error Disabled** –Ports or link aggregation groups can be configured to enter an error disabled state based on an event such as a loop, broadcast flood, multicast flood, etc. In error disabled state, a timer will be assigned to the port or link aggregation in which it will not pass traffic until the timer has reached 0. The reason the port was set to an error disabled state will also be displayed. Once the issue of the event has been resolved, the port can also be manually taken out of error disabled state in this section to function normally.

Port	Reason	Time Left (sec)
GE1	---	---
GE2	---	---
GE3	---	---
GE4	---	---
GE5	---	---

- **Bandwidth Utilization** – This section displays the current transmit and receive bandwidth utilization per port by percentage in graphical format. The **Refresh Rate** option allows you to select the interval that the bandwidth utilization data is updated.



View link aggregation status

Status > Link Aggregation

You may want to check the link aggregation status. The table will display the link aggregation groups, type, link status, and active/inactive port members.

Link Aggregation Table					
LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1		---	---		
LAG 2		---	---		
LAG 3		---	---		
LAG 4		---	---		
LAG 5		---	---		
LAG 6		---	---		
LAG 7		---	---		
LAG 8		---	---		

View the MAC address table

Status > MAC Address Table

You may want to check the MAC address table for reference to the client devices connected to your switch and their MAC addresses. Please note that the entry labeled **CPU/Type: Management** displays the switch MAC address information.

MAC Address Table			
VLAN	MAC Address	Type	Port
1		Management	CPU
1		Dynamic	GE18
1		Dynamic	GE18
1		Dynamic	GE1
1		Dynamic	GE13
1		Dynamic	GE18
1		Dynamic	GE18
1		Dynamic	GE18
1		Dynamic	GE18

Network

The network section allows you to configure your switch IPv4 and IPv6 address, default gateway, and DNS server settings. Additionally, you can configure the date/time settings and idle timeout settings.

Set your IPv4 settings

Network > IP Address

This section allows you to change your switch IPv4 address settings. Typically, the IP address settings should be changed to match your existing network subnet in order to access the switch management page on your network.

Default Switch IPv4 Address: 192.168.10.200

Default Switch IPv4 Subnet Mask: 255.255.255.0

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Network** and click on **IP Address**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
 - **Address Type:** Select **Static** to manually specify your IP address settings or **Dynamic** to allow your switch to obtain IP address settings automatically from a DHCP server on your network.
 - **IP Address:** Enter the new switch IP address. (e.g. 192.168.200.200)
 - **Subnet Mask:** Enter the new switch subnet mask. (e.g. 255.255.255.0)
 - **Default Gateway:** Enter the default gateway IP address. (e.g. 192.168.200.1 or typically your router/gateway to the Internet).
 - **DNS Server 1:** Enter the primary IPv4 DNS server address.
 - **DNS Server 2:** Enter the secondary IPv4 DNS server address.

IPv4 Address	
Address Type	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server 1	168.95.1.1
DNS Server 2	168.95.192.1

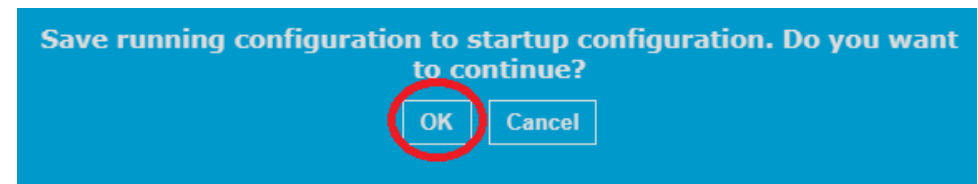
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Set your IPv6 settings

Network > IP Address

Internet Protocol version 6 (IPv6) is a new IP protocol designed to replace IP version 4 (IPv4). The IPv6 address protocol meets the current requirements of new applications and the never ending growth of the Internet. The IPv6 address space makes more addresses available but it must be approached with careful planning. Successful deployment of IPv6 can be achieved with existing IPv4 infrastructures. With proper planning and design, the transition between IP version 4 and 6 is possible today as well.

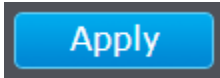
Use the **IPv6 System Settings** page to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch via all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Network** and click on **IP Address**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
 - **Autoconfiguration:** By default, the switch is set to obtain IPv6 address settings automatically via autoconfiguration. Uncheck this option if you would like to assign static IPv6 address settings.
 - **DHCPv6 Client:** Check this option to set the switch to obtain IPv6 address settings automatically from the DHCPv6 server on your network. Uncheck this option if you would like to assign static IPv6 address settings.
 - **IPv6 Address:** If statically assigning IPv6 address settings, enter the IPv6 address in the field provided.
 - **Prefix Length:** Enter the prefix length (0-128) in the field provided.
 - **IPv6 Gateway:** Enter the IPv6 default gateway address.
 - **DNS Server 1:** Enter the primary IPv6 DNS server address.
 - **DNS Server 2:** Enter the secondary IPv6 DNS server address.

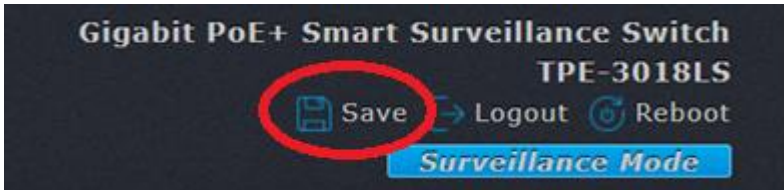
IPv6 Address	
Auto Configuration	<input checked="" type="checkbox"/> Enable
DHCPv6 Client	<input type="checkbox"/> Enable
IPv6 Address	<input type="text"/>
Prefix Length	<input type="text" value="0"/> (0 - 128)
IPv6 Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

- **Operational Status:** This section displays the current IPv4/IPv6 status information.
 - **IPv4 Address:** Displays the currently assigned IPv4 address.
 - **IPv4 Default Gateway:** Displays the currently assigned IPv4 default gateway address.
 - **IPv6 Address:** Displays the currently assigned IPv6 address.
 - **IPv6 Default Gateway:** Displays the currently assigned IPv6 default gateway address.
 - **Link Local Address:** A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the neighbor discovery protocol and the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need globally unique addresses to communicate. IPv6 devices must not forward packets that have link-local source or destination addresses to other links.

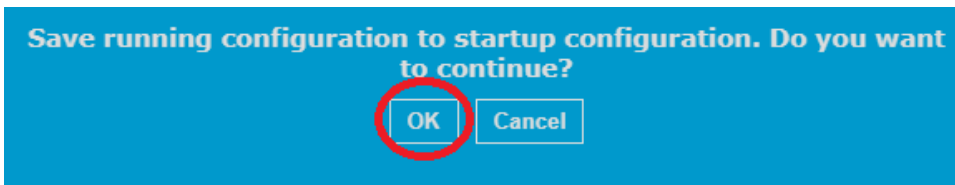
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Set the switch date and time

Network > System Time

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Network** and click on **System Time**.
3. Review the settings. Click **Apply** to save changes.
 - **Time Zone** – Click the drop-down list to select your time zone.
 - **Source** – Select the source where you would like the switch to obtain the date time settings.

Source	<input checked="" type="radio"/> SNTP <input type="radio"/> From Computer <input type="radio"/> Manual Time
--------	---

- **From Computer:** This option will copy the time and date settings from your computer.
- **Manual Time:** This option will allow you to manually set the date and time settings of the switch. If selecting this option, under the Manual Time section, enter the date and time settings in the fields provided.

Note: The time settings is specified in 24-hour format.

Manual Time	
Date	2020-09-30 YYYY-MM-DD
Time	14:11:20 HH:MM:SS

- **SNTP (Simple Network Time Protocol):** Select this option to configure the switch to obtain date and time settings from an external SNTP server.
 - If SNTP is selected, enter the **Server Address** and **Server Port** of the external SNTP server to obtain the date and time settings. Click **Apply** to save the settings.

Note: If the SNTP server is located on the Internet, please make sure to configure your IP address settings, IP address default gateway accordingly to ensure your switch can access

the Internet. If configuring a hostname/domain address, please make sure to configure your DNS server address settings accordingly to ensure your switch can resolve host/domain names to IP addresses.

SNTP	
Address Type	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4
Server Address	<input type="text"/>
Server Port	123 (1 - 65535, default 123)

- **Daylight Saving Time** – Configure the specific daylight savings time settings according to your region.

Daylight Saving Time	
Type	<input type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input checked="" type="radio"/> USA <input type="radio"/> Europe
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week 2 Month Mar Time 02:00
	To: Day Sun Week First Month Nov Time 02:00
Non-recurring	From: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
	To: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM

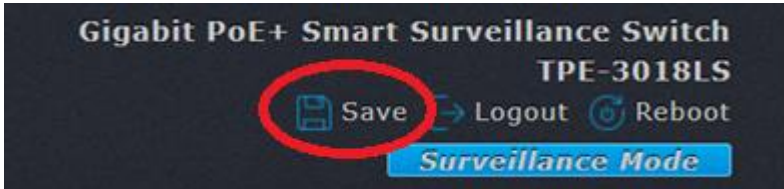
- **Operational Status** – Displays the current date and time settings configured on the device.

Operational Status	
Current Time	2000-01-01 00:20:15 UTC-8

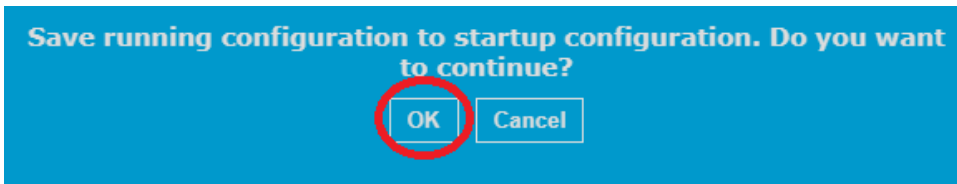
4. Click **Apply**.

Apply

5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Set the web management idle timeout

Network > Timeout Settings

The web management idle timeout settings is amount allowed idle when logged into the web management interface. When the idle timer is reached, you will automatically be logged out of the web management interface.

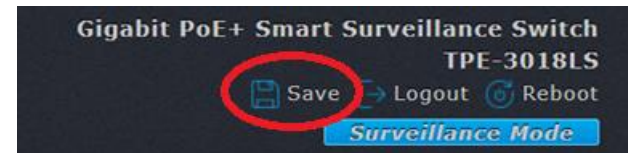
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Network** and click on **Timeout Settings**.
3. Enter the idle time interval in the **Web Idle Timeout** field in minutes, then click **Apply**.



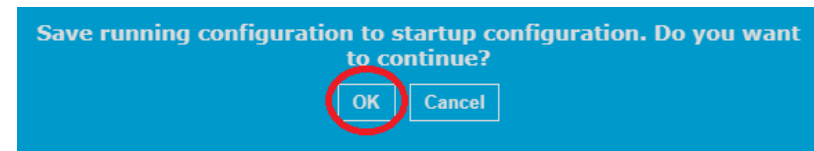
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Port

The port section will allow you to configure the switch enable/disable state, speed, duplex, flow control, and jumbo frame settings. Additionally, this section will also allow you to enable/disable long PoE configuration on each port, configure error disabled state, link aggregation settings and power savings mode.

Configure your switch ports and view port status

Port > Port Setting

This section allows you to configure the physical port parameters such as speed, duplex, flow control, and port description. This section also reports the current link status of each port and negotiated speed/duplex.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Port** and click **Port Setting**.
3. In the left column, check the port or ports you would like to configure and click **Edit** at the bottom of the page. You can configure a single port or multiple ports. State indicates whether the port is disabled or enabled and Link Status Up or Down will indicate whether or not the port is connected or disconnected.

Port Setting Table

■	Entry	Port	Type	Description	State	Link Status	Speed	Duplex
✓	1	GE1	1000M Copper		Enabled	Up	Auto (100M)	Auto (Full)
✓	2	GE2	1000M Copper		Enabled	Down	Auto	Auto
✓	3	GE3	1000M Copper		Enabled	Down	Auto	Auto
■	4	GE4	1000M Copper		Enabled	Down	Auto	Auto

Edit

4. Review the settings below, then click **Apply** to save the configuration changes.

Edit Port Setting

Port	GE1-GE3	
Description	<input style="width: 100%;" type="text"/>	
State	<input checked="" type="checkbox"/> Enable	
Speed	<input checked="" type="radio"/> Auto <input type="radio"/> 10M <input type="radio"/> Auto - 10M <input type="radio"/> 100M <input type="radio"/> Auto - 100M <input type="radio"/> 1000M <input type="radio"/> Auto - 1000M <input type="radio"/> Auto - 10M/100M	
Duplex	<input checked="" type="radio"/> Auto <input type="radio"/> Full <input type="radio"/> Half	
Flow Control	<input type="radio"/> Auto <input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Apply
Close

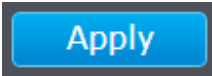
- **Port** – List the port number or range of ports to be configured. GE stands for Gigabit Ethernet followed by the port number.
- **Description** – Enter a comment or description text to more easily identify the device or network connected to the specified port or ports. (Optional)
- **State** – Checking this option enables the port, unchecking this option disables the port.
- **Speed** – Select the speed configuration for the port. Selecting Auto will set the port to auto-negotiate 10Mbps/100Mbps/1000Mbps. Selecting Auto – 100M will auto-negotiate the speed but can only link at a maximum speed of 100Mbps or below 10Mbps. If you would like to set a specific speed without auto-negotiation, select 10M, 100M, or 1000M to lock down the port speed.
- **Duplex** – Select the duplex configuration for the port. Selecting Auto will set the port to auto-negotiate the duplex. If you would like to set a specific duplex setting on a specific port or ports, select Full or Half.

- **Flow Control** – Select the flow control configuration of the port. Selecting Auto will automatically enable or disable flow control on the specific depending on the flow control setting on the other side of the link. If you would like to set a specific flow control setting for the port or ports, select Enable or Disable.

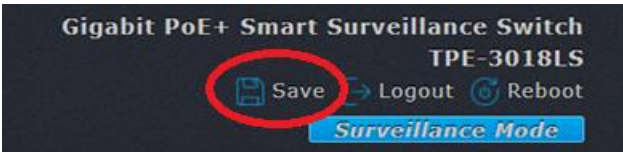
Note: When selecting a **Mode** setting, the following points apply:

- When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch.
- A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.
- The only valid setting for the SFP ports is Auto-Negotiation.

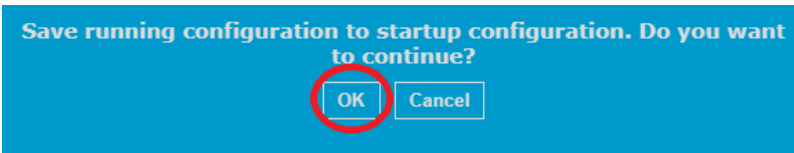
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Enable long-range PoE mode on PoE ports

Port > Long Range Mode

This section allows you to enable or disable long-range PoE feature on the switch PoE+ ports to extend the PoE+ power across the Ethernet cable up to 656 ft. (200m). The PoE+ range will be extended however, the link speed will be limited to only 10Mbps.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Port** and click **Long Range Mode**.
3. In the table, click the drop-down list under **State** next to the port number (ex: GE1 Gigabit Ethernet Port 1) and select **Enable** to enable long-range PoE mode for the PoE+ port.

Long Range Mode Table

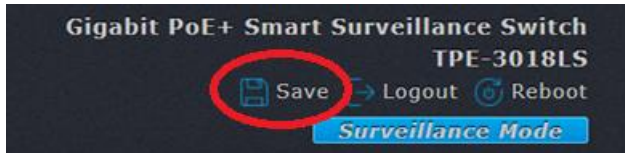
Enable long range mode will double the cabling distance but reduce the speed to 10Mbps.

Port	State
GE1	Disable ▼
GE2	Disable ▼
GE3	Disable ▼

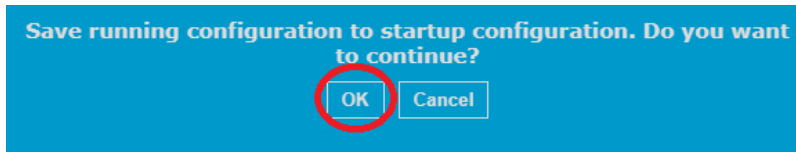
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Error Disabled port state

Port > Error Disabled

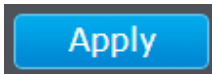
This section will allow you to trigger ports to enter “Error Disabled” state by conditions or events configured in the switch. When switch ports have entered “Error Disabled” state, they will no longer pass traffic to prevent undesired traffic to reach the rest of the network until the end of the configured recovery interval is reached. Once the recovery interval is reached and the triggered event is resolved, the switch port will return to normal operation.

1. Log into your switch management page (see [“Access your switch management page”](#) on page 11).
2. Click on **Port** and click **Error Disabled**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.
 - **Recovery Interval:** Enter the duration in seconds that the port will stay in “error disabled” state when an event is triggered. After the recovery interval has expired, the port will return to normal operation until an event is triggered on the port.
 - **BPDU Guard** – Check this option to trigger “error disabled” port state for the BPDU guard configuration. BPDU guard must be configured under the Spanning Tree > Port Setting section.

- **UDLD** - Check this option to trigger “error disabled” port state for the UDLD configuration. UDLD must be configured under the Diagnostics > UDLD section.
- **Self Loop** - Check this option to trigger “error disabled” port state if there is a loop detected on the switch.
- **Broadcast Flood** - Check this option to trigger “error disabled” port state if there a broadcast flood detected on the switch. Additional configuration for broadcast flood prevention can also be configured under the Security > Storm Control section.
- **Unknown Multicast Flood** - Check this option to trigger “error disabled” port state for the Unknown Multicast Flood configuration. Unknown Multicast Flood must be configured under Multicast > General. Additional configuration for broadcast flood prevention can also be configured under the Security > Storm Control section.
- **Unicast Flood** - Check this option to trigger “error disabled” port state if there is a unicast flood detected on the switch. Additional configuration for broadcast flood prevention can also be configured under the Security > Storm Control section.
- **ACL** - Check this option to trigger “error disabled” port state for the ACL configuration. ACL must be configured under the ACL section.
- **Port Security** - Check this option to trigger “error disabled” port state for the Port Security configuration. Port Security must be configured under the Security > Port Security section.
- **DHCP Rate Limit** - Check this option to trigger “error disabled” port state for the DHCP Rate Limit configuration. DHCP Rate Limit must be configured under the Security > DHCP Snooping > Property section.
- **ARP Rate Limit** - Check this option to trigger “error disabled” port state for the ARP Rate Limit configuration. ARP Rate Limit must be configured under the Security > IP Source Guard > Port Setting section.

Recovery Interval	<input type="text" value="300"/>	Sec (30 - 86400)
BPDU Guard	<input type="checkbox"/>	Enable
UDLD	<input type="checkbox"/>	Enable
Self Loop	<input type="checkbox"/>	Enable
Broadcast Flood	<input type="checkbox"/>	Enable
Unknown Multicast Flood	<input type="checkbox"/>	Enable
Unicast Flood	<input type="checkbox"/>	Enable
ACL	<input type="checkbox"/>	Enable
Port Security	<input type="checkbox"/>	Enable
DHCP Rate Limit	<input type="checkbox"/>	Enable
ARP Rate Limit	<input type="checkbox"/>	Enable

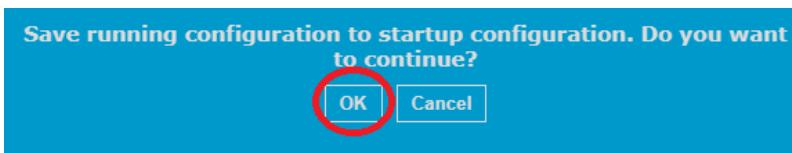
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Trunk/Link Aggregation settings

Port > Link Aggregation

The trunking function enables the cascading of two or more ports for a combined larger total bandwidth. Up to 8 trunk groups may be created. Add a trunking Name and select the ports to be trunked together, and click Apply to activate the selected trunking groups.

Important Note: Do not connect the cables of a port trunk to the ports on the switch until you have configured the ports on both the switch and the end nodes. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Port**, click on **Link Aggregation**, and click on **Group**.
3. Review the settings. For each trunk group, click **Apply** to save changes.
 - **Load Balance Algorithm** – You can select either MAC Address or IP-MAC Address algorithms. The load balance algorithms must be configured to match on both sides of link aggregation link group.

Select a Link Aggregation Group or LAG to configure and click **Edit**. Click **Apply** to save the changes.

	LAG	Name	Type	Link Status
<input checked="" type="radio"/>	LAG 1		---	---
<input type="radio"/>	LAG 2		---	---
<input type="radio"/>	LAG 3		---	---
<input type="radio"/>	LAG 4		---	---
<input type="radio"/>	LAG 5		---	---
<input type="radio"/>	LAG 6		---	---
<input type="radio"/>	LAG 7		---	---
<input type="radio"/>	LAG 8		---	---

- **Name** – Enter a name or description to identify the LAG. (optional)
- **Type** – Select the LAG type, Static or 802.3ad dynamic LACP.
- **Member** – In the Available Port column, select the ports to add to the LAG and click the > add the ports to the Selected Ports list. You can select multiple ports at the same time by holding the Ctrl or Shift key. You can remove ports by selecting the ports in the Selected Port list and clicking < .

Edit Link Aggregation Group

LAG	1		
Name	<input style="width: 90%;" type="text"/>		
Type	<input checked="" type="radio"/> Static <input type="radio"/> LACP		
Member	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	<input type="button" value=">"/> <input type="button" value="<"/>	Selected Port <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>

Under **Link Aggregation** and **Port Setting**, allows you to enable or disable the LAG, configured the speed, duplex, and flow control of the LAG. Select the LAG group in the list and click **Edit**. Click **Apply** to save the changes.

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input checked="" type="checkbox"/>	LAG 1	eth1000M	test	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 2			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Edit Port Setting

Port	LAG1		
Description	<input style="width: 90%;" type="text" value="test"/>		
State	<input checked="" type="checkbox"/> Enable		
Speed	<input checked="" type="radio"/> Auto <input type="radio"/> 10M <input type="radio"/> Auto - 10M <input type="radio"/> 100M <input type="radio"/> Auto - 100M <input type="radio"/> 1000M <input type="radio"/> Auto - 1000M <input type="radio"/> Auto - 10M/100M		
Flow Control	<input type="radio"/> Auto <input type="radio"/> Enable <input checked="" type="radio"/> Disable		

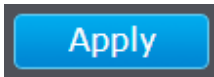
If you are using 802.3ad dynamic LACP, you can the port priority and timeout settings under **Link Aggregation** and **LACP**. Select the port or ports to configure and click **Edit** to modify the configuration.

<input type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input type="checkbox"/>	1	GE1		Long
<input checked="" type="checkbox"/>	2	GE2		Long
<input checked="" type="checkbox"/>	3	GE3		Long

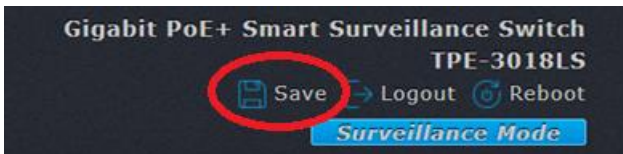
Edit LACP Port Setting

Port	GE2-GE3
Port Priority	<input type="text" value="1"/> (1 - 65535, default 1)
Timeout	<input checked="" type="radio"/> Long <input type="radio"/> Short

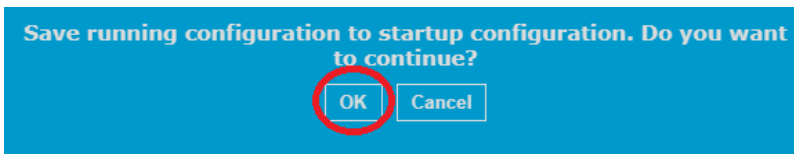
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure port power savings

Port > EEE

The IEEE 802.3az standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.3az EEE compliance. By default, the switch disabled the IEEE 802.3az EEE function. Users can enable this feature via the IEEE802.3az EEE setting page.

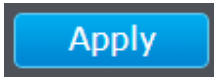
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Port** and click on **EEE**.
3. Check the port or multiple ports to configure EEE power savings and click **Edit**.

<input type="checkbox"/>	Entry	Port	State	Operational Status
<input type="checkbox"/>	1	GE1	Disabled	Disabled
<input type="checkbox"/>	2	GE2	Disabled	Disabled
<input checked="" type="checkbox"/>	3	GE3	Disabled	Disabled
<input type="checkbox"/>	4	GE4	Disabled	Disabled
<input type="checkbox"/>	5	GE5	Disabled	Disabled
<input type="checkbox"/>	6	GE6	Disabled	Disabled
<input type="checkbox"/>	7	GE7	Disabled	Disabled
<input type="checkbox"/>	8	GE8	Disabled	Disabled
<input type="checkbox"/>	9	GE9	Disabled	Disabled
<input type="checkbox"/>	10	GE10	Disabled	Disabled
<input type="checkbox"/>	11	GE11	Disabled	Disabled
<input type="checkbox"/>	12	GE12	Disabled	Disabled
<input type="checkbox"/>	13	GE13	Disabled	Disabled
<input type="checkbox"/>	14	GE14	Disabled	Disabled
<input type="checkbox"/>	15	GE15	Disabled	Disabled
<input type="checkbox"/>	16	GE16	Disabled	Disabled
<input type="checkbox"/>	17	GE17	Disabled	Disabled
<input type="checkbox"/>	18	GE18	Disabled	Disabled

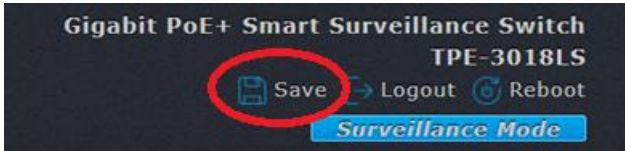
4. In the Edit EEE Setting, check **Enable** to enable EEE power savings on the port or multiple ports.

Edit EEE Setting	
Port	GE3
State	<input checked="" type="checkbox"/> Enable

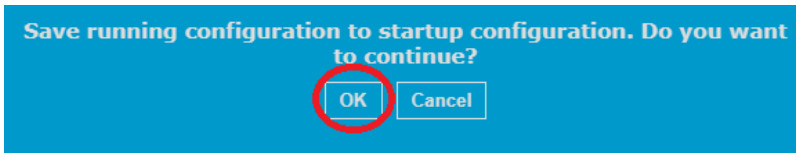
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Enable jumbo frame support

Port > Jumbo Frame

Enabling jumbo frame support will allow your switch to send and receive frames larger than the standard size (Up to 10KB size max.).

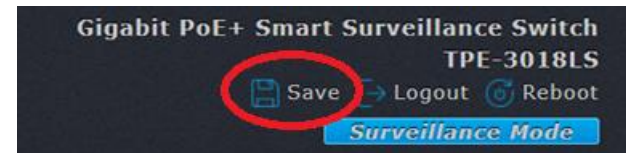
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Port** and click on **Jumbo Frame**.
3. Check the **Enable** option to enable jumbo frame support and enter the max. frame size in the field provided in bytes.

Jumbo Frame	<input checked="" type="checkbox"/> Enable
	<input type="text" value="1518"/> Byte (1518 - 10000, default 1518)

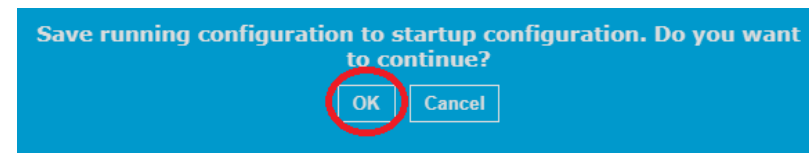
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



ONVIF

This section will allow you to configure the ONVIF features available on the switch such as ONVIF device discovery and authorization. Apply configuration settings to ONVIF compliant IP cameras such as IP address settings, changing passwords, create users, and firmware upgrades. The switch is capable of discovering and applying configuration settings to ONVIF compliant devices connected to the same IP address subnet. The Surveillance Mode User Interface may provide more graphical-based tools in monitoring your devices and applying configuration settings.

Discovering and authorizing ONVIF compliant devices

ONVIF > Discovery > IP Camera

After the surveillance switch has discovered the ONVIF compliant device, the devices must be authorized with the surveillance switch to apply configuration changes to the ONVIF devices.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF**, click on **Discovery**, and click on **IP Camera**. The will list will display a list of the discovered ONVIF compliant IP cameras found on your network. The list will also display the IP address, MAC address, and port the device is connected. If the device or devices are connected to another switch in your network, the list will display the connected port as the uplink port from your surveillance switch to your network.

Device Name	IP Address	MAC Address	Port ID	Status
IPC_GE17	192.168.10.109		GE17	unAuth
IPC_GE01	192.168.10.110		GE1	unAuth
IPC_GE13	192.168.10.161		GE13	unAuth

3. Before the surveillance switch can apply any configuration settings to your ONVIF compliant IP cameras, you must authorize by entering the ONVIF administrator credentials for each device.

Note: The IP camera administrator user name and password must be configured on the IP cameras first before they can be used with the surveillance switch. Some IP cameras may not have configuration options specific to ONVIF but may still comply with ONVIF. In this case, the IP camera management access user name and password may be the same as the ONVIF administrator user name and password.

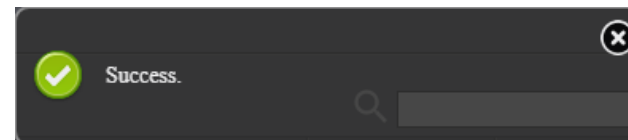
4. To authorize an ONVIF compliant IP camera, check the IP camera in the list and click **Auth**.

Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/> IPC_GE17	192.168.10.109		GE17	unAuth
<input type="checkbox"/> IPC_GE01	192.168.10.110		GE1	unAuth
<input type="checkbox"/> IPC_GE13	192.168.10.161		GE13	unAuth

5. Under the IPC Authorization section, enter the ONVIF administrator user name and password in the fields provided and click **Apply**. A success message will appear indicating that the IP camera has been successfully authorized. Under the Status column next to the device, the status will change from unAuth to Auth.

Note: If you are unable to successfully authorize the IP camera, please double check your ONVIF administrator credentials. You can also try to reboot the IP camera.

Device Name	IPC_GE17
Username	admin
Password



Device Name	IP Address	MAC Address	Port ID	Status
<input type="checkbox"/> IPC_GE17	192.168.10.109		GE17	Auth
<input type="checkbox"/> IPC_GE01	192.168.10.110		GE1	unAuth
<input type="checkbox"/> IPC_GE13	192.168.10.161		GE13	unAuth

Applying IP address settings to ONVIF authorized devices

ONVIF > Discovery > IP Camera

After ONVIF compliant devices have been discovered and successfully authorized, you can apply IP address configuration settings to these devices from the surveillance switch interface.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF**, click on **Discovery**, and click on **IP Camera**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Edit**.

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE17	192.168.10.109		GE17	Auth
<input type="checkbox"/>	IPC_GE01	192.168.10.110		GE1	unAuth
<input type="checkbox"/>	IPC_GE13	192.168.10.161		GE13	Auth

4. Under the IPC Device Info Edit section, you can view additional device information, modify the Device Name and IP address configuration.

IPC Device Info Edit

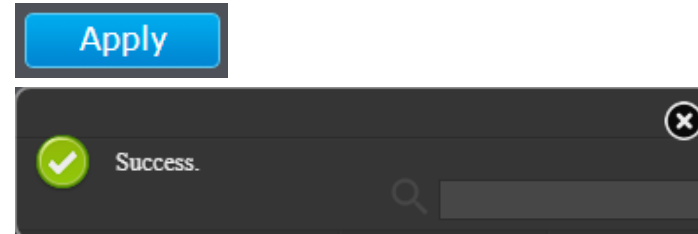
Basic info

Device Name	<input type="text" value="IPC_GE17"/>
MAC Address	
Manufacturer	TRENDnet
Model Name	TV-IP316PI
SN	
HardwareId	88

5. Scroll down the window to view or modify the device IP address configuration.

Firmware Version	V5.4.6 build 190118
IP info	
Address Type	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
IPv4 Address	<input type="text" value="192.168.10.109"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IPv4 Default Gateway	<input type="text" value="192.168.1.1"/>
Token	eth0

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.



Note: After the configuration changes have been successfully applied, the device will appear in the list with the updated information.

Changing the ONVIF device administrator password

ONVIF > Device Authentication

After ONVIF compliant devices have been discovered and successfully authorized, you can change the ONVIF administrator password of the ONVIF compliant devices.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ONVIF** and click on **Device Authentication**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Edit**.

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE17	192.168.10.109		GE17	Auth
<input type="checkbox"/>	IPC_GE01	192.168.10.107		GE1	Auth
<input type="checkbox"/>	IPC_GE13	192.168.10.161		GE13	Auth

4. Under the **IP Camera List** section below, a list of the current user accounts of the ONVIF device will be listed. To modify the ONVIF administrator password, check the device in the list with User Level admin and click **Edit**.

IP Camera List

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Device Name	User name	User Level	Port ID	MAC Address
<input checked="" type="checkbox"/>	IPC_GE17	admin	admin	GE17	

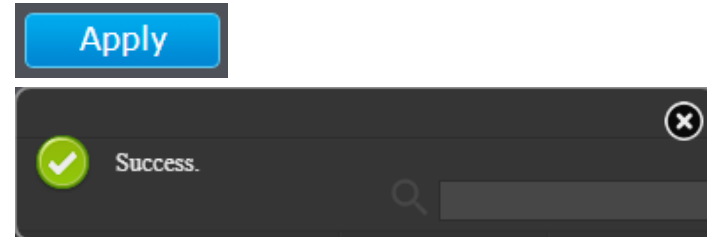
5. Scroll down to the **Edit User Account** section and you can enter in the administrator password settings in the password fields provided.

Note: Please note that the ONVIF user password typically requires eight characters for accounts.

Edit User Account

Username	admin
Password	<input type="password"/>
Confirm Password	<input type="password"/>
User Level	<input checked="" type="radio"/> Admin <input type="radio"/> operator <input type="radio"/> User

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.



Creating new ONVIF users in the ONVIF device

ONVIF > Device Authentication

After ONVIF compliant devices have been discovered and successfully authorized, you create new ONVIF users to those devices if supported.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **ONVIF** and click on **Device Authentication**.
3. For the ONVIF devices that have been successfully authorized, check the device in the list and click **Edit**.

<input type="checkbox"/>	Device Name	IP Address	MAC Address	Port ID	Status
<input checked="" type="checkbox"/>	IPC_GE17	192.168.10.109		GE17	Auth
<input type="checkbox"/>	IPC_GE01	192.168.10.107		GE1	Auth
<input type="checkbox"/>	IPC_GE13	192.168.10.161		GE13	Auth

4. Under the **IP Camera List** section below, a list of the current user accounts of the ONVIF device will be listed. To create a new ONVIF user for the device, check the device in the list and click **Add**.

IP Camera List

Showing entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Device Name	User name	User Level	Port ID	MAC Address
<input checked="" type="checkbox"/>	IPC_GE17	admin	admin	GE17	

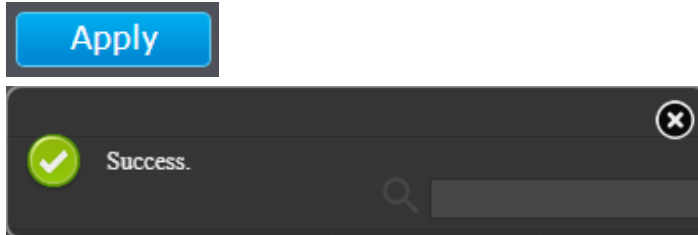
5. Scroll down to the **Add User Account** section and enter the new account user name and password in the fields provided. For the User Level, select Operator or User.

Note: Please note that the ONVIF user password typically requires eight characters for accounts.

Add User Account

Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
User Level	<input type="radio"/> Admin <input type="radio"/> operator <input checked="" type="radio"/> User

6. After you have applied configuration changes, scroll to the bottom of the window and click **Apply**. A success message will appear if the configuration changes were successfully applied.



Upgrade ONVIF device firmware

ONVIF > Device FW Upgrade

After ONVIF compliant devices have been discovered and successfully authorized, you can upgrade the firmware of the ONVIF device from the surveillance switch interface.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **ONVIF** and click on **Device FW Upgrade**.
3. Depending on your web browser at the top, for the **Filename**, click **Browse** or **Choose File** and navigate to the folder on your computer where the unzipped firmware file for the ONVIF device is located and select it. Then click **Apply** to upload the firmware file to the surveillance switch.

Filename	empty
Filename	<input type="button" value="Choose File"/> No file chosen

4. After the firmware file has been successfully uploaded, a success message will appear indicating that the firmware file was successfully uploaded. Click **Done**.

Upgrade Done

5. The firmware file name will now appear under Filename.

Filename	digicap.dav
Filename	<input type="button" value="Choose File"/> No file chosen

6. In the IP Camera List, check the device you would like to upgrade with the previously loaded firmware file, then click **Upgrade**.

Note: If you have multiple devices of the same model that use the same firmware file, you can upgrade multiple devices of the same model by checking multiple devices in the list before clicking Upgrade.

IP Camera List

Showing All entries Showing 1 to 3 of 3 entries

<input type="checkbox"/>	Port ID	Brand	Model	Firmware Version	Status
<input type="checkbox"/>	GE17	TRENDnet	TV-IP316PI	V5.4.6 build 190118	stand by
<input type="checkbox"/>	GE1	TRENDnet	TV-IP318PI	V5.5.3 build 200327	stand by
<input checked="" type="checkbox"/>	GE13	TRENDnet	TV-IP420P	V5.4.3 build 180621	stand by

The Status will change to uploading indicating that the firmware of the ONVIF device is upgrading.

IP Camera List

Showing All entries Showing 1 to 3 of 3 entries

<input type="checkbox"/>	Port ID	Brand	Model	Firmware Version	Status
<input type="checkbox"/>	GE17	TRENDnet	TV-IP316PI	V5.4.6 build 190118	stand by
<input type="checkbox"/>	GE1	TRENDnet	TV-IP318PI	V5.5.3 build 200327	stand by
<input type="checkbox"/>	GE13	TRENDnet	TV-IP420P	V5.4.3 build 180621	uploading

If the firmware upgrade was successful, the Status will indicate that upgrade was successful.

IP Camera List

Showing All entries Showing 1 to 3 of 3 entries

<input type="checkbox"/>	Port ID	Brand	Model	Firmware Version	Status
<input type="checkbox"/>	GE17	TRENDnet	TV-IP316PI	V5.4.6 build 190118	stand by
<input type="checkbox"/>	GE1	TRENDnet	TV-IP318PI	V5.5.3 build 200327	stand by
<input type="checkbox"/>	GE13	TRENDnet	TV-IP420P	V5.4.3 build 180621	upload succeed

Note: After the ONVIF device has successfully upgraded firmware and reboots, you may need to re-authorize the ONVIF device again under Discovery > IP Camera.

PoE (Power over Ethernet)

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE-compatible devices wherever they are needed without having to worry about whether there is power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The Gigabit Smart Surveillance PoE+ Switch is a PSE device which provides DC power to the network cable and functions as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The Gigabit Web Smart PoE+ Switch supports all five classes.

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	25.5W to 38.9W

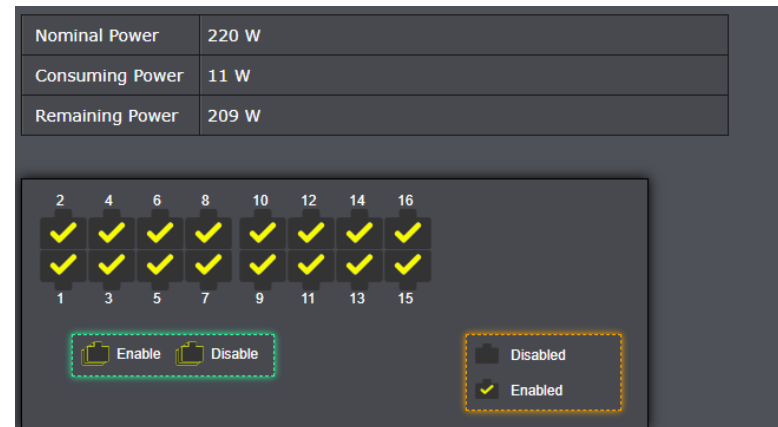
Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs. Port Prioritization As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs.

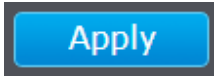
Enable or disable PoE

PoE > PoE Enable/Disable

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **PoE** and click on **PoE Enable/Disable**.
3. By default, all PoE+ ports are configured with PoE enabled indicated by the checkmark. To disable PoE on a specific, click the port to uncheck and click **Apply** to disable PoE on the selected port. To enable PoE on the specific port, click the port to check it and click **Apply** to enable PoE on the selected port.
 - **Nominal Power** – Displays the maximum PoE power budget in watts.
 - **Consuming Power** – Displays the current PoE power provided to PoE devices or PDs (Powered Devices) in watts.
 - **Remaining Power** - Indicates the port with a specific PoE status and that you are configuring.



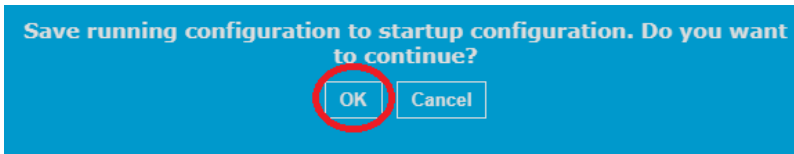
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



PoE Scheduling

PoE > PoE Scheduling

This section allows you to set a schedule for each PoE port when PoE should be enabled.

Note: Please make sure to set your time and date settings accordingly under Network > System Time before using this feature.

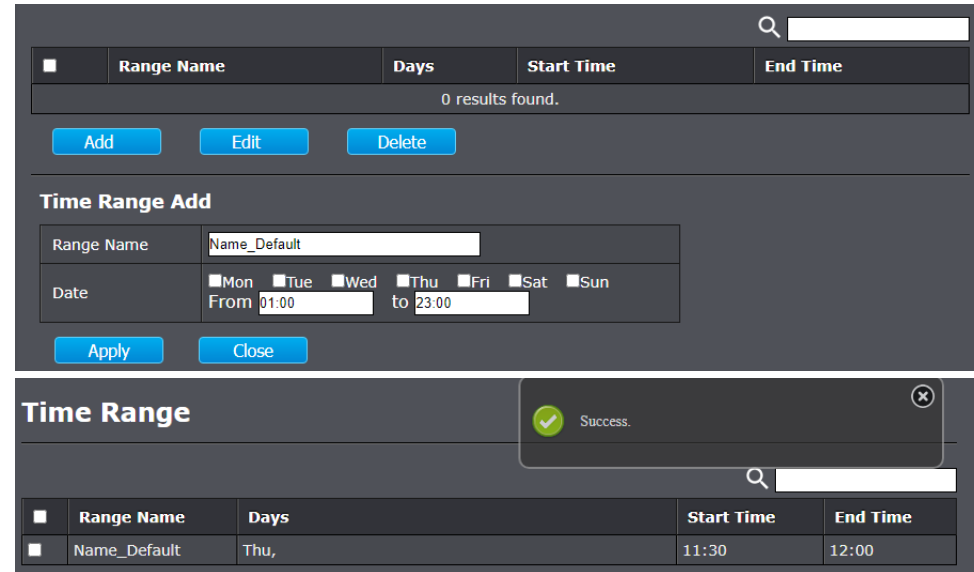
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **Management** and click on **Time Range** and click **Add** to add a new schedule.

3. Review the settings below.

- **Range Name** - Enter a name or description to easily identify the schedule (optional)

- **Date** – Select the days that PoE should be enabled and enter the time range **From** and **To** (24-hour format). Click **Apply** to save the schedule configuration and the schedule entry will appear in the list.

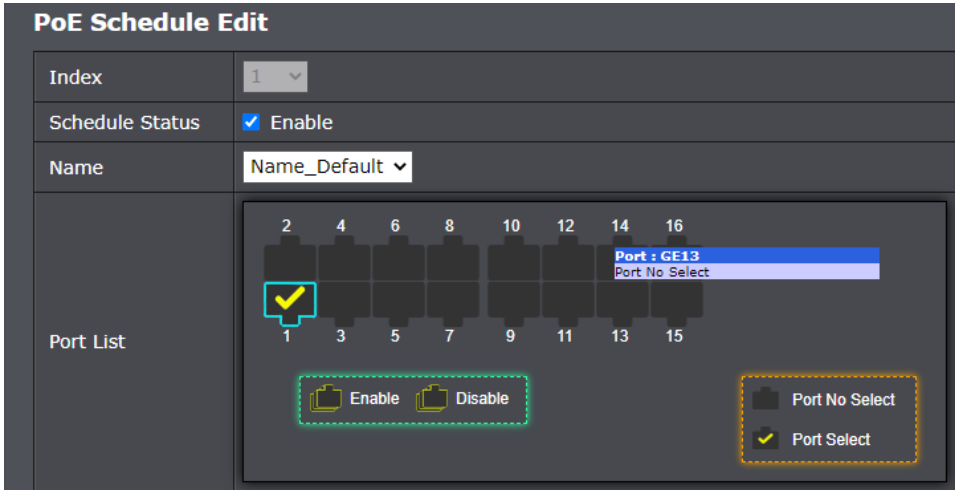


3. Click on **PoE** and click on **PoE Scheduling**. Check the first entry in the list and click **Edit**.

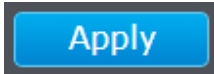
Index	Name	Port List	Schedule Status
1	None		Disable



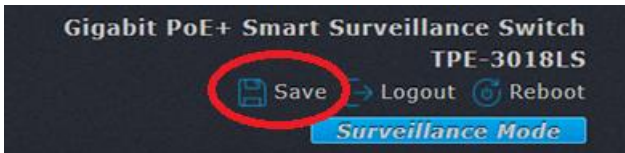
4. Under the PoE Schedule Edit section, check the **Schedule Status** option to enable PoE scheduling. Click the **Name** drop-down list to select the schedule you created and check the PoE port or ports you would like to assign the schedule.



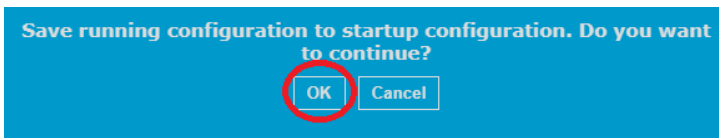
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



PD Alive Check

PoE > PD Alive Check

This section allows you to configure a ping to a specific PoE device on a specific PoE port and if the ping becomes unresponsive the switch will automatically disable and re-enable the PoE port in an attempt to automatically recover the PoE device (PD powered device).

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **PoE** and click on **PD Alive Check**.
3. Check the PoE port with the PoE device connected to you would like to configure for PD alive check and click **Edit**.

Entry	Port	Mode	ping PD IP Address	Interval Time	Retry Count	Action	Reboot Time	Conne
1	GE1	Disable	0.0.0.0	30	2	None	90	Off

Edit

4. Check the **Enable** option for Status to enable PD alive check on the selected port. Enter the IP Address for the PoE device under the **ping PD IP Address** (ex: 192.168.10.107)

Review the additional settings below.

- **Interval Time** – Enter the time in seconds each time the switch will check for a ping response from the PoE device. (Range: 10 – 300)
- **Retry Count** – In the case that a ping response fails, enter the number of times the switch will retry for a ping response before disabling and re-enabling the PoE port. (Range: 1-5)
- **Action** – An option must be selected for PD alive check to function.
 - **None** – If the ping response fails according to the time parameters set, no action will be taken.
 - **PD Reboot** – If the ping response fails according to the time parameters set, the switch will disable and re-enable the PoE port attempting to automatically recover the connected PoE device.

- **Reboot&Alarm** - If the ping response fails according to the time parameters set, the switch will disable and re-enable the PoE port attempting to automatically recover the connected PoE device and also send out an email notification is configured.
- **Alarm** - If the ping response fails according to the time parameters set, the switch will only send out an email notification if configured.
- **Reboot Time** - If the ping response fails according to the time parameters set, enter the time in seconds from the time the PoE port is disabled to the time the PoE port is re-enabled. (Range: 30-180)

PD Alive Check Table	
Port List	GE1
Status	<input checked="" type="checkbox"/> Enable
ping PD IP Address	<input type="text" value="0.0.0.0"/>
Interval Time	<input type="text" value="30"/> Sec (10 - 300, default 30)
Retry Count	<input type="text" value="2"/> (1 - 5, default 2)
Action	None <input type="button" value="v"/>
Reboot Time	<input type="text" value="90"/> Sec (30 - 180, default 90)

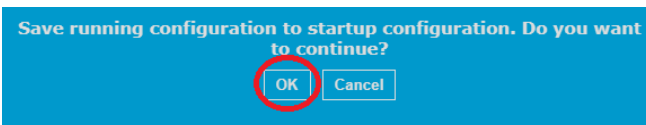
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



VLAN

Add, modify, and remove VLANs

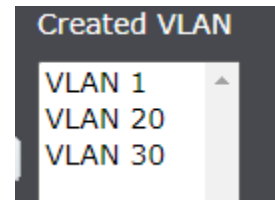
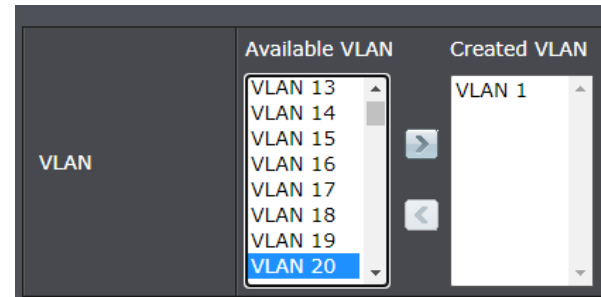
VLAN

A VLAN is a group of ports that can be anywhere in the network but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **VLAN**, click on **VLAN**, and click on **Create VLAN**.
3. To create a new VLAN, under the **Available VLAN** list, select the VLAN with VID and click **>** to add the **Created VLAN** list to create the new VLAN, then click **Apply**.

Note: You can select multiple VLANs by holding shift or ctrl.



4. In the VLAN table, to configure the VLAN name, check the VLAN and click **Edit**. Enter a VLAN name in the field provided and click **Apply**.

<input type="checkbox"/>	VLAN	Name	Type
<input type="checkbox"/>	1	default	Default
<input checked="" type="checkbox"/>	20	VLAN0020	Static
<input type="checkbox"/>	30	VLAN0030	Static

Edit VLAN Name

Name

5. To configure the VLAN port membership, click **VLAN** and click **VLAN Configuration**. Review the settings below and click **Apply** after completing configuration.

- **VLAN** – Click the drop-down list to and select which VLAN to configure VLAN port membership.
- **Excluded** – The port will not be a member of the VLAN but may be added through dynamic protocols.
- **Forbidden** – The port will not be a member of the VLAN and cannot be added to the VLAN through dynamic protocols.
- **Tagged** – The port will be a tagged member of the VLAN.

Note: On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded. Typically, tagged ports are used for VLAN connectivity between links to other managed switches. Some network devices or network cards may have the ability to assign VLAN tag information for connectivity to a tagged VLAN switch port. If a switch port is set as a tagged VLAN member, the other side of the link should also be set as a tagged VLAN member with the same VLAN ID for communication.

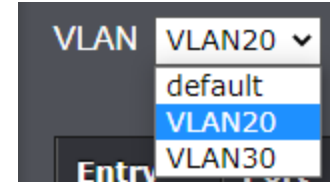
- **Untagged** – The port will be an untagged member of the VLAN.
- Note:** Untagged VLAN ports are used to connect edge devices (VLAN unaware) such as computers, laptops, and printers to a specified VLAN. Any ports set as

untagged members of a VLAN will automatically set the PVID (port VLAN ID) to the same as the VLAN ID. The PVID can be manually configured under VLAN > Port Setting.

Example: In the example below, we will assign ports 1-2 as untagged VLAN members of VLAN VID 20 and ports 3-4 as untagged VLAN members of VLAN VID 30. We will also configure port 18 as a tagged member of both VLAN 20 and VLAN 30 to pass traffic across the single link for both VLANs.

VLAN VID 20 Configuration

- Click the VLAN drop-down list and select **VLAN20**.



- Select **Untagged** for ports 1-2.

Entry	Port	Mode	Membership	PVID
1	GE1	Trunk	<input type="radio"/> Excluded <input type="radio"/> Forbidden <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
2	GE2	Trunk	<input type="radio"/> Excluded <input type="radio"/> Forbidden <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>

- Select **Tagged** for port 18.

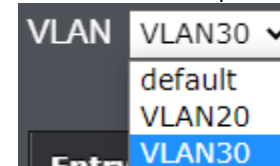
18	GE18	Trunk	<input type="radio"/> Excluded <input type="radio"/> Forbidden <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
----	------	-------	---	--------------------------

- Click **Apply** to save the VLAN 20 port membership configuration.



VLAN VID 30 Configuration

- Click the VLAN drop-down list and select **VLAN30**.



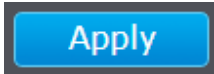
- Select **Untagged** for ports 3-4.

3	GE3	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
4	GE4	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>

- Select **Tagged** for port 18.

18	GE18	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Forbidden	<input checked="" type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>
----	------	-------	--------------------------------	---------------------------------	---	--------------------------------	--------------------------

- Click **Apply** to save the VLAN 30 port membership configuration.



Modify VLAN Port Membership

VLAN > VLAN > Membership

After VLANs have been created, this section allows you to modify VLAN port membership, however, it is still recommended to configure VLAN port membership through the VLAN > VLAN Configuration section. This section is more useful when modifying VLAN membership for a link aggregation group (LAG).

1. Log into your switch management page (see [“Access your switch management page”](#) on page 11).
2. Click on **VLAN**, click on **VLAN**, and click on **Membership**.
3. In the list, select the port or LAG and click **Edit**.

Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input checked="" type="radio"/>	1 GE1	Trunk	20UP	20UP



4. Review the settings below.
 - **Membership** – The list on the left-hand displays the current VLAN membership (VLAN IDs) for the selected port. The list on the right-hand displays the other VLAN IDs available.

Note: The VLAN IDs available in the list may not appear if the VLANs have not been created under VLAN > Create VLAN section.

To modify port membership, select the VLAN ID according and use the arrow buttons to change VLAN port membership.

- **Excluded** – Modifies the type of VLAN membership. The port will not be a member of the VLAN but may be added through dynamic protocols.
- **Forbidden** – Modifies the type of VLAN membership. The port will not be a member of the VLAN and cannot be added to the VLAN through dynamic protocols.
- **Tagged** – Modifies the type of VLAN membership. The port will be a tagged member of the VLAN.

Note: On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded. Typically, tagged ports are used for VLAN connectivity between links to other managed switches. Some network devices or network cards may have the ability to assign VLAN tag information for connectivity to a tagged VLAN switch port. If a switch port is set as a tagged VLAN member, the other side of the link should also be set as a tagged VLAN member with the same VLAN ID for communication.

- **Untagged** – Modifies the type of VLAN membership. The port will be an untagged member of the VLAN.

Note: Untagged VLAN ports are used to connect edge devices (VLAN unaware) such as computers, laptops, and printers to a specified VLAN. Any ports set as untagged members of a VLAN will automatically set the PVID (port VLAN ID) to the same as the VLAN ID. The PVID can be manually configured under VLAN > Port Setting.

Edit Port Setting

Port	GE1	
Mode	Trunk	
Membership	<input type="checkbox"/> 1 <input type="checkbox"/> 30	<input type="checkbox"/> 20UP
	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged <input type="checkbox"/> PVID	

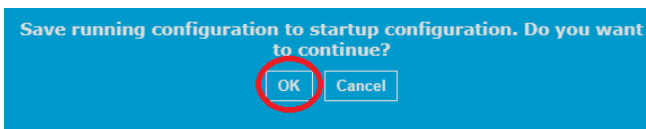
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Modify VLAN port settings

VLAN > VLAN > Port Setting

After VLANs have been created, this section allows you to modify additional VLAN port settings such as mode, port VLAN ID (PVID), acceptable frame type, and ingress filtering.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **VLAN**, click on **VLAN**, and click on **Port Setting**.
3. In the list, select the port or LAG and click **Edit**.

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering
<input checked="" type="checkbox"/>	1	GE1	Trunk	20	All	Enabled



4. Review the settings below.

- **Mode** – Select the VLAN port mode.
 - **Access** - This mode is used to connect edge devices that are VLAN unaware such as workstations. The port can only be assigned membership to a single VLAN as an untagged member port.
 - **Trunk** – This mode can allow traffic for multiple VLANs and is used to connect to other VLAN aware network devices such as switches, access points, and routers. This port can be assigned membership to multiple VLANs as a tagged member port. The port can also be assigned to a single VLAN as an untagged member also known as the native VLAN.
 - **Hybrid** – This mode is similar to Trunk mode however, also allows for control of ingress filtering and acceptable frame type.
- **PVID** – This is port VLAN ID setting for the port and is used for untagged VLAN member ports corresponding to the VLAN ID. When configuring VLAN port membership under VLAN > VLAN Configuration, the PVID is automatically to untagged VLAN member ports. You can also manually enter the PVID setting in the field provided.

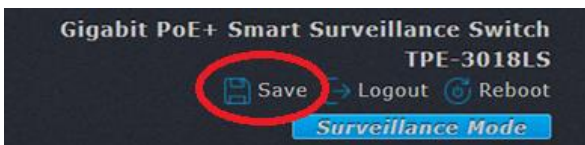
Edit Port Setting

Port	GE1
Mode	<input type="radio"/> Hybrid <input type="radio"/> Access <input checked="" type="radio"/> Trunk
PVID	20 (1 - 4094)
Accept Frame Type	<input type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag Only
Ingress Filtering	<input checked="" type="checkbox"/> Enable

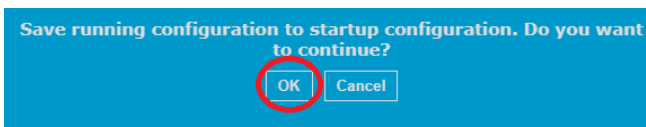
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.

**Voice VLAN**

This chapter contains a description of the Switch's Voice VLAN feature and the procedures to create, modify, and delete a voice VLAN configuration.

The Voice VLAN feature is specifically designed to maintain high quality, uninterrupted voice traffic through the switch. When talking on a voice over IP phone, a user expects to have no interruptions in the conversation and excellent voice quality. The Voice VLAN feature can be configured to meet these requirements.

CoS with Voice VLAN

The Voice VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the switch. CoS must be enabled for the Voice VLAN CoS priority to take effect. The CoS priority level that you config is applied to voice traffic on all ports of the voice VLAN. Normally, most (non-Voice) Ethernet traffic transverses the switch through lower-order egress queues. To avoid delays and interruptions in the voice data flow, the CoS priority level assigned to the voice VLAN should be mapped to a higher-order queue and the scheduling algorithm should be set to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the voice data passes through the switch.

Organization Unique Identifier (OUI)

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is embedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of the IP phone in the first three complete bytes of its MAC address.

Typically, you will find that all of the IP phones you are installing have the same OUI in common. The switch identifies a voice data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature for a port and is a dynamic voice VLAN port.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An "OUI Mask" is automatically generated and applied by the Web Management Utility software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.

It is possible to find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each OUI must be configured in the voice VLAN.

Dynamic Auto-Detection vs Manual Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the voice VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the voice VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN. The ports that you choose to configure as dynamic Auto-Detection ports must be connected directly to an IP phone. When you initially define the ports of a tagged VLAN for your voice VLAN configuration, they must be configured as a "Not Member" ports. The "Not Member" ports are eligible to dynamically join the voice VLAN when voice data is detected with a predefined OUI in the source MAC address. The port will leave the voice VLAN after a specified timeout period. This port behavior is configured with the voice VLAN Auto-Detection feature.

For the Auto-Detection feature to function, your IP phone(s) must be capable of generating 802.1Q packets with embedded VLAN ID tags. You must manually configure your IP phone(s) for the same VLAN ID as the switch's voice VLAN ID. When voice data is detected on one of the "Not Member" ports, the packets from the IP phone will contain the voice VLAN ID so they are switched within the switch's voice VLAN.

One or more ports in your voice VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the voice VLAN and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other voice VLAN network nodes such as other Ethernet switches, a telephone switch, or a DHCP server. The voice VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note: Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This ensures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the switch.

If the IP phone(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the voice VLAN.

Note: Link Layer Discovery Protocol for Media Endpoint Devices (LLDP- MED) is not supported on the switch. Each IP phone that is VLAN aware should be manually

configured for the VLAN ID that matches your voice VLAN ID. Each of the voice VLAN ports connected to an IP phone should be configured as "Not Member" ports of the tagged VLAN.

Create a Voice VLAN

Voice VLAN > Voice VLAN > Property

Note: Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your voice VLAN.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **VLAN**, click on **Voice VLAN**, and click on **Property**.
3. Review the settings. Click **Apply** to save the configuration settings.

Use the following procedure to configure voice VLAN:

- **State** – Checking the **Enable** option will enable the Voice VLAN feature. Unchecking the option will disable the Voice VLAN feature.
- **VLAN** – Click the drop-down list to select the VLAN assigned as the designated voice VLAN ID.
Note: The VLAN must be created under VLAN and VLAN Configuration first before the VLANs are available in the drop-down list.
- **CoS / 802.1p Remarking** – Check the **Enable** option to attach the specified 802.1p CoS priority tag to Voice VLAN traffic. Click the drop-down list to select the 802.1p priority tag to assign to voice VLAN traffic.
Note: For the CoS priority to be effective, QoS must be enabled.
- **Port Aging Time** - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this port will be removed from the voice VLAN. The range is 30 to 65536 minutes.

State	<input type="checkbox"/> Enable
VLAN	None
CoS / 802.1p Remarking	<input type="checkbox"/> Enable 6
Port Aging Time	1440 Min (30 - 65536, default 1440) Note: Aging Time = Port Aging Time + OUI Aging Time(30 mins)

Apply

4. Check the ports you would like to enable for voice VLAN auto-detection and click **Edit**.

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input checked="" type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet

Edit

5. Under the port setting, check **Enable** to enable voice VLAN auto-detection on the port.

- **Mode**
 - **Auto** – This option will allow a connected device to be automatically detected by OUI and automatically configure the port or ports as an untagged member of the voice VLAN.
 - **Manual** – This option will require not automatically configure any ports and the port must be configured in the Voice VLAN manually under VLAN > VLAN Configuration.
- **QoS Policy**
 - **Voice Packet** – This option will apply QoS priority only to VoIP traffic on the voice VLAN. QoS will not be applied to other types of traffic on the voice VLAN.
 - **All** – This option will apply QoS priority to all traffic on the voice VLAN.

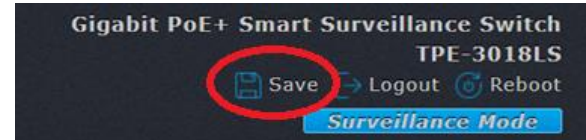
Edit Port Setting

Port	GE1
State	<input type="checkbox"/> Enable
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
QoS Policy	<input checked="" type="radio"/> Voice Packet <input type="radio"/> All

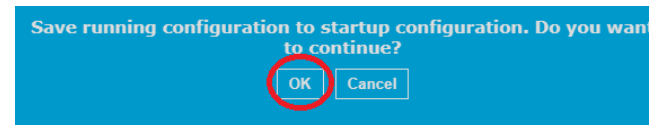
6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



Configure Voice VLAN OUI settings

VLAN > Voice VLAN > Voice OUI

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).

2. Click on **VLAN**, click on **Voice VLAN**, and click on **Voice OUI**.

3. By default, a list of preset OUIs are available. Please double check your device MAC address if the manufacturer OUI is already on the list.

Note: You can check the existing OUI in the list and click **Edit** to modify an existing OUI.

Showing All entries Showing 1 to 8 of 8 entries

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya

4. To add a new OUI to the list, click **Add**.



5. Enter the device **OUI** in the fields provided and enter a description that helps you identify the manufacturer's OUI. Then click **Apply** to add the new OUI.

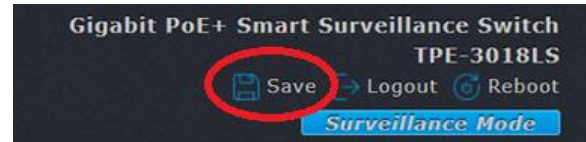
Add Voice OUI

OUI	<input type="text"/> : <input type="text"/> : <input type="text"/>
Description	<input type="text"/>

6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



MAC VLAN

The MAC VLAN feature adds the capability to assign devices to specific a specific VLAN by detecting the device MAC address. MAC address groups are created and filter by MAC address mask to determine which bits to check in the MAC address and assign them to the configured VLAN.

Note: The MAC VLAN feature can only be used if switch ports are set to Hybrid mode under VLAN > Port Setting.

Create MAC-based VLAN groups

VLAN > MAC VLAN > MAC Group

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **VLAN**, click on **MAC VLAN**, and click on **MAC Group**.

3. Click **Add** to add a new MAC VLAN group.



4. Review the settings below.

- **Group ID** – Assign a group ID to the MAC VLAN group.
- **MAC Address** – Enter the MAC address for filtering. (ex: aa:bb:cc:dd:ee:ff)
- **Mask** – Enter the mask used to filter the entered MAC address.

Note: A device MAC address consists of 12 hexadecimal characters (0-9,a-f) and each hexadecimal character is equivalent to 4 bits each character. Therefore, the total bits in a single device MAC address is 48 bits. The bit number entered will be used to determine which bits should match the MAC address entered and which bits can change starting from left to right.

Example: If MAC address aa:bb:cc:dd:ee:ff is entered and the mask entered is 16, this mask will check if the first 16 bits of the MAC address match and the remaining bits of the MAC address will not be checked, meaning all device MAC address matching aa:bb:xx:xx:xx:xx will be filtered for the new MAC VLAN group. If a mask of 48 is entered, the entire MAC address aa:bb:cc:dd:ee:ff must be matched.

Add MAC Group

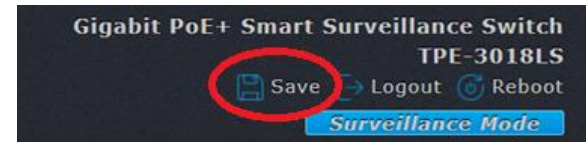
Group ID	<input type="text"/>	(1 - 2147483647)
MAC Address	<input type="text"/>	
Mask	<input type="text"/>	(9 - 48)

5 Click **Apply** save the new MAC VLAN group.



<input type="checkbox"/>	Group ID	MAC Address	Mask
<input type="checkbox"/>	1	AA:BB:CC:DD:EE:FF	16

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.

Save running configuration to startup configuration. Do you want to continue?




Configure MAC VLAN group binding

VLAN > MAC VLAN > Group Binding

After you have created the MAC VLAN group with MAC address and filter mask, you will need to bind the MAC VLAN group to the specific ports and VLAN.

Note: The MAC VLAN feature can only be used if switch ports are set to Hybrid mode under VLAN > Port Setting.

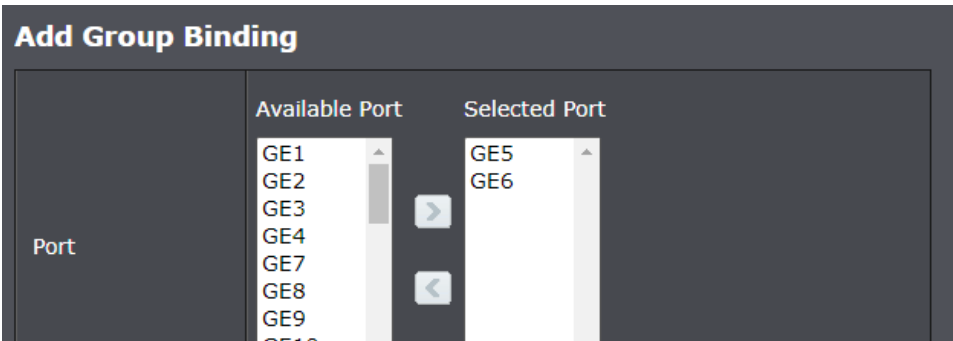
1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **VLAN**, click on **MAC VLAN**, and click on **Group Binding**.

3. Click **Add** to add a new MAC VLAN group.

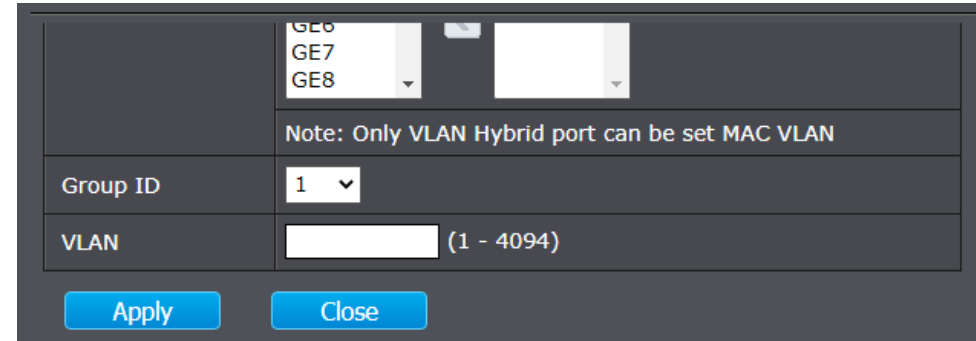


4. In the **Port** section, in the **Available Port** list, select the port to bind to the MAC-based VLAN group and use the buttons to move the port to and from the Select Port list.

Note: You can select multiple ports by hold shift or ctrl.



5. Click the **Group ID** drop-down list to select MAC VLAN group to bind and enter the VLAN ID to move the devices that match the MAC VLAN group filter.

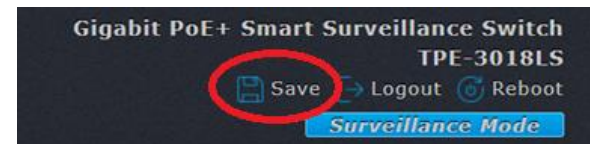


6 Click **Apply** save the new MAC VLAN group.

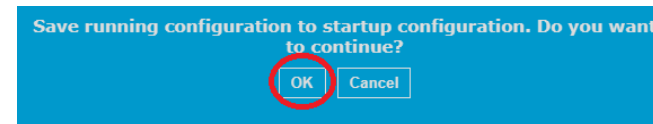


Group ID	MAC Address	Mask
1	AA:BB:CC:DD:EE:FF	16

7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



Surveillance VLAN

This chapter contains a description of the Switch's Surveillance VLAN feature and the procedures to create, modify, and delete a surveillance VLAN configuration.

The Surveillance VLAN feature is specifically designed to maintain high quality, uninterrupted IP camera/NVR video streaming traffic through the switch. When sending video surveillance video traffic, IT may require no interruptions in the traffic and excellent video quality for their surveillance network. The Surveillance VLAN feature can be configured to meet these requirements.

CoS with Surveillance VLAN

The Surveillance VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the switch. CoS must be enabled for the Surveillance VLAN CoS priority to take effect. The CoS priority level that you config is applied to video traffic on all ports of the surveillance VLAN. Normally, most (non-video) Ethernet traffic transverses the switch through lower-order egress queues. To avoid delays and interruptions in the video traffic flow, the CoS priority level assigned to the surveillance VLAN should be mapped to a higher-order queue and the scheduling algorithm should be set to Strict Priority. These settings ensure that the video data packets are processed before other types of data so that the voice quality is maintained as the video data passes through the switch.

Organization Unique Identifier (OUI)

Each IP camera/NVR manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is embedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of the IP camera in the first three complete bytes of its MAC address.

Typically, you will find that all of the IP cameras you are installing have the same OUI in common. The switch identifies a video data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the surveillance VLAN. This is important when the Auto-Detection feature for a port and is a dynamic surveillance VLAN port.

When you are configuring the surveillance VLAN parameters, you must enter the complete MAC address of at least one of your IP cameras. An "OUI Mask" is automatically generated and applied by the Web Management Utility software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is

the same, then no other IP camera MAC addresses need to be entered into the configuration.

It is possible to find more than one OUI from the same manufacturer among the IP cameras you are installing. It is also possible that your IP cameras are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP cameras being installed, then one MAC address representing each OUI must be configured in the surveillance VLAN.

Dynamic Auto-Detection vs Manual Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the surveillance VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the surveillance VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN. The ports that you choose to configure as dynamic Auto-Detection ports must be connected directly to an IP camera. When you initially define the ports of a tagged VLAN for your surveillance VLAN configuration, they must be configured as a "Not Member" ports. The "Not Member" ports are eligible to dynamically join the surveillance VLAN when video data is detected with a predefined OUI in the source MAC address. The port will leave the surveillance VLAN after a specified timeout period. This port behavior is configured with the surveillance VLAN Auto-Detection feature.

For the Auto-Detection feature to function, your IP camera(s) must be capable of generating 802.1Q packets with embedded VLAN ID tags. You must manually configure your IP camera(s) for the same VLAN ID as the switch's voice VLAN ID. When video data is detected on one of the "Not Member" ports, the packets from the IP camera will contain the surveillance VLAN ID so they are switched within the switch's surveillance VLAN.

One or more ports in your surveillance VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the surveillance VLAN and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other surveillance VLAN network nodes such as other Ethernet switches or a DHCP server. The surveillance VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note: Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This ensures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the switch.

If the IP camera(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the surveillance VLAN.

Note: The Surveillance feature can only be used if switch ports are set to Hybrid mode under VLAN > Port Setting.

Create a Surveillance VLAN

Voice VLAN > Surveillance VLAN > Property

Note: Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your surveillance VLAN.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **VLAN**, click on **Surveillance VLAN**, and click on **Property**.
3. Review the settings. Click **Apply** to save the configuration settings.

Use the following procedure to configure surveillance VLAN:

- **State** – Checking the **Enable** option will enable the Surveillance VLAN feature. Unchecking the option will disable the Surveillance VLAN feature.
- **VLAN** – Click the drop-down list to select the VLAN assigned as the designated surveillance VLAN ID.
Note: The VLAN must be created under VLAN and VLAN Configuration first before the VLANs are available in the drop-down list.
- **CoS / 802.1p Remarking** – Check the **Enable** option to attach the specified 802.1p CoS priority tag to Surveillance VLAN traffic. Click the drop-down list to select the 802.1p priority tag to assign to surveillance VLAN traffic.
Note: For the CoS priority to be effective, QoS must be enabled.
- **Port Aging Time** - This parameter indicates the amount of time, in hours, after the last IP camera's OUI was received on a port, after which this port will be removed from the surveillance VLAN. The range is 30 to 65536 minutes.

State	<input type="checkbox"/> Enable
VLAN	None ▾
CoS / 802.1p Remarking	<input type="checkbox"/> Enable 6 ▾
Port Aging Time	1440 Min (30 - 65536, default 1440) Note: Aging Time = Port Aging Time + OUI Aging Time(30 mins)

Apply

4. Check the ports you would like to enable for surveillance VLAN auto-detection and click **Edit**.

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input checked="" type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet

Edit

5. Under the port setting, check **Enable** to enable surveillance VLAN auto-detection on the port.

Note: The Surveillance feature can only be used if switch ports are set to Hybrid mode under VLAN > Port Setting.

- **Mode**
 - **Auto** – This option will allow a connected device to be automatically detected by OUI and automatically configure the port or ports as an untagged member of the surveillance VLAN.
 - **Manual** – This option will require not automatically configure any ports and the port must be configured in the Surveillance VLAN manually under VLAN > VLAN Configuration.

Edit Port Setting	
Port	GE1
State	<input type="checkbox"/> Enable Note: Only VLAN Hybrid port can be set Surveillance VLAN
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

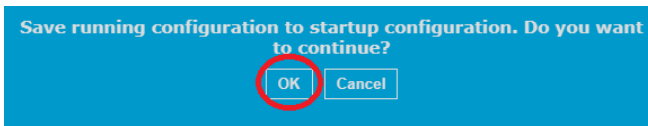
6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



Configure Surveillance VLAN OUI settings

VLAN > Surveillance VLAN > Surveillance OUI

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **VLAN**, click on **Surveillance VLAN**, and click on **Surveillance OUI**.
3. To add a new OUI to the list, click **Add**.



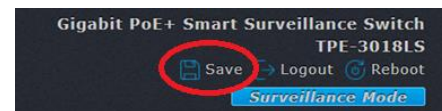
5. Enter the device **OUI** in the fields provided and enter a description that helps you identify the manufacturer's OUI. Then click **Apply to** add the new OUI.

Add Surveillance OUI	
OUI	<input type="text"/> : <input type="text"/> : <input type="text"/>
Description	<input type="text"/>

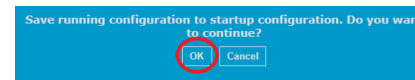
6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



MAC Address Table

This section allows you to view the switch MAC address table, add static MAC address entries to the table, and also add MAC addresses used for filtering.

View the switch MAC address table

MAC Address Table > Dynamic Address

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **MAC Address Table** and click on **Dynamic Address**.
3. The table will display a list of the dynamically learned MAC addresses. You can clear the MAC address table by clicking **Clear** or you can add one of the learned MAC address to the Static MAC address table by checking the entry and click **Add Static Address**.

Dynamic Address Table			
Showing All entries Showing 1 to 8 of 8 entries			
	VLAN	MAC Address	Port
<input type="checkbox"/>	1		GE18
<input type="checkbox"/>	1		GE18
<input type="checkbox"/>	1		GE10
<input type="checkbox"/>	1		GE13
<input type="checkbox"/>	1		GE18
<input type="checkbox"/>	1		GE18
<input type="checkbox"/>	1		GE18
<input type="checkbox"/>	1		GE18

Clear Refresh Add Static Address First Previous 1 Next Last

Add static MAC address entries

MAC Address Table > Static Address

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **MAC Address Table** and click on **Static Address**.
3. To add a static MAC address to the list, click **Add**.



4. Review the settings below.

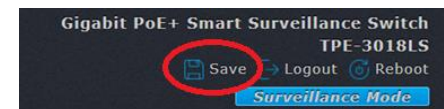
- **MAC Address** – Enter the MAC address. (ex: aa:bb:cc:dd:ee:ff)
- **VLAN** – Enter the VLAN ID that the static MAC address entry should be assigned.
- **Port** – Click the drop-down to select the port that the MAC address should be assigned.

Add Static Address	
MAC Address	<input type="text" value="00:00:00:00:00:00"/>
VLAN	<input type="text" value=""/> (1 - 4094)
Port	<input type="text" value="GE1"/>

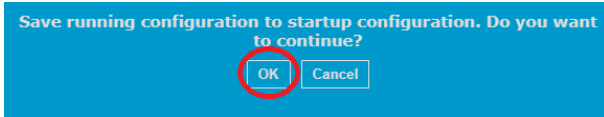
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Add MAC Addresses used in filtering

MAC Address Table > Filtering Address

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **MAC Address Table** and click on **Filtering Address**.

3. To add a static MAC address to the list, click **Add**.



4. Review the settings below.

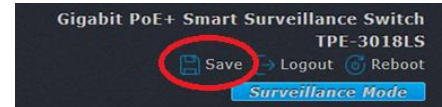
- **MAC Address** – Enter the MAC address. (ex: aa:bb:cc:dd:ee:ff)
- **VLAN** – Enter the VLAN ID that the static MAC address entry should be assigned.

Add Filtering Address	
MAC Address	<input type="text" value="00:00:00:00:00:00"/>
VLAN	<input type="text"/> (1 - 4094)

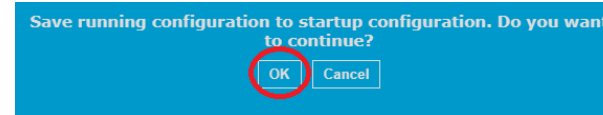
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Spanning Tree (STP, RSTP, MSTP)

Configure Spanning Tree Protocol settings

Spanning Tree > Property

Spanning Tree Protocol (STP) provides network topology for any arrangement of bridges/switches. STP also provides a single path between end stations on a network, eliminating loops. Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Spanning Tree** and click on **Property**.
3. Review the settings. Click **Apply** to save changes.
 - **State:** Check the **Enable** option to enable spanning tree on the device. Uncheck the option to disable spanning tree.
 - **Operation Mode:** Specifies the Spanning Tree Protocol (STP) mode to enable on the switch. The possible field values are:
 - **STP** – Enables STP 802.1d on the device.
 - **RSTP** – Enables Rapid STP 802.1w on the device. This is the default value.
 - **MSTP** – Enables Multiple STP 802.1s on the device.
 - **Path Cost:** Select the path cost range for calculation. This will depend on your path cost calculation method.
 - **Short** – Range 1 - 65536
 - **Long** – Range 1 – 200,000,000
 - **BPDU Handling**
 - **Filtering** – If BPDU filtering is selected for spanning tree protocol, it will check ports for sending and receiving BPDUs. If selecting filtering, then all ports with edge devices such as workstations should have BPDU Filter enabled under Spanning > Port Setting. Do not enable

BPDU filtering on ports that are connected to other switches that would be BPDU spanning tree protocol information.

- **Flooding** - If BPDU flooding is selected, this is the standard behavior where ports are flooded with BPDU information for the spanning tree protocol topology or changes in STP topology.
- **Priority:** The **Bridge Priority** has a range 0 to 61440 in increments of 4096. Specify the increment that represents the desired bridge priority value.
- **Hello Time:** The Hello Time is frequency with which the root bridge sends out a BPDU.
- **Max Age:** The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds
- **Forward Delay:** The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.
- **Tx Hold Count:** The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.
- **Region Name:** A configured name set on the switch to uniquely identify the MST (Multiple Spanning Tree). If a configuration name is not set, this field shows the MAC address of the device running MSTP.
- **Revision (0-65535):** This value, together with the configuration name, and identical vlans mapped for STP instance IDs identifies the MST region configured on the switch.
- **Max Hop:** The Max Hop Count is a parameter set in a BPDU packet when it originates. It is decremented by 1 each time it is retransmitted by the next bridge. When the Hop Count value reaches zero, the bridge drops the BPDU packet. Its range is 6 - 40 hops.
- **Bridge Identifier:** Displays the current bridge priority along with the bridge identifier (MAC Address).
- **Designated Root Bridge:** Displays the MAC address of the currently designated root bridge in the spanning tree protocol configuration.
- **Root Port:** Displays the currently assigned root port in the STP topology.
- **Root Path Cost:** Displays the current root path cost.
- **Topology Change Count:** Displays the number times the STP topology has changes since enabling the spanning tree protocol.

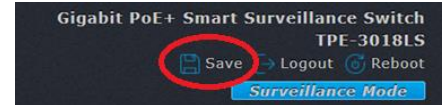
- **Last Topology Change:** Displays the time and date of the last spanning tree protocol topology change.

State	<input type="checkbox"/> Enable
Operation Mode	<input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP
Path Cost	<input checked="" type="radio"/> Long <input type="radio"/> Short
BPDU Handling	<input type="radio"/> Filtering <input checked="" type="radio"/> Flooding
Priority	<input type="text" value="32768"/> (0 - 61440, default 32768)
Hello Time	<input type="text" value="2"/> Sec (1 - 10, default 2)
Max Age	<input type="text" value="20"/> Sec (6 - 40, default 20)
Forward Delay	<input type="text" value="15"/> Sec (4 - 30, default 15)
Tx Hold Count	<input type="text" value="6"/> (1 - 10, default 6)
Region Name	<input type="text" value="3C:8C:F8:F9:D0:4A"/>
Revision	<input type="text" value="0"/> (0 - 65535, default 0)
Max Hop	<input type="text" value="20"/> (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-XX:XX:XX:XX:XX:XX
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

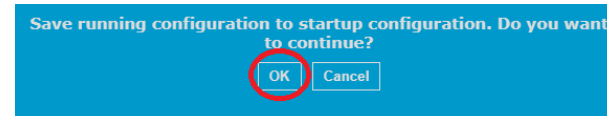
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure Spanning Tree Protocol Port settings

Spanning Tree > Port Setting

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Spanning Tree** and click on **Port Setting**.
3. Check the ports in the list you would like to edit for spanning tree protocol and click **Edit**.

<input type="checkbox"/>	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge
<input checked="" type="checkbox"/>	1	GE1	Enabled	20000	128	Disabled	Disabled	Enabled

Edit

4. In Edit Port section, review the settings below. Click **Apply** to save the configuration changes.
 - **State** – Check **Enable** to enable the port for spanning tree. By default, all ports are enabled for spanning tree but the protocol is not active until enabling spanning tree globally under Spanning Tree > Property.
 - **Path Cost** - The path cost (or bridge priority value) to the root bridge can be entered manually or enter 0 for the path cost to be determined automatically.
 - **Priority**: Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost.
The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 lists the values that are valid.

Valid Port Priority Values

Step	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Port Priority	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240

- **Edge Port** – Check the option to set the port as an edge port. Edge ports are connected edge devices such as hosts or workstations that are not switches part of the spanning tree protocol topology. If ports are set to edge ports, they can start forwarding traffic immediately as soon as the link is up. MSTP requires, that edge ports and non-edge ports are manually set.
- **BPDU Filter** - If BPDU filtering is selected for spanning tree protocol, it will check ports for sending and receiving BPDUs. If selecting filtering, then all ports with edge devices such as workstations should have BPDU Filter enabled under Spanning > Port Setting. Do not enable BPDU filtering on ports that are connected to other switches that would be BPDU spanning tree protocol information. For BPDU filtering to work, the BPDU handling option under Spanning Tree > Property must be set to BPDU filtering.
- **BPDU Guard** – Enabling BPDU Guard adds an extra layer of security to spanning tree by temporarily disabling all edge ports upon receiving BPDU data from other switches about the spanning tree status and topology. This prevents possible attacks to the flow of network traffic through spanning tree from edge port devices and limiting spanning tree control information to and from only the designated ports connected to other switches part of the spanning tree topology.
- **Point-to-Point** – This option specifies the spanning tree link type and is taken from the port duplex mode. For 802.1w Rapid Spanning Tree or MSTP to use fast transition, these spanning tree protocols only use point-to-point links between switches meaning full duplex mode. It is recommended to keep this setting as Auto.
- **Port State** – Displays the current spanning tree state of the selected port.
- **Designated Bridge** – Displays the current MAC address of the designated bridge in the spanning tree topology/configuration.
- **Designated Port ID** – Displays the current designated port in the spanning tree topology/configuration.
- **Operational Edge** – Displays if the selected port is configured as an edge port.
- **Operational Point-to-Point** – Displays if the selected port is configured as a point-to-point spanning tree link to another switch in the spanning tree topology/configuration.

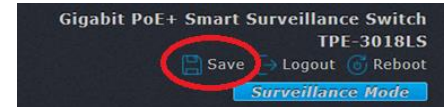
Edit Port Setting

Port	GE1
State	<input checked="" type="checkbox"/> Enable
Path Cost	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
Priority	128 ▾
Edge Port	<input checked="" type="checkbox"/> Enable
BPDU Filter	<input type="checkbox"/> Enable
BPDU Guard	<input type="checkbox"/> Enable
Point-to-Point	<input checked="" type="radio"/> Auto <input type="radio"/> Enable <input type="radio"/> Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	True
Operational Point-to-Point	False

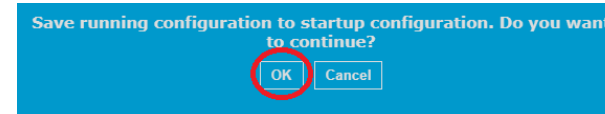
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure Spanning Tree Protocol MST settings (MSTP)

Spanning Tree > MST Instance

Note: The following configuration settings only apply to MSTP multiple spanning tree protocol configuration. MSTP must be selected for the Operation Mode under Spanning Tree > Property. In order to use MSTP, LLDP flooding cannot be used and must be changed to Filtering or Bridge under Discovery > LLDP > Property under LLDP Handling.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).



2. Click on **Spanning Tree**, and click on **MST Instance**.

3. In the MST Instance table, click the radio button for the 1st instance in the list and click **Edit**.

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	F
<input type="radio"/>	0	32768	32768-3C:8C:F8:F9:D0:4A	0-00:00:00:00:00:00	N/A	0	
<input checked="" type="radio"/>	1	32768	32769-3C:8C:F8:F9:D0:4A	0-00:00:00:00:00:00	N/A	0	



4. Review the settings. For each section, click **Apply** to save changes.

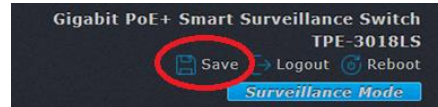
- **VLAN** – Select the VLANs from the Available VLAN list and you can use the arrow   buttons to add and remove to the Selected VLAN list.
Note: Multiple VLAN IDs can be selected at the same time by holding the Shift or Ctrl key.
- **Priority** - Enter the new priority in the Priority field. The user may set a priority value between **0-61440**.
- **Bridge Identifier** – Displays the current Bridge Identifier for MSTP topology/configuration.
- **Designated Root Bridge** – Displays the designated root bridge for the current MSTP topology/configuration.
- **Root Port** – Displays the current root port for the MSTP topology/configuration.
- **Root Path Cost** – Displays the current root path cost for the MSTP topology/configuration.
- **Remaining Hop** – Displays the current remaining hops of the MSTP topology/configuration.

Edit MST Instance Setting	
MSTI	1
VLAN	Available VLAN
	Selected VLAN
Priority	32768 (0 - 61440, default 32768)
Bridge Identifier	32769-3C:8C:F8:F9:D0:4A
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	
Root Path Cost	0
Remaining Hop	0

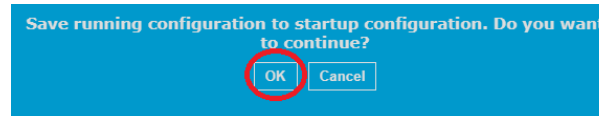
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure Spanning Tree Protocol MST Port settings (MSTP)

Spanning Tree > MST Port Setting

Note: The following configuration settings only apply to MSTP multiple spanning tree protocol configuration. MSTP must be selected for the Operation Mode under Spanning Tree > Property. In order to use MSTP, LLDP flooding cannot be used and must be changed to Filtering or Bridge under Discovery > LLDP > Property under LLDP Handling.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Spanning Tree**, and click on **MST Port Setting**.
3. Select the ports in the list to modify the MST configuration and click **Edit**.

Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
<input checked="" type="checkbox"/>	1 GE1	20000	128	Disabled	Disabled	MSTP	Internal	0-00:00:00:00:00:00	128-1	20000	20

Edit

4. Review the settings below and click **Apply** to save the configuration.
 - **Path Cost (0 = Auto)** - This is the port cost used by MSTP when calculating path cost to the root bridge.
 - **Priority** - This is the port priority used by MSTP in calculating path costs when two ports on the switch have the same port cost.
 - **Port Role** – Displays the currently assigned port role for the MSTP topology/configuration.
 - **Mode** – Displays the current spanning tree protocol mode.
 - **Type** – Displays the port type for the MSTP topology/configuration.
 - **Designated Bridge** – Displays the designated bridge ID.
 - **Designated Port ID** – Displays the designated port ID.
 - **Designated Cost** – Displays the designated cost.
 - **Remaining Hop** – Displays the current remaining hops of the MSTP topology/configuration.

Edit MST Port Setting

MSTI	0
Port	GE1
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Port Role	Disabled
Port State	Disabled
Mode	MSTP
Type	Internal
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Remaining Hop	20

5. Click **Apply**.

Apply

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.

Gigabit PoE+ Smart Surveillance Switch
TPE-3018LS

Save Logout Reboot

Surveillance Mode

7. Click **OK**.

Save running configuration to startup configuration. Do you want to continue?

OK Cancel

View your Spanning Tree Protocol Instance Statistics Information (MSTP)


Spanning Tree > Statistics

This section will display the sent and received BPDUs on each port.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Spanning Tree** and click on **Statistics**.
3. Select the port to view and click **View**.

Note: You select which port to view statistics and click **View** which will display the receive and transmit BPDU statistics and allow you to set the Refresh Rate interval for the statistical data to display.

■	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
<input checked="" type="checkbox"/>	1	GE1	0	0	0	0	0	0



LLDP (Link-Layer Discovery Protocol)

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices.

Configure LLDP settings

Discovery > LLDP > Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Discovery**, click on **LLDP**, and click on **Property**.
3. Review the settings.

Enabling or Disabling LLDP

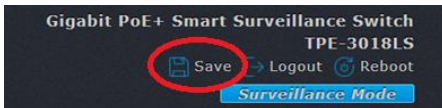
- **State** - Check the **Enable** option to enable the LLDP global state.
- **LLDP Handling** – This option specifies how the switch will handle LLDP packets received when LLDP is disabled.
 - **Filtering** – LLDP packets will be dropped.
 - **Bridging** – LLDP packets are forwarded to all ports.
 - **Flooding** – LLDP packets are flooding to all ports.
- **TLV Advertise Interval:** Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 5 - 32767 seconds.
- **Hold Multiplier:** Sets the hold multiplier value. The hold time multiplier is multiplied by the transmit interval to give the Time To Live (TTL) that the switch advertises to the neighbors. The range is from 2 to 10.
- **Reinitializing Delay:** Sets the reinitialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds.
- **Transmit Delay:** Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8191 seconds

LLDP	
State	<input type="checkbox"/> Enable
LLDP Handling	<input type="radio"/> Filtering <input checked="" type="radio"/> Bridging <input type="radio"/> Flooding
TLV Advertise Interval	30 <small>Sec (5 - 32767, default 30)</small>
Hold Multiplier	4 <small>(2 - 10, default 4)</small>
Reinitializing Delay	2 <small>Sec (1 - 10, default 2)</small>
Transmit Delay	2 <small>Sec (1 - 8191, default 2)</small>

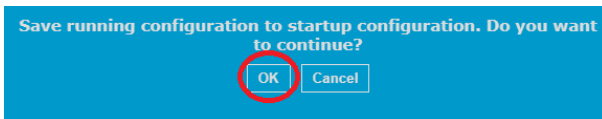
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure LLDP Port Settings

Discovery > LLDP > Port Setting

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).

2. Click on **Discovery**, click on **LLDP**, and click on **Port Setting**.

3. Select the port or ports to modify the LLDP configuration and click **Edit**.

<input type="checkbox"/>	Entry	Port	Mode	Selected TLV
<input checked="" type="checkbox"/>		1 GE1	Normal	802.1 PVID
<input checked="" type="checkbox"/>		2 GE2	Normal	802.1 PVID



4. Review the settings.

- Mode** – By default, all ports are set to transmit and receive LLDP frames however, you can set specific configuration of LLDP frames.
 - Transmit** – Only allow LLDP traffic to be transmitted from the selected port or ports. Received LLDP traffic will be dropped.
 - Receive** – Only allow LLDP traffic to be received on the selected port or ports. LLDP traffic will not be transmitted from the port or ports.
 - Normal** – Default setting. LLDP traffic can be both transmitted and received on the port or ports.
 - Disable** – Disables all LLDP traffic from being transmitted or received on the selected port or ports.
- Optional TLV** – Select the optional TLVs (type-length-values) or additional information to be sent in the LLDP traffic for the switch in the Available TLV list and you can use the arrow buttons to add and remove to the Selected TLV list.

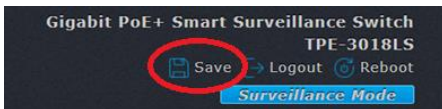
Note: Multiple TLVs can be selected at the same time by holding the Shift or Ctrl key.
- 802.1 VLAN Name** - Select the VLAN IDs to advertise the LLDP traffic for the switch in the Available VLAN list and you can use the arrow buttons to add and remove to the Selected VLAN list.

Note: Multiple VLANs can be selected at the same time by holding the Shift or Ctrl key.

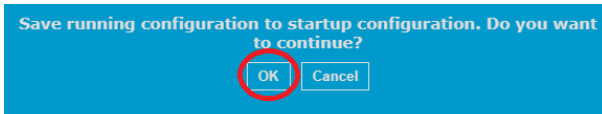
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



View LLDP Packet View Detail

Discovery > LLDP > Packet View

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Discovery**, click on **LLDP**, and click on **Packet View**.
3. Select the port to view the LLDP packet statistics and click **Detail**.

<input type="radio"/>	1	GE1	48	1440	Not Overloading
<input checked="" type="radio"/>	2	GE2	48	1440	Not Overloading



Under the Packet View Detail section, you can check the LLDP packet statistics of the selected port.

Packet View Detail	
Port	GE2
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted

View LLDP Local Information

Discovery > LLDP > Local Information

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Discovery**, click on **LLDP**, and click on **Local Information**.

Under the Device Summary section, you can view the LLDP local device information and capabilities.

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	3C:8C:F8:F9:D0:4A
System Name	Switch
System Description	TPE-3012LS
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID Subtype	Local

3. You can also select the port to view more details about local LLDP information. Select the port and click **Detail**.

	Entry	Port	LLDP State
<input type="radio"/>	1	GE1	Normal
<input checked="" type="radio"/>	2	GE2	Normal

Detail

Local Information Detail

Chassis ID Subtype	MAC address		
Chassis ID	3C:8C:F8:F9:D0:4A		
System Name	Switch		
System Description	TPE-3012LS		
Supported Capabilities	Bridge		
Enabled Capabilities	Bridge		
Port ID	GE8		
Port ID Subtype	Local		
Port Description			
Management Address Table			
Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			
MAC/PHY Detail			
Auto-Negotiation Supported	N/A		
Auto-Negotiation Enabled	N/A		

View LLDP Neighbors

Discovery > LLDP > Neighbor

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Discovery**, click on **LLDP**, and click on **Neighbor**.
3. Select the port to view the LLDP neighbor information and click **Detail**.

<input type="checkbox"/>	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID
<input type="checkbox"/>	GE10	MAC address	D8:EB:97:85:42:40	Interface alias	Gi0/8
<input checked="" type="checkbox"/>	GE10	MAC address	D8:EB:97:83:8E:FB	Interface alias	Gi0/8
<input type="checkbox"/>	GE10	MAC address	D8:EB:97:89:3F:3A	Interface alias	Gi0/19
<input type="checkbox"/>	GE10	MAC address	1C:87:2C:CA:9B:62	MAC address	1C:87:2C:CA:9B:62

Detail

Under the Neighbor Detail section, you scroll down to view the LLDP neighbor information.

Neighbor Information Detail	
Local Port	GE10
Basic Detail	
Chassis ID Subtype	MAC address
Chassis ID	D8:EB:97:85:42:40
Port ID Subtype	Interface alias
Port ID	Gi0/8
Port Description	TEG-082WS 3.01.004 Port 08

View LLDP Statistics Counters

Discovery > LLDP > Statistics

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Discovery**, click on **LLDP**, and click on **Statistics**.

You can view the total statistics counters for LLDP traffic.

Global Statistics

Insertions	9
Deletions	5
Drops	0
AgeOuts	0

Clear **Refresh**

<input type="checkbox"/>	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout
			Total	Total	Discard	Error	Discard	Unrecognized	
<input checked="" type="checkbox"/>	1	GE1	0	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	0

3. Select the port to view the LLDP neighbor information and click **Detail**.

View LLDP System Information

- **Chassis ID Subtype:** This parameter describes the Chassis ID subtype which is "macAddress". You cannot change this parameter.
- **Chassis ID:** This parameter lists the MAC Address of the switch.
- You cannot change this parameter.
- **System Name:** This parameter lists the System Name of the switch. You can assign the system name.
- **System Description:** This parameter lists the product name of the switch. You cannot change this parameter

LLDP System Information	
Chassis ID Subtype:	macAddress
Chassis ID:	00:01:02:03:04:05
System Name:	
System Description:	

Set LLDP Port State

For each port, click the **State** drop-down list and choose from the following options.

- **Disabled:** Indicates LLDP is disabled on the port. The port cannot receive or transmit LLDP data packets.
- **Enabled:** Indicates LLDP is enabled on the port. The port can receive and transmit LLDP data packets.
- **RxOnly:** Indicates LLDP is enabled on the port. The port can receive LLDP data packets.
- **TxOnly:** Indicates LLDP is enabled on the port. The port can transmit LLDP data packets.

Note: You can select the row labeled **ALL** to apply settings to all ports.

Click **Apply** to save the settings.

LLDP Port State Settings		
Port	State	Action
All	Disabled ▾	Apply
1	RxTx ▾	Apply
2	RxTx ▾	Apply

4. Click **Save Settings to Flash (menu)**.

Save Settings to Flash

5. Click **Save Settings to Flash (button)**, then click **OK**.

Note: This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.

[Save Settings to Flash](#)

View LLDP Neighbor Information

LLDP > LLDP Neighbor Information

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **LLDP** and click on **LLDP Neighbor Information**.
3. View the LLDP neighbor information.
 - **Entity:** This parameter is a number assigned to the reporting neighbors in the order that the LLDP information is received from them.
 - **Port:** This parameter specifies the TPE-1020WS local port number where the LLDP information was received.
 - **Chassis ID Subtype:** This parameter describes the Chassis ID subtype of the neighboring network device which is reporting the LLDP information.
 - **Chassis ID:** This parameter is the neighboring device's chassis ID.
 - **Port ID Subtype:** This parameter describes the Port ID subtype of the neighboring network device's port that is connected directly to the TPE-1020WS switch port.
 - **Port ID:** This parameter specifies the neighboring network device's port number from which the LLDP information was transmitted.
 - **Port Description:** This parameter describes the neighboring network device's port.
 - **Show Normal:** If you click on this button, a detailed report of the neighboring network device will be displayed.

If the entries span multiple pages, you can navigate page number in the **Page** field and click **Go** or you can click **First**, **Previous**, **Next**, and **Last Page** to navigate the pages.

LLDP Neighbors Information							
Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Normal
Page 0/0 First Page Previous Page Next Page Last Page Page <input type="text"/> GO							

Multicast

The multicast section will allow you to configure IGMP and MLD snooping for multicast traffic filtering on the switch.

Configure unknown multicast and multicast forwarding method

Multicast > General > Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **General**, and click **Property**.
3. Review the settings. Click on **Apply** to save the configuration changes.
 - **Unknown Multicast Action** –
 - **Flood:** When the switch receives unknown multicast traffic, flood the traffic out all switch ports.
 - **Drop:** When the switch receives unknown multicast traffic, drop the traffic.
 - **Forward to Router Port:** When the switch receives unknown multicast traffic, forward the traffic to the multicast router port.
 - **Age-Out Timer** – Enter the amount of time in seconds that you want your switch to wait before it purges an inactive dynamic MAC address.
 - **Multicast Forward Method** – Select the method the switch should forward IPv4 multicast traffic.
 - **DMAC-VID:** Multicast frames are forwarded by destination MAC address.
 - **DIP-VID:** Multicast frames are forwarded by destination IP address.

Unknown Multicast Action	<input checked="" type="radio"/> Flood <input type="radio"/> Drop <input type="radio"/> Forward to Router Port
Multicast Forward Method	
IPv4	<input checked="" type="radio"/> DMAC-VID <input type="radio"/> DIP-VID

4. Click **Save Settings to Flash** (menu).

Save Settings to Flash

5. Click **Save Settings to Flash** (button), then click **OK**.

Note: This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.

Save Settings to Flash

Add static multicast group addresses

Multicast > General > Group Address

Static multicast group addresses can be added to the table in addition to the multicast group addresses that are learned by the switch dynamically.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **General**, and click **Group Address**.
3. Click **Add** to add a new static multicast address entry.



- **VLAN:** Click the drop-down list to select the VLAN ID to assign the multicast address.
- **IP Version** – Select the IP address version of the multicast static address, **IPv4** or **IPv6**.
- **Group Address** – Enter the the multicast static address.
- **Member** – In the Available Port list, select the ports to assign the multicast static group address. You can use the arrow buttons to add and remove to the Selected Port list.
- **Note:** Multiple ports can be selected at the same time by holding the Shift or Ctrl key.

Add Group Address

VLAN	1	
IP Version	IPv4	
Group Address	<input type="text"/>	
Member	Available Port	Selected Port
	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

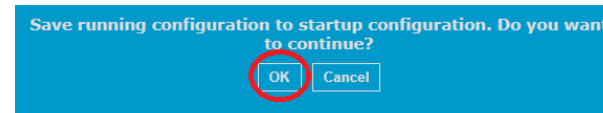
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.







Add multicast router ports

Multicast > General > Router Port

Static router ports can be specified for multicast traffic in this section.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **General**, and click **Router Port**.
3. Click **Add** to add a new static multicast address entry.



- **VLAN** – In the Available VLAN list, select the VLAN IDs to assign the multicast router ports. You can use the arrow   buttons to add and remove to the Selected VLAN list.
Note: Multiple VLAN IDs can be selected at the same time by holding the Shift or Ctrl key.
- **IP Version** – Select the IP address version of the multicast static address, **IPv4** or **IPv6**.
- **Port** – In the Available Port list, select the static multicast router ports to configure. You can use the arrow   buttons to add and remove to the Selected Port list.
Note: Multiple ports can be selected at the same time by holding the Shift or Ctrl key.

Add Router Port

VLAN	Available VLAN	Selected VLAN
	1	
IP Version	IPv4	
Type	<input checked="" type="radio"/> Static <input type="radio"/> Forbidden	
Port	Available Port	Selected Port
	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.

Save running configuration to startup configuration. Do you want to continue?




Configure IGMP snooping settings*Multicast > IGMP Snooping > Property*

Configure IGMP snooping settings for IPv4 multicast traffic.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **IGMP Snooping**, and click **Property**.
3. Review the settings. Click on **Apply** to save the configuration changes.
 - **State:** Check the **Enable** option to enable IGMP snooping. Uncheck to disable IGMP snooping.
 - **Version:** Select the IGMP snooping version. **IGMPv2** or **IGMPv3**.
 - **Report Suppression:** Enable the report suppression option to limit the amount of IGMP multicast reports to the multicast router to reduce multicast traffic overhead.

State	<input type="checkbox"/> Enable
Version	<input checked="" type="radio"/> IGMPv2 <input type="radio"/> IGMPv3
Report Suppression	<input checked="" type="checkbox"/> Enable

Under the VLAN Setting table, the active VLANs will be listed. To edit the IGMP snooping settings for a specific VLAN, select the VLAN and click **Edit**.

- **State:** Check the **Enable** option to enable IGMP snooping for the specific VLAN. Uncheck to disable IGMP snooping.
- **Router Port Auto Learn:** Check the **Enable** option to configure the router port(s) to be dynamically learned by the switch for the specific VLAN
- **Immediate Leave:** Check the **Enable** option to enable IGMP immediate leave for IGMP snooping. Enabling this option allows the switch to remove an

interface from the forwarding table without first sending out IGMP group specific queries to the interface and the VLAN interface can be removed from the multicast tree to ensure optimal bandwidth for multicast traffic.

- **Version:** Select the IGMP snooping version. **IGMPv2** or **IGMPv3**.
- **Report Suppression:** Enable the report suppression option to limit the amount of IGMP multicast reports to the multicast router to reduce multicast traffic overhead.
- **Query Robustness:** Enter the the variable number of unacknowledged snooping queries that switch can send before removing the multicast client from the group list. Default: 2, Range: 1-7
- **Query Interval:** Enter the interval time/period between each IGMP membership query message the switch will send out. Default: 125, Range: 30-18000
- **Query Response Interval:** Enter the interval time/period the switch will wait for an IGMP response after each IGMP membership query message is sent out by the switch. Default: 10, Range: 5-20
- **Last Member Query Counter:** Enter the number of query messages the router sends in response to an IGMP leave message. Default: 2, Range: 1-7
- **Last Member Query Interval:** Enter the interval time/period for sending query messages to active IGMP interfaces. Default: 1, Range: 1-25
- **Operational Status:** Displays a summary of all the IGMP snooping configuration settings.

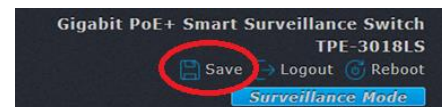
Edit VLAN Setting

VLAN	1	
State	<input type="checkbox"/> Enable	
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable	
Immediate leave	<input type="checkbox"/> Enable	
Query Robustness	<input type="text" value="2"/>	(1 - 7, default 2)
Query Interval	<input type="text" value="125"/>	Sec (30 - 18000, default 125)
Query Max Response Interval	<input type="text" value="10"/>	Sec (5 - 20, default 10)
Last Member Query Counter	<input type="text" value="2"/>	(1 - 7, default 2)
Last Member Query Interval	<input type="text" value="1"/>	Sec (1 - 25, default 1)
Operational Status		
Status	Disabled	
Query Robustness	2	
Query Interval	125 (Sec)	
Query Max Response Interval	10 (Sec)	
Last Member Query Counter	2	
Last Member Query Interval	1 (Sec)	

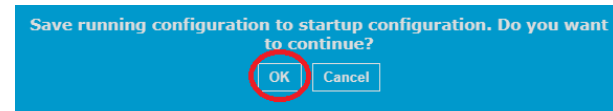
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure multicast querier settings

Multicast > IGMP Snooping > Querier

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Multicast**, click on **IGMP Snooping**, and click **Querier**.
3. Review the settings. Click on **Apply** to save the configuration changes.
 - **State:** Check the **Enable** option to enable IGMP snooping querier for the selected VLAN. Uncheck to disable IGMP snooping querier for the selected VLAN.
 - **Version:** Select the IGMP querier version for the selected VLAN. **IGMPv2** or **IGMPv3**.

Querier Table

■	VLAN	State	Operational Status	Version	Querier Address
<input checked="" type="checkbox"/>	1	Disabled	Disabled		

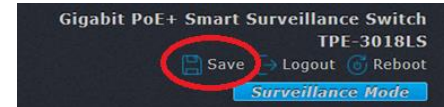
Edit Querier

VLAN	1
State	<input checked="" type="checkbox"/> Enable
Version	<input type="radio"/> IGMPv2 <input type="radio"/> IGMPv3

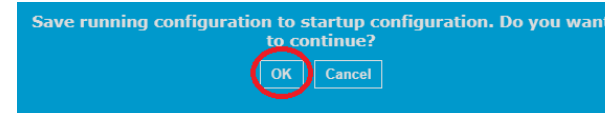
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



View IGMP snooping statistics*Multicast > IGMP Snooping > Statistics*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **IGMP Snooping**, and click **Statistics**.
3. Review the settings. You can click **Refresh** to force the statistics to be updates to most recent or clear to reset all statistics to 0.
 - **Receive Packet:** Displays the multicast statistics received by the switch.
 - **Total:** Displays the number of all multicast packets received by the switch.
 - **Valid:** Displays the total number of valid multicast packets received by the switch.
 - **InValid:** Displays the total number of invalid multicast packets received by the switch.
 - **Other:** Displays other non-multicast packets such as ICMP packets.
 - **Leave:** Displays the total of IGMP leave packets received by the switch.
 - **Report:** Displays the total of IGMP report packets received by the switch.
 - **General Query:** Displays the total number of IGMP query packets received by the switch.
 - **Special Group Query:** Displays the total number of special group query packets including querier special group queries received by the switch.
 - **Source-specific Group Query:** Displays the total number of source-specific group queries received by the switch.
 - **Transmit Packet:** Displays the multicast statistics transmitted by the switch.
 - **Leave:** Displays the total of IGMP leave packets transmitted by the switch.
 - **Report:** Displays the total of IGMP report packets transmitted by the switch.
 - **General Query:** Displays the total number of IGMP query packets transmitted by the switch.

- **Special Group Query:** Displays the total number of special group query packets including querier special group queries transmitted by the switch.
- **Source-specific Group Query:** Displays the total number of source-specific group queries transmitted by the switch.

Receive Packet	
Total	15
Valid	4
InValid	0
Other	0
Leave	0
Report	4
General Query	0
Special Group Query	0
Source-specific Group Query	0
Transmit Packet	
Leave	0
Report	0
General Query	1
Special Group Query	0
Source-specific Group Query	0

Configure MLD snooping settings*Multicast > MLD Snooping > Property*

Configure MLD snooping settings for IPv6 multicast traffic.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **MLD Snooping**, and click **Property**.
3. Review the settings. Click on **Apply** to save the configuration changes.
 - **State:** Check the **Enable** option to enable MLD snooping. Uncheck to disable MLD snooping.
 - **Version:** Select the MLD snooping version. **MLDv1** or **MLDv2**.
 - **Report Suppression:** Enable the report suppression option to limit the amount of MLD multicast reports to the multicast router to reduce multicast traffic overhead.

State	<input type="checkbox"/> Enable
Version	<input checked="" type="radio"/> MLDv1 <input type="radio"/> MLDv2
Report Suppression	<input checked="" type="checkbox"/> Enable

Under the VLAN Setting table, the active VLANs will be listed. To edit the MLD snooping settings for a specific VLAN, select the VLAN and click **Edit**.

- **State:** Check the **Enable** option to enable MLD snooping for the specific VLAN. Uncheck to disable MLD snooping.
- **Router Port Auto Learn:** Check the **Enable** option to configure the router port(s) to be dynamically learned by the switch for the specific VLAN
- **Immediate Leave:** Check the **Enable** option to enable MLD immediate leave for MLD snooping. Enabling this option allows the switch to remove an interface

from the forwarding table without first sending out MLD group specific queries to the interface and the VLAN interface can be removed from the multicast tree to ensure optimal bandwidth for multicast traffic.

- **Version:** Select the MLD snooping version. **MLDv1** or **MLDv2**.
- **Report Suppression:** Enable the report suppression option to limit the amount of MLD multicast reports to the multicast router to reduce multicast traffic overhead.
- **Query Robustness:** Enter the the variable number of unacknowledged snooping queries that switch can send before removing the multicast client from the group list. Default: 2, Range: 1-7
- **Query Interval:** Enter the interval time/period between each MLD membership query message the switch will send out. Default: 125, Range: 30-18000
- **Query Response Interval:** Enter the interval time/period the switch will wait for an MLD response after each MLD membership query message is sent out by the switch. Default: 10, Range: 5-20
- **Last Member Query Counter:** Enter the number of query messages the router sends in response to an MLD leave message. Default: 2, Range: 1-7
- **Last Member Query Interval:** Enter the interval time/period for sending query messages to active MLD interfaces. Default: 1, Range: 1-25
- **Operational Status:** Displays a summary of all the MLD snooping configuration settings.

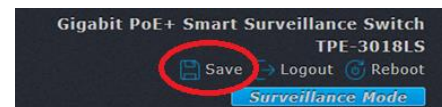
Edit VLAN Setting

VLAN	1	
State	<input type="checkbox"/> Enable	
Router Port Auto Learn	<input checked="" type="checkbox"/> Enable	
Immediate leave	<input type="checkbox"/> Enable	
Query Robustness	<input type="text" value="2"/>	(1 - 7, default 2)
Query Interval	<input type="text" value="125"/>	Sec (30 - 18000, default 125)
Query Max Response Interval	<input type="text" value="10"/>	Sec (5 - 20, default 10)
Last Member Query Counter	<input type="text" value="2"/>	(1 - 7, default 2)
Last Member Query Interval	<input type="text" value="1"/>	Sec (1 - 25, default 1)
Operational Status		
Status	Disabled	
Query Robustness	2	
Query Interval	125 (Sec)	
Query Max Response Interval	10 (Sec)	
Last Member Query Counter	2	
Last Member Query Interval	1 (Sec)	

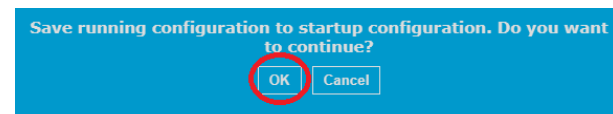
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



View MLD snooping statistics*Multicast > MLD Snooping > Statistics*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **MLD Snooping**, and click **Statistics**.
3. Review the settings. You can click **Refresh** to force the statistics to be updates to most recent or clear to reset all statistics to 0.
 - **Receive Packet:** Displays the multicast statistics received by the switch.
 - **Total:** Displays the number of all multicast packets received by the switch.
 - **Valid:** Displays the total number of valid multicast packets received by the switch.
 - **InValid:** Displays the total number of invalid multicast packets received by the switch.
 - **Other:** Displays other non-multicast packets such as ICMP packets.
 - **Leave:** Displays the total of MLD leave packets received by the switch.
 - **Report:** Displays the total of MLD report packets received by the switch.
 - **General Query:** Displays the total number of MLD query packets received by the switch.
 - **Special Group Query:** Displays the total number of special group query packets including querier special group queries received by the switch.
 - **Source-specific Group Query:** Displays the total number of source-specific group queries received by the switch.
 - **Transmit Packet:** Displays the multicast statistics transmitted by the switch.
 - **Leave:** Displays the total of MLD leave packets transmitted by the switch.
 - **Report:** Displays the total of MLD report packets transmitted by the switch.
 - **General Query:** Displays the total number of MLD query packets transmitted by the switch.

- **Special Group Query:** Displays the total number of special group query packets including querier special group queries transmitted by the switch.
- **Source-specific Group Query:** Displays the total number of source-specific group queries transmitted by the switch.

Receive Packet	
Total	15
Valid	4
InValid	0
Other	0
Leave	0
Report	4
General Query	0
Special Group Query	0
Source-specific Group Query	0
Transmit Packet	
Leave	0
Report	0
General Query	1
Special Group Query	0
Source-specific Group Query	0

Configure MVR settings

Multicast > MVR > Property

For layer 2 IP multicast networks, it may be necessary for multicast clients/subscribers in different IP subnets/VLANs to access the same multicast group. MVR (Multicast VLAN Registration) will allow the sending multicast packets received in a multicast source VLAN to one or more multicast receive VLANs.

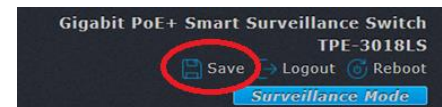
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **MVR**, and click **Property**.
3. Review the settings. Click on **Apply** to save the configuration changes.
 - **State:** Check the **Enable** option to enable MVR. Uncheck to disable MVR.
 - **VLAN:** Click the drop-down list to select the MVR source VLAN.
 - **Mode:** Select the MVR mode.
 - **Compatible:** In this mode, multicast data received by MVR hosts is forwarded to all MVR data ports, regardless of MVR host membership on those ports.
 - **Dynamic:** in this mode, multicast data received by MVR hosts is forwarded only to those MVR data and clients ports that the MVR hosts have joined which eliminates using unnecessary bandwidth on MVR data port links.
 - **Group Start:** Enter the IPv4 multicast starting range. (ex: 228.1.2.240)
 - **Group Count:** Enter the number of total multicast groups included for MVR. The count will count the IPv4 multicast group specified in the Group Start field and count the next ascending sequential multicast groups.
 - **Query Time:** Enter the time in seconds to wait for MVR report memberships to be received on a port before the switch removes the port from multicast group membership.
 - **Operational Group:** Displays a summary of the maximum MVR groups allowed and currently active MVR groups on the switch.

State	<input checked="" type="checkbox"/> Enable
VLAN	1
Mode	<input type="radio"/> Compatible <input checked="" type="radio"/> Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

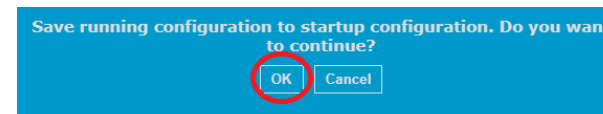
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure MVR port settings

Multicast > MVR > Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **MVR**, and click **Port Setting**.
3. Select the port in the list and click **Edit** to configure the MVR port settings.
 - **Port**: Displays the selected port number.
 - **Role**: Set the MVR port role.
 - **Immediate Leave**: Check the option to enable IGMP immediate leave on the selected port.

Port Setting Table

■	Entry	Port	Role	Immediate Leave
✓	1	GE1	None	Disabled

Edit Port Setting

Port	GE1
Role	<input checked="" type="radio"/> None <input type="radio"/> Receiver <input type="radio"/> Source
Immediate Leave	<input type="checkbox"/> Enable

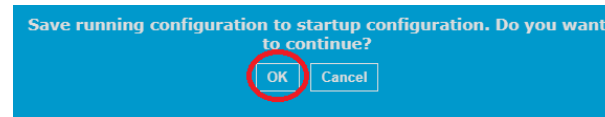
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.





6. Click **OK**.



Configure MVR Group Address Table

Multicast > MVR > Group Address

Displays the groups that have been dynamically learned by the switch and allowed you statically add MVR groups to the switch.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Multicast**, click on **MVR**, and click **Group Address**.
3. Click **Add** to a static MVR group address.
 - **Group Address:** Enter the multicast group address to statically add to the table.
 - **Member** – In the Available Port list, select the ports to statically assign for the MVR multicast group. You can use the arrow   buttons to add and remove to the Selected port list.

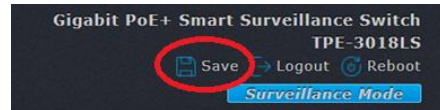
Note: Multiple ports can be selected at the same time by holding the Shift or Ctrl key.

VLAN	1	
Group Address	<input type="text"/>	(0.0.0.0 - 0.0.0.0)
Member	Available Port	Selected Port
	<input type="text"/>	<input type="text"/>

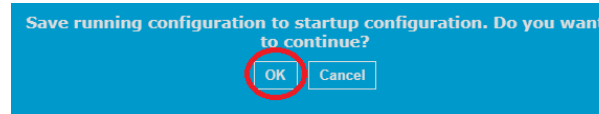
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Security

This chapter contains information about the Port-based security features and the procedures for setting this feature.

Configure RADIUS settings

Security > RADIUS

This section contains information and configuration procedures for the Port-based Access Control. Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch port. With this feature, the switch does not allow an end node to send or receive traffic through a port until the user of the node logs on by entering a user name and password.

This feature can prevent an unauthorized individual from connecting a computer to a port or using an unattended workstation to access your network resources. Only those users to whom you have assigned a user name and password are able to use the switch to access the network.

This feature can be used with one of two authentication methods:

- The RADIUS authentication protocol requires that a remote RADIUS server is present on your network. The RADIUS server performs the authentication of the user name and password combinations.
- The Dial-in User (local) authentication method allows you to set up the authentication parameters internally in the switch without an external server. In this case, the user name and password combinations are entered in the associated with an optional VLAN when they are defined. Based on these entries, the authentication process is done locally by the Web Management Utility using a standard EAPOL transaction.

Note: RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **RADIUS**.

3. Review the settings. Click **Apply** to save the settings.

Configure the following parameters as required:

- **Retry:** Set the number of retries to authorize RADIUS servers.
- **Timeout:** Set the timeout period in seconds before starting the retry process again for authorization of RADIUS servers.
- **Key String:** Set the RADIUS shared secret for all RADIUS servers.

Use Default Parameter	
Retry	<input type="text" value="3"/> (1 - 10, default 3)
Timeout	<input type="text" value="3"/> Sec (1 - 30, default 3)
Key String	<input type="text"/>

To add a RADIUS server, click **Add**.

- **Address Type** – Select the address type to identify the RADIUS server on the network. **Hostname, IPv4, or IPv6**
- **Server Address** – Depending on the address type selected in the previous, enter the Hostname, IPv4 address, or IPv6 address in the field provided to identify the RADIUS server.
- **Server Port** – Enter the RADIUS server port. By default, the RADIUS server port is set to 1812.
- **Priority** – Enter the RADIUS server priority value. The lower the number, the higher the priority value. This can apply if you have multiple RADIUS servers listed and which will indicate which RADIUS servers to take priority over others in the list.
- **Key String** – By default, the Use Default setting is checked to use the Default Key String/Shared Secret specified in the global settings. If the key string/shared secret for a specified RADIUS server, uncheck the Use Default option and enter the key string/shared secret in the field provided.
- **Retry** – By default, the Use Default setting is checked to use the Retry number specified in the global settings. If the Retry number for a specified RADIUS server, uncheck the Use Default option and enter the Retry number in the field provided.

- **Timeout** – By default, the Use Default setting is checked to use the timeout interval specified in the global settings. If the timeout interval for a specified RADIUS server, uncheck the Use Default option and enter the timeout interval in the field provided.
- **Usage** – Select the authentication type to use for RADIUS clients.
 - **Login** – Only use basic user and password authentication from the switch local user database.
Note: Local authentication users must be specified under the Management > Users with the User Privilege.
 - **802.1X** – Only use the user credentials specified in the externally connected RADIUS server(s).
 - **All** – Use either Login or 802.1X to authenticate users access to the switch.
- **NAS ID** - This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.
- **Port Access Control** - This parameter enables or disables Port Access Control. Select one of the following choices from the pulldown menu:
 - **Enable:** The Port Access Control feature is activated.
 - **Disable:** The Port Access Control feature is de-activated.
- **Authentication Method** - This parameter indicates the authentication method used by the switch. Select one of the following choices:
 - **RADIUS:** This parameter configures port security for remote authentication. After completing steps, you must configure the "RADIUS Client" section.
 - **Local:** This parameter configures port security for local authentication. After completing steps, you must configure the parameters for "Dial-in User— Local Authentication" section.
 - **TACACS+:** This parameter configures port security for terminal authentication. After completing steps, you must configure the "TACACS+ Settings" section.

Add RADIUS Server

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Server Port	<input type="text" value="1812"/> (0 - 65535, default 1812)
Priority	<input type="text"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 10, default 3)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> Sec (1 - 30, default 3)
Usage	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All

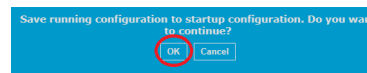
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure RADIUS network authentication settings

Security > Authentication Manager > Property

This section allows the configuration of ports to require authorization/authentication, guest VLAN assignment for unauthenticated users, and authentication methods required on network access ports.

1. Log into your switch management page (see [“Access your switch management page”](#) on page 11).
2. Click on **Security**, click on **Authentication Manager**, and click on **Property**.
3. Review the settings. Click **Apply** to save the settings.

Configure the following parameters as required:

- **Authentication Type:** Check the 802.1X option to enable 802.1X.
- **Guest VLAN:** Check the Enable option and click the drop-down list to select the guest VLAN assignment for unauthorized/authenticated users.
Note: VLANs must be created under the VLAN > VLAN > Create VLAN section to be available in the drop-down list.
- **MAC-Based User ID Format:** Click the drop-down list to select the MAC User Name/Password ID format used for port authentication.



Authentication Type	<input checked="" type="checkbox"/> 802.1x
Guest VLAN	<input checked="" type="checkbox"/> Enable
	1 ▾
MAC-Based User ID Format	XXXXXXXXXXXX ▾

To configure the ports to set/require for 802.1X authentication, select the port or ports in the list and click **Edit**.

Port Mode Table

<input type="checkbox"/>	Entry	Port	Authentication Type	Host Mode	Method	Guest VLAN	VLAN Assign Mode
<input checked="" type="checkbox"/>	1	GE1	802.1x Disabled	Multiple Authentication	RADIUS	Disabled	Static

Edit

- **Port:** Displays the specified port or ports to configure.
- **Authentication Type:** Check the 802.1X to require authentication for the selected port or ports.
- **Host Mode:** Select the host mode.
 - **Multiple Authentication:** Using this mode, all 802.1X clients must authenticate individually for network access.
 - **Multiple Hosts:** In this mode, only a single 802.1X client must be authenticated, all clients afterwards will also be provided network access.
 - **Single Host:** In this mode, only a single 802.1X client can be authenticated and provide network access at any given time. The client must logout or deauthenticate before another 802.1X client can be allowed network access.
- **Method:** In the Available Method list, select the authentication methods allowed for the authentication on the selected port or ports. You can use the arrow   buttons to add and remove to the Selected Method list.
Note: Multiple methods can be selected at the same time by holding the Shift or Ctrl key.
- **Guest VLAN:** Check the Enable option to allow unauthorized users to be assigned to the guest VLAN assignment. The Guest VLAN ID can be assigned in the global settings.
Note: VLANs must be created under the VLAN > VLAN > Create VLAN section to be available in the drop-down list.

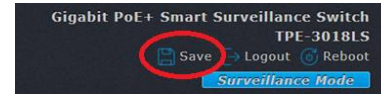
- **VLAN Assign Mode:**
 - **Disable:** Ignores VLAN authorization result and keeps the original VLAN ID of host.
 - **Reject:** Use VLAN authorization if received, and reject host if VLAN is unauthorized.
 - **Static:** Use VLAN authorization information if received and if VLAN information in unauthorized, keep original VLAN ID of host.

Edit Port Mode	
Port	GE1
Authentication Type	<input checked="" type="checkbox"/> 802.1x
Host Mode	<input checked="" type="radio"/> Multiple Authentication <input type="radio"/> Multiple Hosts <input type="radio"/> Single Host
Method	Available Method: Local Select Method: RADIUS
Guest VLAN	<input checked="" type="checkbox"/> Enable
VLAN Assign Mode	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure RADIUS network port settings

Security > Authentication Manager > Port Settings

This section will allow you to configure RADIUS network port settings.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **Authentication Manager**, and click on **Port Settings**.
3. Select the port you would like to configure and click **Edit**. Review the settings. Click **Apply** to save the settings.

Port Setting Table

■	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			80
						Reauthentication	Inactive	Quiet	
✓	1	GE1	Disabled	Disabled	256	3600	60	60	

Edit

- **Port:** Displays the selected port(s).
- **Port Control:**
 - **Disabled:** Disable authentication and allows clients network access.
 - **Force Authorized:** Port forces authorization and allows client network access.
 - **Force Unauthorized:** Port prevents authorization and denies client network access.
 - **Auto:** Authentication is required for clients to allow network access.
- **Reauthentication:** Check **Enabled** to allow clients to attempt re-authentication automatically after the reauthentication period has expired.
- **Max Hosts:** Specify the max. number of hosts allowed. (Applies to multiple authentication mode only)

Common Timer

- **Reauthentication:** Set the reauthentication interval in seconds to in which a client will automatically attempt reauthentication.
- **Inactive:** Set the idle timeout period in seconds to automatically de-authenticate a client if no traffic is received and the client is idle.
- **Quiet:** When a port is in locked state after authentication fails several times, the host will be locked in quiet period. Only after the quiet period has expired, the client will be able to reauthenticate.

802.1x Parameters

- **TX Period:** Set the time period in seconds that the device will wait for a response to an EAP (Extensible Authentication Protocol) request/identity frame from the supplicant (client) before resending the request.
- **Supplicant Timeout:** Set the time period allowed to receive a response from the supplicant (client) in the authentication process.
- **Server Timeout:** Set the time period allowed before EAP requests are resent to the supplicant (client).
- **Max Requests:** Set maximum allowed number of EAP requests sent.

Edit Port Setting

Port	GE1	
Port Control	<input checked="" type="radio"/> Disabled <input type="radio"/> Force Authorized <input type="radio"/> Force Unauthorized <input type="radio"/> Auto	
Reauthentication	<input checked="" type="checkbox"/> Enable	
Max Hosts	<input type="text" value="256"/>	(1 - 256, default 256)
Common Timer		
Reauthentication	<input type="text" value="3600"/>	Sec (300 - 4294967294, default 3600)
Inactive	<input type="text" value="60"/>	Sec (60 - 65535, default 60)
Quiet	<input type="text" value="60"/>	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Supplicant Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Server Timeout	<input type="text" value="30"/>	Sec (1 - 65535, default 30)
Max Request	<input type="text" value="2"/>	(1 - 10, default 2)

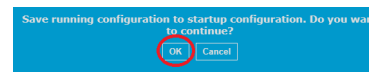
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



View authenticated sessions

Security > Authentication Manager > Sessions

This section displays details about the current sessions.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **Authentication Manager**, and click on **Sessions**.
3. Review details below. **Clear** can be used to delete all sessions
 - **Session ID:** Displays the session ID.
 - **Port:** Displays the port number for the session.
 - **MAC Address:** Displays the MAC address of the device connected for the session.
 - **Current Type:**
 - **802.1X:** 802.1X authentication is used for the session.
 - **MAC-Based:** MAC-based authentication is used for the session.
 - **Web-Based:** Web-based authentication is used for the session.
 - **Status:**
 - **IP Version:** IPv4 or IPv6 is used in the session.
 - **Disable:** Session is ready to be deleted.
 - **Running:** Authentication is in process.
 - **Authorized:** Authentication has passed and obtaining network access.
 - **Unauthorized:** Authentication has failed and restricted network access.
 - **(Operational Info.) VLAN:** Displays the associated VLAN ID of the session.
 - **(Operational Info.) Session Time:** In Authorized state, displays total the session has been currently active.
 - **(Operational Info.) Inactive Time:** In Authorized state, displays the time period the client has been idle.
 - **(Operational Info.) Quiet Time:** In Locked state, displays the time period the connected device has been in set to quiet time.
 - **(Authorized Info.) VLAN:** Displays the VLAN ID assigned after authentication was successful.
 - **(Authorized Info.) Reauthentication:** Displays the reauthentication period provided from authorization.

- **(Authorized Info.) Inactive Timeouts:** Displays inactive timeout provided from authorization.

Sessions Table										
Showing <input type="text" value="All"/> entries		Showing 0 to 0 of 0 entries								
■	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Author
						VLAN	Session Time	Inactivated Time	Quiet Time	VLAN
0 results found.										

Configure Management Access

Security > Management Access > Management Service

This section allows the configuration of ports to require authorization/authentication, guest VLAN assignment for unauthenticated users, and authentication methods required on network access ports.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **Management Access**, and click on **Management Service**.
3. Review the settings. Click **Apply** to save the settings.

Management Service

- **Telnet:** Enables Telnet command line management access to the switch.
- **SSH:** Enables SSH command line management access to the switch.
- **HTTP:** Enables HTTP web management access to the switch. By default, HTTP management access is enabled.
- **HTTPS:** Enables HTTPS web management access to the switch.
- **SNMP:** Enables SNMP management access to the switch.

Management Service	
Telnet	<input type="checkbox"/> Enable
SSH	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
HTTPS	<input type="checkbox"/> Enable
SNMP	<input type="checkbox"/> Enable

- **Session Timeout:** Configure the idle timeout settings to automatically log out of the specified management session during times of inactivity. Enter the 0 value to disable automatic logout.
- **Console:** Enables Telnet command line management access to the switch.

SSH: Enables SSH command

Session Timeout		
Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

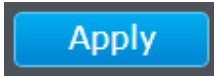
- **Password Retry Count:** Configure the number of failed attempts allowed for the specified management access before access is locked for the period specified under Silent Time.

Password Retry Count		
Console	<input type="text" value="3"/>	(0 - 120, default 3)
Telnet	<input type="text" value="3"/>	(0 - 120, default 3)
SSH	<input type="text" value="3"/>	(0 - 120, default 3)

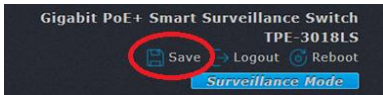
- **Silent Time:** Configure the silent time period defining amount of time the management access prevents logins after the max. password retry count is reached.

Silent Time		
Console	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
Telnet	<input type="text" value="0"/>	Sec (0 - 65535, default 0)
SSH	<input type="text" value="0"/>	Sec (0 - 65535, default 0)

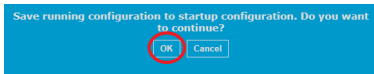
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Management ACL/ACE (Access Control Lists/Access Control Entries)

Security > Management Access > Management ACL

Access Control configuration allows you to control different aspects of the Ethernet traffic as it enters the switch ports and is process through the Switch. You can specify what traffic is permitted or denied to flow through the switch by setting up specific filter criteria at an ingress port. You can also manage the switching priority of Ethernet packets. All of this is done by specifying policies that define the filtering and priority behavior.

Create new access control list

Security > Management Access > Management ACL

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **Management Access**, and click on **Management ACL**.
3. In the **ACL Name** field, enter a name for the new access control list. Click **Apply**.

After creating the new ACL, it will appear in the Management ACL Table

ACL Name	State	Rule
ACL1	Deactive	0

4. To create a new policy under the new ACL, click on **Security**, click on **Management Access**, and click on **Management ACE**.

5. Make sure the correct ACL is selected in the **ACL Name** drop-down list. Click **Add** to a new policy under the ACL.

Management ACE Table

ACL Name

Add

6. Review the ACE policy settings below.

- **ACL Name:** Displays the ACL name in which the new policy will be added.
- **Priority:** Specify the priority value for the policy. (Lower number is higher priority. Ex: A value of 1 specifies the highest priority.)
- **Service:** Select the service or protocol for the policy.
 - **All:** All ports and protocols.
 - **HTTP:** Policy will only filter HTTP traffic.
 - **HTTPS:** Policy will only filter HTTPS traffic.
 - **SNMP:** Policy will only filter SNMP traffic.
 - **SSH:** Policy will only filter SSH traffic.
 - **Telnet:** Policy will only filter Telnet traffic.
- **Action:** Select the action for the policy.
 - **Permit:** Forward the traffic based on the parameters specified in the policy.
 - **Deny:** Drop the traffic based on the parameters specified in the policy.
- **Port:** In the Available port list, select the ports the policy will be applied. You can use the arrow buttons to add and remove to the Selected Ports list.

Note: Multiple ports can be selected at the same time by holding the Shift or Ctrl key.
- **IP Version:** Select the IP version used to identify the source IP address of the traffic to apply policy.
 - **All:** The policy will be applied to both IPv4 and IPv6 address source traffic, all IPv4 and IPv6 addresses.
 - **IPv4:** The policy will be applied only to IPv4 address source traffic.
 - **IPv6:** The policy will be applied only to IPv6 address source traffic.

- **IPv4:** If applying the policy to IPv4 traffic, enter the specific IPv4 and subnet mask to apply the policy.
- **IPv6:** If applying the policy to IPv6 traffic, enter the specific IPv6 address and subnet mask to apply the policy.

Add Management ACE

ACL Name	ACL1	
Priority	1 (1 - 65535)	
Service	<input type="radio"/> All <input type="radio"/> Http <input type="radio"/> Https <input checked="" type="radio"/> Snmp <input type="radio"/> SSH <input type="radio"/> Telnet	
Action	<input type="radio"/> Permit <input checked="" type="radio"/> Deny	
Port	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	Selected Port (Empty)
IP Version	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6	
IPv4	/ 255.255.255.255	
IPv6	/ 128 (1 - 128)	

- After the policy has been created under the ACL, click on **Security**, click on **Management Access**, and click on **Management ACL**. Check the ACL to activate and click **Active** to activate the ACL.

Management ACL Table

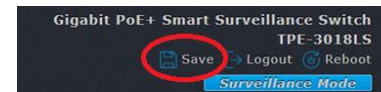
Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	ACL Name
<input checked="" type="checkbox"/>	ACL1

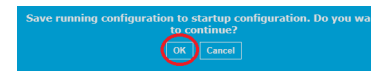
- Click **Apply**.



- In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



- Click **OK**.



Configure Port Security

Security > Port Security

This page allows users to configure port security settings for each port based on MAC address learning.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Port Security**.
3. In the Port Security Table, check the ports to apply port security and click **Edit**.

Port Security Table

<input type="checkbox"/>	Entry	Port	State	MAC Address	Action
<input checked="" type="checkbox"/>	1	GE1	Disabled		1 Discard

Edit

4. Review the settings below.

- **Port:** Displays the port or ports to be configured.
- **State:** Checking the **Enable** option will enable port security for the selected port or ports.
- **MAC Address:** Specify the max. number of MAC address that can be learning on the selected port or ports.
- **Action:** Select the action after the max. number of MAC addresses is reached on the selected port or ports.
 - **Forward:** Forwards the traffic any new source MAC address learned after the max number MAC addresses is reached on the selected port or ports.
 - **Discard:** Discard or drop any packets from new source MAC address detected after max. number of learned MAC addresses is reached.
 - **Shutdown:** Selected port or ports will shutdown after the max. number of learned MAC addresses I reached.

Edit Port Security

Port	GE1
State	<input type="checkbox"/> Enable
MAC Address	<input type="text" value="1"/> (0 - 255, default 1)
Action	<input type="radio"/> Forward <input checked="" type="radio"/> Discard <input type="radio"/> Shutdown

8. Click **Apply** at the bottom to apply the port security settings.

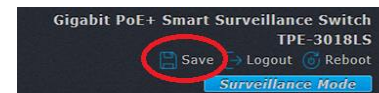


9. At the top of the page, check the **Enable** option and click **Apply** to enable the. port security function

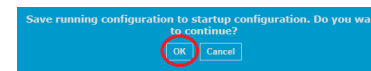
State	<input checked="" type="checkbox"/> Enable
-------	--

Apply

10. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



11. Click **OK**.



Configure Protected Ports

Security > Protected Ports

This page allows users to configure protected ports. Protected ports will not be allowed to communicate to another protected port, only communication between protected and unprotected ports will be allowed.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Protected Ports**.
3. In the table, select the ports to set as protected ports and click **Edit**.

<input type="checkbox"/>	Entry	Port	State
<input checked="" type="checkbox"/>	1	GE1	Unprotected

Edit

4. For the **State**, check the **Protected** setting to set the selected port or ports as Protected.

Edit Protected Port

Port	GE1
State	<input checked="" type="checkbox"/> Protected

Apply **Close**

5. Click **Apply**.

Apply

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.

Gigabit PoE+ Smart Surveillance Switch
TPE-3018LS

Save Logout Reboot

Surveillance Mode

7. Click **OK**.

Save running configuration to startup configuration. Do you want to continue?

OK Cancel

Configure Storm Control

Security > Storm Control

This page allows users to configure rate limits for broadcast, multicast, and unicast storms.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security** and click on **Storm Control**.
3. The configuration settings at the top of the page are for storm control global configuration. Review the configuration settings below and click **Apply** to apply the configuration settings.
 - **Mode:** Set the units used for storm control configuration.
 - **Packet / Sec:** Storm control configuration values are set to packets per second.
 - **Kbits / Sec:** Storm control configuration values are set to kilobits per second.
 - **IFG:** Set IFG settings to whether or not to calculate with or without Preamble and IFG (20 bytes)
 - **Exclude:** Exclude the preamble & IFG when counting the ingress storm control rate.
 - **Include:** Include the preamble & IFG when counting the ingress storm control rate.

4. In the table, select the ports to configure storm control rate limits and click **Edit**.

Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
<input checked="" type="checkbox"/>	1 GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Edit

4. Review the settings below.

- **Port:** Displays the port or ports to be configured.
- **State:** Checking the **Enable** option will enable storm control for the selected port or ports.
- **Broadcast:** Check the **Enable** option to enable the broadcast storm control for the selected port. Depending on the units set in the global storm control configuration, set the rate limit accordingly.
 - **Packet Per Second (pps) Range 1 – 262,143**
 - **Kilobits Per Second (Kbps) Range 16 – 1,000,000**
- **Unknown Multicast:** Check the **Enable** option to enable the unknown multicast storm control for the selected port. Depending on the units set in the global storm control configuration, set the rate limit accordingly.
 - **Packet Per Second (pps) Range 1 – 262,143**
 - **Kilobits Per Second (Kbps) Range 16 – 1,000,000**
- **Unknown Unicast:** Check the **Enable** option to enable the unknown unicast storm control for the selected port. Depending on the units set in the global storm control configuration, set the rate limit accordingly.
 - **Packet Per Second (pps) Range 1 – 262,143**
 - **Kilobits Per Second (Kbps) Range 16 – 1,000,000**
- **Action:** Select the action when the rate limit settings are reached the storm control configuration.
 - **Drop:** Traffic that has exceeded the storm control rate limits will be dropped.
 - **Shutdown:** The port will be shutdown if the traffic has exceeded the storm control weight limit settings.

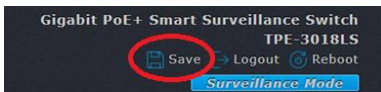
Edit Port Setting

Port	GE1
State	<input type="checkbox"/> Enable
Broadcast	<input type="checkbox"/> Enable
	<input type="text" value="10000"/> Kbps (16 - 1000000, default 10000)
Unknown Multicast	<input type="checkbox"/> Enable
	<input type="text" value="10000"/> Kbps (16 - 1000000, default 10000)
Unknown Unicast	<input type="checkbox"/> Enable
	<input type="text" value="10000"/> Kbps (16 - 1000000, default 10000)
Action	<input checked="" type="radio"/> Drop <input type="radio"/> Shutdown

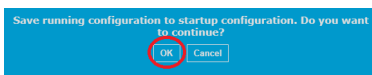
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Denial of Service (DoS)

Security > DoS

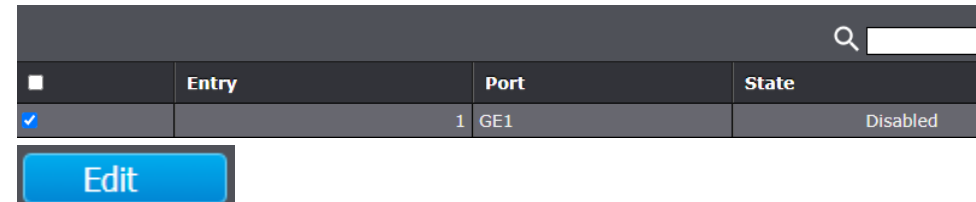
The switch has built-in DoS prevention features to restrict specific type of traffic associated denial of service attacks on your network. By default, DoS is disabled on all ports. For additional security, DoS can be enabled on all ports or specific ports as needed.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **DoS**, click on **Property**.
3. Review the settings below.
 - **POD:** Enable this option to block the ping of death DoS attacks.
 - **Land:** Enable this option to block LAND DoS attacks.
 - **UDP Blat:** Enable this option to block UDP flood DoS attacks.
 - **TCP Blat:** Enable this option to block TCP flood DoS attacks.
 - **DMAC = SMAC:** Enable this option to block traffic where the destination MAC is same as the source MAC.
 - **Null Scan Attack:** Enable this option to block TCP port scans on the switch to prevent discovery which ports are listening.
 - **X-Mas Scan Attack:** Enable this option to block X-Mas Scan attacks to prevent discovery of which devices/protocols are being used via TCP/IP.
 - **TCP SYN-FIN Attack:** Enable this option to block TCP SYN-FIN DoS attacks.
 - **TCP SYN-RST Attack:** Enable this option to block TCP SYN-RST DoS attacks
 - **ICMP Fragment:** Enable this option to block ICMP fragment DoS attacks.
 - **TCP-SYN:** Enable this option to block TCP-SYN flood attacks.
 - **TCP Fragment:** Enable this option to block TCP fragment DoS attacks, also known as teardrop.
 - **Ping Max Size (IPv4):** Enable this option to set the maximum size for ICMP ping packets.
 - **TCP Min Hdr Size:** Enable this option to set the maximum size for TCP headers.
 - **IPv6 Min Fragment:** Enable this option to set the minimum IPv6 fragment size.
 - **Smurf Attack:** Enable this option to set the subnet mask maximum length to prevent smurf DoS attacks.

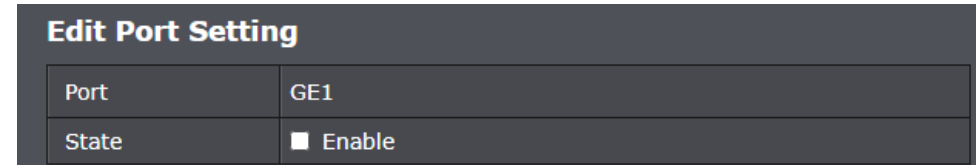
POD	<input checked="" type="checkbox"/> Enable
Land	<input checked="" type="checkbox"/> Enable
UDP Blat	<input checked="" type="checkbox"/> Enable
TCP Blat	<input checked="" type="checkbox"/> Enable
DMAC = SMAC	<input checked="" type="checkbox"/> Enable
Null Scan Attack	<input checked="" type="checkbox"/> Enable
X-Mas Scan Attack	<input checked="" type="checkbox"/> Enable
TCP SYN-FIN Attack	<input checked="" type="checkbox"/> Enable
TCP SYN-RST Attack	<input checked="" type="checkbox"/> Enable
ICMP Fragment	<input checked="" type="checkbox"/> Enable
TCP-SYN	<input checked="" type="checkbox"/> Enable Note: Source Port < 1024
TCP Fragment	<input checked="" type="checkbox"/> Enable Note: Offset = 1
Ping Max Size	<input checked="" type="checkbox"/> Enable IPv4 <input type="text" value="512"/> Byte (0 - 65535, default 512)
TCP Min Hdr size	<input checked="" type="checkbox"/> Enable <input type="text" value="20"/> Byte (0 - 31, default 20)
IPv6 Min Fragment	<input checked="" type="checkbox"/> Enable <input type="text" value="1240"/> Byte (0 - 65535, default 1240)
Smurf Attack	<input checked="" type="checkbox"/> Enable <input type="text" value="0"/> Netmask Length (0 - 32, default 0)

5. Click on **Security**, click on **DoS**, and click on **Port Setting**.

6. Check the ports to enable DoS and click **Edit**.



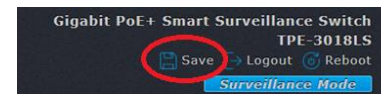
7. For the State, check the **Enable** option to enable DoS for the selected port or ports.



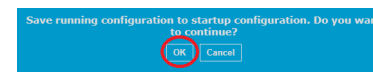
8. Click **Apply**.



9. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



10. Click **OK**.



DHCP Snooping

Security > DHCP Snooping > Property

Here is a summary of the rules to observe when you configure DHCP Snooping:

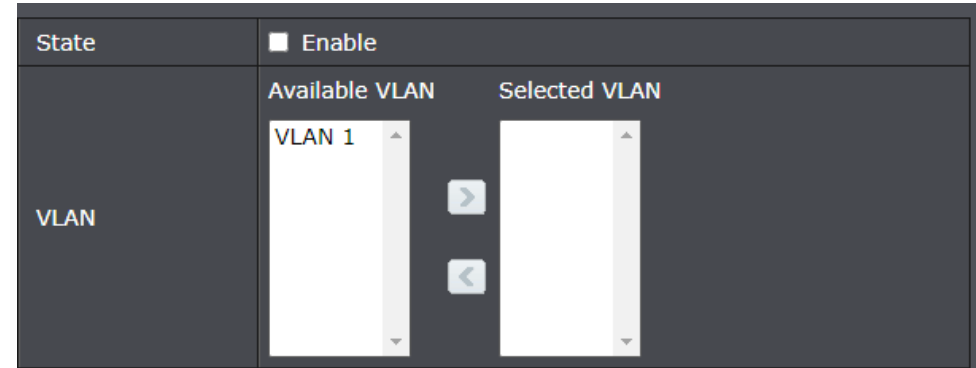
- A trusted port is connected to one of the following:
 - Directly to the legitimate trusted DHCP Server.
 - A network device relaying DHCP messages to and from a trusted server.
 - Another trusted source such as a switch with DHCP Snooping enabled.
 - Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.
- The VLANs to which the DHCP Snooping feature applies must be specified in the DHCP Snooping VLAN Setting configuration.
- Any static IP addresses on the network must be manually added to the Binding Database.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

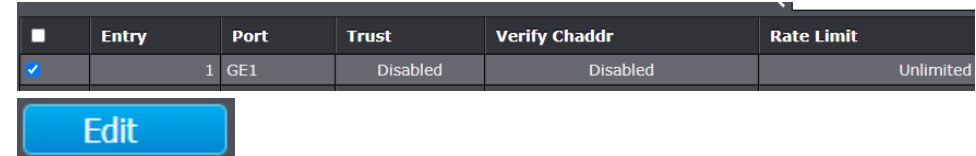
2. Click on **Security**, click on **DHCP Snooping**, and click on **Property**.

3. Configure the DHCP global settings..

Item	Description
State	Set checkbox to enable/disable DHCP Snooping function.
VLAN	Select VLANs in left box then move to right to enable DHCP Snooping. Or select VLANs in right box then move to left to disable DHCP Snooping.



4. In the table, select the ports to configure for DHCP snooping and click **Edit**.



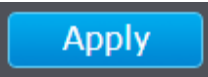
5. Review the settings below.

Item	Description
Port	Display selected port to be edited
Trust	Set checkbox to enable/disable trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled.
Verify Chaddr	Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
Rate Limit	Input rate limitation of DHCP packets. The unit is pps. 0 means unlimited. Default is unlimited.

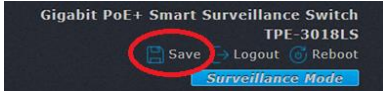
Edit Port Setting

Port	GE1
Trust	<input type="checkbox"/> Enable
Verify Chaddr	<input type="checkbox"/> Enable
Rate Limit	0 pps (0 - 300, default 0), 0 is Unlimited

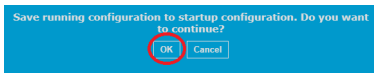
6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



View DHCP Snooping Statistics

Security > DHCP Snooping > Statistics

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **DHCP Snooping**, and click on **Statistics**.
3. Review the statistics settings below.

Item	Description
Port	Display port ID.
Forwarded	Display how many packets forwarded normally.
Chaddr Check Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.

Statistics Table

■	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
■	1	GE1	0	0	0	0	0
■	2	GE2	0	0	0	0	0

Configure DHCP Option 82 settings

Security > DHCP Snooping > Option82 Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **DHCP Snooping**, and click on **Option82 Property**.
3. Review the settings below.

Item	Description
User Defined	Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.
Remote ID	Input user-defined remote ID. Only available when enable user-define remote ID.

Remote ID	<input type="checkbox"/> User Defined <input type="text"/>
Operational Status	
Remote ID	3c:8c:f8:f9:d0:4a (Switch Mac in Byte Order)

4. In the table, select the ports to configure for Option 82 and click **Edit**.

Item	Description
Port	Display selected port to be edited
State	Set checkbox to enable/disable option82 function of interface.

Allow untrusted	<p>Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop.</p> <ul style="list-style-type: none"> • Keep: Keep original option82 content. • Replace: Replace option82 content by switch setting • Drop: Drop packets with option82
-----------------	--

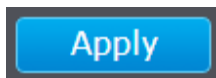
<input type="checkbox"/>	Entry	Port	State	Allow Untrust
<input checked="" type="checkbox"/>	1	GE1	Disabled	Drop

[Edit](#)

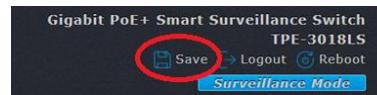
Edit Port Setting

Port	GE1
State	<input checked="" type="checkbox"/> Enable
Allow Untrust	<input type="radio"/> Keep <input checked="" type="radio"/> Drop <input type="radio"/> Replace

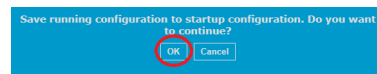
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure DHCP Option 82 Circuit ID settings

Security > DHCP Snooping > Option Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Security**, click on **DHCP Snooping**, and click on **Option82 Circuit ID**.
3. Click **Add**. Review the settings below.

Item	Description
Port	Select port from list to associate to CID entry. Only available on Add dialog.
VLAN	Input VLAN ID to associate to circuit ID entry. VLAN ID is not mandatory. Only available on Add dialog.
Circuit ID	Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

Option82 Circuit ID Table

Showing All entries Showing 0 to 0 of 0 entries

Port	VLAN	Circuit ID
0 results found.		

Add Edit Delete First Previous 1 Next Last

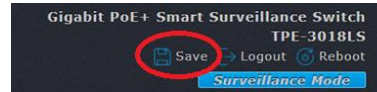
Add Option82 Circuit ID

Port	GE1
VLAN	(1 - 4094) (Keep empty to set without VLAN)
Circuit ID	

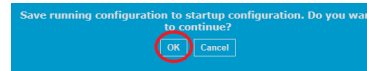
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure IP Source Guard

Security > IP Source Guard > Port Setting

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Security**, click on **IP Source Guard**, and click on **Port Setting**.
3. In the table, select the ports to configure for IP Source Guard and click **Edit**.

<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input checked="" type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited

Edit

4. Review the setting below.

Item	Description
Port	Display selected port to be edited.
Status	Set checkbox to enable or disable IP Source Guard function. Default is disabled.
Verify Source	Select the mode of IP Source Guard verification <ul style="list-style-type: none"> • IP: Only verify source IP address of packet. • IP-MAC: Verify source IP and source MAC address of packet.
Max Entry	Input the maximum number of entries that a port can be bounded. Default is un-limited on all ports. No entry will be bound if limitation reached.

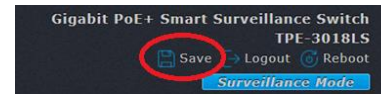
Edit Port Setting

Port	GE1
State	<input type="checkbox"/> Enable
Verify Source	<input checked="" type="radio"/> IP <input type="radio"/> IP-MAC
Max Entry	<input type="text" value="0"/> (0 - 50, default 0), 0 is Unlimited

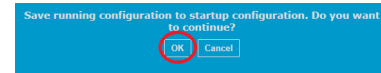
5. Click **Apply**.

Apply

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Configure IP Source Guard IMPV Binding

Security > IP Source Guard > IMPV Binding

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Security**, click on **IP Source Guard**, and click on **IMPV Binding**.
3. Click **Add** and review the settings below.

Item	Description
Port	Select port from list of a binding entry.
VLAN	Specify a VLAN ID of a binding entry.
Binding	Select matching mode of binding entry <ul style="list-style-type: none"> • IP-MAC-Port-VLAN: packet must match IP address、 MAC address、 Port and VLAN ID. • IP-Port-VLAN: packet must match IP address or
MAC Address	Input MAC address. Only available on IP-MAC-Port-VLAN mode.
IP Address	Input IP address and mask. Mask only available on IP-MAC-Port mode.

IP-MAC-Port-VLAN Binding Table

Showing All entries Showing 0 to 0 of 0 entries

Search:

Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.						

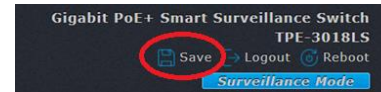
Add IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	<input type="text"/> (1 - 4094)
Binding	<input checked="" type="radio"/> IP-MAC-Port-VLAN <input type="radio"/> IP-Port-VLAN
MAC Address	<input type="text"/>
IP Address	<input type="text"/> / <input type="text"/> 255.255.255.255

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Save DHCP Snooping Database

Security > IP Source Guard > Save Database

This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Security**, click on **IP Source Guard**, and click on **Save Database**.
3. Review the settings below.

Item	Description
Type	Select the type of database agent. <ul style="list-style-type: none"> • None: Disable database agent service. • Flash: Save DHCP dynamic binding entries to flash. • TFTP: Save DHCP dynamic binding entries to remote TFTP
Filename	Input filename for backup file. Only available when selecting type “flash” and “TFTP”.
Address Type	Select the type of TFTP server. <ul style="list-style-type: none"> • Hostname: TFTP server address is hostname.
Server Address	Input remote TFTP server hostname or IP address. Only available when selecting type “TFTP”
Write Delay	Input delay timer for doing backup after change happened. Default is 300 seconds.

Timeout	Input aborts timeout for doing backup failure. Default is 300 seconds.	
Type	<input checked="" type="radio"/> None <input type="radio"/> Flash <input type="radio"/> TFTP	
Filename	<input type="text"/>	
Address Type	<input type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6	
Server Address	<input type="text"/>	
Write Delay	<input type="text" value="300"/>	Sec (15 - 86400, default 300)
Timeout	<input type="text" value="300"/>	Sec (0 - 86400, default 300)

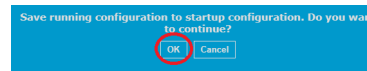
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



ACL

This section allows users to configure traffic access control lists and access control policies/entries.

Configure MAC ACL

ACL > MAC ACL

This section allows users to configure access control lists filtered based on MAC address.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ACL** and click on **MAC ACL**.
3. Review the settings below.

Item	Description
ACL Name	Input MAC ACL name.
ACL Name	Display MAC ACL name.
Rule	Display the number ACE rule of ACL.
Port	Display the port list that bind this ACL.

ACL Name

ACL Table

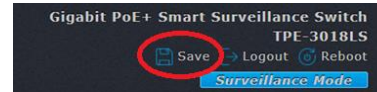
Showing All entries Showing 0 to 0 of 0 entries

■	ACL Name	Rule	Port
0 results found.			

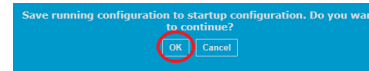
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure MAC ACE

ACL > MAC ACE

This section allows users to configure access control entries/policies for the MAC ACLs defined and filtered based on MAC address.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ACL** and click on **MAC ACE**.
3. Review the settings below.

Item	Description
ACL Name	Display the ACL name to which an ACE is being added..
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
Action	<p>Select the action after ACE match packet. ⓘ</p> <ul style="list-style-type: none"> ● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria. ● Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
Source MAC	<p>Select the type for source MAC address. ⓘ</p> <ol style="list-style-type: none"> 1. Any: All source addresses are acceptable. ⓘ 2. User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.

Destination MAC	<p>Select the type for Destination MAC address. ⓘ</p> <ul style="list-style-type: none"> ● Any: All destination addresses are acceptable. ⓘ ● User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.
Ethertype	<p>Select the type for Ethernet frame type. ⓘ</p> <ul style="list-style-type: none"> ● Any: All Ethernet frame type is acceptable. ⓘ ● User Defined: Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
VLAN	<p>Select the type for VLAN ID. ⓘ</p> <ul style="list-style-type: none"> ● Any: All VLAN ID is acceptable. ⓘ ● User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
802.1p	<p>Select the type for 802.1p value. ⓘ</p> <ul style="list-style-type: none"> ● Any: All 802.1p value is acceptable. ⓘ ● User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

ACE Table

ACL Name **ACL1** ▾

Showing **All** ▾ entries Showing 0 to 0 of 0 entries 🔍

■	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p		
			Address	Mask	Address	Mask			Value	Mask	
0 results found.											

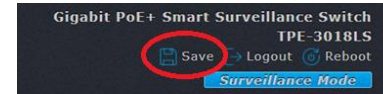
Add ACE

ACL Name	ACL1
Sequence	<input type="text"/> (1 - 2147483647)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Source MAC	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Destination MAC	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Ethertype	<input checked="" type="checkbox"/> Any 0x <input type="text"/> (0x600 ~ 0xFFFF)
VLAN	<input checked="" type="checkbox"/> Any <input type="text"/> (1 - 4094)
802.1p	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Value / Mask) (0 - 7)

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure IPv4 ACL

ACL > IPv4 ACL

This section allows users to configure access control lists filtered based on IPv4 address.

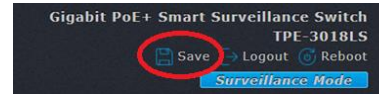
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ACL** and click on **IPv4 ACL**.
3. Review the settings below.

Item	Description
ACL Name	Input IPv4 ACL name.
ACL Name	Display IPv4 ACL name.
Rule	Display the number ACE rule of ACL.
Port	Display the port list that bind this ACL.

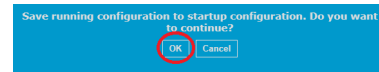
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure IPv4 ACE

ACL > IPv4 ACE

This section allows users to configure access control entries/policies for the IPv4 ACLs defined and filtered based on IPv4 address.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ACL** and click on **IPv4 ACE**.
3. Review the settings below.

Item	Description
ACL Name	Display the ACL name to which an ACE is being added.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first (1 is the highest sequence). Only available on Add dialog.
Action	<p>Select the action for a match. [?]</p> <ul style="list-style-type: none"> ● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria. <p>Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received.</p>
	Such ports can be reactivated from the Port Settings page.

Protocol	<p>Select the type of protocol for a match. [?]</p> <ul style="list-style-type: none"> ● Any (IP): All IP protocols are acceptable. [?] ● Select from list: Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPv6:FRAG/RSVP/IPV6:ICMP/OSPF/PIM/L2TP) ● Protocol ID to match: Enter the protocol ID.
Source IP	<p>Select the type for source IP address. [?]</p> <ul style="list-style-type: none"> ● Any: All source addresses are acceptable. [?] ● User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
Destination IP	<p>Select the type for destination IP address. [?]</p> <ul style="list-style-type: none"> ● Any: All destination addresses are acceptable. [?] ● User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.

Source Port	<p>Select the type of protocol for a match. Only available when protocol is TCP or UDP. [?]</p> <ul style="list-style-type: none"> Any: All source ports are acceptable. [?] Single: Enter a single TCP/UDP source port to which packets are matched. [?] Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	<p>Select the type of protocol for a match. Only available when protocol is TCP or UDP. [?]</p> <ul style="list-style-type: none"> Any: All source ports are acceptable. [?] Single: Enter a single TCP/UDP source port to which packets are matched. [?] Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

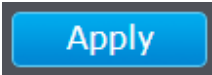
Destination Port	<p>Select the type of protocol for a match. Only available when protocol is TCP or UDP. [?]</p> <ul style="list-style-type: none"> Any: All source ports are acceptable. [?] Single: Enter a single TCP/UDP source port to which packets are matched. [?] Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
TCP Flags	<p>Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.</p>
Type of Service	<p>Select the type of service for a match. [?]</p> <ul style="list-style-type: none"> Any: All types of service are acceptable. [?] DSCP to match: Enter a Differentiated Services Code Point (DSCP) to match. [?] IP Precedence to match: Enter a IP Precedence to
ICMP Type	<p>Either select the message type by name or enter the message type number. Only available when protocol is ICMP. [?]</p> <ul style="list-style-type: none"> Any: All message types are acceptable. [?] Select from list: Select message type by name.

ICMP Code	<p>Select the type for ICMP code. Only available when protocol is ICMP. ⓘ</p> <ul style="list-style-type: none"> Any: All codes are acceptable. ⓘ User Defined: Enter an ICMP code to match.
-----------	--

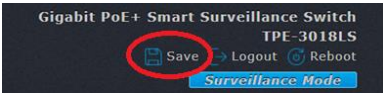
Add ACE

ACL Name	ACLIPV41
Sequence	<input type="text"/> (1 - 2147483647)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="ICMP"/> <input type="button" value="v"/> <input type="radio"/> Define <input type="text"/> (0 - 255)
Source IP	<input checked="" type="radio"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Destination IP	<input checked="" type="radio"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> (0 - 63) <input type="radio"/> IP Precedence <input type="text"/> (0 - 7)
Source Port	<input type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
Destination Port	<input type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
TCP Flags	Urg: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care Ack: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care Psh: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care Rst: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care Syn: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care Fin: <input type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't care
ICMP Type	<input type="radio"/> Any <input type="radio"/> Select <input type="text" value="Echo Reply"/> <input type="button" value="v"/> <input type="radio"/> Define <input type="text"/> (0 - 255)
ICMP Code	<input type="radio"/> Any <input type="radio"/> Define <input type="text"/> (0 - 255)

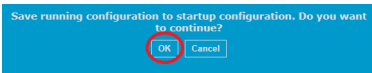
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure ACL Port Binding

ACL > ACL Binding

This section allows users to bind MAC or IPv4 ACLs to specific switch ports or link aggregation groups.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **ACL** and click on **ACL Binding**.
3. Review the settings below.

Item	Description
Port	Display port entry ID.
MAC ACL	Select mac ACL name from list to bind.
IPv4 ACL	Select IPv4 ACL name from list to bind.
IPv6 ACL	Select IPv6 ACL name from list to bind.

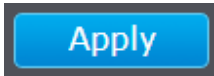
ACL Binding Table

Entry	Port	MAC ACL	IPv4 ACL
1	GE1		

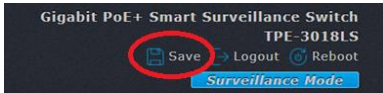
Add ACL Binding

Port	GE1
	Note: ACL without any rules cannot be bound
MAC ACL	None ▼
IPv4 ACL	None ▼

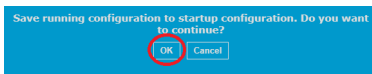
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



QoS

This section allows users to configure traffic priority.

Configure QoS Global Settings

QoS > General > Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **QoS**, click on **General**, and click on **Property**.
3. Review the settings below.

Item	Description
State	Set checkbox to enable/disable QoS.
Trust	Select QoS trust mode <ul style="list-style-type: none"> • CoS: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. • IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

State	<input type="checkbox"/> Enable
Trust Mode	<input checked="" type="radio"/> CoS <input type="radio"/> IP Precedence
<input type="button" value="Apply"/>	

4. In the table, select the ports to configure for QoS and click **Edit**.

■	Entry	Port	CoS	Trust	Remarking	
					CoS	IP Precedence
<input checked="" type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled
<input type="button" value="Edit"/>						

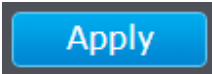
5. Review the settings below.

Item	Description
Port	Selected port list.
CoS	Set default CoS/802.1p priority value for the selected
Trust	Set checkbox to enable/disable port trust state.
Remarking	Set checkbox to enable/disable port CoS remarking.
Remarking (IP)	Set checkbox to enable/disable port IP Precedence remarking.

Edit Port Setting

Port	GE1
CoS	<input type="text" value="0"/> (0 - 7)
Trust	<input checked="" type="checkbox"/> Enable
Remarking	
CoS	<input type="checkbox"/> Enable
IP Precedence	<input type="checkbox"/> Enable

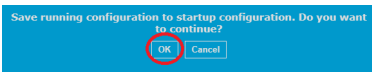
6. Click **Apply**.



7. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



8. Click **OK**.



Configure Queue Scheduling

QoS > General > Queue Scheduling

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).

2. Click on **QoS**, click on **General**, and click on **Queue Scheduling**.

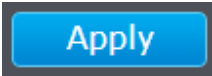
3. Review the settings below.

Item	Description
Queue	Queue ID to configure.
Strict Priority	Set queue to strict priority type.
WRR	Set queue to Weight round robin type.
Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth	Percentage of WRR queue bandwidth.

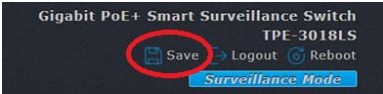
Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="1"/>	
2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="2"/>	
3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="3"/>	
4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="4"/>	
5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="5"/>	
6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="6"/>	
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="13"/>	
8	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="15"/>	

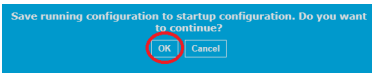
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure CoS Mapping

QoS > General > CoS Mapping

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).

2. Click on **QoS**, click on **General**, and click on **CoS Mapping**.

3. Review the settings below.

Item	Description
CoS to Queue Mapping	
CoS	CoS value.
Queue	Select queue id for the CoS value.
Queue to CoS Mapping	
Queue	Queue ID
CoS	Select CoS value for the queue id.

CoS to Queue Mapping	
CoS	Queue
0	2 ▾
1	1 ▾
2	3 ▾
3	4 ▾
4	5 ▾
5	6 ▾
6	7 ▾
7	8 ▾

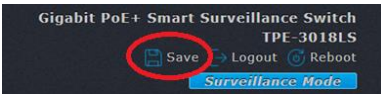
Queue to CoS Mapping

Queue	CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

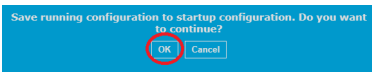
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure IP Precedence Mapping

QoS > General > IP Precedence Mapping

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **QoS**, click on **General**, and click on **IP Precedence Mapping**.
3. Review the settings below.

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	IP Precedence value.
Queue	Queue value which IP Precedence is mapped.
Queue to IP Precedence Mapping	
Queue	Queue ID.
IP Precedence	IP Precedence value which queue is mapped.

IP Precedence to Queue Mapping

IP Precedence	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

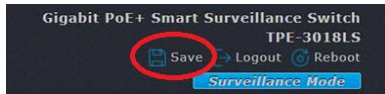
Queue to IP Precedence Mapping

Queue	IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

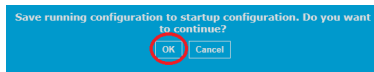
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Rate Limiting per port

QoS > Rate Limit > Ingress/Egress Port

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).

2. Click on **QoS**, click on **Rate Limit**, and click on **Ingress/Egress Port**.

3. In the table, select the ports to configure for QoS and click **Edit**.

	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
<input checked="" type="checkbox"/>	1	GE1	Disabled		Disabled	



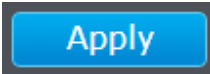
4. Review the settings below.

Item	Description
Port	Select port list.
Ingress	Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned.
Egress	Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

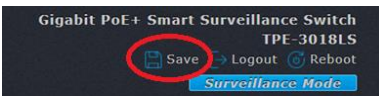
Edit Ingress / Egress Port

Port	GE1	
Ingress	<input type="checkbox"/> Enable	
	<input type="text" value="1000000"/>	Kbps (16 - 1000000)
Egress	<input type="checkbox"/> Enable	
	<input type="text" value="1000000"/>	Kbps (16 - 1000000)

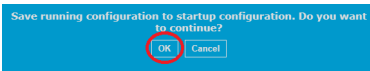
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Diagnostics

This section provides diagnostics tools for troubleshooting.

Configure Logging

Diagnostics > Logging > Property

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Diagnostics**, click on **Logging**, and click on **Property**.
3. Review the settings below.

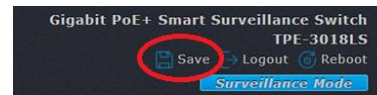
Item	Description
State	Enable/Disable the global logging services. When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.
Console Logging	
State	Enable/Disable the console logging service
Minimum Severity	The minimum severity for the console logging.
RAM Logging	
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.
Flash Logging	
State	Enable/Disable the flash logging service.

Minimum	The minimum severity for the flash logging.
State	<input checked="" type="checkbox"/> Enable
Console Logging	
State	<input checked="" type="checkbox"/> Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	<input checked="" type="checkbox"/> Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	<input type="checkbox"/> Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

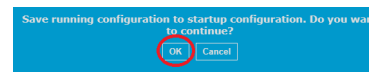
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Remote Logging/Syslog Server

Diagnostics > Logging > Remote Server

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Diagnostics**, click on **Logging**, and click on **Remote Server**.
3. Click **Add** and review the settings below.

Item	Description
Server	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0,local1, local2, local3, local4, local5, local6, and local7.
Severity	<p>The minimum severity.</p> <ul style="list-style-type: none"> • Emergence: System is not usable. • Alert: Immediate action is needed. • Critical: System is in the critical condition. • Error: System is in error condition
	<p>has occurred.</p> <ul style="list-style-type: none"> • Informational: Device information. • Debug: Provides detailed information about an event.

Remote Server Table

■	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					
		Add	Edit	Delete	

Address Type

Server Address

Server Port (1 - 65535, default 514)

Facility

Minimum Severity

Note: Emergency, Alert, Critical, Error, Warning, Notice

Hostname

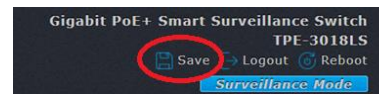
IPv4

IPv6

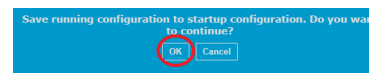
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure Port Mirroring

Diagnostics > Mirroring

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Diagnostics** and click on **Mirroring**.
3. In the table, select the session to configure for port mirroring and click **Edit**.

Mirroring Table

Session ID	State	Monitor Port	Ingress Port	Egress Port
1	Disabled	---	---	---

Edit

4. Review the settings below.

Item	Description
Session ID	Selected mirror session ID.
State	Select mirror session state : port-base mirror or disable <ul style="list-style-type: none"> • Enabled: Enable port based mirror • Disabled: Disable mirror.
Monitor	Select mirror session monitor port, and select whether
Ingress	Select mirror session source rx ports.
Egress port	Select mirror session source tx ports.

Edit Mirroring

Session ID: 1

State: Enable

Monitor Port: GE1 Send or Receive Normal Packet

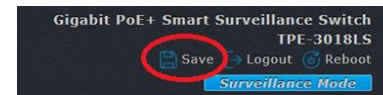
Ingress Port: Available Port (GE1-GE8) Selected Port

Egress Port: Available Port (GE1-GE8) Selected Port

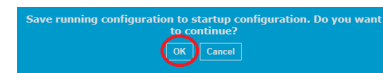
5. Click **Apply**.

Apply

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Ping Test*Diagnostics > Ping*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics** and click on **Ping**.
3. Review the settings below.

Item	Description
Address Type	Specify the address type to "Hostname" or "IPv4".
Server Address	Specify the Hostname/IPv4 address for the remote logging server.
Count	Specify the numbers of each ICMP ping request.

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Count	<input type="checkbox"/> User Defined <input type="text" value="4"/> (1 - 65535)
<input type="button" value="Ping"/> <input type="button" value="Stop"/>	

Ping Result**Packet Status**

Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

Round Trip Time

Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

Ping Watchdog

Diagnostics > Ping Watchdog

This section allows users to configure a connectivity test to remote host. If connectivity is lost to the remote host, the switch will reboot automatically.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Diagnostics** and click on **Ping Watchdog**.
3. In the table, select the port to configure for ping watchdog and click **Edit**.

■	Entry	Port	Reboot Enable	Ping Host	Ping Interval	Retry Count
☑	1	GE1	Disable	0.0.0.0	5	2



4. Review the settings below.

Item	Description
Port	Displays the port or ports currently selected to configure for ping watchdog.
Reboot Enable	Checking the Enable option will automatically reboot the switch on ping failure to the remote host.
Ping Host	Enter the IPv4 address of the remote host to ping.
Ping Interval	Enter the time period between each ping send to the host in minutes.
Retry Count	Enter the number of retries allowed if ping fails to the host. After the retry count is reached, the switch will automatically reboot.

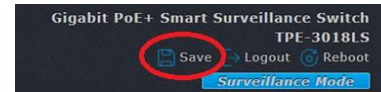
Ping Watchdog

Port	GE1	
Reboot Enable	<input type="checkbox"/> Enable	
Ping Host	0.0.0.0	
Ping Interval	5	Min (1 - 60, default 5)
Retry Count	2	(1 - 100, default 2)

5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Traceroute

Diagnostics > Traceroute

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics** and click on **Traceroute**.
3. Review the settings below.

Item	Description
Address Type	Specify the address type to "Hostname" or "IPv4".
Server Address	Specify the Hostname/IPv4 address for the host address for traceroute.
Time to Live	Specify the max hops of hosts for traceroute.

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
Server Address	<input type="text"/>
Time to Live	<input type="checkbox"/> User Defined <input type="text" value="30"/> (2 - 255, default 30)
<input type="button" value="Apply"/> <input type="button" value="Stop"/>	

Copper Test

Diagnostics > Copper Test

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics** and click on **Copper Test**.
3. Review the settings below.

Item	Description
Port	Specify the interface for the copper test.
Copper Test Result	
Port	The interface for the copper test.
Result	The status of copper test. It include: <ul style="list-style-type: none"> ● OK: Correctly terminated pair. ● Short Cable: Shorted pair. ● Open Cable: Open pair, no link partner. ● Impedance Mismatch: Terminating impedance is not in the reference range.
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

Port	GE1
<input type="button" value="Copper Test"/>	

Fiber Module

Diagnostics > Fiber Module

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics** and click on **Fiber Module**.
3. In the table, select the SFP slot/fiber module and click click **Detail**.

Fiber Module Table

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)
<input checked="" type="radio"/>	GE11	N/A	N/A	N/A	N/A	N/A
<input type="radio"/>	GE12	N/A	N/A	N/A	N/A	N/A

Detail

4. Review the settings below.

Item	Description
Port	Interface or port number.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured TX output power in milliwatts.
Input Power	Measured RX received power in milliwatts.
Transmitter Fault	State of TX fault.

OE Present	Indicate transceiver has achieved power up and data is
Loss of Signal	Loss of signal.
Refresh	Refresh the page.
Detail	The detail information on the specified port.

Fiber Module Status	
Port	GE11
OE Present	Remove
Loss of Signal	Loss
Transceiver Type	N/A
Connector Type	N/A
Ethernet Compliance Code	N/A
Transmission Media	N/A
Wavelength	N/A
Bitrate	N/S
Vendor OUI	N/A
Vendor Name	N/A
Vendor PN	N/A
Vendor Revision	N/A
Vendor SN	N/A
Date Code	N/A
Temperature (C)	N/A
Voltage (V)	N/A
Current (mA)	N/A
Output Power (mW)	N/A
Input Power (mW)	N/A

UDLD

Diagnostics > UDLD > Property

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics**, click on **UDLD**, and click on **Property**.
3. Review the settings below.

Item	Description
Message Time	Input the interval for sending message. Range is 1 -90 seconds.
Port	Display port ID of entry.
Mode	Display UDLD running mode of interface.
Bidirectional	Display bidirectional state of interface.
Operational	Display operational status of interface.
Neighbor	Display the number of neighbor of interface.

Message Time	<input type="text" value="15"/>	Sec (1 - 90, default 15)
<input type="button" value="Apply"/>		

4. In the table, select the port to configure for UDLD and click click **Edit**.

Item	Description
Port	Display selected port to be edited.

Mode	<p>Select UDLD running mode of interface. ?</p> <ul style="list-style-type: none"> ● Disabled: Disable UDLD function. ? ● Normal: Running on normal mode that port goes to Link Up One phase after last neighbor ages out. ? ● Aggressive: Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.
------	---

Port Setting Table

■	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
✓	1	GE1	Disabled	Unknown		0

[Edit](#)

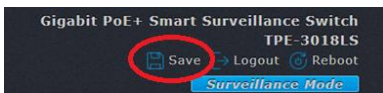
Edit Port Setting

Port	GE1
Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> Normal <input type="radio"/> Aggressive

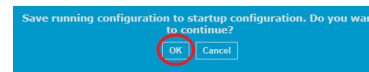
5. Click **Apply**.

[Apply](#)

6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



View UDLD Neighbors*Diagnostics > UDLD > Neighbor*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Diagnostics**, click on **UDLD**, and click on **Neighbor**.
3. Review the settings below.

Item	Description
Entry	Display entry index.
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbor current state.
Device ID	Display neighbor device ID.
Device Name	Display neighbor device name.
Port ID	Display neighbor port ID that connected.
Message Interval	Display neighbor message interval.
Timeout Interval	Display neighbor timeout interval.

Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval
0 results found.							

Management

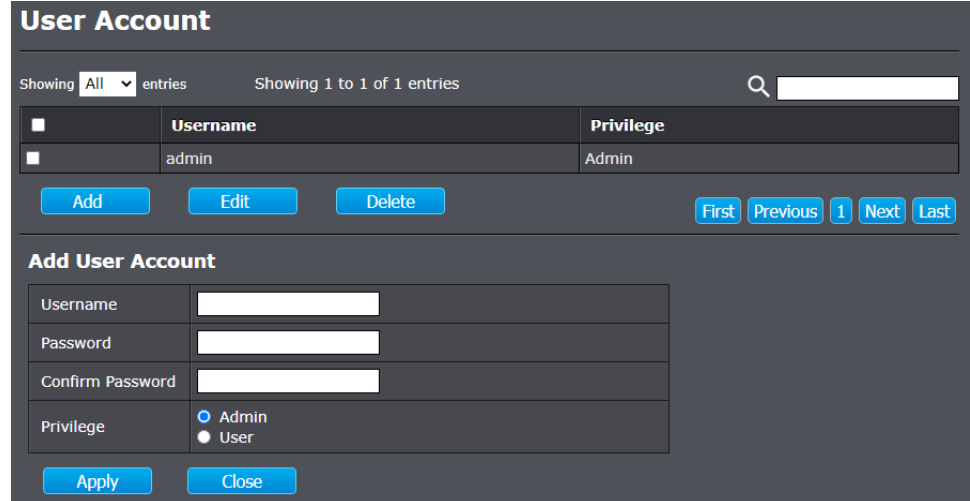
This section allows users to modify the admin password, create users, upgrade firmware, backup/restore configuration, create schedules, and configure SNMP/RMON management settings.

Modify admin password and create new users

Management > User Account

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Management** and click on **User Account**.
3. Click **Add** to create a new user or select the account to modify and click **Edit**. Review the settings below.

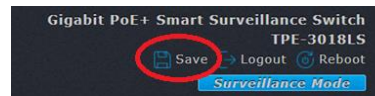
Item	Description
Username	User name of the account.
Password	Set password of the account.
Confirm Password	Set the same password of the account as in “Password” field.
Privilege	<p>Select privilege level for new account.</p> <ul style="list-style-type: none"> • Admin: Allow to change switch settings. Privilege value equals to 15. • User: See switch settings only. Not allow to change it. Privilege level equals to 1.



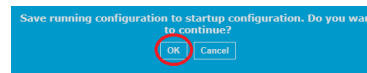
5. Click **Apply**.



6. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



7. Click **OK**.



Upgrade switch firmware*Management > Firmware > Upgrade / Backup*

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **Firmware**, and click on **Upgrade / Backup**.
3. Review the settings below. After the firmware has been selected, click **Apply** to start the firmware upgrade process.

HTTP

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT. • Backup: Backup firmware image from DUT to remote host.
Method	Firmware upgrade / backup method. <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware. • HTTP: Using WEB browser to upgrade/backup firmware.
Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.

Action	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
Method	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
Filename	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>
<input type="button" value="Apply"/>	

TFTP

Item	Description
Action	Firmware operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware. • HTTP: Using WEB browser to upgrade/backup firmware.
Address Type	Specify TFTP server address type <ul style="list-style-type: none"> • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

Action	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
Method	<input checked="" type="radio"/> TFTP <input type="radio"/> HTTP
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Filename	<input type="text"/>

Backup/Restore switch Configuration

Management > Configuration > Upgrade / Backup

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **Configuration**, and click on **Upgrade / Backup**.
3. Review the settings below.

HTTP

Item	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware • HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> • Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file
Filename	Use browser to upgrade configuration, you should select configuration file on your host PC.

Action	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
Method	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
Configuration	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
Filename	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>
<input type="button" value="Apply"/>	

Address Type	Specify TFTP server address type <ul style="list-style-type: none"> • Hostname: Use domain name as server address • IPv4: Use IPv4 as server address
Server Address	Specify TFTP server address address
Filename	File name saved on remote TFTP server

Action	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
Method	<input checked="" type="radio"/> TFTP <input type="radio"/> HTTP
Configuration	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Filename	<input type="text"/>
<input type="button" value="Apply"/>	

TFTP

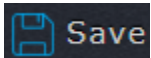
Item	Description
Action	Configuration operations <ul style="list-style-type: none"> • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method <ul style="list-style-type: none"> • TFTP: Using TFTP to upgrade/backup firmware
Configuration	Configuration types <ul style="list-style-type: none"> • Running Configuration: Merge to current running configuration file • Startup Configuration: Replace startup configuration file

Save switch configuration to NV-RAM / Restore to default

Management > Configuration > Save Configuration

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **Firmware**, and click on **Save Configuration**.
3. Review the settings below.

Note: After applying configuration changes you must also save configuration the Running Configuration to NV-RAM/Startup Configuration to ensure the configuration settings are saved after a switch reboot. Clicking the **Save** icon in the top right-hand side of the page will configuration settings to NV-RAM/Startup Configuration.



Source File	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration
Destination File	<input checked="" type="radio"/> Startup Configuration
<input type="button" value="Apply"/> <input type="button" value="Restore Factory Default"/>	

Item	Description
Source File	Source file types <ul style="list-style-type: none"> • Running Configuration: Copy running configuration file to destination. • Startup Configuration: Copy startup configuration file to destination.

Destination File	Destination file <ul style="list-style-type: none"> • Startup Configuration: Save file as startup configuration. • Backup Configuration: Save file as backup configuration.
------------------	---

Note: Clicking Restore Factory Default will reset all switch configuration settings to factory defaults.

SNMP

You can manage a switch by viewing and configuring the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). This section describes how to configure SNMP. A Group Name, IP address of the switch and at least one community string is the minimum required to manage the switch using SNMP.

Configure the SNMP View Table

Management > SNMP > View Table

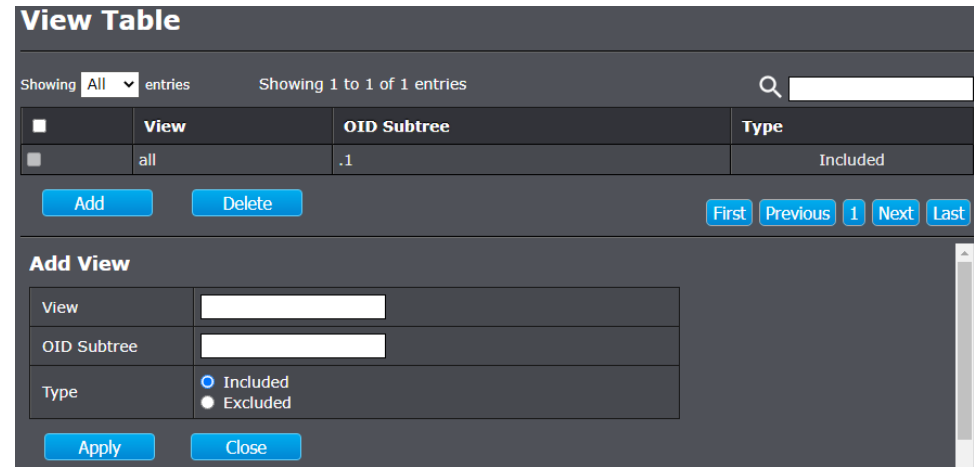
The SNMP View table specifies the MIB object access criteria for each View Name. If the View Name is not specified on this page, then it has access to all MIB objects. You can specify specific areas of the MIB that can be accessed or denied based on the entries in this table. You can create and delete entries in the View table.

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Management**, click on **SNMP**, and click on **View**.
3. Click **Add** to add a new SNMP view table. Review the settings.

Item	Description
View	The SNMP view name. Its maximum length is 30 characters
OID Subtree	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view
Type	Include or exclude the selected MIBs in the view

- Enter the **Subtree OID**.
- Select the **View Type**.

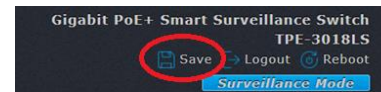
- **Included:** This selection allows the specified MIB object to be included in the view.
- **Excluded:** This selection blocks the view of the specified MIB object.



4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure the SNMP Group Table

Management > SNMP > Group Access Table

The SNMP View Names are defined in the SNMP Group Access table and are based on the User and Group Names

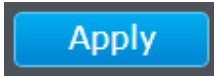
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **Group**.
3. Click **Add** to a new SNMP group table. Review the settings.

Item	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version <ul style="list-style-type: none"> • SNMPv1: SNMP Version 1. • SNMPv2: Community-based SNMP Version 2. • SNMPv3: User security model SNMP version 3.
Security Level	Specify SNMP security level <ul style="list-style-type: none"> • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet authentication with encryption is performed.
View	

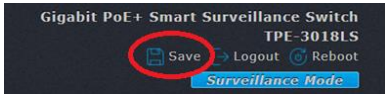
Read	Select read view name if Read is checked.
Write	Select write view name, if Write is checked.
Notify	Select notify view name, if Notify is checked.

The screenshot shows the 'Group Table' configuration page. At the top, it says 'Showing All entries' and 'Showing 0 to 0 of 0 entries'. Below this is a table with columns: Group, Version, Security Level, and View. The View column has sub-columns for Read, Write, and Notify. Below the table, it says '0 results found.' and 'Configure SNMP View to associate a non-default view with a group.' There are 'Add', 'Edit', and 'Delete' buttons. Below that is the 'Add Group' form with fields for Group, Version (radio buttons for SNMPv1, SNMPv2, SNMPv3), Security Level (radio buttons for No Security, Authentication, Authentication and Privacy), and View (checkboxes for Read, Write, Notify, each with a dropdown menu set to 'all').

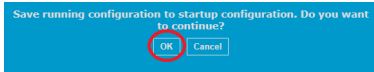
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure the SNMP Community Table

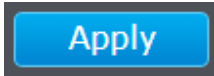
Management > SNMP > Community

A community string has attributes for controlling who can use the string and what the string will allow a network management station to do on the switch. You must first define an SNMP User and Group Name on the SNMP User/Group pages and then define a Community Name on the SNMP Community Table page.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **Community**.
3. Click **Add** to a new SNMP community table. Review the settings.

Item	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode <ul style="list-style-type: none"> • Basic: SNMP community specifies view and access right. • Advanced: SNMP community specifies group.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode <ul style="list-style-type: none"> • Read-Only: Read only. • Read-Write: Read and write.
Group	Specify the SNMP group configured by the command snmp group to define the object available to the community.

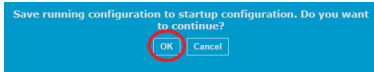
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure the SNMP Users

Management > SNMP > User

An SNMP group must be created first in order to assign SNMP users.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **User**.
3. Click **Add** to a new SNMP user. Review the settings.

Item	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode <ul style="list-style-type: none"> • No Security : Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed. • Authentication and Privacy: Specify that no packet
Authentication	

Method	<p>Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy.</p> <ul style="list-style-type: none"> • None: No authentication required. • MD5: Specify the HMAC-MD5-96 authentication protocol. • SHA: Specify the HMAC-SHA-96 authentication protocol.
Password	The authentication password, The number of character range is 8 to 32 characters.
Privacy	
Method	<p>Encryption Protocol</p> <ul style="list-style-type: none"> • None: No privacy required. • DES: DES algorithm
Password	The privacy password, The number of character range is 8 to 64 characters.

User Table

Showing **All** entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy
0 results found.					

[First](#) [Previous](#)

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

[Add](#) [Edit](#) [Delete](#)

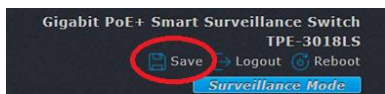
Add User

User	<input type="text"/>
Group	SNMPGROUP1 ▼
Security Level	<input type="radio"/> No Security <input type="radio"/> Authentication <input checked="" type="radio"/> Authentication and Privacy
Authentication	
Method	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Password	<input type="text"/>
Privacy	
Method	<input type="radio"/> None <input checked="" type="radio"/> DES
Password	<input type="text"/>

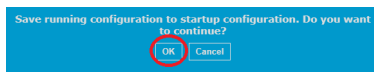
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Set the SNMP Engine ID

Management > SNMP > Engine ID

The SNMP Engine ID screen allows network managers to define the SNMP Engine ID or to assign the default Engine ID to SNMP.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **User**.
3. Review the settings.

Local Engine ID	
Item	Description
Engine ID	<p>If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID.</p> <p>The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.</p>

Local Engine ID

User Defined

Engine ID (10 - 64 Hexadecimal Characters)

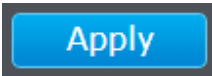
Apply

Item	Description
Address	Remote host address type for Hostname/IPv4/IPv6.
Server Address	Remote host.
Engine ID	Specify Remote SNMP engine ID. The engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

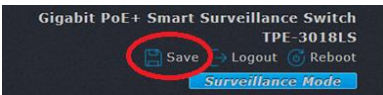
Add Remote Engine ID

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Engine ID	<input type="text"/> (10 - 64 Hexadecimal Characters)

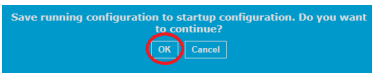
4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration.



6. Click **OK**.



Configure the SNMP Trap Management

Management > SNMP > Trap Management

A Host IP address is used to specify a management device that needs to receive SNMP traps sent by the switch. This IP address is associated with the SNMP Version and a valid Community Name in the Host table of the switch.

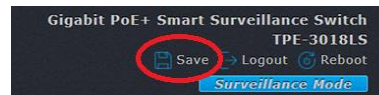
1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **Trap Event**.
3. Review the settings.

Item	Description
Authentication Failure	SNMP authentication failure trap, when community not match or user authentication password not match.
Link Up/Down	Port link up or down trap.
Cold Start	Device reboot configure by user trap.
Warm Start	Device reboot by power down trap.

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.



Configure the SNMP Notification

Management > SNMP > Trap Management

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **SNMP**, and click on **Notification**.
3. Review the settings.

Item	Description
Address Type	Notify recipients host address type.
Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP notification version <ul style="list-style-type: none"> • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type <ul style="list-style-type: none"> • Trap: Send SNMP traps to the host. • Inform: Send SNMP informs to the host.(version 1 have no inform)
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community

Security Level	SNMP notification packet security level, the security level must less than or equal to the community/user name <ul style="list-style-type: none"> • No Security: Specify that no packet authentication is performed. • Authentication: Specify that no packet authentication without encryption is performed.
Server Port	Recipients server UDP port number, if "use default" checked the value is 162, else user configure.
Timeout	Specify the SNMP informs timeout, if "use default" checked the value is 15, else user configure.
Retry	Specify the SNMP informs retry count, if "use default" checked the value is 3, else user configure.

Notification Table

Showing All entries Showing 0 to 0 of 0 entries Q

■	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

For SNMPv1,2 Notification, **SNMP Community** needs to be defined.
For SNMPv3 Notification, **SNMP User** must be created.

First
Previous
1
Next
Last

Add
Edit
Delete

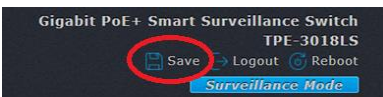
Add Notification

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Version	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
Type	<input checked="" type="radio"/> Trap <input type="radio"/> Inform
Community / User	sec_private ▾
Security Level	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
Server Port	<input checked="" type="checkbox"/> Use Default <input type="text" value="162"/> (1 - 65535, default 162)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="15"/> Sec (1 - 300, default 15)
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 255, default 3)

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.



RMON

The RMON (Remote MONitoring) MIB is used with SNMP applications to monitor the operations of network devices. The Switch supports the four RMON MIB groups listed here:

- **Statistic** group— This group is used to view port statistics remotely with SNMP programs.
- **History** group— This group is used to collect histories of port statistics to identify traffic trends or patterns.
- **Event** group— This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed.
- **Alarm** group— This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded.

You can use your SNMP Network Management System (NMS) software and the RMON section of the MIB tree to view the RMON statistics, history and alarms associated with specific ports. Since RMON uses the SNMP agent for communicating with your NMS software, the SNMP Agent must be enabled and the SNMP feature must be configured on your switch. Since RMON works in conjunction with the SNMP agent, the SNMP agent must be enabled for the RMON feature to be active.

View RMON Statistics

Management > RMON > Statistic

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **RMON**, and click on **Statistic**.
3. Review the settings.

Item	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.

Drop Events	Number of packets that were dropped.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packets	Number of undersized packets (less than 64 octets) received.
Oversize Packets	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	<p>Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: ☐</p> <ul style="list-style-type: none"> • Packet data length is greater than MRU. • Packet has an invalid CRC. • RX error event has not been detected.
Colisions	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.

Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127	Number of frames, containing 65 to 127 bytes that were received.
Frames of 128 to 225	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1023	Number of frames, containing 512 to 1023 bytes that were received.
Frames Greater	Number of frames, containing 1024 to 1518 bytes that were received.
Clear	Clear the statistics for the selected ports.
View	View the statistics on the specified port.

Configure RMON History Table

Management > RMON > History

1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Management**, click on **RMON**, and click on **History**.
3. Click "Add/Edit" button to Add/Edit the History menu. Review the settings.

Item	Description
Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).

History Table

Showing All entries Showing 0 to 0 of 0 entries

Entry	Port	Interval	Owner	Sample	
				Maximum	Current
0 results found.					

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Buttons: Add Edit Delete View

Add History

Entry: 1

Port: GE1

Max Sample: 50 (1 - 50, default 50)

Interval: 1800 (1 - 3600, default 1800)

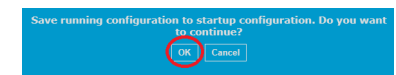
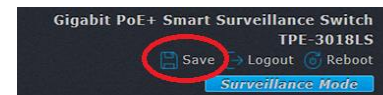
Owner:

Buttons: Apply Close

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.



Configure RMON Event Table

Management > RMON > Event

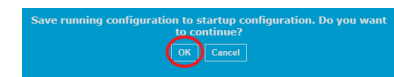
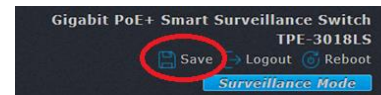
1. Log into your switch management page (see “[Access your switch management page](#)” on page 11).
2. Click on **Management**, click on **RMON**, and click on **Event**.
3. Click "Add/Edit" button to Add/Edit an event. Review the settings.

Item	Description
Notification	<p>Specify the notification type for the event, and the possible value are: ?</p> <ul style="list-style-type: none"> • None: Nothing for notification. ? • Event Log: Logging the event in the RMON Event Log table • Trap: Send a SNMP trap. ?
Community	Specify the SNMP community when the notification type is specified as “Trap” pr “Event Log and Trap”
Description	Specify the description for the event.
Owner	Specify owner for the event.

4. Click **Apply**.






5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.










Configure RMON Alarm Table

Management > RMON > Alarm

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management**, click on **RMON**, and click on **Alarm**.
3. Click "Add/Edit" button to Add/Edit an alarm. Review the settings.

Item	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling  <ul style="list-style-type: none"> • Drop Event: Total number of events received in which the packets were dropped.  • Received Bytes (Octets): Octets. • Received Packets: Number of packets. • Broadcast Packets Received: Broadcast packets. • Multicast Packets Received: Multicast packets. • CRC and Align Error: CRC alignment error. 

	<ul style="list-style-type: none"> • Oversize Packets: Number of oversized packets. • Fragments: Total number of packet fragment. • Jabbers: Total number of packet jabber.  • Collisions: Collision.  • Frames of 64 Bytes: Number of packets size 64 octets. • Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets.  • Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets.  • Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets.  • Frames of 512 to 1023 Bytes: Number of packets
Sampling	Specify the sampling type.  <ul style="list-style-type: none"> • Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval.  • Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.
RISING	

Threshold	Specify the threshold for firing rising event.
Event	Specify the index of rising event when alarm was fired.
Falling	
Threshold	Specify the threshold for firing falling event.
Event	Specify the index of falling event when alarm was fired.

Alarm Table

Showing All entries Showing 0 to 0 of 0 entries

Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling
		Name	Value					Threshold	Event	Threshold
0 results found.										

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

First Previous 1 Next

Add Edit Delete

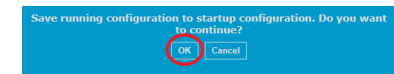
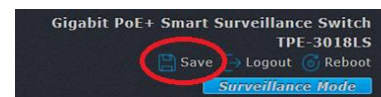
Add Alarm

Entry	1
Port	GE1
Counter	Drop Events
Sampling	<input checked="" type="radio"/> Absolute <input type="radio"/> Delta
Interval	100 Sec (1 - 2147483647, default 100)
Owner	
Trigger	<input checked="" type="radio"/> Rising <input type="radio"/> Falling <input type="radio"/> Rising and Falling
Rising	
Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description
Falling	
Threshold	20 (0 - 2147483647, default 20)
Event	1 - Default Description

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.



Create Schedules

Management > Time Range

Create schedules to be used in applicable switch features such as PoE.

1. Log into your switch management page (see "[Access your switch management page](#)" on page 11).
2. Click on **Management** and click on **Time Range**.
3. Click "Add/Edit" button to Add/Edit a schedule. Review the settings.

Item	Description
Range Name	Input Time Range name.
Date	Select a valid time for this schedule.

Time Range

■	Range Name	Days	Start Time	End Time
0 results found.				
<div style="display: flex; justify-content: space-around; margin-top: 5px;"> Add Edit Delete </div>				

Time Range Add

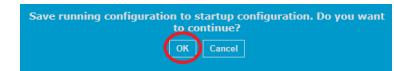
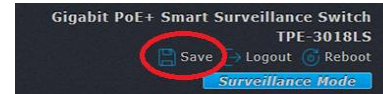
Range Name	<input style="width: 90%; border: none; border-bottom: 1px solid #ccc;" type="text" value="Name_Default"/>
Date	<div style="display: flex; align-items: center; gap: 5px;"> <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun </div> <div style="display: flex; align-items: center; gap: 10px; margin-top: 5px;"> From <input style="width: 50px; border: none; border-bottom: 1px solid #ccc;" type="text" value="01:00"/> to <input style="width: 50px; border: none; border-bottom: 1px solid #ccc;" type="text" value="23:00"/> </div>

Apply
Close

4. Click **Apply**.



5. In the top right, click **Save** to save the configuration settings to NV-RAM/startup configuration. Click **OK**.



Technical Specifications

TPE-3012LS

Standards

- IEEE 802.1d
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3z
- IEEE 802.3ab
- IEEE 802.3ad
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3az

Device Interface

- 8 x Gigabit PoE+ ports
- 2 x Gigabit ports
- 2 x 100/1000Mbps SFP slots
- LED indicators
- 4-Digit PoE LED display (total power budget, available power, consumption per port)

Data Transfer Rate

- Ethernet: 10Mbps (half duplex), 20Mbps (full duplex)
- Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex)
- Gigabit Ethernet: 2000Mbps (full duplex)

Performance

- Switch fabric: 24Gbps
- RAM buffer: 512KB
- MAC address table: 8K entries
- Jumbo frames: 10KB
- Forwarding mode: store and forward
- Forwarding rate: 17.8Mpps (64-byte packet size)

Management

- HTTP / HTTPS web-based GUI – Standard or Surveillance Mode
- CLI command line interface (Telnet / SSHv2)
- SNMP v1, v2c, v3
- IPv4/IPv6 support
- Multiple user accounts
- Dynamic/static unicast MAC address table
- Enable or disable 802.3az power saving per port
- Syslog
- System message logging severity levels
- Port mirroring (transmit, receive, one-to-one, many-to-one)
- ICMPv4/ICMPv6
- Traceroute
- LLDP
- Cable diagnostics test
- SFP DDM (Digital-diagnostic-monitoring)
- UDLD (UniDirectional Link Detection)
- Port error disabled/Errdisable state
- Ping watchdog

MIB

- RMON MIB RFC 1271
- IPV4 MIB RFC 1213 (read only)
- SNMP MIB RFC 3415

Spanning Tree

- STP (spanning tree)
- RSTP (rapid spanning tree)
- MSTP (multiple spanning tree)

Link Aggregation

- Static link aggregation and dynamic LACP (Up to 8 groups)

Quality of Service (QoS)

- 802.1p Class of Service (CoS)
- DSCP (Differentiated Services Code Point)
- Bandwidth limit per port
- Queue Scheduling: strict priority (SP), weighted round robin (WRR)

VLAN

- Multiple management VLAN assignment
- 802.1Q Tagged VLAN
- MAC-based VLAN
- Surveillance VLAN
- Voice VLAN
- Up to 256 VLAN groups, ID Range 1-4094

Multicast

- IGMP Snooping v2/v3
- IGMP immediate/fast leave
- IGMP querier
- Dynamic/static multicast MAC address table
- MVR (Multicast VLAN registration)
- Up to 1K multicast entries

Access Control

- 802.1X port-based authentication (Local user database, RADIUS, Guest VLAN)
- DHCP Snooping / Option 82
- Loopback detection
- Denial of Service (DoS) prevention

- Storm control (broadcast, unknown multicast, unknown unicast, min: 16Kbps)
- Head-of-line (HoL) blocking prevention
- IP Source Guard / IP-MAC-Port-VLAN binding
- Protected ports
- Port Security/MAC address learning restriction (Up to 255 entries)

Access Control List (ACL)

- MAC Address (VLAN ID, EtherType, 802.1p)
- IPv4 (IP Protocol, TCP/UDP Port, 802.1p, DSCP, TCP flag, ICMP type, ICMP code)

Surveillance Mode (ONVIF)

- Surveillance mode GUI for simplified configuration and network monitoring
- Device discovery for ONVIF compliant devices such as IP cameras and NVRs
- Upload floor plans to create a visual overview of the network
- Change camera IP address configuration
- Upgrade IP camera firmware
- Change IP camera administrator user name and password

PoE

- PoE budget: 110W
- 802.3at: up to 30W per port (ports 1-8)
- PoE Mode A: Pins 1,2 f and pins 3,6 for power
- PoE power scheduling
- PD alive check
- Over current/short circuit protection

Power

- Input: 100 – 240V AC, 50/60Hz, internal power supply
- Max. consumption: 10W (No PoE load)

Surge

Protection

- 6kV (Ports 9 & 10)

Fan/Acoustics

- Fanless

MTBF

- 434,157 hours

Operating Temperature

- 0° – 40° C (32° – 104° F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 330 x 230 x 44.45mm (12.9 x 9.1 x 1.75 in.)
- 1U rack mountable

Weight

- 2.26kg (4.98 lbs.)

Certifications

- CE
- FCC
- ETL

TPE-3018LS**Standards**

- IEEE 802.1d
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3z
- IEEE 802.3ab
- IEEE 802.3ad
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3az

Device Interface

- 16 x Gigabit PoE+ ports
- 2 x Shared Gigabit ports (RJ-45 or SFP (100/1000Mbps))
- LED indicators
- PoE power status LED display (total power budget, available power, consumption per port)

Data Transfer Rate

- Ethernet: 10Mbps (half duplex), 20Mbps (full duplex)
- Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex)
- Gigabit Ethernet: 2000Mbps (full duplex)

Performance

- Switch fabric: 36Gbps
- RAM buffer: 512KB
- MAC address table: 8K entries
- Jumbo Frames: 10KB
- Forwarding mode: store and forward
- Forwarding rate: 26.7Mpps (64-byte packet size)

Management

- HTTP / HTTPS web-based GUI – Standard or Surveillance Mode
- CLI command line interface (Telnet / SSHv2)
- SNMP v1, v2c, v3
- IPv4/IPv6 support
- Multiple administrator or user accounts
- Dynamic/static unicast MAC address table
- Enable or disable 802.3az power saving per port
- Syslog
- System message logging severity levels
- Port mirroring (transmit, receive, one-to-one, many-to-one)
- ICMPv4/ICMPv6
- Traceroute
- LLDP
- Cable diagnostics test
- SFP DDM (Digital-diagnostic-monitoring)
- UDLD (UniDirectional Link Detection)
- Port error disabled/Errdisable state
- Ping watchdog

MIB

- RMON MIB RFC 1271
- IPV4 MIB RFC 1213 (read only)
- SNMP MIB RFC 3415

Spanning Tree

- STP (spanning tree)

- RSTP (rapid spanning tree)
- MSTP (multiple spanning tree)

Link Aggregation

- Static link aggregation and dynamic LACP (Up to 8 groups)

Quality of Service (QoS)

- 802.1p Class of Service (CoS)
- DSCP (Differentiated Services Code Point)
- Bandwidth limit per port
- Queue Scheduling: strict priority (SP), weighted round robin (WRR)

VLAN

- Multiple management VLAN assignment
- 802.1Q Tagged VLAN
- MAC-based VLAN
- Surveillance VLAN
- Voice VLAN
- Up to 256 VLAN groups, ID Range 1-4094

Multicast

- IGMP Snooping v2/v3
- IGMP immediate/fast leave
- IGMP querier
- Dynamic/static multicast MAC address table
- MVR (Multicast VLAN registration)
- Up to 1K multicast entries

Access Control

- 802.1X port-based authentication (Local user database, RADIUS, Guest VLAN)
- DHCP Snooping / Option 82
- Loopback detection
- Denial of Service (DoS) prevention
- Storm control (broadcast, unknown multicast, unknown unicast, min: 16Kbps)
- Head-of-line (HoL) blocking prevention

- IP Source Guard / IP-MAC-Port-VLAN binding
- Protected ports
- Port Security/MAC address learning restriction

Access Control List (ACL)

- MAC Address (VLAN ID, EtherType, 802.1p)
- IPv4 (IP Protocol, TCP/UDP Port, 802.1p, DSCP, TCP flag, ICMP type, ICMP code)

Surveillance Mode (ONVIF)

- Surveillance mode GUI for simplified configuration and network monitoring
- Device discovery for ONVIF compliant devices such as IP cameras or NVRs
- Upload virtual maps
- Change IP camera IP address settings
- Upgrade IP camera firmware
- Change IP camera administrator user name and password

PoE

- PoE budget: 220W
- 802.3at: up to 30W per port (ports 1-16)
- PoE Mode A: Pins 1,2 and pins 3,6 for power
- PoE power scheduling
- PD alive check
- Over current/short circuit protection

Power

- Input: 100 – 240V AC, 50 – 60Hz, internal power supply
- Max. consumption: 14W (No PoE load)

Protection

- 6kV (Ports 17 & 18)

Fan/Acoustics

- Quantity: 1 (Hot swappable)
- Noise Level: 60.1 dBA (max.)

MTBF

- 331,516 hours

Operating Temperature

- 0 – 40°C (32 – 104°F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 440 x 195 x 44.45mm (17.3 x 9.8 x 1.74 in.)
- Rack mountable 1U height

Weight

- 2.93kg (6.45 lbs.)

Certifications

- CE
- FCC
- ETL

Troubleshooting

Q: I typed <http://192.168.10.200> in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the switch management page?

Answer:

1. Check your hardware settings again. See "[Switch Installation](#)" on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to Use the following IP address or Static IP(see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8/8.1

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: I changed the IP address of the switch, but I forgot it. How do I reset my switch?

Answer:

Using a paper clip, push and hold the reset button on the front of the switch and release after 15 seconds.

The default IP address of the switch is 192.168.10.200. The default user name and password is "admin".

Appendix

How to find your IP address?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Command Prompt Method

Windows 2000/XP/Vista/7/8/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type **cmd** to bring up the command prompt.
3. In the command prompt, type **ipconfig /all** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type **ipconfig getifaddr <en0 or en1>** to display the wired or wireless IP address settings.

Note: **en0** is typically the wired Ethernet and **en1** is typically the wireless Airport interface.

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

How to configure your network settings to use a static IP address?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Windows 7/8/8.1/10

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Ethernet connection.

In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.

In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use a static IP.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply Now** button.

In MAC 10.5/10.6, from the **Configure** drop-down list, select **Manually** and assign your network adapter a static IP address . Then click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7/8/8.1,

Your computer MAC addresses are also displayed in this window, however, you can type **getmac -v** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

- EN 62368-1: 2014 + A1: 2017
- EN 55032:2015+AC:2016
- EN 55035:2017
- EN 61000-3-2:2014 Class A
- EN 61000-3-3:2013
- EN 61000-4-2:2009
- EN 61000-4-3:2006+A1:2008+A2:2010
- EN 61000-4-4:2012
- EN 61000-4-5:2014+A1:2017
- EN 61000-4-6:2014
- EN 61000-4-8:2010
- EN 61000-4-11:2004+A1:2017

Directives:

EMC Directive 2014/30/EU

RoHS Directive (EU)2015/863

WEEE Directive 2012/19/EU

REACH Regulation (EC) No. 1907/2006

Low Voltage Directive 2014/35/EU



CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use, or (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. International customers

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN

CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit <http://www.trendnet.com/gpl> or the support section on <http://www.trendnet.com> and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

PWP07172015v3

2020/11/12



Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA