

Moxa's Managed Switch TSN-G5000 Series User's Manual

Version 1.0, June 2020



© 2020 Moxa Inc. All rights reserved.

Moxa's Managed Switch TSN-G5000 Series User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2020 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. About This Manual	1-1
Symbols for the Meanings in the Web Interface Configurations.....	1-2
About Note, Attention, and Warning.....	1-3
Configuration Reminders	1-4
A: About Mandatory Parameters.....	1-4
B: Configurations before Enable/Disable.....	1-4
2. Getting Started	2-1
Log in by Web Interface	2-2
Connecting to the Switch.....	2-3
Log in by RS-232 Console.....	2-4
Log in by Telnet.....	2-7
3. Web Interface Configuration	3-1
Function Introduction	3-2
Device Summary	3-3
Model Information	3-4
Panel Status	3-4
Event Summary (Last 3 Days)	3-5
CPU Utilization History	3-6
Top 5 Interface Error Packet	3-7
Top 5 Interface Utilization	3-7
System.....	3-8
System Management	3-8
Account Management.....	3-17
Network	3-22
Time.....	3-30
Port	3-36
Port Interface	3-36
Layer 2 Switching	3-39
VLAN	3-39
MAC	3-46
Multicast	3-48
Network Redundancy	3-49
Layer 2 Redundancy	3-50
Management.....	3-58
Network Management.....	3-58
Security.....	3-64
Device Security.....	3-64
Network Security.....	3-70
Authentication	3-72
Login Authentication	3-73
Diagnostics	3-76
System Status	3-77
Event Notification	3-81
Diagnosis	3-88
Maintenance and Tool	3-93
Standard/Advanced Mode.....	3-93
Disable Auto Save	3-94
Locator	3-95
Reboot.....	3-96
Reset to Default.....	3-97
Log Out of the Switch	3-97
A. Account Privileges List	A-1
Account Privileges List.....	A-2
B. Event Log Description	B-1
Event Log Description	B-2
C. SNMP MIB File	C-1
Standard MIB Installation Order	C-2
MIB Tree	C-3

About This Manual

Thank you for purchasing Moxa's managed switch. Read this user's manual to learn how to connect your Moxa switch with various interfaces and how to configure all settings and parameters via the user-friendly web interface.

Three methods can be used to connect to the Moxa's switch, which all will be described in the next two chapters. See the following descriptions for each chapter's main functions.

Chapter 2: Getting Started

In this chapter, we explain the instruction on how to initialize the configuration on Moxa's switch. We provide three interfaces to access the configuration settings: RS-232 console interface, telnet interface, and web interface.

Chapter 3: Web Interface Configuration

In this chapter, we explain how to access a Moxa switch's various configuration, monitoring, and management functions. The functions can be accessed by web browser. We describe how to configure the switch functions via web interface, which provides the most user-friendly way to configure a Moxa switch.

Appendix A: Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switch.

Appendix B: Event Log Description
























In this appendix, users can check the event log name and its event log description. When any event occurs, this appendix helps users quickly check the detailed definition for each event.

Appendix C: SNMP MIB File

This appendix contains the SNMP MIB files so that users can manage the entities in a network with Moxa's switch.

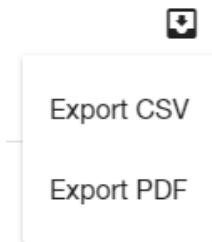
Symbols for the Meanings in the Web Interface Configurations

The Web Interface Configuration includes various symbols. For your convenience, refer to the following table for the meanings of the symbols.

Symbols	Meanings
	Add
	Read detailed information
	Clear all
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configurations.
	Export*
	Edit
	Re-authentication
	Delete
	Panel View
	Expand
	Collapse
	Hint Information
	Settings
	Data Comparison
	Menu icon
	Change mode
	Locator
	Reboot
	Reset to default
	Logout
	Increase

Symbols	Meanings
↓	Decrease
↕	Equal
☰	Menu
🔍	Search

*The **Export** function helps users save the current configurations or information for the specific functions. It is located on the upper part of the configuration area. There are two formats available: **CSV**, or **PDF**. Select the format and save in your local computer.




About Note, Attention, and Warning

Throughout the whole manual, users will see some notes, attentions, and warnings. Here are the explanations for each definition.


Note: It indicates the additional explanations for the situation that users might encounter. Here is the example:

NOTE By default, the password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help keep your system secure.

Attention: It indicates the situations where users might take some extra care or it might bring some problems. Here is the example:

 **ATTENTION** When a different type of module has been inserted into the switch, we suggest you configure the settings, or use reset-to-default.

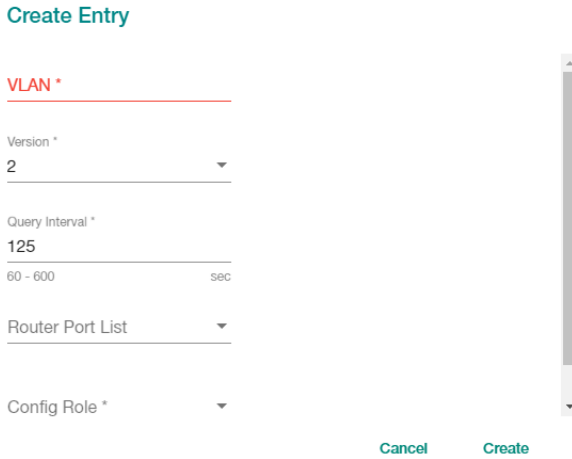
Warning: It indicates the situations where users need to pay particular attention to, or it might bring serious damage to the system or the switch. Here is an example:

 **WARNING** There is a risk of explosion if the battery is replaced by an incorrect type.

Configuration Reminders

In this section, several examples will be used to remind users when configuring the settings for Moxa's switch.

A: About Mandatory Parameters

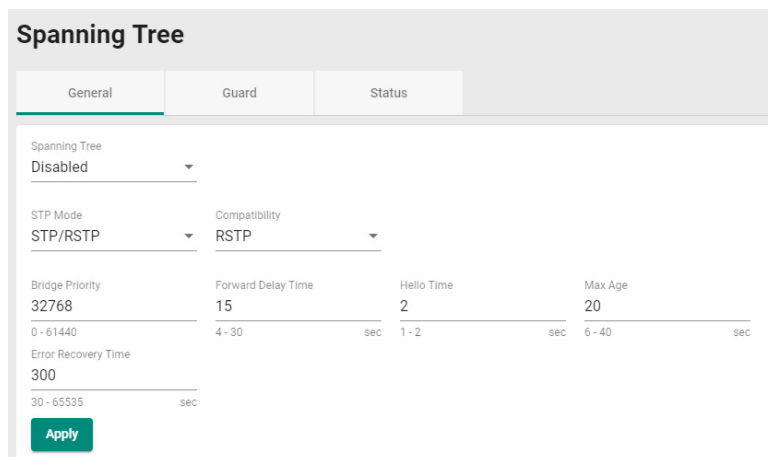


1. The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for VLAN, Version, and Query Interval all need to be provided, or it will not be created or applied.
2. If the item is marked with red it means this item has been skipped. You need to fill in the parameters or you cannot apply or create the function.

In addition, some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.

B: Configurations before Enable/Disable

In another situation, some settings can be configured first, but remain disabled. Users can decide to enable them when necessary without configuring the same settings again. This is particularly convenient and user-friendly when configuring various settings. For example, in Spanning Tree configuration page, users can configure the Guard settings first, but later select to disable the Guard settings in the **General** tab. When users decide to enable the Guard settings, they only need to select **Enable** in General settings, so that the Guard setting can be enabled at the same time.



Getting Started

In this chapter, we explain how to log in a Moxa's switch for the first time. There are three ways to access the Moxa switch's configuration settings: RS-232 console, or web-based interface.

The following topics are covered in this chapter:

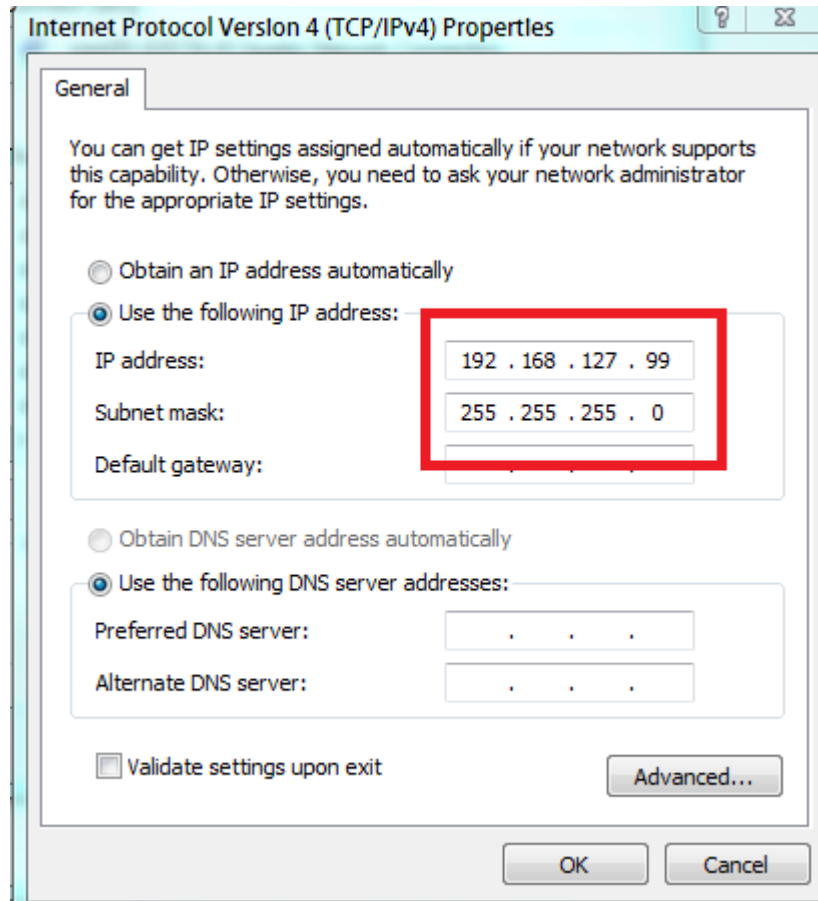
- ❑ **Log in by Web Interface**
 - Connecting to the Switch
- ❑ **Log in by RS-232 Console**
- ❑ **Log in by Telnet**

Log in by Web Interface

You can directly connect Moxa's switch to your computer with a standard network cable or install your computer at the same intranet as your switch. Then you need to configure your computer's network setting. The default IP address for the Moxa's switch is:

192.168.127.253

For example, you can configure the computer's IP setting as **192.168.127.99**, and the subnet mask as 255.255.255.0.



Click **OK** when finished.

Connecting to the Switch

Open a browser, such as Google Chrome, Internet Explorer 11, or Firefox, and connect to the following IP address:

http://192.168.127.253



The default username and password are:

Username: **admin**

Password: **moxa**

Click **Login** to continue. If you have logged in before, you will see a screen indicating the previous login information. Click **Close**.

System Message

Welcome admin

The latest successful login time was: 2018-12-21 23:50:29.

Close

Another system message will appear, reminding you to change the default password. We recommend you change your password, or a message will appear whenever you log in. You can change the password in the **Account Management** section. Click **Close** to continue.

System Message

Please change the default username and password in order to enhance security.

Close

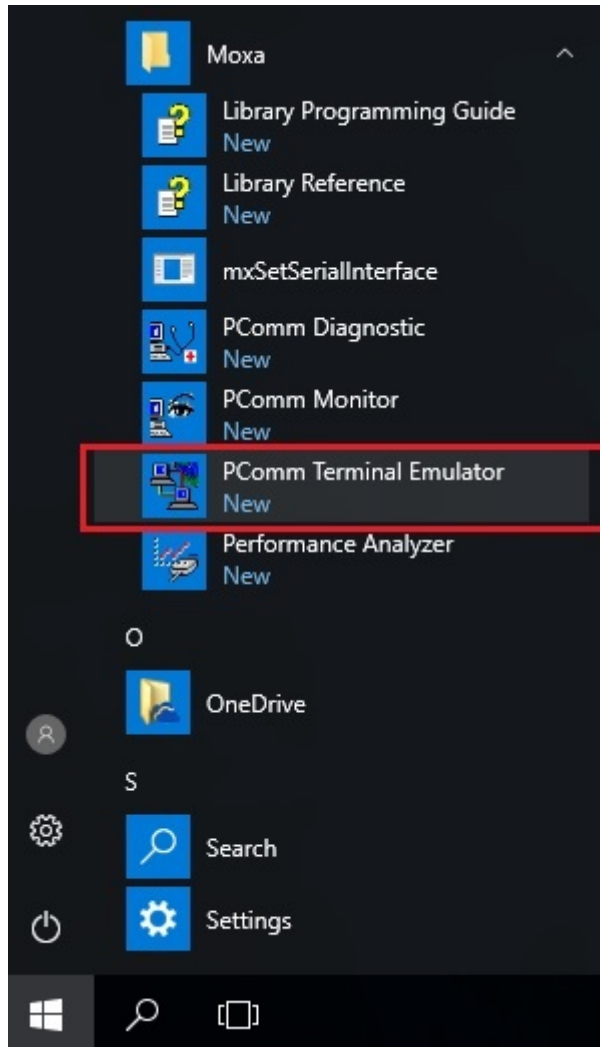
Log in by RS-232 Console

The Moxa's managed switch offers a serial console port, allowing users to connect to the switch and configure the settings. Do the following steps for the serial connection and configuration.

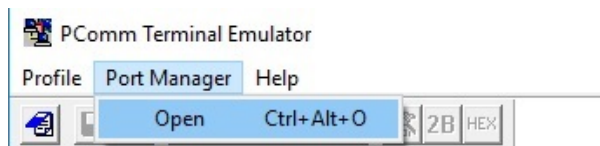
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface end to the console port on the switch, and the other end to the computer.
3. We recommend you use **PComm Terminal Emulator** for serial communication. The software can be downloaded free of charge from Moxa's website.

After installing PComm Terminal Emulator, open the Moxa switch's console as follows:

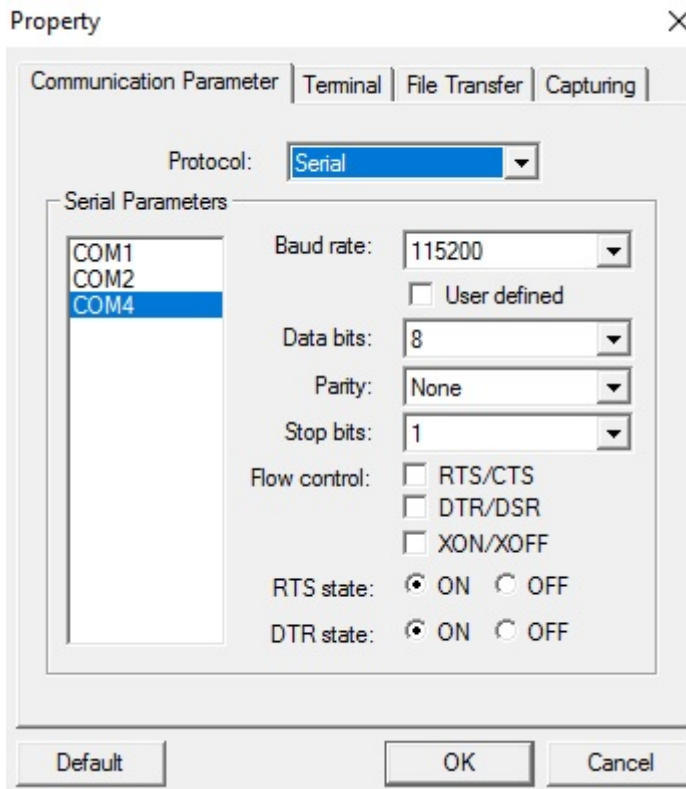
1. From the Windows desktop, click **Start → Moxa → PComm Terminal Emulator**.



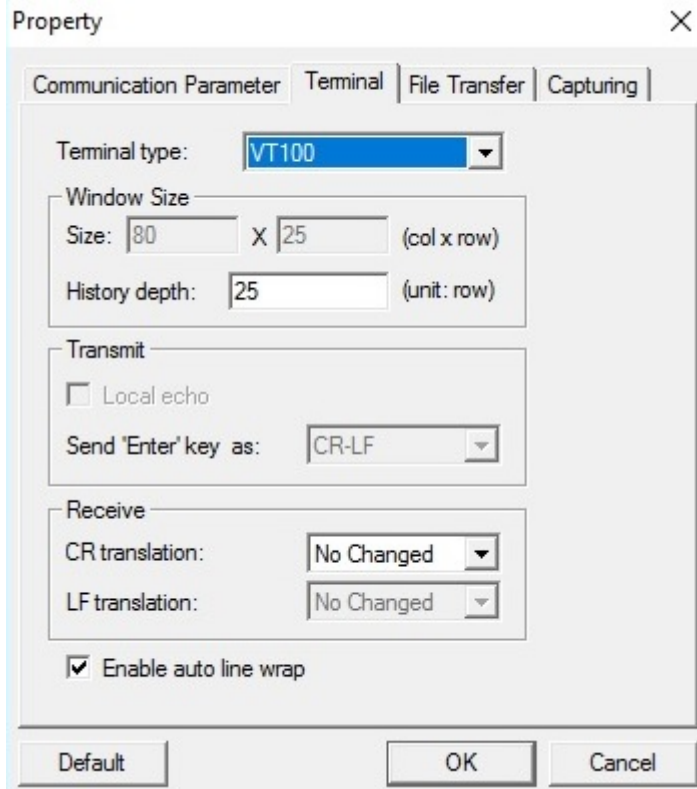
2. Select **Open** under the **Port Manager** menu to open a new connection.



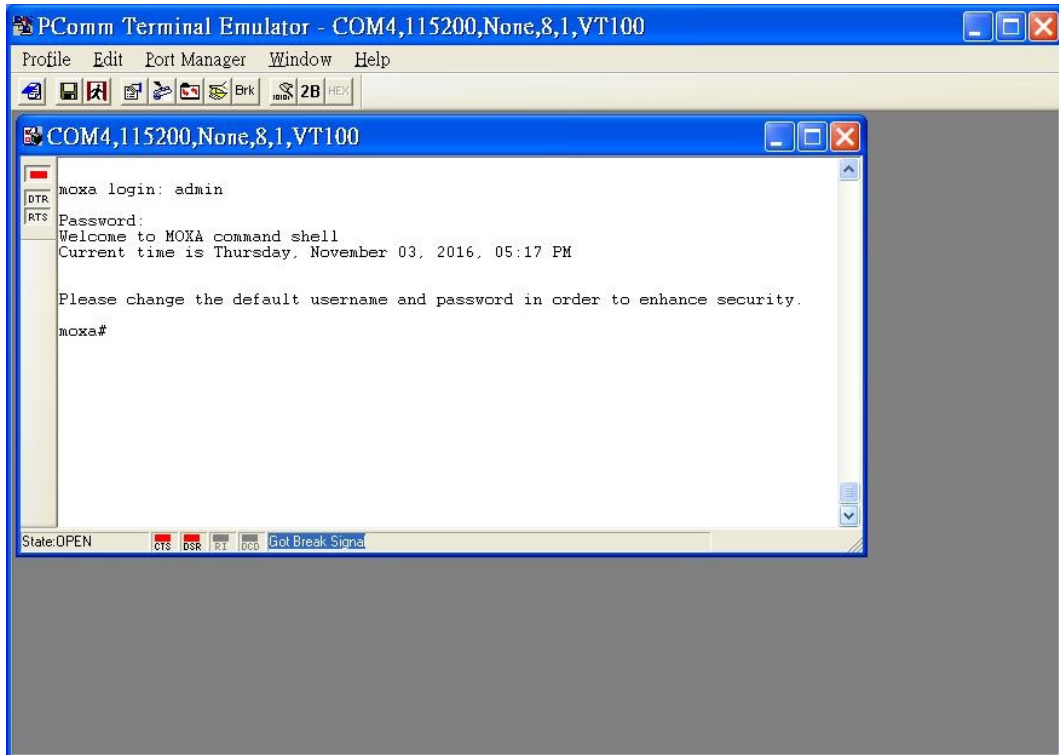
3. The **Property** window should open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



4. On the **Terminal** tab, select **VT100** for **Terminal Type**, and then click **OK** to continue.



- The console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



- After successfully connecting to the switch by serial console, users can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.

NOTE By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

Log in by Telnet

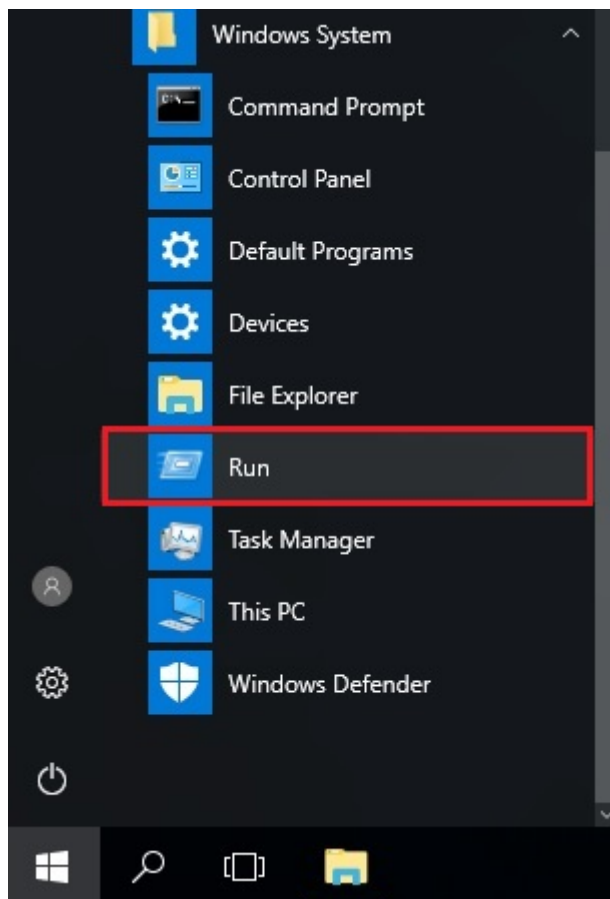
Opening the Moxa switch's Telnet or web console over a network requires that the PC host and Moxa switch are on the same logical subnet. You might need to adjust your PC host's IP address and subnet mask. By default, the Moxa switch's IP address is 192.168.127.253 and the Moxa switch's subnet mask is 255.255.255.0. Your PC's IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.

NOTE When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You can use either a straight-through or cross-over Ethernet cable.

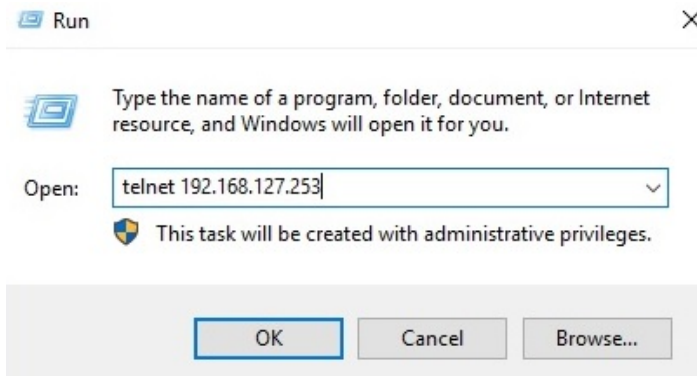
NOTE The Moxa switch's default IP address is 192.168.127.253.

After making sure that the Moxa switch is connected to the same LAN and logical subnet as your PC, open the Moxa switch's Telnet console as follows:

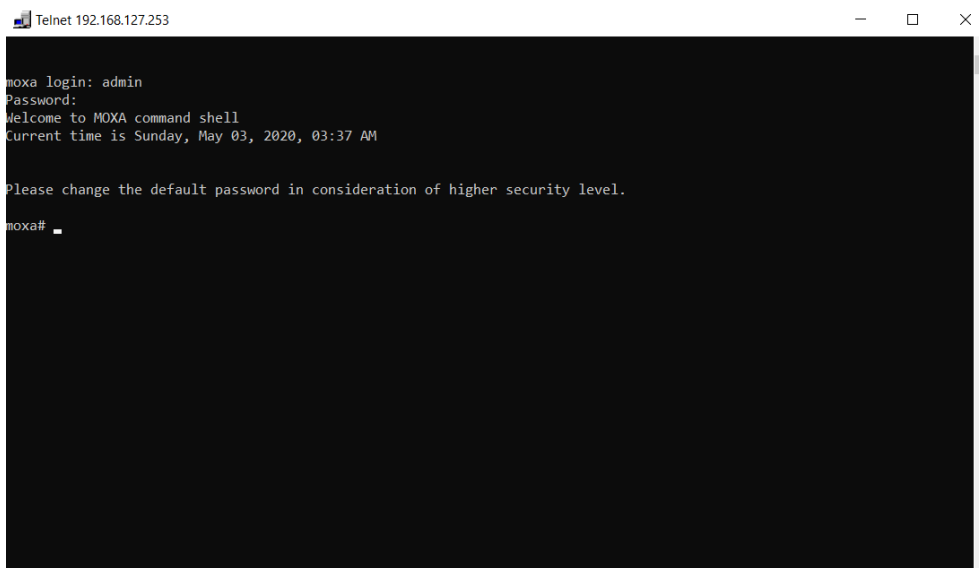
1. Click **Start** → **Run** from the Windows Start menu and then Telnet to the Moxa switch's IP address from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



- Next, use Telnet to connect the Moxa switch's IP address (192.168.127.253) from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



- The Telnet console will prompt you to log in. The default login name is **admin**, and the password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



- After successfully connecting to the switch by Telnet, users can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.

NOTE By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

Web Interface Configuration

Moxa's managed switch offers a user-friendly web interface for easy configurations. Users find it simple to configure various settings over the web interface. All configurations for the Moxa's managed switch can be easily set up and done via this web interface, essentially reducing system maintenance and configuration effort.

The following topics are covered in this chapter:

❑ **Function Introduction**

❑ **Device Summary**

- Model Information
- Panel Status
- Event Summary (Last 3 Days)
- CPU Utilization History
- Top 5 Interface Error Packet
- Top 5 Interface Utilization

❑ **System**

- System Management
- Account Management
- Network
- Time

❑ **Port**

- Port Interface

❑ **Layer 2 Switching**

- VLAN
- MAC
- Multicast

❑ **Network Redundancy**

- Layer 2 Redundancy

❑ **Management**

- Network Management

❑ **Security**

- Device Security
- Network Security
- Authentication
- Login Authentication

❑ **Diagnostics**

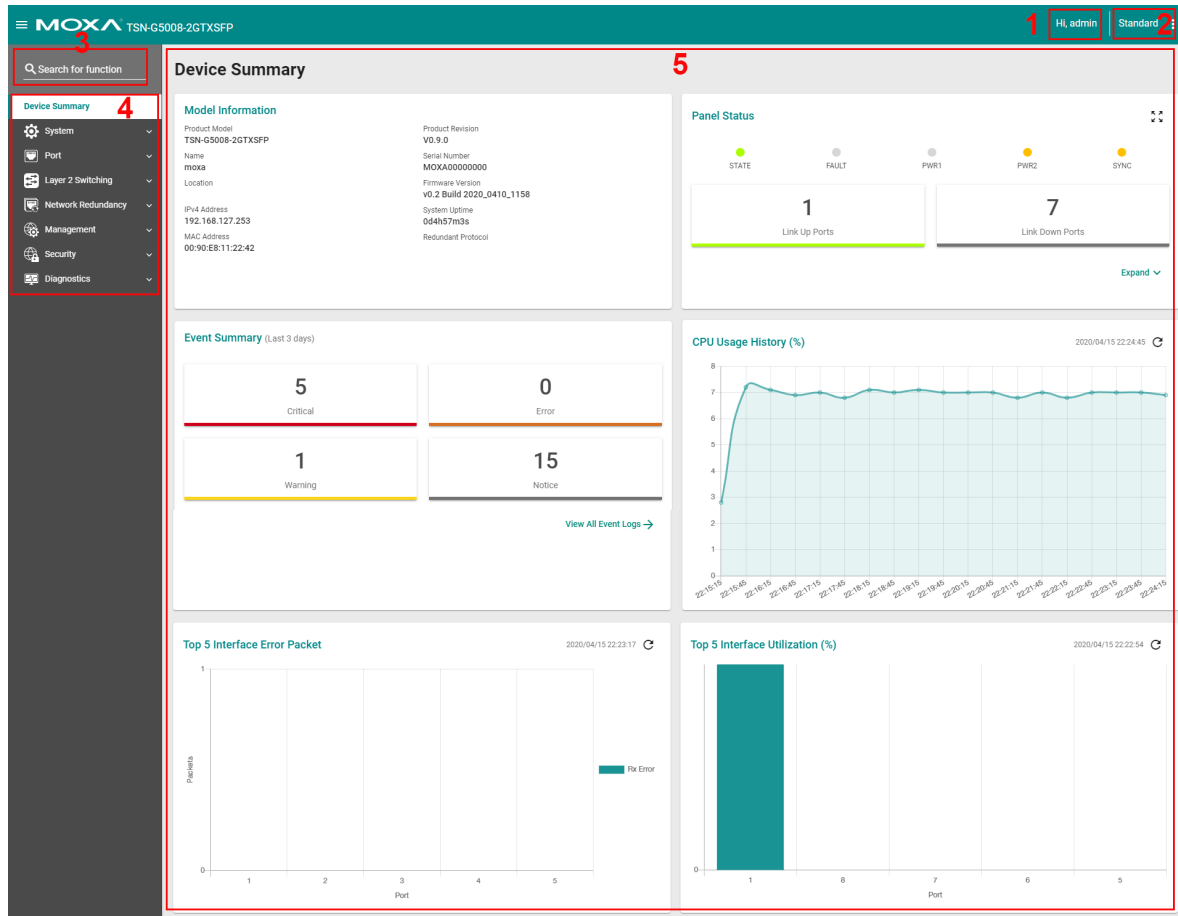
- System Status
- Event Notification
- Diagnosis

❑ **Maintenance and Tool**

- Standard/Advanced Mode
- Disable Auto Save
- Locator
- Reboot
- Reset to Default
- Log Out of the Switch

Function Introduction

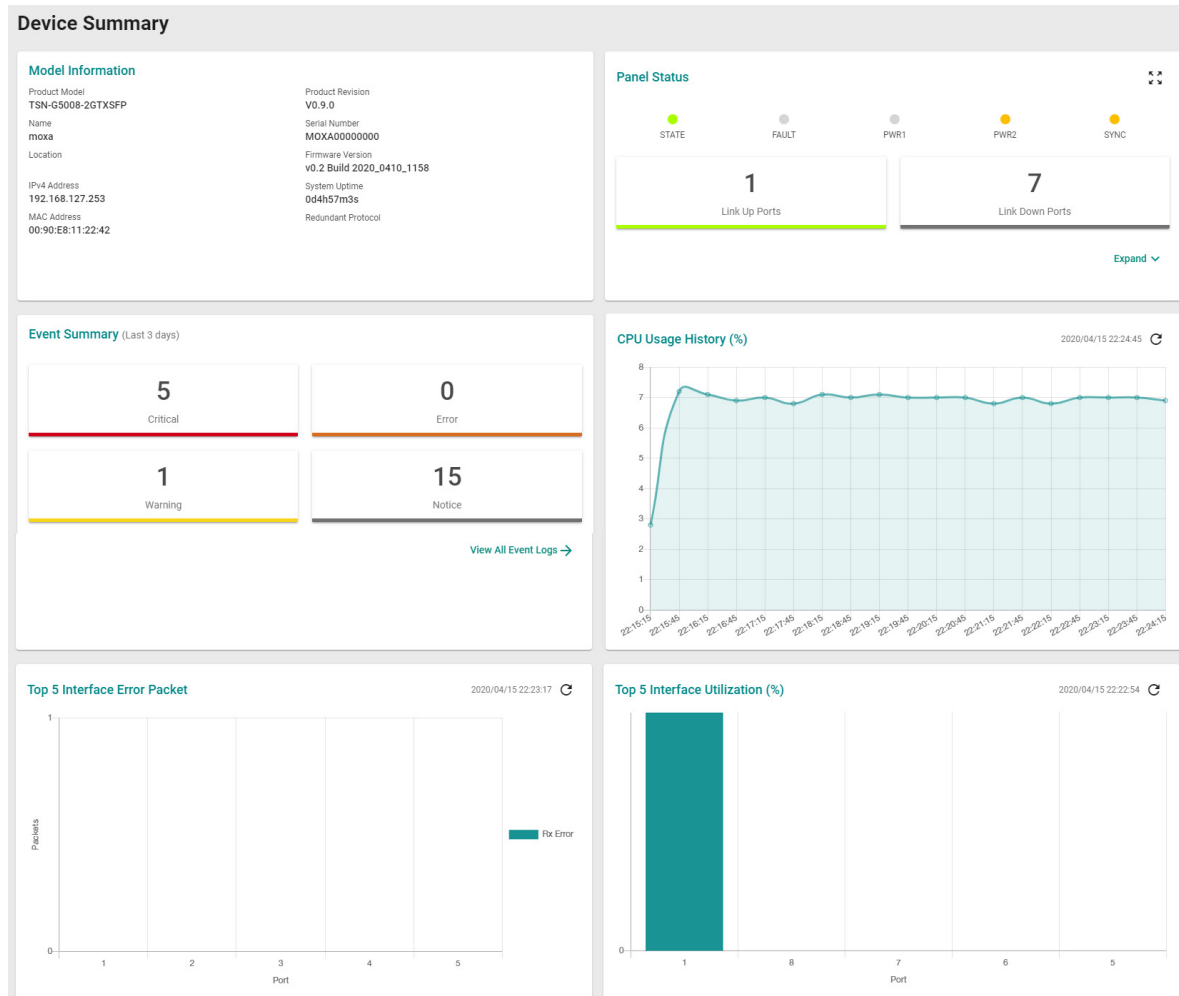
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** It shows the role of the login name.
2. **Configuration Mode:** Two modes can be shown: **Standard Mode** and **Advanced Mode**.
 - **Standard Mode:** Some of the features and parameters will be hidden to make the configurations simpler (default).
 - **Advanced Mode:** More features and parameters will be shown for users to configure detailed settings.
3. **Search Bar:** Type the items you want to search of the function menu tree.
4. **Function Menu:** All functions of the switch are shown here. Click the function you want to view or configure.
5. **Device Summary:** All important device information of the functions will be shown here.

Device Summary

After successfully connecting to the switch, the **Device Summary** will automatically appear. You can view the whole web interface on the screen. If you are in the middle of performing configurations, simply click **Device Summary** on the Function Menu and you can view the detailed information of the switch.



See the following sections for detailed descriptions for the specific items.

Model Information

This shows the model information, including product model name, serial number, firmware version, system uptime, etc.

Model Information

Product Model	TSN-G5008-2GTXSFP	Product Revision	V0.9.0
Name	moxa	Serial Number	MOXA00000000
Location		Firmware Version	v0.2 Build 2020_0410_1158
IPv4 Address	192.168.127.253	System Uptime	0d5h27m3s
MAC Address	00:90:E8:11:22:42	Redundant Protocol	

Panel Status

This section illustrates the panel status. For example, the connecting ports will be shown in green, while the disconnected ports will be shown in gray. Click **Expand** to view more detailed information on the panel status and click **Collapse** to return.


Panel Status 

STATE FAULT PWR1 PWR2 SYNC

1 Link Up Ports 7 Link Down Ports

Expand 


Click **Expand** to view more detailed information on the panel status and click **Collapse** to return.

Panel Status 


STATE FAULT PWR1 PWR2 SYNC

1 Link Up Ports 7 Link Down Ports

1 2 3 4 5 6 7 8

Collapse 

Panel View

By clicking this icon, , users can view the device port status by a graphic figure. Click the close icon on the upper right corner to return to the main page.

The following panel view is TSN-G5008-2GTXSFP. If you purchase the TSN-G5004 Series, it will look different.



Event Summary (Last 3 Days)

This section shows the event summary for the past three days.

Event Summary (Last 3 days)



[View All Event Logs →](#)

Click **View All Event Logs** to go to the Event Log page, where you can view all event logs.

Event Log

Event Log

Threshold Setting

Oversize-Action
 Overwrite the oldest event log ▼

Apply

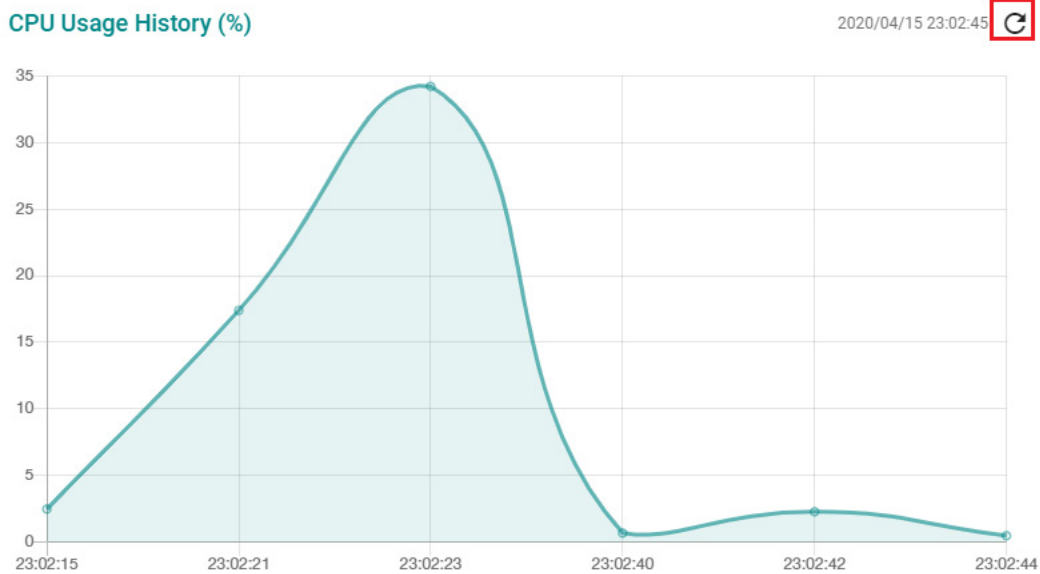
↻
🗑️
📄

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	4	Notice	2018-12-22 00:22:45	0d5h29m18s	[Account.admin] successfully logged in via local.
2	4	Notice	2018-12-21 23:50:29	0d4h57m2s	[Account.admin] successfully logged in via local.
3	4	Notice	2018-12-21 23:48:58	0d4h55m31s	[Account.admin] successfully logged in via local.
4	4	Info	2018-12-21 20:31:14	0d1h37m47s	LLDP Table Changed.

For Event Log settings, refer to **Event Log** under the **Diagnosis** section.

CPU Utilization History


This section shows the CPU usage. The data will be shown as a percentage over time. Click the refresh icon on the page to show the latest information.

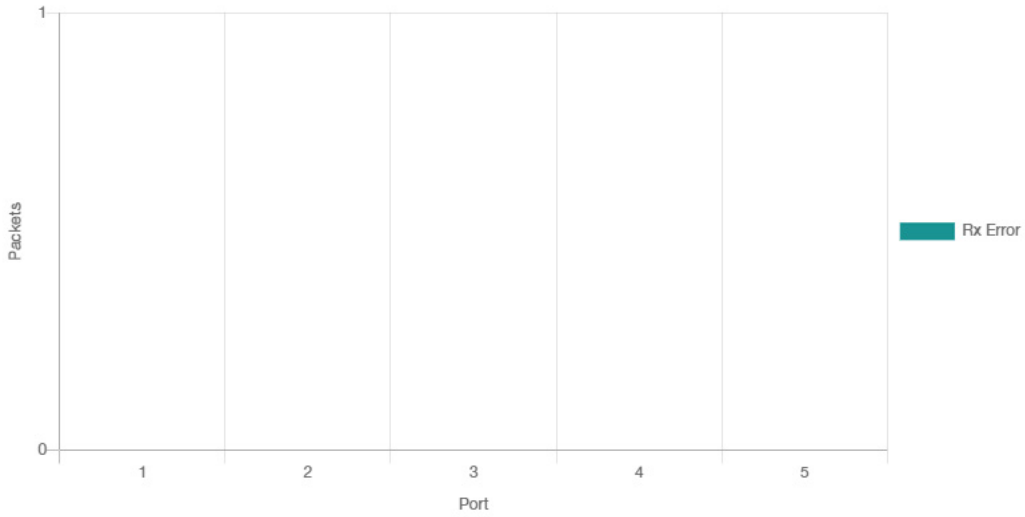


Top 5 Interface Error Packet

If any error packets occur, top 5 error packets will be shown here. Click the refresh icon on the page to show the latest information.

Top 5 Interface Error Packet


2020/04/15 23:03:47 

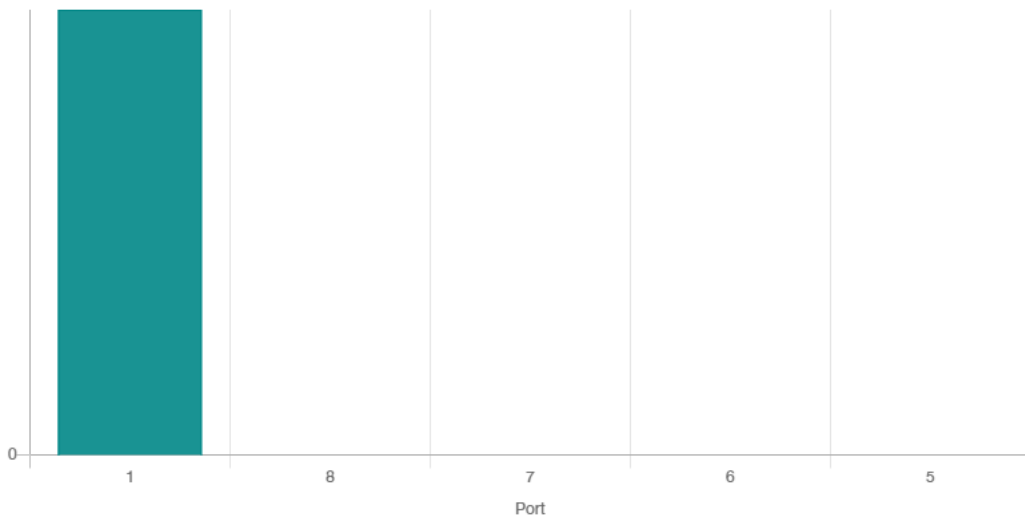


Top 5 Interface Utilization

The top 5 interface utilizations will be shown here. Click the refresh icon on the page to show the latest information.

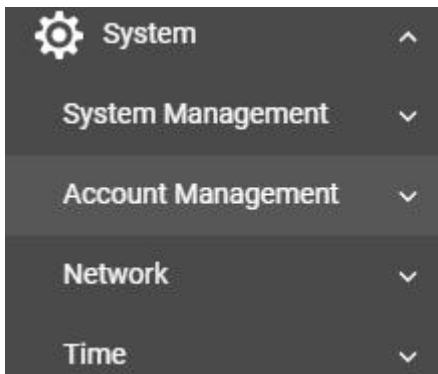
Top 5 Interface Utilization (%)

2020/04/15 23:04:53 



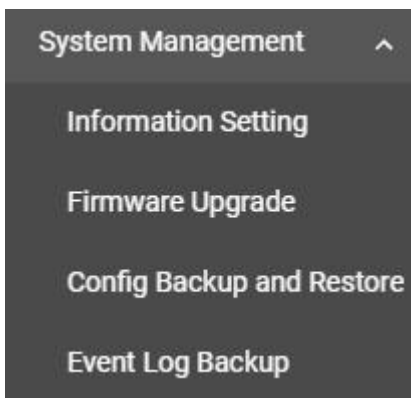
System

Click **System** on the function menu. You can configure the **System Management**, **Account Management**, **Network**, and **Time** configurations.



System Management

Click **System Management**, four functions can be configured under this section: **Information Setting**, **Firmware Upgrade**, **Configure Backup and Restore**, and **Event Log Backup**.



Information Setting

Define **Information Setting** items to make it easier to identify different switches that are connected to your network.

Information Setting

Device Name
moxa

4 / 255

Location

0 / 255

Description

0 / 255

Contact Information

0 / 255

Apply

Device Name

Setting	Description	Factory Default
1 to 255 characters	This option is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty.	moxa

NOTE The Device Name field follows the PROFINET I/O naming rule. The name can only include the following characters, **a-z/0-9/-**. The prefix cannot start from port-x where x=0~9.

Location

Setting	Description	Factory Default
Max. 255 characters	This option is for differentiating between the locations of different switches. Example: production line 1.	None

Description

Setting	Description	Factory Default
Max. 255 characters	This option is for recording a more detailed description of the unit.	None

Contact Information

Setting	Description	Factory Default
Max. 255 characters	Users can input contact information such as email address, or telephone number when problems occur.	None

When finished, click **Apply** to save your changes.

Firmware Upgrade

There are three ways to update your Moxa switch's firmware: from a local *.rom file, by remote SFTP server, and remote TFTP server.

Local

Select **Local** tab.

Select File

Before performing firmware upgrade, download the updated firmware (*.rom) file first from Moxa's website (www.moxa.com).

Setting	Description	Factory Default
Select the firmware file	Select the firmware file from the location where the updated firmware is located.	None
Browse for the (*.rom) file, and then click the Upgrade button.	This option allows users to select the updated firmware file and perform the firmware upgrade.	None

SFTP

Select **SFTP** tab.

Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server.	Input the server IP address of the computer where the new firmware file (*.rom) is located.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	The account must be authorized in order for the SFTP Server to have a secure connection.	None

Password

Setting	Description	Factory Default
Input the password for the SFTP server	The account has to be specified in order to authorize the SFTP Server for secure connection.	None

File Name

Setting	Description	Factory Default
Input the file name of the firmware	Input the file name of the new firmware.	None

When finished, click **Upgrade** to perform the firmware upgrade. The switch will reboot automatically and perform the firmware upgrade.

TFTP Server

Users can also upgrade firmware via the TFTP server. Click **TFTP** tab first.

The screenshot shows the 'Firmware Upgrade' section of a web interface. At the top, there are three tabs: 'Local', 'SFTP', and 'TFTP'. The 'TFTP' tab is currently selected and highlighted with a green underline. Below the tabs, there are two input fields: 'Server IP Address *' and 'File Name *'. At the bottom left of the form area, there is a green button labeled 'Upgrade'.

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Input the IP address of the TFTP server where the new firmware file (*.rom) is located.	None

File Name

Setting	Description	Factory Default
Input the file name of the firmware	Input the file name of the new firmware.	None

When finished, click **Upgrade** to perform the firmware upgrade.

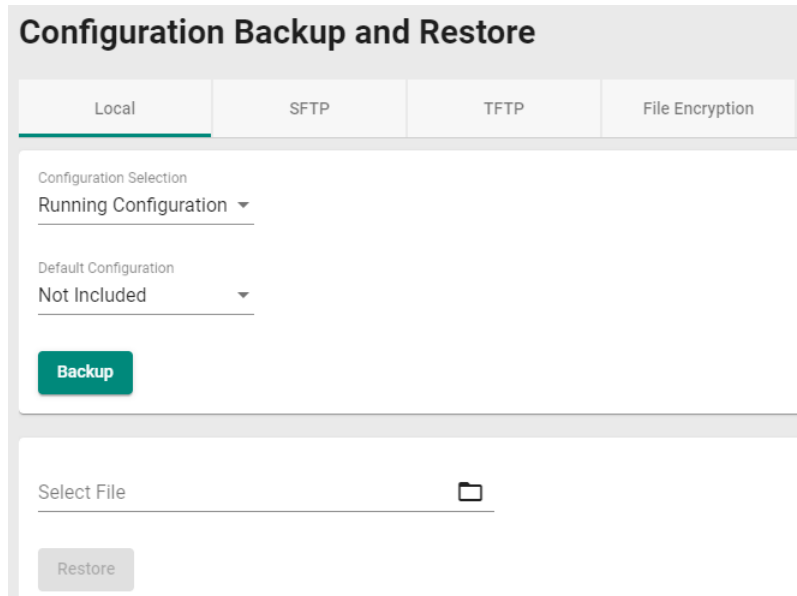
NOTE After the firmware has been updated, refresh the web service or reconnect the web service to make sure your browser gets the latest data.

Configuration Backup and Restore

There are three ways to back up and restore your Moxa switch's configuration: from a local configuration file, by remote SFTP server, or by remote TFTP server. In addition, file encryption is also provided for your safety concern.

Local

Click **Local** tab first.



Configuration Selection

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running
Startup Configuration	Back up the start-up configuration.	Configuration

Default Configuration

Setting	Description	Factory Default
Not Included	Back up the configuration without default settings.	Not Included
Included	Back up the configuration with default settings.	

Select File

Setting	Description	Factory Default
Click the Backup button to back up the configuration file to a local drive.	Back up the system file to your local computer.	None
Browse for a configuration file on a local disk, and then click the Restore button.	Select the configuration file and perform system restoration.	None

SFTP Server

Click **SFTP** tab first.

Configuration Backup and Restore

Local
SFTP
TFTP
File Encryption

Server IP Address *

Account *

Password *

File Name *

Backup
Restore

Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server where the new firmware file (*.rom) is located.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be provided to authorize the SFTP server for secure connection.	None

Password

Setting	Description	Factory Default
Input the passwords for the SFTP server	The account and password have to be specified in order to authorize the SFTP Server for secure connection.	None

File Name

Setting	Description	Factory Default
Input the backup/restore file name (support up to 54 characters, including the .ini file extension).	Input the file name of the configuration backup or restoration file.	None

When finished, click **Backup or Restore** to back up or restore the system configuration file.

TFTP Server

Click **TFTP** tab first.

The screenshot shows the 'Configuration Backup and Restore' web interface. At the top, there are four tabs: 'Local', 'SFTP', 'TFTP', and 'File Encryption'. The 'TFTP' tab is currently selected and highlighted with a green underline. Below the tabs, there are two input fields: 'Server IP Address *' and 'File Name *'. At the bottom of the form, there are two green buttons labeled 'Backup' and 'Restore'.

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Users can input the IP address of the TFTP server.	None

File Name

Setting	Description	Factory Default
Input the backup/restore file name (supports up to 54 characters, including the .ini file extension).	Users can input the file name to back up or restore the system configuration file.	None

When finished, click **Backup** or **Restore** to perform the firmware upgrade.

File Encryption

To encrypt the configuration file, click the **File Encryption** tab first.

The screenshot shows the 'Configuration Backup and Restore' web interface. At the top, there are four tabs: 'Local', 'SFTP', 'TFTP', and 'File Encryption'. The 'File Encryption' tab is currently selected and highlighted with a green underline. Below the tabs, there is a dropdown menu labeled 'Configuration File Encryption' with 'Disabled' selected. Below the dropdown is a 'Password' input field. At the bottom of the form, there is a green button labeled 'Apply'.

Enable Configuration File Encryption

Setting	Description	Factory Default
Enabled	Enable the configuration file to be encrypted.	Disabled
Disabled	Disable the feature that allows the configuration file to be encrypted.	

Password

Setting	Description	Factory Default
4 to 16 characters, numbers only.	Input the password when users encrypt the configuration file.	None

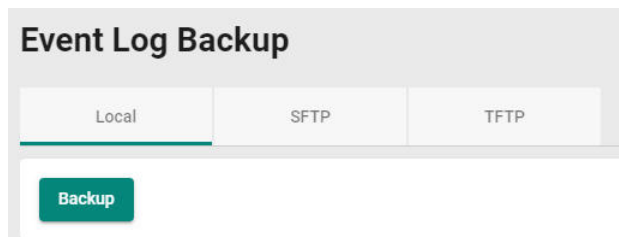
When finished, click **Apply** to save your changes.

Event Log Backup

There are three ways to back up Moxa switch’s log files: from a local drive, by remote SFTP server, or by remote TFTP.

Local

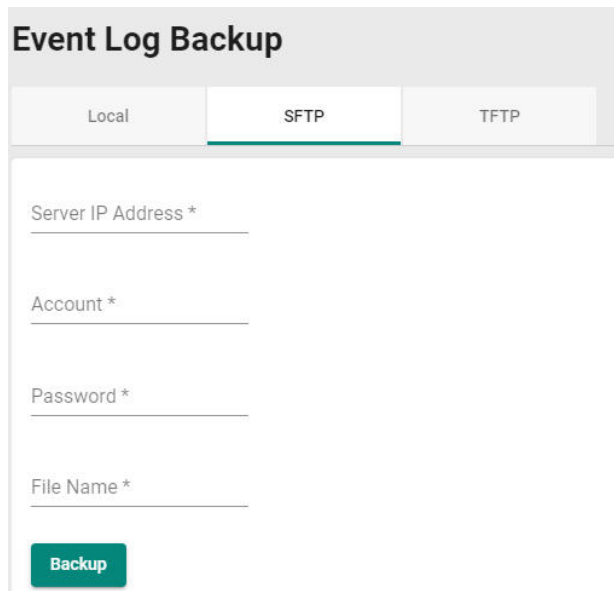
Click **Local** tab.



Click **Backup** to back up the log file to a local drive.

SFTP Server

Click **SFTP** tab.



Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Users can input the IP address of the SFTP server.	None

Port

Setting	Description	Factory Default
Input the port of the SFTP server, 1 to 65535	Specify the port used in the SFTP server.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be specified to authorize the SFTP server for secure connection.	None

Password

Setting	Description	Factory Default
Input the password for the SFTP server	The password has to be entered in order to authorize the SFTP Server for secure connection.	None

File Name

Setting	Description	Factory Default
Input the file name for event log backup	Users can input the file name of the event log.	None

When finished, click **Backup** to back up the event log file.

TFTP Server

Click **TFTP** tab.

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Users can input the IP address of the TFTP server.	None

Port

Setting	Description	Factory Default
Input the port of the TFTP server, 1 to 65535	Users can input the port used in the TFTP server.	None

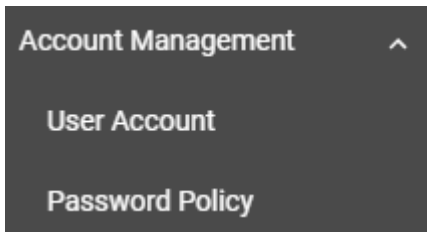
File Name

Setting	Description	Factory Default
Input the file name for event log backup	Users can input the file name of the event log.	None

When finished, click **Backup** to back up the event log file.

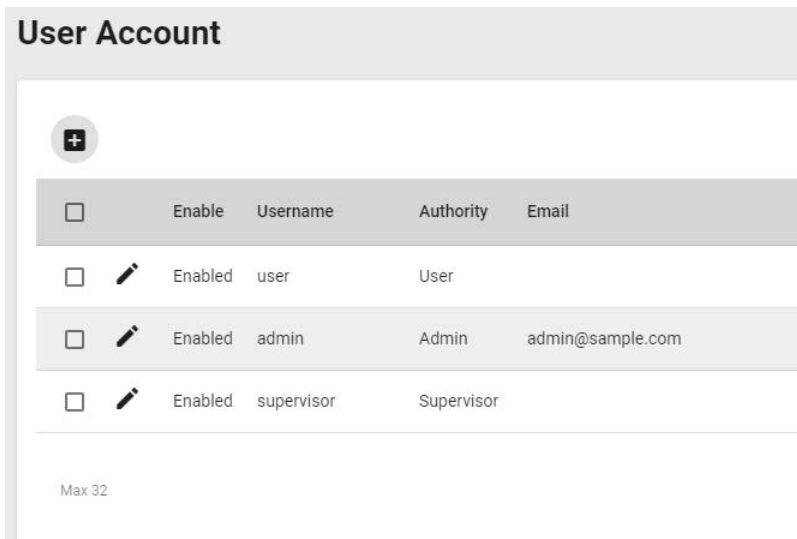
Account Management

The **Account Management** feature allows users to manage the accounts of the switch. You can enable different accounts with different roles to facilitate convenient management and safe access.



User Account

This section describes how to manage the existing accounts of the switch. Here, you can add, edit, and delete user accounts for the switch. By default, there is only one account: admin. In order to enhance security, we suggest you create a new account with the user authority.



There is a search function on the upper right of the User Account page. Type the username you want to search for.



Editing Existing Accounts

Select the account you want to edit and click the edit icon.

User Account

+

	Enable	Username	Authority	Email
<input type="checkbox"/>		Enabled	user	User
<input type="checkbox"/>		Enabled	admin	Admin admin@sample.com
<input type="checkbox"/>		Enabled	supervisor	Supervisor

Max 32

Configure the following settings.

Edit Account Setting

Enable *

Username
 Change Password
At least 4 characters 4 / 32

Authority *

Email
 15 / 63

Cancel

Apply

Enabled

Setting	Description	Factory Default
Enabled	It allows users to enable this account.	Enabled
Disabled	It allows users to disable this account.	

Username

Information	Description	Factory Default
Show the username (read only)	It displays the username.	username

Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	admin
supervisor	This account has read/write access of some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

Email

Setting	Description	Factory Default
Input an email address	Input an email address for the account.	None

To change the password, click Change Password.

Edit Account Password

Username
 test
At least 4 characters 4 / 32

New Password *
At least 4 characters 0 / 63

Confirm Password *
At least 4 characters 0 / 63

Back

Apply

Username

Information	Description	Factory Default
Show the username (read only)	It displays the username.	username

New Password

Setting	Description	Factory Default
4 to 63 characters	It allows users to provide a new password for this account.	None

Confirm Password

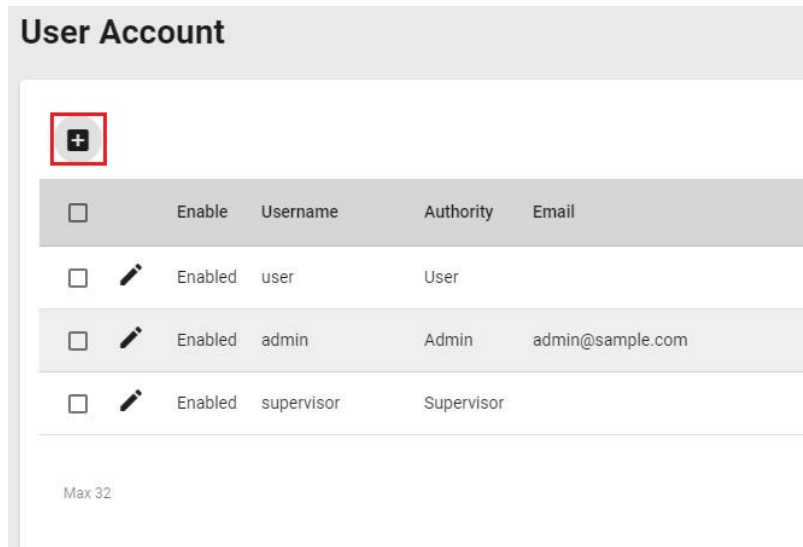
Setting	Description	Factory Default
4 to 63 characters	Input the same password for confirmation.	None

When finished, click **Apply** to save your changes.

NOTE Refer to **Appendix A** for detailed descriptions for read/write access privileges for the admin, supervisor, and user authority levels.

Creating a New Account

You can create new account by clicking the + icon on the configuration page.



Configure the following settings.

Create New Account

Enable
 Enabled ▼

Username *
 At least 4 characters 0 / 32

Authority *
▼

New Password *
 At least 4 characters 0 / 63

Confirm Password *
 At least 4 characters 0 / 63

Email
 0 / 63

Cancel
Create

Enabled

Setting	Description	Factory Default
Enabled	This enables the account.	Enabled
Disabled	This disables the account.	

Username

Setting	Description	Factory Default
Input a username, 4 to 32 characters	Input a new username for this account.	None

Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	None
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

In order to enhance security, we suggest you create a new account with the user authority.

New Password

Setting	Description	Factory Default
4 to 63 characters	Input a new password for this account.	None

Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Reenter the password to confirm.	None

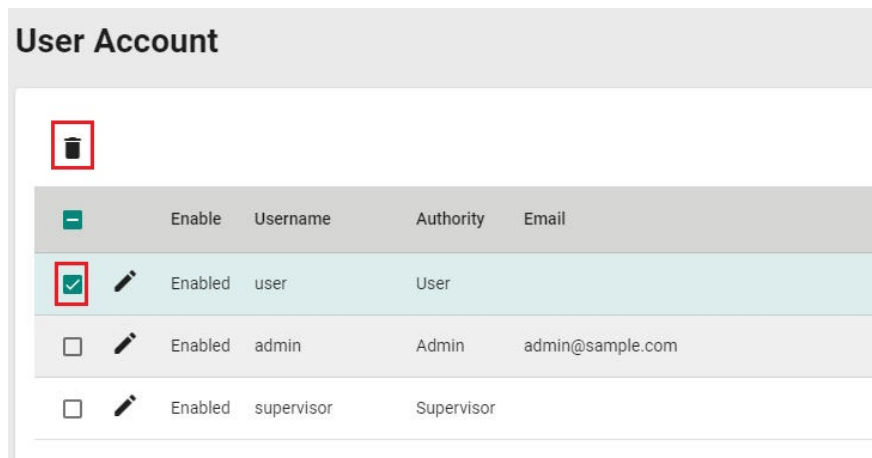
Email

Setting	Description	Factory Default
Input an email address	Input an email address for the account if required.	None

When finished, click **Create** to complete.

Delete an Existing Account

To delete the existing account, simply select the account you want to delete, and then click the delete icon on the configuration page.



Click **Delete** to delete the account.

Delete Account

Are you sure you want to delete the selected account?



Password Policy

In order to prevent hackers from cracking weak passwords, a password policy can be set. The password policy can force users to create passwords with a minimum length and complexity, and can also set a maximum lifetime for the password to ensure it is changed periodically.

Password Policy

Minimum Length *

4

4 - 63

Password Complexity Strength Check

At least one digit (0-9)

At least one upper case letter (A-Z)

At least one lower case letter (a-z)

At least one special character (~!@#\$%^&*._|;:,.<>{}|())

Password Max-life-time *

0

0 - 365 day

Apply

Minimum Length

Setting	Description	Factory Default
Input from 4 to 63	This sets the minimum length of the password.	4

Password Complexity Strength Check

Setting	Description	Factory Default
digit, letter cases, special characters	These determine the required complexity for the password. Multiple options may be checked.	None

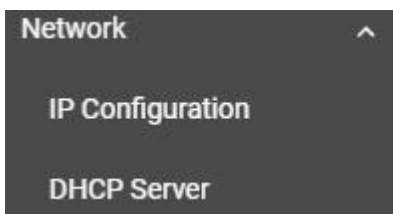
Password Max-life-time (day)

Setting	Description	Factory Default
Input from 0 to 365	This determines how long the password can be used before it must be changed.	0

When finished, click **Apply** to save your changes.

Network

This section describes how to configure the switch's network settings, including **IP Configuration** and the **DHCP Server**.



IP Configuration

Users can configure the IP settings of the switch.

IP Configuration

Get IP From
Manual

IP Address *
192.168.127.253

Subnet Mask
24 (255.255.255.0) Default Gateway

DNS Server 1 DNS Server 2

IPv6 Global Unicast Ad...

IPv6 DNS Server 1 IPv6 DNS Server 2

IPv6 Global Unicast Ad... IPv6 Link-Local Address
fe80::290:e8ff:fe00:9

Apply

Get IP From

Setting	Description	Factory Default
Manual	The IP address of the switch must be set manually.	Manual
DHCP	The IP address of the switch will be assigned automatically by the network's DHCP server.	

IP Address

Setting	Description	Factory Default
Input the IP address for the switch	Specify the IP address to use for the switch.	192.168.127.253

Subnet Mask

Setting	Description	Factory Default
Input the subnet mask for the switch	Specify the subnet mask to use for the switch.	24(255.255.255.0)

Default Gateway

Setting	Description	Factory Default
Input the IP address for the gateway	Specify the IP address of the gateway that connects the LAN to a WAN or another network.	None

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1 st DNS server	Specify the IP address of the 1 st DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2 nd DNS server	Specify the IP address of the 2 nd DNS server used by your network. The switch will use the secondary DNS server if the first DNS server fails to connect.	None

IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to the RFC 2373 IPv6 Addressing Architecture, using 8 colon-separated 16-bit hexadecimal values. One double colon can be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. Note: This feature is only available in Advanced Mode .	None

IPv6 DNS Server 1

Setting	Description	Factory Default
Input the IPv6 IP address of the 1 st DNS server	Specify the IPv6 address of the 1 st DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address. Note: This feature is only available in Advanced Mode .	None

IPv6 DNS Server 2

Setting	Description	Factory Default
Input the IPv6 address of the 2 nd DNS server	Specify the IPv6 address of the 2 nd DNS server used by your network. The Moxa switch will use the secondary DNS server if the first DNS server fails to connect. Note: This feature is only available in Advanced Mode .	None

IPv6 Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits of the address. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode .	None

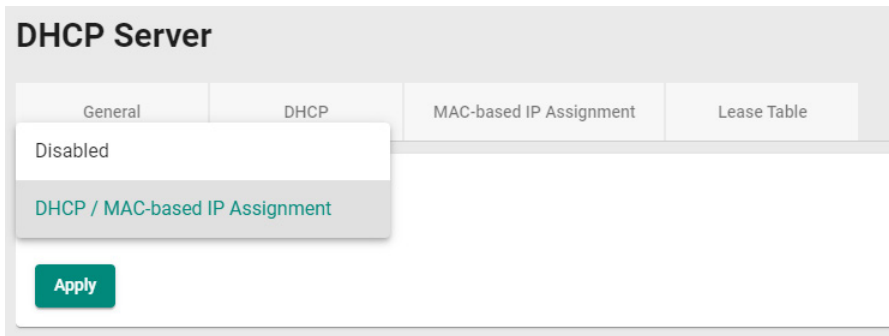
IPv6 Link-Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode .	None

When finished, click **Apply** to save your changes.

DHCP Server

This section describes how to configure the DHCP server settings for Moxa's switch. First, click the **General** tab.



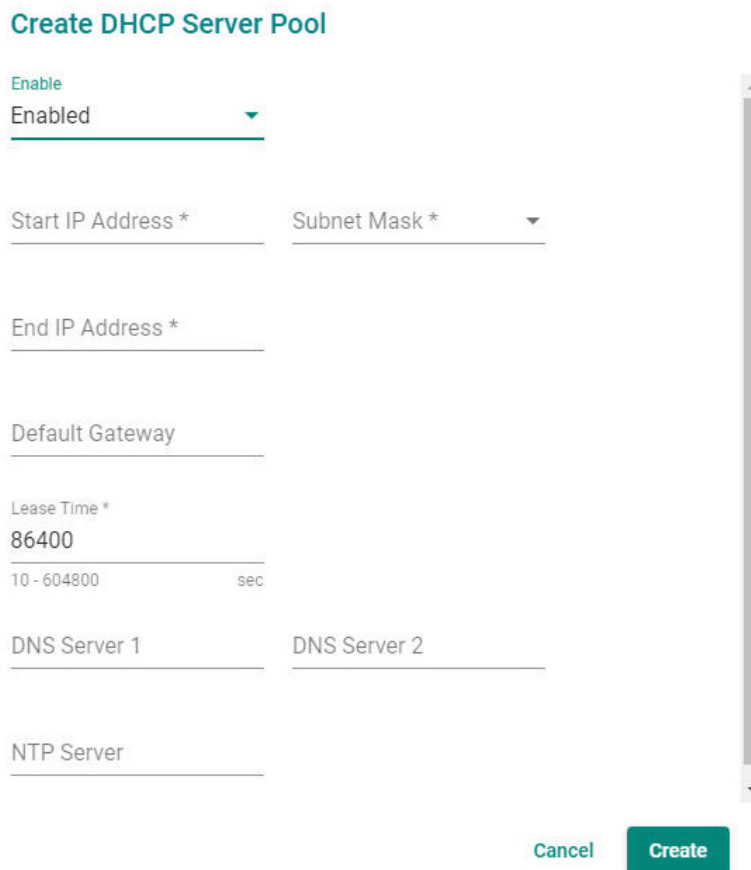
Then select **DHCP / MAC-based IP Assignment**, and click **Apply**.

DHCP

Select the **DHCP** tab and then click the **+** icon on the configuration page to create a new DHCP server pool.



Configure the following parameters.



NOTE Users can only create one IP pool. It can be connected to different network subnets with the Management IP of the switch.

Enable

Setting	Description	Factory Default
Enabled	Enables the DHCP server pool.	Enabled
Disable	Disables the DHCP server pool.	

Start IP Address

Setting	Description	Factory Default
Input the first IP address	Specify the first IP address for the pool.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask for the pool.	None

End IP Address

Setting	Description	Factory Default
Input the last IP address	Specify the last IP address for the pool.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for clients to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604,800 seconds (up to 7 days)	Specify the lease time for DHCP IP assignments.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1 st DNS server	Specify the IP address of the 1 st DNS server for clients to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2 nd DNS server	Specify the IP address of the 2 nd DNS server for clients to use.	None

NTP Server

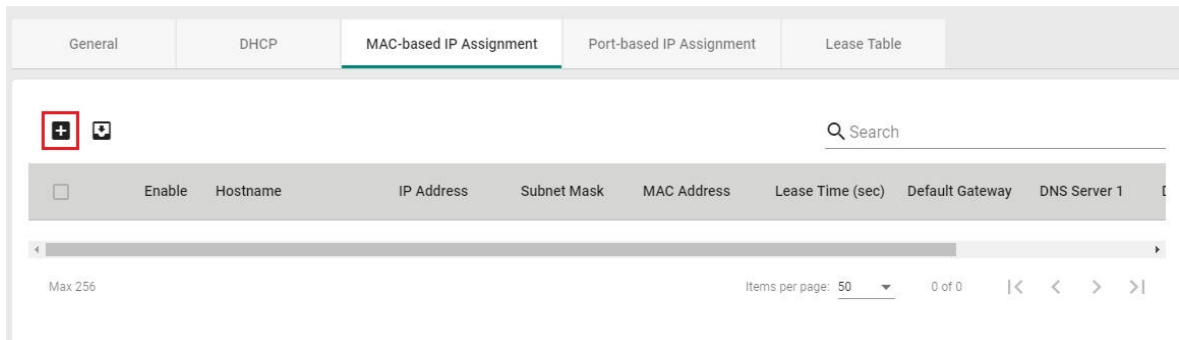
Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server clients will use.	None

When finished, click **Create**.

MAC-based IP Assignment

Users can assign an IP address for a specific MAC address. This can be useful if you always want the same IP address to be assigned to a specific device, even if it is reconnected or connected to a different port.

Click the **MAC-based IP Assignment** tab, and then click the **+** icon on the configuration page. Note that the MAC-based IP Assignment has a higher priority than the DHCP server.



Configure the following parameters.

Create Entry

Enable
Enabled

Hostname * i
0 / 63

IP Address * Subnet Mask *

MAC Address *

Default Gateway

Lease Time *
86400
10 - 86400 sec

DNS Server 1 DNS Server 2

Cancel **Create**

Enable

Setting	Description	Factory Default
Enabled	Enables the MAC-based IP assignment entry.	Enabled
Disabled	Disables the MAC-based IP assignment entry.	

Hostname

Setting	Description	Factory Default
Enter a hostname between 0 and 63 characters	Specify a hostname to use for the DHCP client.	None

IP Address

Setting	Description	Factory Default
Input the assigned IP address	Specify the IP address to assign to the client.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask to use for the client.	None

MAC Address

Setting	Description	Factory Default
Input the assigned MAC address	Specify the MAC address of the device you want to assign an IP address to. Make sure the MAC address is entered in the correct format. Here is an example: 28-d2-44-D3-e3-f2 or 28:d2:44:D3:e3:f2.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for the client to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604800.	Define how long before the IP address needs to be reassigned.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1 st DNS server	Specify the IP address of the 1 st DNS server for the client to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2 nd DNS server	Specify the IP address of the 2 nd DNS server for the client to use.	None

NTP Server

Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server the client will use.	None

When finished, click **Create**.

Lease Table

Click **Lease Table** to view detailed information for the hostname, IP address, MAC address, and time left for each port.

DHCP Server

General
DHCP
MAC-based IP Assignment
Port-based IP Assignment
Lease Table

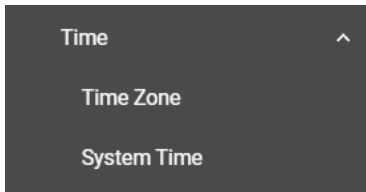
Search

Hostname	IP Address	MAC Address	Time Left
CINDY-YANG01	192.168.127.1	c8:cb:b8:02:26:5f	23 h: 57 m: 41 s

Item	Description
Hostname	The hostname of the client.
IP Address	The IP address of the client.
MAC Address	The MAC address of the client.
Time Left	The amount of time left on the DHCP lease for the client.

Time

This section describes how to configure the **Time Zone** and **System Time** settings for the switch. The switch has a time calibration function based on information from an NTP server or a user-specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.



NOTE The user must update the Current Time and Current Date after the switch has been powered off for an extended period of time (e.g., three days). The user must pay particular attention to this when there is no NTP server or Internet connection available.

Time Zone

Users can configure the time zone for the switch.

Time Zone

System Uptime
0d3h30m56s

Current Time
Fri Dec 21 2018 22:24:24 UTC+00:00

Time Zone
UTC+00:00

Daylight Saving
Disabled

Start Date * 1/9/2020 Start Time * 04:33 PM

End Date * 1/9/2020 End Time * 04:33 PM

Offset
00:00

Apply

System Uptime

Setting	Description	Factory Default
System-specified time	This indicates how long the switch has been running since the last cold start.	N/A

Current Time

Setting	Description	Factory Default
User-specified time	Shows the current system time.	None

Time Zone

Setting	Description	Factory Default
---------	-------------	-----------------

Select from the drop-down list	Specify the time zone to use for the switch.	GMT (Greenwich Mean Time)
--------------------------------	--	---------------------------

Daylight Saving Time

The Daylight Saving Time settings are used to automatically adjust the time according to regional standards.

Daylight Saving
 Enabled ▼

Start Date * Start Time *
 5/16/2019 📅 08:20 PM 🕒

End Date * End Time *
 5/16/2019 📅 08:20 PM 🕒

Offset
 00:00

Apply

Configure the following settings.

Daylight Saving Time

Setting	Description	Factory Default
Enabled	Enables Daylight Saving Time.	Disabled
Disabled	Disables Daylight Saving Time.	

Start Date

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour	Specify the offset (in HH:MM format) to use during Daylight Saving Time.	None

When finished, click **Apply** to activate the time zone settings.

System Time

This section describes how to configure the time, NTP server, and NTP authentication settings.

Time

The section describes how to configure the system time. Click the **Time** tab.

System Time

Time

NTP Server

NTP Authentication

Current Time
Thu May 16 2019 20:24:3

Clock Source
Local

Date *
5/16/2019

Time
08:24 PM

Apply
Sync From Browser
Refresh

Current Time

Setting	Description	Factory Default
None	This automatically shows the current time according to your default settings.	Local

Clock Source

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to set the time manually (Local), from an SNTP server, an NTP server.	Local

Clock Source is from Local

Date

Setting	Description	Factory Default
Select the date	Select the current date.	Local

APR 2020 < >

S	M	T	W	T	F	S
APR			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Time

Setting	Description	Factory Default
Input the current time	Specify the current time. You can manually input the time, or you can click Sync From Browser to set the time based on the time used by your web browser.	None

Clock Source is from SNTP**Time Server 1**

Setting	Description	Factory Default
Input the address of the 1 st SNTP time server	Specify the IP or domain address of the 1 st SNTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

Time Server 2

Setting	Description	Factory Default
Input the address of the 2 nd SNTP time server	Specify the IP or domain address of the secondary SNTP server to use if the first SNTP server fails to connect.	None

Click **Apply** to complete.

Clock Source is from NTP

If the switch is connecting to an NTP server that requires authentication, refer to the **NTP Authentication** section to configure the NTP key to use.

Time Server 1

Setting	Description	Factory Default
Input the address of the 1 st NTP time server	Specify the IP or domain address of the 1 st NTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP authentication for Time Server 1.	Disabled

Time Server 2

Setting	Description	Factory Default
Input the address of the 2 nd time server	Specify the IP or domain address of the secondary NTP server to use if the first NTP server fails to connect.	None

Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP Authentication for Time Server 2.	Disabled

Click **Apply** to complete.

NTP Server

Click the **NTP Server** Tab to perform further configuration.

The screenshot shows the 'System Time' configuration page. At the top, there are three tabs: 'Time', 'NTP Server', and 'NTP Authentication'. The 'NTP Server' tab is selected and highlighted with a green underline. Below the tabs, there are two dropdown menus. The first is labeled 'NTP Server' and is currently set to 'Disabled'. The second is labeled 'Client Authentication' and is also set to 'Disabled'. At the bottom left of the configuration area, there is a green 'Apply' button.

Enable

Setting	Description	Factory Default
Enabled	Enable the NTP server.	Disabled
Disabled	Disable the NTP server.	

Client Authentication

Setting	Description	Factory Default
Enabled	Enable NTP authentication.	Disabled
Disabled	Disable NTP authentication.	

When finished, click **Apply** to save your changes.

NTP Authentication

This section describes how to configure NTP Authentication. Click the **NTP Authentication** tab, and then click the + icon on the page.

The screenshot shows the 'System Time' configuration page with the 'NTP Authentication' tab selected and highlighted with a green underline. In the main configuration area, a red square box highlights a plus sign icon (+) in the top left corner. Below this icon is a table header for NTP authentication keys. The header row contains a checkbox, followed by the labels 'Key ID', 'Type', and 'Key String'.

Configure the following settings.

Create Entry

Key ID

Type

Key String *

0 / 32

Cancel

Key ID

Setting	Description	Factory Default
Input the Key ID from 1 to 10	Input the Key ID to use for NTP authentication.	None

Type

Setting	Description	Factory Default
Input the authentication type	Input the authentication type.	MD5

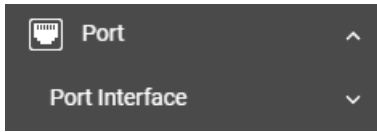
Key String

Setting	Description	Factory Default
Input the key string for authentication, from 0 to 32 characters.	Input the password to use for the authentication key.	None

When finished, click **Create**.

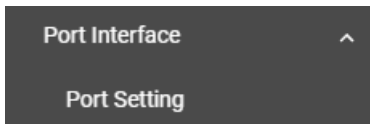
Port

This section describes how to configure the **Port Interface** functions for the switch.



Port Interface

You can configure **Port Setting** in the section.



Port Setting

Under **Port Setting**, select the **Setting** tab and then click the edit icon on the port you want to configure.

Port Setting

Setting

Status

Port	Admin Status	Media Type	Description	Speed/Duplex	MDI/MDIX
1	Enabled	1000Combo.		Auto	Auto
2	Enabled	1000Combo.		Auto	Auto
3	Enabled	1000TX,RJ45.		Auto	Auto
4	Enabled	1000TX,RJ45.		Auto	Auto
5	Enabled	1000TX,RJ45.		Auto	Auto
6	Enabled	1000TX,RJ45.		Auto	Auto
7	Enabled	1000TX,RJ45.		Auto	Auto
8	Enabled	1000TX,RJ45.		Auto	Auto

Configure the following parameters.

Edit Port 1 Setting

Admin Status
 Enabled ▼

Media Type
 1000Combo

Description

Speed/Duplex
 Auto ▼

MDI/MDIX
 Auto ▼

Copy Config to Ports ▼ i

Cancel

Apply

Admin Status

Setting	Description	Factory Default
Enable	Allows data transmission through this port.	Enabled
Disabled	Disables data transmission through this port.	

Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each module's port.	1000TX,RJ45

Description

Setting	Description	Factory Default
Max. 63 characters	Specify an alias for the port to help differentiate between different ports (e.g., PLC1).	None

Speed/Duplex

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection. Choose a fixed speed option if the connected Ethernet device has trouble auto-negotiating line speed.	Auto
10M Half		
10M Full		
100M Half		
100M Full		
1G Full		

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device, and changes the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-detecting the port type.	
MDIX		

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **Apply** to save your changes.

Port Status

To view the status of the ports, click the **Status** tab.

Port Setting

Setting

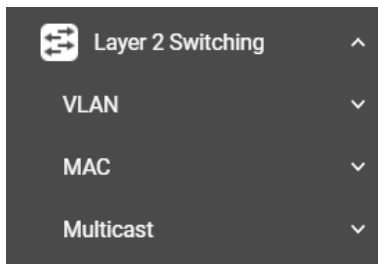
Status

↻
📄

Port	Admin Status	Media Type	Link Status	Description	MDI/MDIX	Port State
1	Enabled	1000Combo.	100M, Full (Auto)		MDI (Auto)	Forwarding
2	Enabled	1000Combo.	Link Down		Invalid	Discarding
3	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding
4	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding
5	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding
6	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding
7	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding
8	Enabled	1000TX,RJ45.	Link Down		Invalid	Discarding

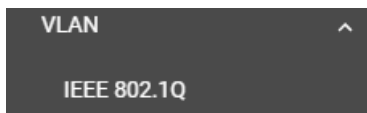
Layer 2 Switching

This section describes how to configure various parameters, such as **VLAN**, **MAC**, and **Multicast**, for Moxa's switch. Click **Layer 2 Switching** on the function menu.



VLAN

This section includes **IEEE802.1Q** configurations.



IEEE 802.1Q Overview

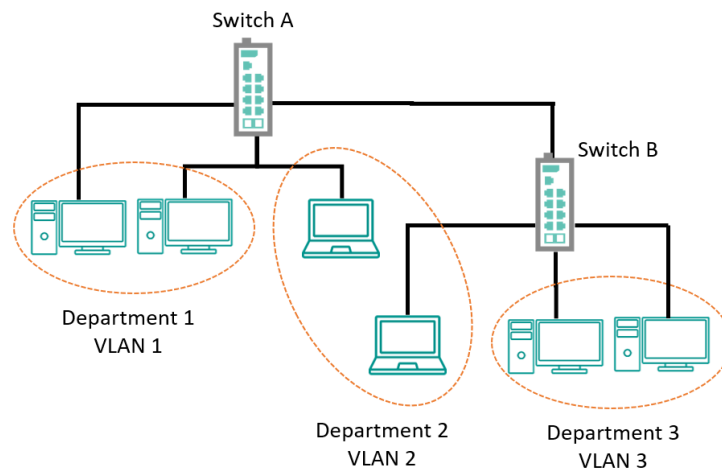
The IEEE 802.1Q is a network communication protocol that falls under the IEEE 802.1 standard regulation, allowing various segments to use a physical network at the same time to block broadcast packets by different segmentations. It specifies the VLAN tagging for Ethernet frames on switches that can control the path process.

How A VLAN Works

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network into:

- **Departmental groups**—You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on the Marketing VLAN is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on the Marketing VLAN. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and the Rackmount switch

Your Moxa switch includes support for VLANs using IEEE Std 802.1Q-2005. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-2005 standard allows each port on your Moxa switch to be placed as follows:

- On a single VLAN defined in the switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your Moxa switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized Moxa switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the Moxa switch over the network.

Communication Between VLANs

If devices connected to a VLAN need to communicate with devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs need to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

Moxa's switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged or tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, a tagged membership must be defined.

A typical host (e.g., clients) will be an untagged member of one VLAN, defined as an **Access Port** in a Moxa switch, while an inter-switch connection will be a tagged member of all VLANs, defined as a **Trunk Port** in a Moxa switch.

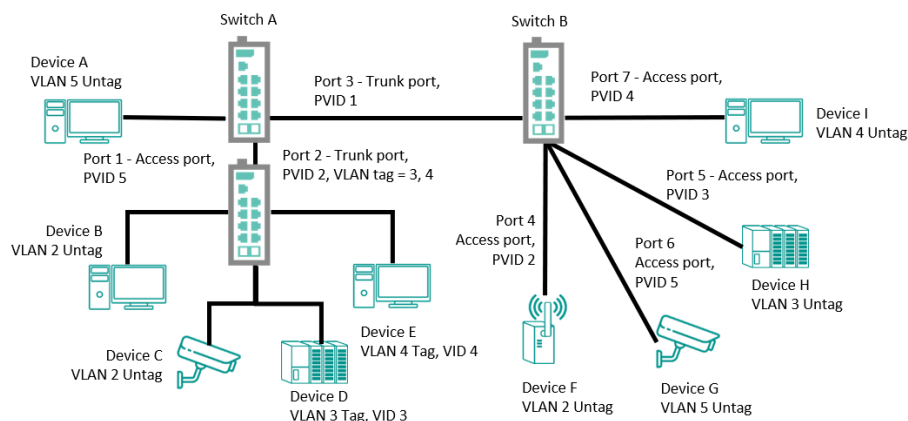
The IEEE Std 802.1Q-2005 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a *tagged* frame.

To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

Moxa's switch supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices, and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the default port PVID as its VID.

The following section illustrates how to use these ports to set up different applications.



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as an **Access Port** with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as a **Trunk Port**. GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as an **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as an **Access Port** with PVID 3.

- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as an **Access Port** with PVID 4.

After the application is properly configured:

- Packets from Device A will travel through **Trunk Port 3** with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through **Access Port 2** with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through **Trunk Port 3** with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through **Trunk Port 3** with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through **Trunk Port 3** with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through **Trunk Port 3** with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

VLAN Settings

To configure VLAN, click **VLAN** on the function menu, then select **IEEE 802.1Q**. Click **Global** tab.

VLAN Management Port Quick Setting

You can quickly configure VLAN setting.

The screenshot shows the 'IEEE 802.1Q' configuration page with three tabs: 'Global', 'Setting', and 'Status'. The 'Global' tab is active. Under 'Management VLAN', the value '1' is selected. Below this is the 'Management Port Quick Setting' section, where 'Management Port' is set to '1'. At the bottom, there are four dropdown menus: 'Mode' (set to 'Access'), 'PVID' (set to '1'), 'Tagged VLAN' (set to '1'), and 'Untagged VLAN' (set to '1'). A green 'Apply' button is located at the bottom left of the configuration area.

Configure the following settings.

Management VLAN

Setting	Description	Factory Default
Display the first VLAN number	Show the name of the VLAN.	1

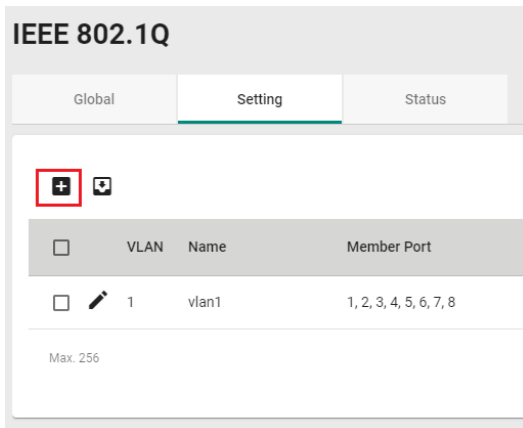
Management Port

Setting	Description	Factory Default
Select the port(s) as the VLAN port(s) from the drop-down list	To select the port(s) as the VLAN port(s).	None

When finished, click **Apply** to save your changes.

Detailed VLAN Settings

On the IEEE 802.1Q page, first click the **Setting** tab, and then click the edit icon.



Configure the following parameters.

Create VLAN

VID * i
Max. 10 VLANs

Name
0 / 32

Member Port ▼

Cancel

Create

VID

Setting	Description	Factory Default
Input a VLAN ID, (10 VLANs max.)	Input a VLAN ID.	None

Name

Setting	Description	Factory Default
Input a name for the VLAN, (32 characters max.)	Specify a name for the VLAN.	None

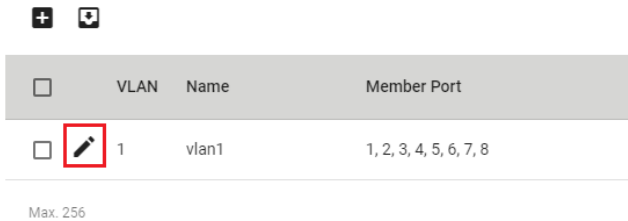
Member Port

Setting	Description	Factory Default
Select the port from the drop-down list.	Specify the ports that are the member ports for the VLAN.	None

When finished, click **Create**.

Editing the Existing VLAN Settings

To edit the existing VLAN settings, click the edit icon of the VLAN you want to edit.



Configure the following settings.

Edit VLAN 1 Setting

VID
1
.....
Max. 10 VLANs

Name
vlan1
.....
5 / 32

Member Port
1, 2, 3, 4, 5, 6, 7, 8 ▼

Cancel **Apply**

VID

Setting	Description	Factory Default
Show the VLAN ID	Display the VLAN ID.	None

Name

Setting	Description	Factory Default
Show the name of the VLAN	Display the VLAN name.	None





Member Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are member ports for the VLAN.	None

When finished, click **Apply** to save your changes.

Editing the Port Settings

To edit the port settings, in the **VLAN** tab select the edit icon on the port you want to configure on the lower part of the page.

Port	Mode	PVID	Untagged VLAN	Tagged VLAN
 1	Access	1	1	
 2	Access	1	1	
 3	Access	1	1	
 4	Access	1	1	

Configure the following settings.


Edit Port 1 Setting

Mode
Access

PVID
1

Tagged VLAN

Untagged VLAN
1

Copy Config to Ports 

Cancel **Apply**

Mode

Setting	Description	Factory Default
Access	When this port is connected to a single device, without tags.	Access
Trunk	When this port is connected to another 802.1Q VLAN aware switch.	

PVID

Setting	Description	Factory Default
1 to 4094	Sets the default VLAN ID for untagged devices connected to the port.	None

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	This field will be active only when selecting the Trunk type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VLANs.	Port Name

Untagged VLAN (currently disabled)





Setting	Description	Factory Default
VID range from 1 to 4094	This field is only active when the Hybrid port type is selected. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	Same as the PVID

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **Apply** to save your changes.

You can view the VLAN status in the figure below:

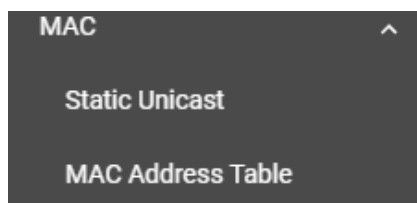
Port	Mode	PVID	Untagged VLAN	Tagged VLAN
 1	Access	1	1	
 2	Access	1	1	
 3	Access	1	1	
 4	Access	1	1	

See the description below for more information.

Port	Mode	PVID	Untagged VLAN	Tagged VLAN
Port number on the switch	VLAN Mode: Access or Trunk	Port default VID of the VLAN	The untagged VLAN list	The tagged VLAN list

MAC

This section explains Independent VLAN learning and describes how to configure **Static Unicast** and the **MAC Address Table**.



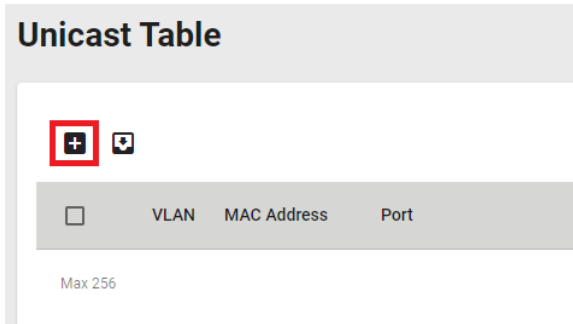
Independent VLAN Learning

Moxa's switch uses the **Independent VLAN Learning (IVL)** mode.

In an **IVL Mode**, a MAC table will be created in each VLAN, which will constitute many MAC tables. However, the same VID record will be selected and put in a table. A MAC table will be stored in the format of MAC + VID, the same MAC will be stored in different tables with different VIDs.

Static Unicast

Click **Static Unicast** on the function menu page and click the + icon on the configuration page.



Configure the following settings.

Add Static Unicast Entry

VID

MAC Address

Port

Cancel

VID

Setting	Description	Factory Default
Input a VLAN ID	Input a VLAN ID.	None

MAC Address

Setting	Description	Factory Default
MAC address of the port	Input the MAC address of the port, for example 00:90:e8:01:01:01.	None

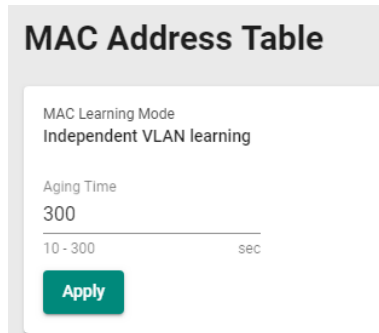
Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the port you want to create a VLAN for.	None

When finished, click **Create**.

MAC Address Table

Select **MAC Address Table**, and configure the following settings.



MAC Learning Mode

Information	Description	Factory Default
Independent VLAN learning	Show the current MAC Learning Mode.	Independent VLAN learning

Aging Time

Setting	Description	Factory Default
10 to 300	Input a VLAN ID.	None

When finished, click **Apply** to save your changes.

You can view the current MAC Address Table on the bottom part of the configuration page.

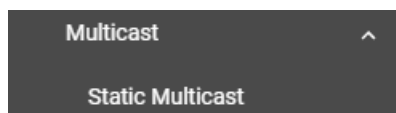


Index	VLAN	MAC Address	Type	Port
1	1	c8:cb:b8:02:26:5f	Learnt Unicast	3/4

Item Name	Description
Index	The number of the MAC address.
VLAN	The VLAN number
MAC Address	The MAC address on this device.
Type	Learnt Unicast, Learnt Multicast, Static Unicast, Static: Multicast
Port	The forwarding port of this MAC address.

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section will explain the **Static Multicast** settings for the Layer 2 Multicast functions.

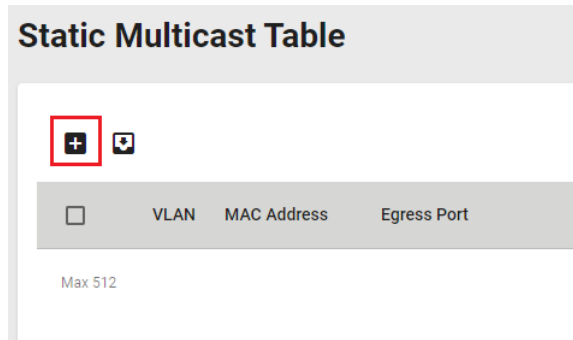


Static Multicast

Click **Static Multicast** on the menu to view the current multicast table.

Adding Static Multicast Entry

To add more tables, click the + icon.



Configure the following settings.

Add Static Multicast Entry

VID *

MAC Address *

Egress Port * ▼

Cancel

Create

VID (VLAN ID)

Setting	Description	Factory Default
Input the VID	Specify the multicast group's associated VLAN ID.	None

MAC Address

Setting	Description	Factory Default
Input the MAC address	Specify the multicast MAC address, for example 01:00:5e:01:01:01.	None

Egress Port

Setting	Description	Factory Default
Input the port from the drop-down list	Set the port(s) as an egress port(s) so that multicast streams can be forwarded to this port.	None

When finished, click **Create**.

Network Redundancy

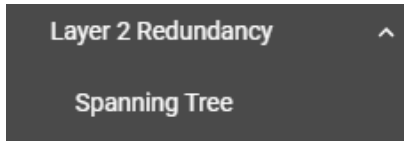
Setting up the Redundancy Protocol on your network helps protect critical links against failure, protects against network loops, and keeps network downtime to a minimum.

The Redundancy Protocol allows you to set up redundant paths on the network to provide a backup data transmission route in the event that a cable or one of the switches is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it can take several minutes to address the link down port or failed switch. For example, if a Moxa switch is used as a key communications device for a production line, several minutes of downtime can cause a big loss in production and revenue. Moxa switches support the following Redundancy Protocol functions:

- **Spanning Tree**

Layer 2 Redundancy

First select **Network Redundancy** on the menu and then click **Layer 2 Redundancy**.



Spanning Tree

Spanning Tree Overview

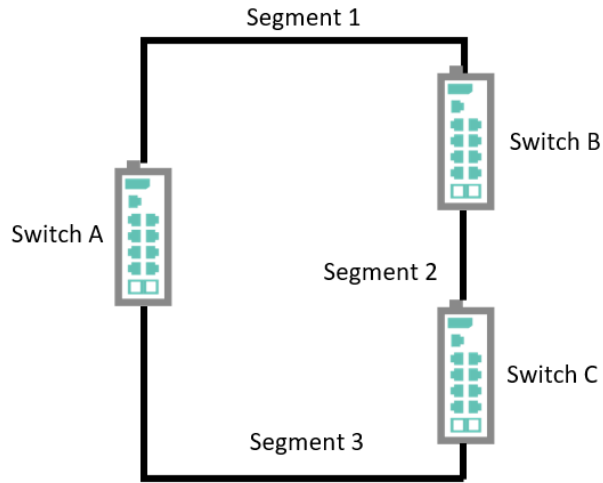
Spanning Tree Protocol (STP) was designed to help construct a loop-free logical topology on an Ethernet network, and provide an automatic means of avoiding any network loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Moxa switches' STP feature is disabled by default. To be completely effective, you must enable STP/RSTP on every Moxa switch connected to your network.

STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

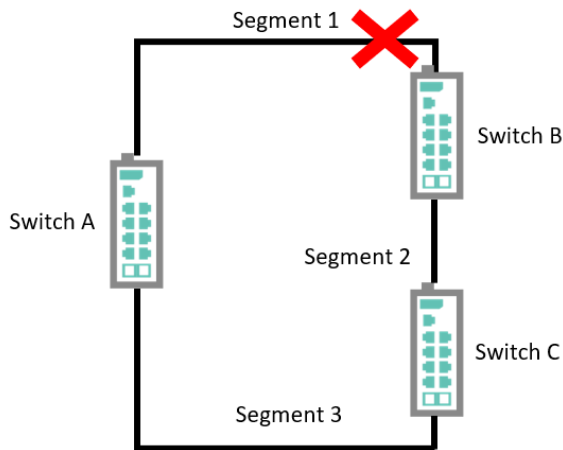
- Locate and then disable less efficient paths (e.g., paths that have lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

How STP Works

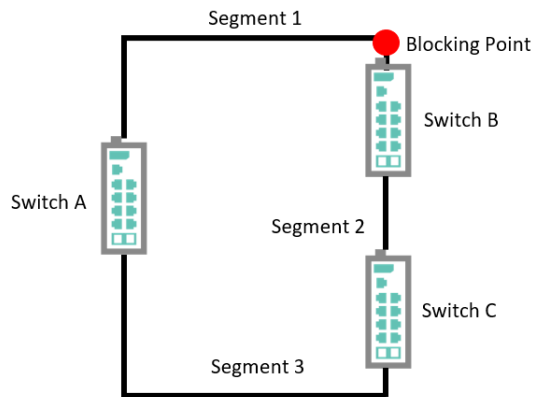
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



If STP is enabled, it will detect duplicate paths or block one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through switches C and A since this path has become shorter and is therefore more efficient. However, switch B on segment 1 is a blocking port.



What happens if a link failure is detected? As shown in the figure below, the STP will change the blocking port to forwarding state so that traffic from LAN segment 2 flows through switch B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

Difference Between STP and RSTP

RSTP is similar to STP but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

STP/RSTP Settings and Status

This section describes how to configure Spanning Tree settings.

General

Click **Spanning Tree** on the menu and then select the **General** tab.

Spanning Tree

General

Guard

Status

Spanning Tree
Disabled ▼

STP Mode Compatibility
STP/RSTP ▼ RSTP ▼

Bridge Priority	Forward Delay Time	Hello Time	Max. Age
32768	15	2	20
0 - 61440	4 - 30 sec.	1 - 2 sec.	6 - 40 sec.

Apply

Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enable Spanning Tree.	Disabled
Disabled	Disable Spanning Tree.	

STP Mode

Setting	Description	Factory Default
STP/RSTP	Use the STP/RSTP mode as the Spanning Tree protocol.	STP/RSTP

Compatibility

Setting	Description	Factory Default
STP	To be compatible with STP mode only	RSTP
RSTP	To be compatible with RSTP and STP modes	

Bridge Priority

Setting	Description	Factory Default
0 to 61440	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay Time (sec.)

Setting	Description	Factory Default
4 to 30	The amount of time the device waits before checking to see if it should change to a different state.	15

Hello Time (sec.)

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2




Max Age (sec.)

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

When finished, click **Apply** to save your changes.

Editing Spanning Tree for a Port

To edit the spanning tree settings for a specific port, click the edit icon on the port you want to configure.


Port	Edge	Priority	Path Cost	Link Type
 1	Auto	128	0	Auto
 2	Auto	128	0	Auto
 3	Auto	128	0	Auto
 4	Auto	128	0	Auto

Configure the following settings.


Edit Port 1 Setting

Edge
Auto

Priority *
128
0 - 240, multiples of 16

Path Cost *
0 
0 - 200000000

Link Type
Auto

Copy Config to Ports 

Cancel

Apply

Enable

Setting	Description	Factory Default
Enabled	Enable Spanning Tree.	Disabled
Disabled	Disable Spanning Tree.	

Priority

Setting	Description	Factory Default
0 to 240	Increase the priority of a port by selecting a lower number. A port with a higher priority has a greater chance of being a root port.	128

Path Cost

Setting	Description	Factory Default
0 to 20000000	The path cost value will be automatically assigned according to the different port speed if the value is set to zero.	0

Link Type (in Advanced Mode only)

Setting	Description	Factory Default
Point-to-Point	Set to Point-to-Point mode in full-duplex mode. The port should be connected to a single switch at the other end of the link.	Auto
Shared	Set to Shared mode in half-duplex mode. The port should be connected to shared media, such as a hub at the other end of the link.	
Auto	Automatically select Point-to-Point mode or Shared mode.	

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

Click **Apply** to finish.

BPDU Overview

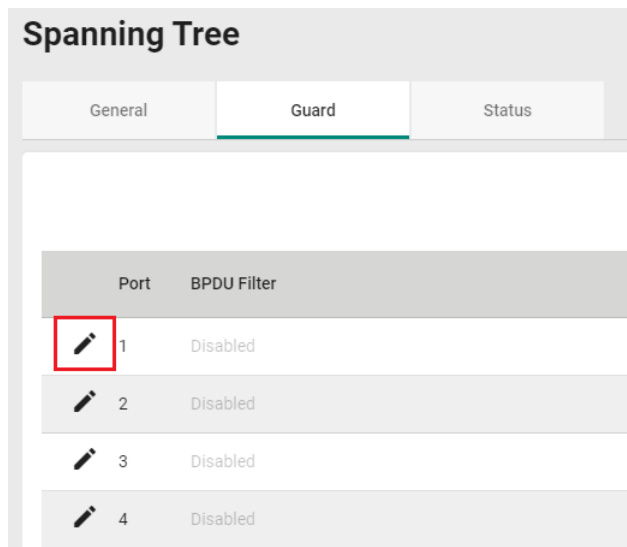
BDPUs (Bridge Protocol Data Units) are the network communication frames used in the STP (Spanning Tree Protocol). When two switches exchange messages, BDPUs are used to calculate the STP topology, and determine the network communication route. A BPDU filter is often used to screen sending or receiving BDPUs on a specific port of the switch.

BPDU Filter

BPDU Filter prevents a port from sending and processing BDPUs. A BPDU filter enabled port cannot transmit any BDPUs and drop all received BPDU either.

Configuring BPDU Filter Settings

First click **Spanning Tree** on the menu and then select the **Guard** tab. Next, click the edit icon on the port you want to configure.



Configure the following settings.

Edit Port 1 Setting

BPDU Filter
 Disabled

Copy Config to Ports

Cancel

NOTE To establish a redundant port e.g. it is highly recommended that you do not enable BPDU filter.

BPDU Filter

Setting	Description	Factory Default
Enabled	Enable BPDU Filter.	Disabled
Disabled	Disable BPDU Filter.	

Copy Config to Port

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the same settings to other port(s).	None

When finished, click **Apply** to save your changes.

Viewing Current Spanning Tree Status

Click the **Status** tab to view the current Spanning Tree status.

Spanning Tree

General
Guard
Status

Root Information ↻

Bridge ID
0/00:00:00:00:00:00

Root Path Cost
0

Forward Delay Time
15 (sec)

Hello Time
2 (sec)

Max Age
20 (sec)

Bridge Information ↻

Bridge ID
32768/00:90:E8:00:00:09

Running Protocol
RSTP

Forward Delay Time
15 (sec)

Hello Time
2 (sec)

Max Age
20 (sec)

In addition, the status for each port will also be shown below.

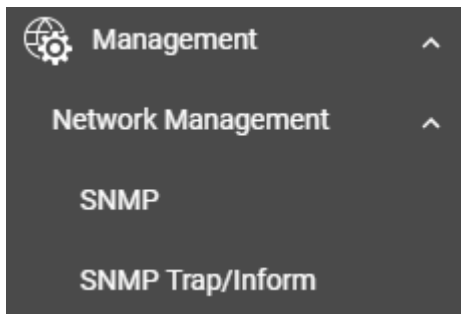
Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type
1	No	Disabled	Discarding	0	20000	Shared-LAN
2	No	Disabled	Discarding	0	20000	Shared-LAN
3	No	Disabled	Discarding	0	20000	Shared-LAN
4	No	Disabled	Discarding	0	20000	Shared-LAN
5	No	Disabled	Discarding	0	20000	Shared-LAN
6	No	Disabled	Discarding	0	20000	Shared-LAN
7	No	Disabled	Discarding	0	20000	Shared-LAN
8	No	Disabled	Discarding	0	20000	Shared-LAN

Refer to the following table for detailed description of each item.

Item	Description
Port	The port number on this device.
Edge	Show if this port is connected to an edge device.
Port Rule	Root: The port is connected directly or indirectly to the root device. Designated: The port is designated if it can send the best BPDU on the segment to which it is connected. Alternate: The alternate port receives more useful BPDU from another bridge and is the blocked port. Backup: The backup port receives more useful BPDU from the same bridge and is the blocked port. Disabled: The function is disabled.
Port State	Forwarding: The traffic can be forwarded through this port. Discarding: The traffic will be blocked. Disabled: The function is disabled.
Root Path Cost	The total path cost to the root bridge.
Path Cost	The path cost on this link.

Management

This section describes how to configure **Network Management** including **SNMP** and **SNMP Trap/Inform**.



Network Management

This section demonstrates how to configure SNMP and SNMP Trap/Inform settings.

SNMP

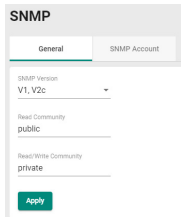
Moxa switches support SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the table below. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	None	No	No	Uses an account with admin or user to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	Disabled	Uses authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key: DES, AES	Uses authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

General Settings

First click **SNMP** on the menu and then click **General**.



Configure the following settings.

SNMP Version

Setting	Description	Factory Default
V1, V2c, V3	Specify V1, V2c, and V3 as the SNMP version.	V1, V2c
V1, V2c	Specify V1 and V2c as the SNMP version.	
V3 only	Specify V3 as the SNMP version.	

Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	public

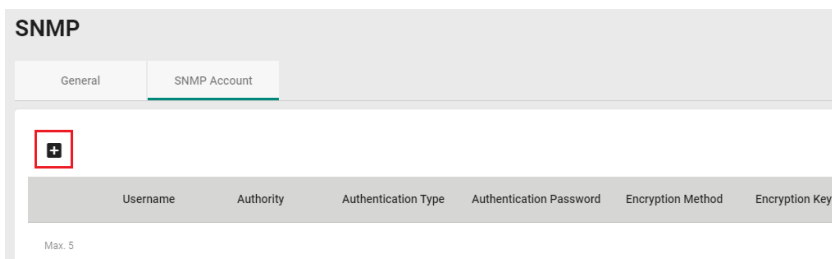
Read/Write Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	private

When finished, click **Apply** to save your changes.

Creating an SNMP Account

Click **SNMP** on the menu and then click the **SNMP Account**. Next click the **+** icon on the page.



Configure the following settings.

Create SNMP Account Setting

Username *
At least 4 characters 0 / 32

Authority
 Read/Write ▼

Authentication Type
 None ▼

Encryption Method
 Disabled ▼

Cancel **Create**

Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

Authority

Setting	Description	Factory Default
Read/Write	The user has read/write access.	Read/Write
Read Only	The user only has read access.	

Authentication type

Setting	Description	Factory Default
None	No authentication will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

Authentication password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

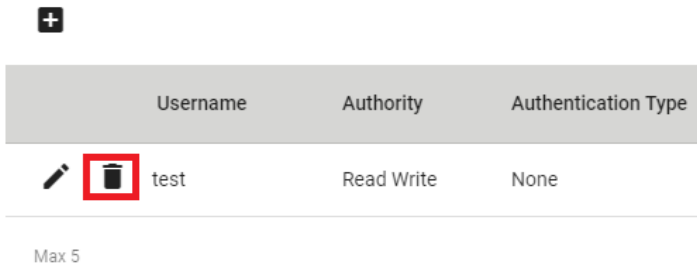
Encryption Key

Setting	Description	Factory Default
8 to 64 characters	Enable data encryption.	None

When finished, click **Create**.

Deleting an Existing SNMP Account

To delete an existing SNMP account, select the delete icon on the account.



Click **Delete** to delete the SNMP account.

Delete Account

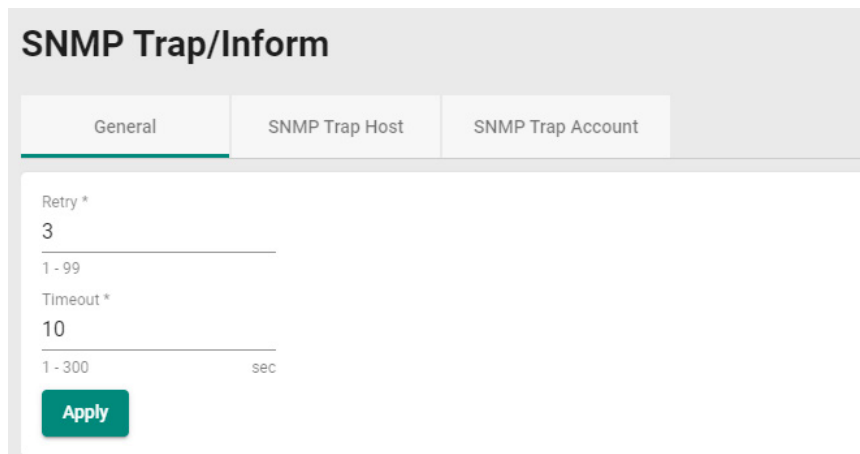
Are you sure you want to delete the selected account?



SNMP Trap/Inform

General Settings

First select **SNMP Trap/Inform** on the menu and then click **General**.



Configure the following settings.

Retry

Setting	Description	Factory Default
1 to 99	Input the retry value.	3

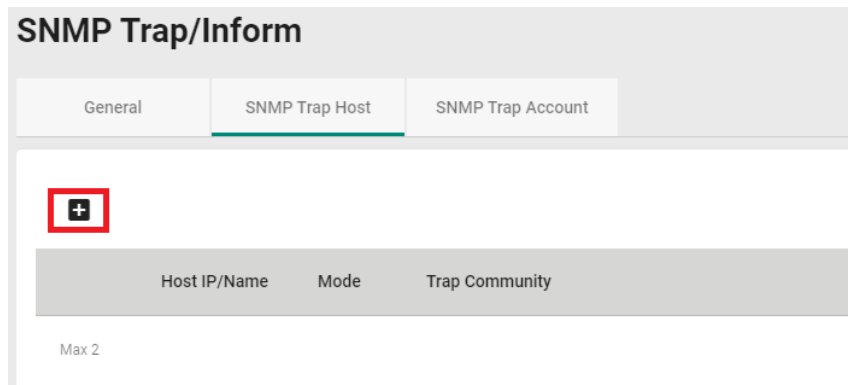
Timeout

Setting	Description	Factory Default
1 to 300	Input the timeout value.	10

When finished, click **Apply** to save your changes.

SNMP Trap Host Settings

SNMP Trap allows an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: **Trap** mode and **Inform** mode. Click **SNMP Trap/Inform** on the menu, and then click **SNMP Trap Host**. Then select the **+** icon on the page.



Configure the following settings.

Create Host Setting

Host IP/Name 0 / 32

Mode *

Trap Community * At least 4 characters 0 / 32

Host IP/Name

Setting	Description	Factory Default
Input a host IP or name, (max. 32 characters)	Specify the name of the primary trap server used by your network.	None

Mode

Setting	Description	Factory Default
Trap V1	Set the trap version to Trap V1.	None
Trap V2c	Set the trap version to Trap v2c.	
Inform V2c	Set the inform version to Inform V2c.	
Trap V3	Set the trap version to Trap V3.	
Inform V3	Set the inform version to Inform V3.	

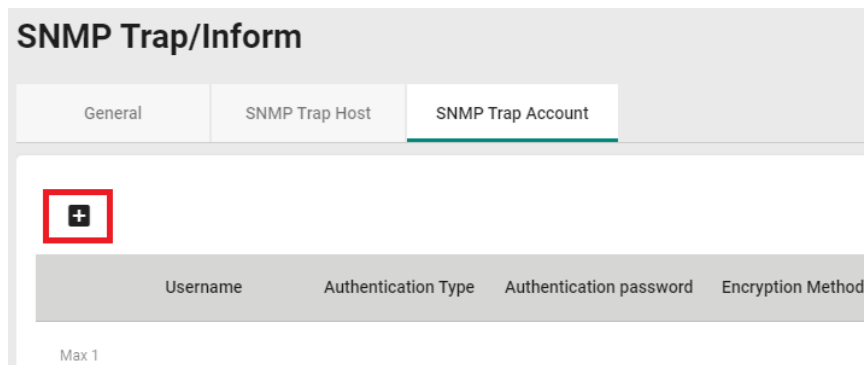
Trap Community

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Specify the community string that will be used for authentication.	None

When finished, click **Create**.

SNMP Trap Account Settings

Click **SNMP Trap/Inform** on the menu, and then click **SNMP Trap Account**. Next click the + icon on the page.



Configure the following settings

Create SNMP Trap Account Setting

Username

At least 4 characters 0 / 32

Authentication Type
None

Encryption Method
Disabled

Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

Authentication type

Setting	Description	Factory Default
None	No authentication type will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

Authentication Password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

Encryption Key

Setting	Description	Factory Default
8 to 64 characters	Enable data encryption.	None

When finished, click **Create**.

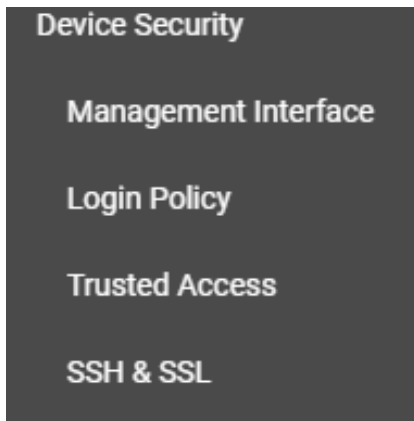
Security

This section describes how to configure **Device Security**, **Network Security**, and **Authentication**.



Device Security

This section includes information about the **Management Interface**, **Login Policy**, **Trusted Access**, and **SSH & SSL** configurations.



Management Interface

Click **Management Interface** on the menu.

Management Interface

HTTP	HTTP - TCP Port *	
Enabled	80	80, 1024 - 65535
<hr/>		
HTTPS	HTTPS - TCP Port *	
Enabled	443	443, 1024 - 65535
<hr/>		
Telnet	Telnet - TCP Port *	
Enabled	23	23, 1024 - 65535
<hr/>		
SSH	SSH - TCP Port *	
Enabled	22	22, 1024 - 65535
<hr/>		
SNMP	SNMP - Transport Layer Protocol	SNMP - UDP Port *
Enabled	UDP	161
<hr/>		
Moxa Service	Moxa Service(Encrypted) - TCP Port	Moxa Service(Encrypted) - UDP Port
Enabled	443	40404
<hr/>		
Maximum number of Login Sessions For HTTP+HTTPS *		
5		
1 - 10		
<hr/>		
Maximum number of Login Sessions For Telnet+SSH *		
1		
1 - 5		

Apply

Configure the following settings.

HTTP

Setting	Description	Factory Default
Enabled	Enable the HTTP connection.	Enabled
Disabled	Disable the HTTP connection.	

HTTP – TCP Port

Setting	Description	Factory Default
80, 1024 - 65535	Specify the HTTP connection port number.	80

HTTPS

Setting	Description	Factory Default
Enabled	Enable the HTTPS connection.	Enabled
Disabled	Disable the HTTPS connection.	

HTTPS – TCP Port

Setting	Description	Factory Default
443, 1024 - 65535	Specify the HTTP connection port number.	443

Telnet

Setting	Description	Factory Default
Enabled	Enable a Telnet connection.	Enabled
Disabled	Disable a Telnet connection.	

Telnet – TCP Port

Setting	Description	Factory Default
23, 1024 - 65535	Specify the Telnet connection port number.	23

SSH

Setting	Description	Factory Default
Enabled	Enable the SSH connection.	Enabled
Disabled	Disable the SSH connection.	

SSH – TCP Port

Setting	Description	Factory Default
22, 1024 - 65535	Input the SSH connection port number.	22

SNMP

Setting	Description	Factory Default
Enabled	Enable the SNMP connection.	Enabled
Disabled	Disable the SNMP connection.	

SNMP – Transport Layer Protocol

Setting	Description	Factory Default
UDP	Select UDP as the transport layer protocol for SNMP.	UDP
TCP	Select TCP as the transport layer protocol for SNMP.	

SNMP – UDP Port

Setting	Description	Factory Default
161, 1024 - 65535	Input the SNMP connection port number.	161

Moxa Service (in Advanced Mode)

Setting	Description	Factory Default
Enabled	Enable Moxa Service.	Enabled
Disabled	Disable Moxa Service.	

NOTE Moxa Service is only for Moxa network management software suite.

Moxa Service (Encrypted) – TCP Port (in Advanced Mode)

Setting	Description	Factory Default
443 (read only)	Enable a Moxa Service TCP port.	443

Moxa Service (Encrypted) – UDP Port (in Advanced Mode)

Setting	Description	Factory Default
40404 (read only)	Enable a Moxa Service UDP port.	40404

Maximum number of Login Sessions for HTTP

Setting	Description	Factory Default
1 to 10	Specify the maximum amount of HTTP login sessions that can happen at the same time.	5

Maximum number of Login Sessions for Telnet

Setting	Description	Factory Default
1 to 5	Specify the maximum amount of Telnet login sessions that can happen at the same time.	1

When finished, click **Apply** to save your changes.

Login Policy

Click **Login Policy** on the menu.

Login Policy

Login Message

0 / 500

Login Authentication Failure Message.

0 / 500

Account Login Failure Lockout
Disabled ▼

Retry Failure Threshold *

1 - 10 times

Lockout Time *

1 - 10 min

Auto Logout Setting *

0 - 1440 min

Apply

Configure the following settings.

Login Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed to users when they log in.	None

Login Authentication Failure Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed when users fail to log in.	None

Account Login Failure Lockout

Setting	Description	Factory Default
Enabled	Enable the lockout function when a user fails to log in.	Disabled
Disabled	Disable the lockout function when a user fails to log in.	

Retry Failure Threshold (times)

Setting	Description	Factory Default
1 to 10	Input the maximum number of retry failure times.	5

Lockout Time (min.)

Setting	Description	Factory Default
1 to 60	Specify the amount of times log in credentials can be entered incorrectly before the user is logged out.	5

Auto Logout Setting (min.)

Setting	Description	Factory Default
0 to 1440	Specify how long a user has to be inactive before getting logged out.	5

When finished, click **Apply** to save your changes.

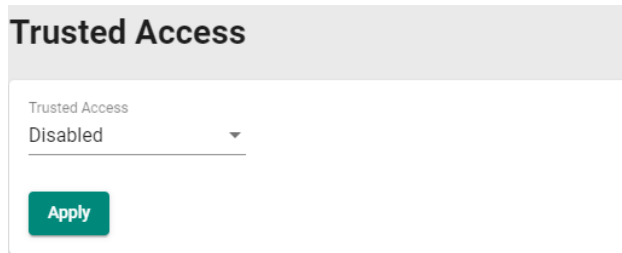
Trusted Access

Trusted Access Overview

Trusted Access is a mechanism that provides a secure connection to Moxa's switch. Users can use this method to allow the connection from the assigned IP address to ensure safe data transmission.

Trusted Access Settings and Status

Click **Trusted Access** on the menu.



Configure the following settings.

Enable

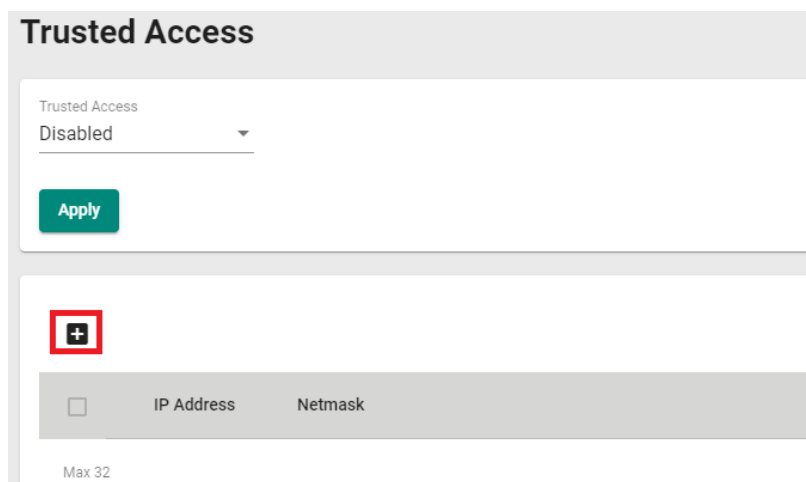
Setting	Description	Factory Default
Enabled	Enable Trusted Access.	Disabled
Disabled	Disable Trusted Access.	

NOTE

1. Trusted Access has to be added before it can be enabled.
2. In order to avoid being disconnected after you enable Trusted Access, you must first add the current IP subnet to Trusted Access. In order to use this function, you should use an RS-232 console to log in or set the device to factory default.

When finished, click **Apply** to save your changes.

Next, click the **+** icon.



Configure the following settings.

IP Address

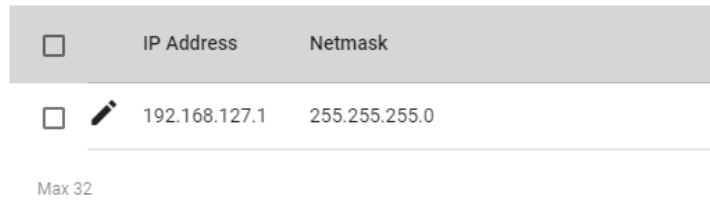
Setting	Description	Factory Default
Input IP address	Specify the IP address that is allowed to connect to Moxa's switch.	None

Netmask

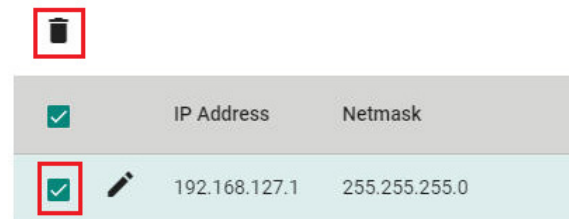
Setting	Description	Factory Default
Input Netmask	Specify the Netmask that is allowed to connect to Moxa's switch.	None

When finished, click **Create**.

You can view the Trusted Access status on the figure below.



To delete the trusted access source, select the item and then click the delete icon on the top of the page.



Click **Delete** to delete the item.

Delete Entry

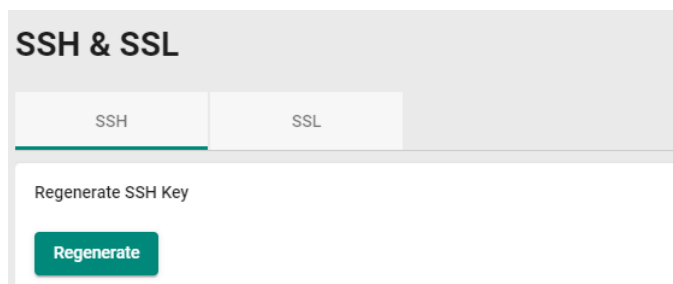
Are you sure you want to delete the selected entry?



SSH & SSL

SSH Key Regeneration

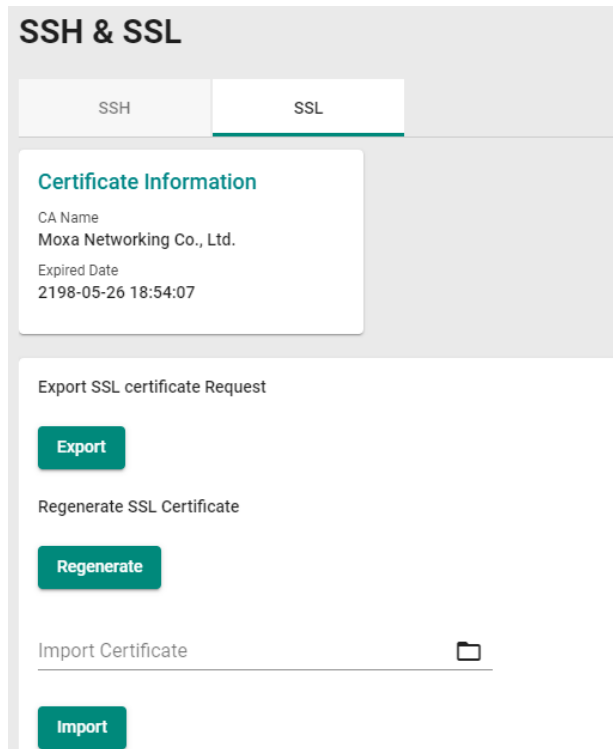
Click **SSH & SSL** on the menu and then select the **SSH** tab.



Click **Regenerate** to regenerate the key.

SSL Certification Regeneration

Click **SSH & SSL** on the menu and select the **SSL** tab. The Certificate Information is shown on this screen.



Configure the following settings.

Export SSL Certificate Request

Setting	Description	Factory Default
Export	Export the SSL certificate to your local computer.	None

Regenerate SSL Certificate

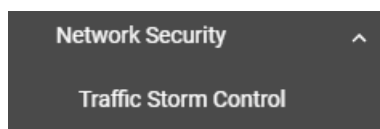
Setting	Description	Factory Default
Regenerate	Regenerate the SSL certificate.	None

Import Certificate

Setting	Description	Factory Default
Select the file	Import the SSL certificate from the location where the SSL certificate is located.	None

Network Security

This section demonstrates how to configure network security settings for **Traffic Storm Control**.



Traffic Storm Control

A traffic storm can happen when packets flood the network; this causes excessive traffic and slows down the network performance. To counter this, Traffic Storm Control provides an efficient design to prevent the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer. The feature can handle packets from both ingress and egress data.

First click **Traffic Storm Control** on the menu, and then click the edit icon on the specific port you want to configure.

Traffic Storm Control

Port	Broadcast	Multicast	Threshold (fps)
1	Enabled	Disabled	13000
2	Enabled	Disabled	13000
3	Enabled	Disabled	13000
4	Enabled	Disabled	13000
5	Enabled	Disabled	13000
6	Enabled	Disabled	13000
7	Enabled	Disabled	13000
8	Enabled	Disabled	13000

Configure the following settings.

Edit Port 1 Setting

Broadcast

Multicast

Threshold *
 i
 625 - 1488100 fps

Copy Config to Ports i

Cancel
Apply

There are two methods that can be used for traffic storm control: Broadcast and Multicast.

Broadcast

Setting	Description	Factory Default
Enabled	Enable Broadcast when a traffic storm occurs.	Disabled
Disabled	Disable Broadcast when a traffic storm occurs.	

Multicast

Setting	Description	Factory Default
Enabled	Enable multicast when a traffic storm occurs.	Disabled
Disabled	Disable multicast when a traffic storm occurs.	

Threshold (fps)

Setting	Description	Factory Default
1 to 1488100	Define the threshold for a traffic storm.	13000

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) you want to have the same configurations for.	None

When finished, click **Apply** to save your changes.

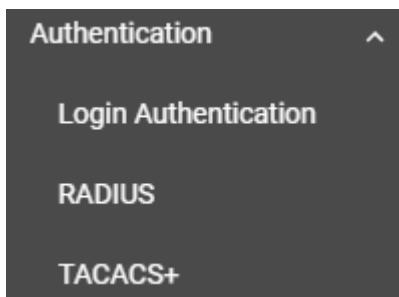
Authentication

This section describes how to configure system authentication including RADIUS and TACACS+. Moxa switches have three different user login authentications: TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service), and Local. The TACACS+ and RADIUS mechanisms are centralized "AAA" (Authentication, Authorization, and Accounting) systems for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

There are five combinations available for users to choose from:

1. **TACACS+, Local:** Check the TACACS+ database first. If checking the TACACS+ database fails, then check the Local database.
2. **RADIUS, Local:** Check the RADIUS database first. If checking the RADIUS database fails, then check the Local database.
3. **TACACS+:** Only check TACACS+ database.
4. **RADIUS:** Only check the RADIUS database.
5. **Local:** Only check the Local database.

This section includes the configurations for **Login Authentication**, **RADIUS**, and **TACACS+**.



Login Authentication

This section allows users to select the login authentication protocol.

Select **Login Authentication**.

Configure the following settings.

Authentication Protocol

Setting	Description	Factory Default
Local	Select Local as the authentication protocol.	Local
RADIUS	Select RADIUS as the authentication protocol.	
TACACS+	Select TACACS+ as the authentication protocol.	
RADIUS, Local	Select RADIUS and Local as the authentication protocol.	
TACACS+, Local	Select TACACS+ and Local as the authentication protocol.	

When finished, click **Apply** to save your changes.

RADIUS

Click **RADIUS** on the menu and configure the following settings.

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1 st server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Input the share key for 1 st server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before timeout.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Define the retry interval when trying to reconnect to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the 2 nd server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 2 nd server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Set the retry interval when trying to reconnect to a server.	1

When finished, click **Apply** to save your changes.

NOTE The RADIUS service will be operated via the 1st server; if it fails, it will run on the 2nd server.

TACACS+

Click **TACACS+** on the menu and then configure the following settings.

TACACS+ Server

Server Address 1 *	TCP Port *
0.0.0.0	49
Share Key	i
Auth Type *	CHAP ▼
Time out *	5
Retry *	1
Server Address 2 *	TCP Port *
0.0.0.0	49
Share Key	i
Auth Type *	CHAP ▼
Time out *	5
Retry *	1

Apply

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1 st server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 1 st server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the 2 nd server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 2 nd server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry

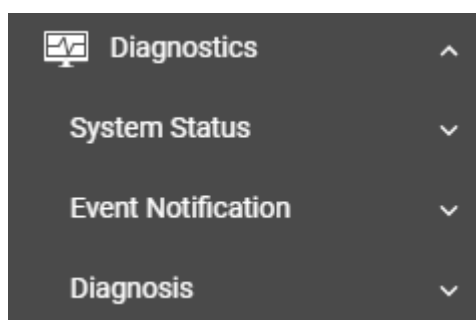
Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

When finished, click **Apply** to save your changes.

NOTE The TACACS+ service will be operated via the 1st server; if it fails, it will run on the 2nd server.

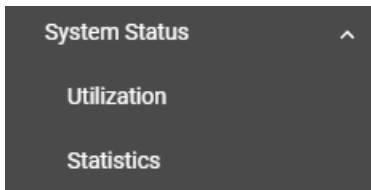
Diagnostics

This section describes the diagnostics functions of Moxa's switch. Click **Diagnostics** on the function menu.



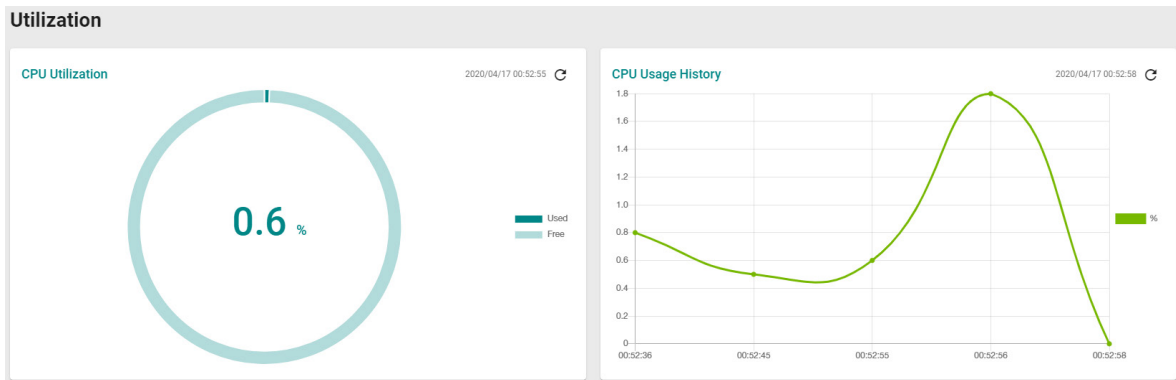
System Status

This section allows users to view the current system status including **Utilization** and **Statistics**.



Utilization

Click **Utilization** on the function menu to view the current utilization status including CPU utilization, memory history, power consumption, and power history. All of the information is displayed via graphics, making it easier for users to view the system status. In addition, a refresh icon is available on the upper right corner of each figure, which allows users to view the latest status for each function.

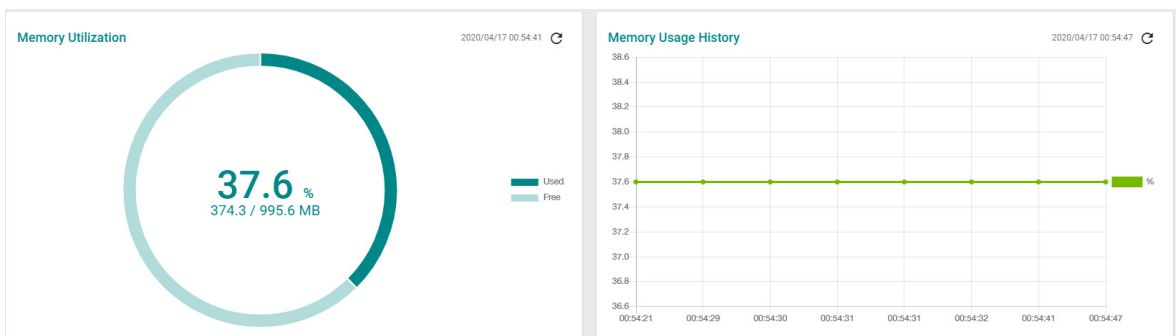


CPU Utilization

Setting	Description	Factory Default
Read-only	Displays the current utilization of the CPU.	None

CPU Usage History

Setting	Description	Factory Default
Read-only	Displays the CPU usage history trend in a chart.	None



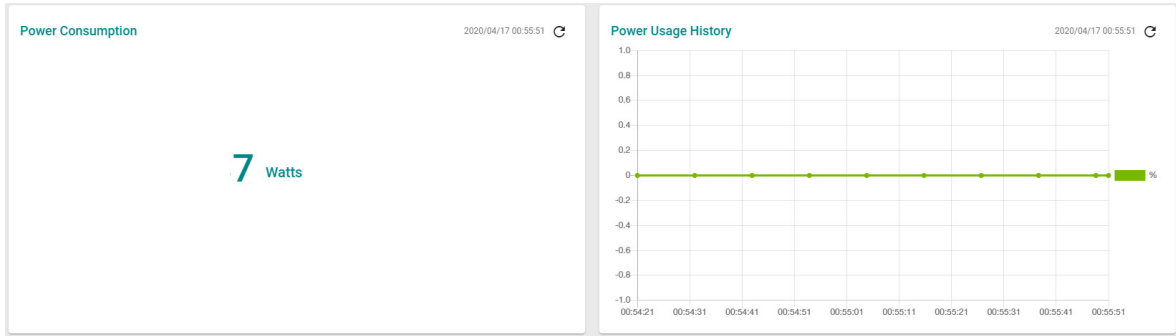
Memory Utilization

Setting	Description	Factory Default
Read-only	Displays the memory status.	None

Memory Usage History

Setting	Description	Factory Default

Read-only	Displays the history of the memory usage.	None
-----------	---	------



Power Consumption (watt)

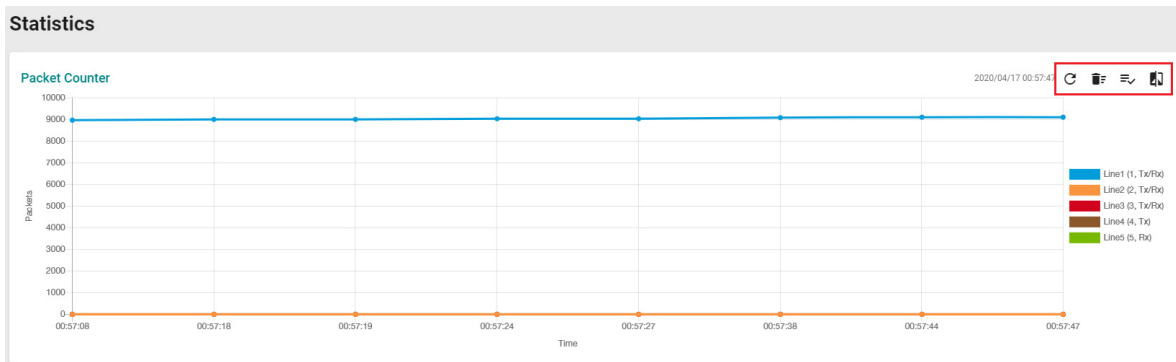
Setting	Description	Factory Default
Read-only	Displays the power consumption status.	None

Power Usage History

Setting	Description	Factory Default
Read-only	Displays the history of the power usage.	None

Statistics




Click **Statistics** on the function menu. The first figure shows the packet counter status.




The status of the different ports will be shown in different colors. A maximum of five ports will have their information displayed.

- Line1 (1, Tx/Rx)
- Line2 (2, Tx/Rx)
- Line3 (3, Tx/Rx)
- Line4 (4, Tx)
- Line5 (5, Rx)

There are four icons on the right upper corner of the page. The table below provides a description for each one.

Item	Name	Description
	Refresh	All statistical data will be refreshed.
	Reset Statistics Graph	The packet counter will be cleared and the graphs will be reset.
	Display Setting	All selected setting items will be shown here.

	Data Comparison	Select the data you want to compare.
---	-----------------	--------------------------------------

Refreshing the Statistics

Click the **Refresh** button and all statistical data will be refreshed immediately.

Resetting Statistics Graph

Click the **Reset** button and select **Clear** to clear the packet counter and reset the graph.

Reset Statistics Graph

Are you sure to clear all graph data?



Display Setting

Click the **Display Setting** icon and all settings will be displayed. You can select the display mode from the drop-down list.

Display Setting

Display Mode *
 Packet Counter ▾

Line 1 Monitoring Port * Line 1 Sniffer *
 1 ▾ Tx/Rx ▾

Line 2 Monitoring Port * Line 2 Sniffer *
 2 ▾ Tx/Rx ▾

Line 3 Monitoring Port * Line 3 Sniffer *
 3 ▾ Tx/Rx ▾

Line 4 Monitoring Port * Line 4 Sniffer *
 4 ▾ Tx ▾

Line 5 Monitoring Port * Line 5 Sniffer *
 5 ▾ Rx ▾



The Monitoring Port is the port you want to view or monitor. The sniffer port is the port that you can choose to view its receiving or transmission status or both.

Display Mode

Setting	Description	Factory Default
Packet Counter	The packet statistics will be displayed.	Packet Counter
Bandwidth Utilization	The bandwidth statistics will be displayed.	

Click **Apply** to complete.

Comparing Data

Click the **Data Comparison** icon and then select the items from the relevant fields.

Data Comparison

Benchmark Line * Benchmark Line - Ti...

Comparison Line * Comparison Line - Ti...

Close

Click **Close** to complete.

The data comparison figure will be shown. Click **Close** to finish.

Data Comparison

Benchmark Line * Benchmark Line - Time *

1, Tx/Rx 00:59:49

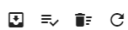
Comparison Line * Comparison Line - Time

2, Tx/Rx 00:59:49

Tx Total Octets	-5088519	↓	∨
Tx Total Packets	-6578	↓	∨
Tx Unicast Packets	-3764	↓	∨
Tx Multicast Packets	-2814	↓	∨
Tx Broadcast Packets	0	↕	∨
Rx Total Octets	-452097	↓	∨
Rx Total Packets	-2899	↓	∨
Rx Unicast Packets	-2241	↓	∨
Rx Multicast Packets	-514	↓	∨
Rx Broadcast Packets	-144	↓	∨

Close

The detailed packet transmission activity for each port can be seen in the table below.



Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets
1	0	0	0	0	0	64462	721
2	0	0	0	0	0	0	0
3	14586450	12132	10042	2090	0	650018	6496
4	0	0	0	0	0	0	0

Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	CRC Align Error Packets	Drop Packets	Undersize	Oversize Packets
0	586	135	0	0	0	0
0	0	0	0	0	0	0
5784	610	134	0	80	0	0
0	0	0	0	0	0	0

Port: port number

Tx Total Octets: Number of octets transmitted including bad packets and FCS octets. Framing bits are not included.

Tx Total Packets: Number of packets transmitted.

Tx Unicast Packets: Number of Unicast packets transmitted.

Tx Multicast Packets: Number of Multicast packets transmitted.

Tx Broadcast Packets: Number of good Broadcast packets transmitted. Multicast packets are not included.

Rx Total Octets: Number of octets received, including bad packets and FCS octets. Framing bits are not included.

Rx Total Packets: Number of packets received.

Rx Unicast Packets: Number of Unicast packets received.

Rx Multicast Packets: Number of Multicast packets received.

Rx Broadcast Packets: Number of good Broadcast packets received. Multicast packets are not included.

CRC Align Error Packets: Number of CRC and Align errors that have occurred.

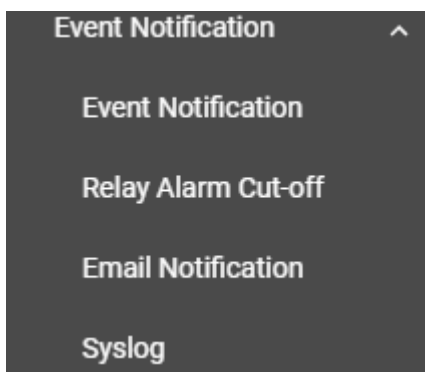
Drop Packets: Number of packets that were dropped.

Undersize: Number of undersized packets (less than 64 octets) received.

Oversize Packets: Number of oversized packets (over 1518 octets) received.

Event Notification

This section includes the information regarding **Event Notification**, **Relay Output**, **Email Notification**, and **Syslog**.



Event Notification

There are two functions within Event Notification: System and Function, and Port.

In the **Event Notification** menu, click the **System and Function** tab, and then click the edit icon on the specific event you want to configure. For example, select the edit icon for warm start when the switch reboots.

Group	Event Name	Enabled	Severity	Registered Action
General	Warm start	Enabled	Notice	Trap, Email
General	Password changed	Enabled	Notice	Trap, Email
General	Login success	Enabled	Notice	Trap, Email
General	Configuration changed	Enabled	Notice	Trap, Email
General	Configuration imported	Enabled	Notice	Trap, Email

Configure the following settings.

Edit Event Notification

Event Name
Warm start

Enabled
Enabled

Registered Action
Trap, Email

Cancel **Apply**

Enable

Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

Registered Action

Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	
Relay	Trigger Relay for event notifications.	

When finished, click **Apply** to save your changes.

In addition, use the same method to edit other events, such as login lockout, warm start, password changed, etc.

Next, in the **Event Notification** menu, click the **Port** tab, and then click the edit icon on the specific port status on **Event Name**. For example, select the edit icon for event notifications when the port status is on.

Event Notification					
System and Function		Port			
Event Name	Enable	Severity	Registered Action	Registered Port	
Port On	Enabled	Notice	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8	
Port Off	Enabled	Notice	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8	

Configure the following settings.

Edit Event Notification

Event Name
Port On

Enabled
Enabled

Registered Action
Trap, Email

Registered Port
All Ports

Cancel

Apply

Enable

Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

Registered Action

Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	
Relay	Trigger Relay for event notifications.	

Registered Port

Setting	Description	Factory Default
Select port(s) from the drop-down list	Specify the port(s) that use the registered action.	All Ports

When finished, click **Apply** to save your changes.

In addition, use the same method to edit other events such as, port status is off, port shutdown by port security, and port recovery by rate limit, etc.

Check the following table for the severity degree of each event.

System & Function	
Event Name	Severity
Cold start	Critical
Warm start	Notice
Configuration changed	Notice
Login success	Notice
Login fail	Warning
Login lockout	Warning
Account setting changed	Notice
Configuration imported	Notice
SSL certification changed	Notice
Log capacity threshold	Warning
Password changed	Notice
PWR Off->On	Notice
PWR On->Off	Notice
DI On	Notice
DI Off	Notice
RSTP topology changed	Warning
LLDP table changed	Information

Port	
Event Name	Severity
Port On	Notice
Port Off	Notice

Relay Output Overview

A relay is an electrically operated switch that often uses an electromagnet to mechanically operate a switch. Relays are used to control a circuit by a separate low-power signal, or where several circuits must be controlled by one signal. This is typically safe when the problem or malfunction occurs in a remote device.

Relay Alarm Cut-off

This function helps you cut off the relay alarm.

Relay Alarm Cut-off

Relay

Apply

Relay

Setting	Description	Factory Default
Relay	Cut off the relay alarm.	None

When finished, click **Apply** to save your changes.

Email Notification

Select **Email Notification** on the function menu and configure the following settings.

Email Notification

Mail Server *
0.0.0.0 7 / 60

TCP Port
25 1 - 65535

Username 0 / 60 Password 0 / 60

TLS Enable
Disabled ▼

Sender Address
admin@localhost.com 19 / 60

1st Recipient Email Add... 0 / 60 2nd Recipient Email Ad... 0 / 60 3rd Recipient Email Add... 0 / 60

4th Recipient Email Add... 0 / 60 5th Recipient Email Add... 0 / 60

Apply

Mail Server

Setting	Description	Factory Default
IP address or URL	The IP Address or URL of the email server.	0.0.0.0

TCP Port

Setting	Description	Factory Default
1 to 65535	The TCP port number of your email server.	25

User Name

Setting	Description	Factory Default
Max. of 60 characters	Your email account name.	None

Password

Setting	Description	Factory Default
Max. of 60 characters	Your email account password.	None

TLS Enable

Setting	Description	Factory Default
Enabled	Enable TLS (Transport Layer Security).	Disabled
Disabled	Disable TLS (Transport Layer Security).	

Sender Address

Setting	Description	Factory Default
Max. 60 characters	The sender's email address.	admin@localhost

1st to 5th Email Addresses

Setting	Description	Factory Default
Max. of 60 characters	You can set up to five email addresses to receive alert emails from the Moxa switch.	None

When finished, click **Apply** to save your changes.

Syslog Settings

Click **Syslog** on the function menu and configure the following settings.

Syslog

Syslog
 Disabled ▼

Syslog Server 1
 Disabled ▼

Address 1 UDP Port
 514
1 - 65535

Syslog Server 2
 Disabled ▼

Address 2 UDP Port
 514
1 - 65535

Syslog Server 3
 Disabled ▼

Address 3 UDP Port
 514
1 - 65535

Apply

Logging Enable

Setting	Description	Factory Default
Enabled	Enable logging.	Disabled
Disabled	Disable logging.	

Syslog Server 1

Setting	Description	Factory Default
Enabled	Enable the 1 st log server.	Disabled
Disabled	Disable the 1 st log server.	

Address 1

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog 1 st server that is used by your network.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

Syslog Server 2

Setting	Description	Factory Default
Enabled	Enable the 2 nd syslog server.	Disabled
Disabled	Disable the 2 nd syslog server.	

Address 2

Setting	Description	Factory Default
IP Address	Input the IP address of Syslog 2 nd server that is used by your network.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

Syslog Server 3

Setting	Description	Factory Default
Enabled	Enable the 3 rd syslog server.	Disabled
Disabled	Disable the 3 rd syslog server.	

Address 3

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog 3 rd server that is used by your network.	None

UDP Port

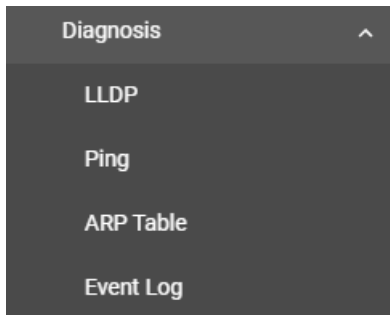
Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

When finished, click **Apply** to save your changes.

NOTE If the syslog server cannot receive the previous logs, it is possible that the receiving port of the syslog server is not ready. We suggest you enable the Linkup Delay function to delay the log delivery time.

Diagnosis

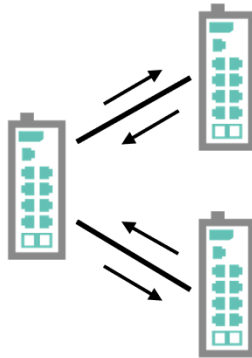
This section explains the configurations for system diagnoses such as **LLDP**, **Ping**, **ARP Table**, and **Event Log**.



LLDP Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. With SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.

From the switch's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview to automatically display the network's topology and system setup details, such as VLAN and Trunking for the entire network.



LLDP Settings and Status

Click **LLDP** on the menu and then select the **Setting** tab to configure the following settings.

LLDP

Setting

Status

LLDP

Transmit Interval: sec.

Holdtime Multiplier: times

LLDP

Setting	Description	Factory Default
Enabled	Enable LLDP.	Enabled
Disabled	Disable LLDP.	

Transmit Interval (sec.)

Setting	Description	Factory Default
5 to 32768	Set the transmit interval of LLDP messages	30

When finished, click **Apply** to save your changes.

Each port for the LLDP settings can also be configured. Select the edit icon for the port you want to configure.

Port	Port Status
1	Tx and Rx
2	Tx and Rx
3	Tx and Rx
4	Tx and Rx

Configure the following settings.

Edit Port 1 Setting

Port Status

Copy Config to Ports

Cancel

Port Status

Setting	Description	Factory Default
Tx Only	Set Tx as the port status.	Tx and Rx
Rx Only	Set Rx as the port status.	
Tx and Rx	Set both Tx and Rx as the port status.	

Copy Config to Port

Setting	Description	Factory Default
Select the port from the list	Copy the same configurations to other port(s).	None

When finished, click **Apply** to save your changes.

To view the LLDP status, click the **Status** tab on the LLDP page, and the status of all LLDP will be shown on the page.

LLDP

Setting
Status

Local Information

Enable
Enabled

Chassis ID
00:90:e8:11:22:42

Local Timer

Transmit Interval
30 (sec)

Holdtime Multiplier
4 (x)

Refer to the following table for the detailed description of each item.

Local Information	
Enable	Show if LLDP has been enabled or disabled.
Chassis ID	Show the chassis ID.
Local Timer	
Transmit Interval (sec.)	The interval between regular LLDP packet transmissions.
Holdtime Multiplier	The amount of time that the receiving device holds an LLDP packet before discarding it.

To view the LLDP status for a specific port, click the detailed information icon on the port. All information will be shown on the right side of the page.

LLDP

Setting
Status

Local Information

Enable
Enabled

Chassis ID
00:90:e8:11:22:31

Local Timer

Transmit Interval
30 (sec.)

Holdtime Multiplier
4 (times)

🔄 📄
🔍 Search

Port	Tx Status	Rx Status	Neighbor Port ID	Neighbor Chassis ID
1	Enabled	Enabled	00:60:6e:ba:ba:0b	00:60:6e:ba:ba:0b
2	Enabled	Enabled		
3	Enabled	Enabled		
4	Enabled	Enabled		

Detailed Information

Port Local Interface

Port ID SubType
Local

Port ID
1

Port Description
Ethernet Interface Port 1

Port Traffic Statistics

Total Frames Out
96

Total Entries Aged
0

Total Frames In
6

Total Frames Received In Error
0

Total Frames Discarded
0

Total TLVS Unrecognized
1

Ping

The **Ping** function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function most unique feature of the function is that even though the ping command is entered from the user's PC, the actual ping command originates from the Moxa switch itself. This allows the user to essentially sit on top of the Moxa switch and send ping commands out through its ports.

To use the Ping function, click **Ping** on the menu, and enter the IP address or domain name you want to ping. After clicking **Ping**, the result will be shown.

ARP Table

To view the ARP Table, select **ARP Table** and the information will be displayed.

Index	IP Address	MAC Address
1	192.168.127.199	00:60:6e:ba:ba:0b

Max. 2000

Event Log

To edit the event log overseize-action, click **Event Log** on the menu, and then select **Event Log** on the page.

Configure the following settings when the event log file is full.

Oversize-Action

Setting	Description	Factory Default
Overwrite the oldest event log	Overwrite the oldest event log.	Overwrite the oldest event log
Stop recording event log	Disable Port Mirror for this port.	

Click **Apply** to finish.

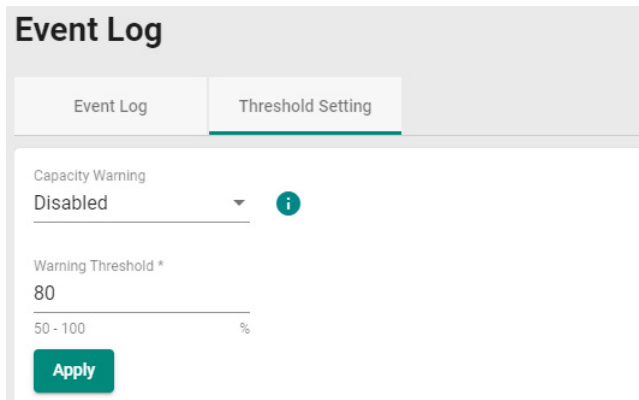
To view all of the event formation, check the lower part of the event log page.



Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	3	Notice	2016-11-03 17:17:24	0d0h0m50s	[Account:admin] successfully logged in via local.
2	3	Critical	2016-11-03 17:17:09	0d0h0m35s	System has performed a cold start.
3	3	Info	2016-11-03 17:17:00	0d0h0m26s	LLDP remote table changed.
4	3	Notice	2016-11-03 17:17:00	0d0h0m26s	Port 1/3 link up.
5	3	Notice	2016-11-03 17:16:46	0d0h0m11s	The hardware revision of Power Module 2 is not allowed.
6	2	Notice	2016-11-05 13:54:16	1d20h37m43s	[Account:admin] successfully logged in via local.
7	2	Notice	2016-11-05 13:49:37	1d20h33m3s	[Account:admin] successfully logged in via local.
8	2	Info	2016-11-05 13:47:33	1d20h31m0s	LLDP remote table changed.
9	2	Notice	2016-11-05 13:47:33	1d20h30m59s	Port 1/3 link up.
10	2	Notice	2016-11-05 13:47:23	1d20h30m50s	Port 1/1 link down.
11	2	Notice	2016-11-05 13:47:16	1d20h30m42s	Configuration [Mgmt IP] changed by admin.
12	2	Notice	2016-11-03 17:30:01	0d0h13m28s	Configuration [Account] changed by admin.
13	2	Notice	2016-11-03 17:28:55	0d0h12m22s	[Account:admin] successfully logged in via local.
14	2	Notice	2016-11-03 17:19:52	0d0h3m19s	[Account:admin] successfully logged in via local.
15	2	Notice	2016-11-03 17:19:30	0d0h2m57s	Configuration [Web] changed by admin.
16	2	Notice	2016-11-03 17:18:53	0d0h2m19s	Configuration [Web] changed by admin.

Threshold Settings

To configure the event log threshold, click the **Threshold Setting** tab on the Event Log Page. The event log threshold can be set up to send an early warning when the event log entries have reached the percentage of the threshold. The maximum recorded event log entries is 10,000.



Configure the following settings.

Capacity Warning

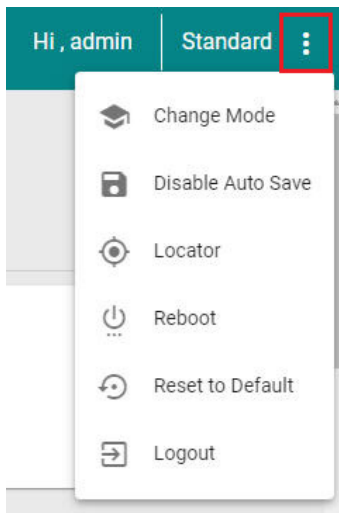
Setting	Description	Factory Default
Enabled	Enable capacity warning event log.	Disabled
Disabled	Disable capacity warning event log.	

Warning Threshold (%)

Setting	Description	Factory Default
50 to 100	Set the warning threshold as a percentage.	80

Maintenance and Tool

This section explains how to maintain Moxa’s switch and the tools that help users operate the switch. Click the icon on the upper right corner of the page.

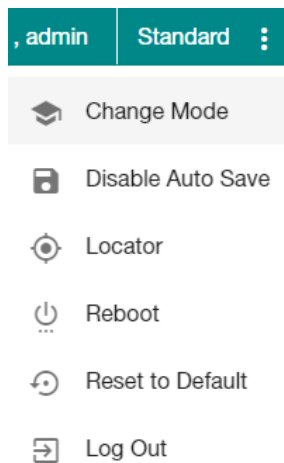


Standard/Advanced Mode

There are two configuration modes available for users: **Standard Mode** and **Advanced Mode**.

1. In **Standard Mode**, some of the features/parameters will be hidden to make it easier to perform configurations (this is the default setting).
2. In **Advanced Mode**, some advanced features/parameters will be available for users to adjust these settings.

To switch to Advanced Mode, click the change mode icon on the upper right corner of the page, and then select **Change Mode**.



Click **Change** to change to **Advanced Mode**.

Change to Advanced mode

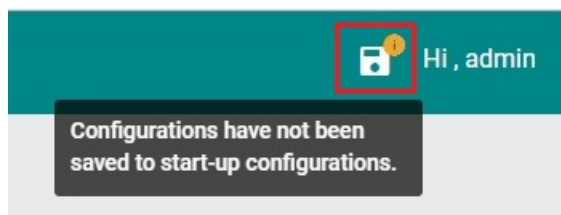
Are you sure you want to change from Standard mode to Advanced mode?



Advanced Mode offers more detailed system configurations for specific functions. Use the same process if you want to return to Standard Mode.

Disable Auto Save

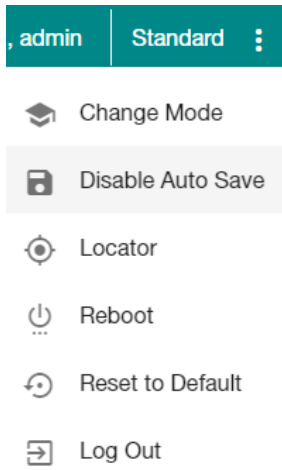
Auto Save allows users to save the settings to the start-up configurations; all parameters will be effective when applied immediately, even when the switch has restarted. When users select **Disable Auto Save**, all parameters will be temporarily stored in the running config (memory), and a disk icon will appear on the upper right corner of the page. Users need to save the running-configuration to the startup-configuration when changing any parameters or function after clicking **Apply**.



It is highly recommended that you always manually save all configurations by clicking Save Disk icon when **Disable Auto Save** is applied, or all information will have disappeared after the switch has restarted.

When **Disable Auto Save** is applied, only the configurations that are running will be saved; users can unplug the power or perform a warm start to recover the network before manually saving the configurations. When Auto Save is enabled, the start-up configurations will be saved in the switch.

To disable the **Auto Save** function, click **Disable Auto Save** in the menu.



Click **Disable**.

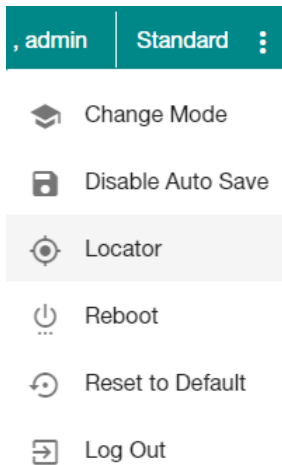
Disable auto save mode

Are you sure you want to disable auto save mode?



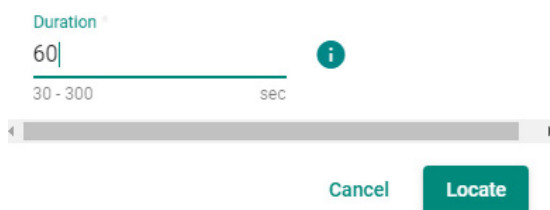
Locator

Users can trigger the device locator by clicking this icon. This will cause the LED indicators on the switch to flash for one minute. This helps users easily find the location of the switch in a field site.



Click **Locate** to finish.

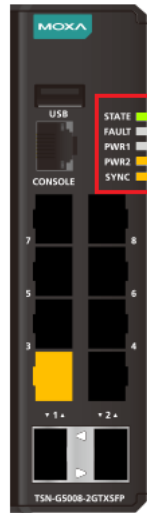
Switch Locator



Duration (sec.)

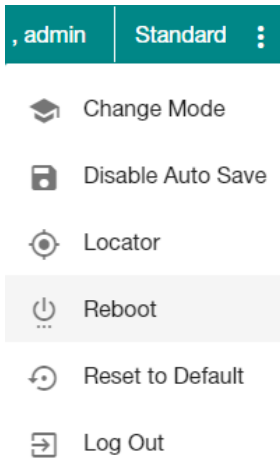
Setting	Description	Factory Default
30 to 300	Specify the length of time the indicators will remain flashing.	60

Click **Locate** to activate the switch locator. The LED indicators are located on the upper right corner of the switch, where **STATE**, **FAULT**, and **SYNC** will keep flashing.



Reboot

To reboot the device, select **Reboot**.



Click **Restart** to reboot the device.

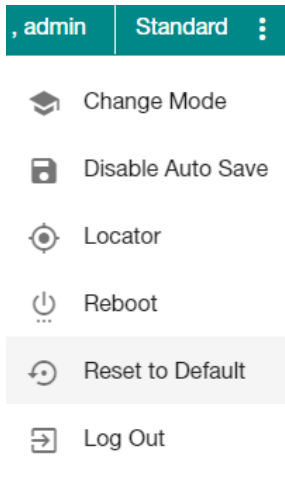
Restart the device

Are you sure you want to restart the device?



Reset to Default

To reset the switch to the default status, select **Reset to Default**.



To return the switch to factory default settings, click **Reset**.

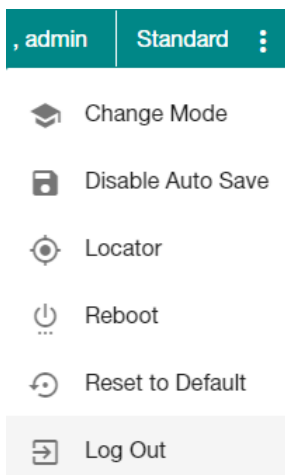
Factory default

Are you sure you want to reset the system configurations to factory default?



Log Out of the Switch

To log out of the switch, select **Log Out**.



Click **Log Out** to log out of the switch.

Logout

Are you sure you want to logout?



A

Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switches.

The following topic is covered in this appendix:

- **Account Privileges List**

Account Privileges List

This appendix lists the privileges for different account roles.

Please note, **R** stands for **Read** and **W** stands for **Write**.

Function	Account Privilege		
	Admin	Supervisor	User
Information Setting	R/W	R/W	R
Firmware Upgrade	Execute	No Access	No Access
Configuration Backup and Restore	Execute	Execute	No Access
Event log backup	Execute	Execute	Execute
User Account	R/W	No Access	No Access
Password Policy	R/W	No Access	No Access
IP Configuration	R/W	R/W	R
DHCP Server	R/W	R/W	R
Time Zone	R/W	R/W	R
System Time	R/W	R/W	R
Port			
Port Setting	R/W	R/W	R
VLAN			
IEEE 802.1Q	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
Multicast			
Static Multicast	R/W	R/W	R
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Network Management			
SNMP	R/W	No Access	No Access
SNMP Trap/Inform	R/W	No Access	No Access

System	Admin	Supervisor	User
Security			
Management Interface	R/W	R/W	R
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	Execute	Execute	No Access
Traffic Storm Control	R/W	R/W	R
Authentication			
RADIUS	R/W	No Access	No Access
TACACS+	R/W	No Access	No Access
Login Authentication	R/W	No Access	No Access
Diagnostics			
Event Notification	R/W	R/W	R
Relay Alarm Cut-off	R/W	R/W	R
Email Notification	R/W	R	R
Syslog	R/W	R	R
Event Log	R/W	R/W	R
LLDP	R/W	R/W	R
Ping	Execute	Execute	Execute
ARP Table	R/W	R/W	R
Utilization	R	R	R
Statistics	R	R	R
Maintenance and Tool			
Standard/Advanced Mode	Execute	Execute	Execute
Disable Auto Save	R/W	R/W	R
Locator	R/W	R/W	Execute
Reboot	Execute	Execute	No Access
Reset to default	R/W	No Access	No Access

B

Event Log Description

This appendix describes all of the information for the event logs. When an event occurs, it will be recorded in the event log files. Users can check the event log name and its event log description.

The following topic is covered in this appendix:

- **Event Log Description**

Event Log Description

Event Log Name	Event Log Description
Login success	[Account:{{user_name}}] successfully logged in via {{interface}}.
Login fail	[Account:{{user_name}}] log in failed via {{interface}}.
Login lockout	[Account:{{user_name}}] locked due to {{failed_times}} failed login attempts.
Account setting changed	Account settings of [Account:{{user_name}}] has been updated. Account settings of [Account:{{user_name}}] has been deleted. Account settings of [Account:{{user_name}}] has been created.
SSL Certification changed	SSL certificate has been changed. SSL certificate has been regenerated.
Password changed	The password of [Account:{{user_name}}] has been changed.
Cold start	The system has performed a cold start.
Warm start	The system has performed a warm start.
Configuration Changed	Configurations {{modules}} have been changed by [Account:{{user_name}}].
Configuration Imported	Configuration import has {{'successful'/'failed'}} by [Account:{{user_name}}].
Log capacity threshold	The threshold of event log entries {{numbers}} has been reached.
PWR On	Power {{index}} has turned on.
PWR Off	Power {{index}} has turned off.
DI On	Digital Input {{index}} has turned on.
DI Off	Digital Input {{index}} has turned off.
Port link up	Port {{number}} link up.
Port link down	Port {{number}} link down.
Topology Changed (RSTP)	Topology has been changed by RSTP.
LLDP Table Changed	LLDP remote table changed.
Relay Override Message	Relay alarm is on due to {{Event Name}}.
SSH Key Generate	SSH key has been regenerated.
Configuration Export	Configuration export {{successful /failed}} by [Account:{{user_name}}].
FWR upgrade success	Firmware Successfully Upgraded.
Relay Cut Off	{relay_name} relay alarm has been cut off.
TACACS+ Auth. Success	[Account:{{user_name}}] successfully logged in via {{interface}}.
TACACS+ Auth. Fail	[Account:{{user_name}}] log in failed via {{interface}}.
RADIUS Auth. Success	[Account:{{user_name}}] successfully logged in via {{interface}}.
RADIUS Auth. Fail	[Account:{{user_name}}] log in failed via {{interface}}.

C

SNMP MIB File

This appendix contains the SNMP MIB file for the managed switch.

The following topics are covered in this appendix:

- **Standard MIB Installation Order**
- **MIB Tree**

Standard MIB Installation Order

If you need to import the MIB one-by-one, please install the MIBs in the following order.

1. RFC1213-MIB.mib
2. SNMP-FRAMEWORK-MIB.mib
3. SNMPv2-SMI.mib
4. SNMPv2-TC.mib
5. SNMPv2-CONF.mib
6. SNMPv2-MIB.mib
7. IANAifType-MIB.mib
8. IF-MIB.mib
9. EtherLike-MIB.mib
10. BRIDGE-MIB.mib
11. RMON2-MIB.mib
12. INET-ADDRESS-MIB.mib
13. IEEE8021-TC-MIB.mib
14. IEEE8021-SPANNING-TREE-MIB.mib
15. IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
16. LLDP-MIB.mib

MIB Tree

Refer to the following content for the MIB Tree structure.

```

iso(1)
|-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)
    |-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
|-org(3)
|-dod(6)-internet(1)
    |-mgmt(2)-mib-2(1): SNMPv2-MIB.mib
        |-system(1): RFC1213-MIB.mib
            |-interface(2): RFC1213-MIB.mib
                |-at(3): RFC1213-MIB.mib
                |-snmp(11): RFC1213-MIB.mib
                |-dot1dBridge(17): BRIDGE-MIB.mib, Q-BRIDGE-MIB.mib
                |-ifMIB(31): IF-MIB.mib
                |-etherMIB(35): EtherLike-MIB.mib
|-private(4)-moxa(8691)
    |-product(600): mxGeneralInfo.mib, mxProductInfo.mib,
    |-general(602): mxGeneral.mib, mxDeviceIo.mib, mxDhcpSvr.mib, mxEmailC.mib,
        mxEventLog.mib,
        :mxGene.mib, mxLocator.mib, mxManagementIp.mib,
        mxPorte.mib,
        : mxRelayC.mib, mxSnmp.mib, mxSwe.mib, mxSysLoginPolicySvr.mib,
        : mxSyslogSvr.mib, mxSysPasswordPolicySvr.mib, mxSystemInfo.mib,
        : mxSysTrustAccessSvr.mib, mxSysUtilSvr.mib, mxTimeSetting.mib,
        : mxTimeZone.mib, mxTrapC.mib, mxUiServiceMgmt.mib
    |-switching(603): mxSwitching.mib
        |- portInterfacce : mxPort.mib
        |- basicLayer2: mxLhc.mib, mxQos
        |- layer2Redundancy: mxRstp.mib, mxTrv2.mib,
        |- layer2Security: mxStcl.mib
        |- layer2Diagnostic: mxLldp.mib, mxTcst.mib
        |- layer3Diagnostic
        |- layer2Multicast
        |- layer3Multicast
    |-snmpV2(6)-snmpModules(3)
        |-snmpFrameworkMIB(10): SNMP-FRAMEWORK.mib
|-ieee(111)-standards-association-numbers-series-standards(2)-lan-man-stds(802)-ieee802dot1(1)-

```

ieee802dot1mibs(1)-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib