Hardened Managed Ethernet Switch

SmartE Series

User Manual

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at:

www.etherwan.com

Products Supported by this Manual:

SmartE Series Switches

Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
A	1	04/20/2021	First version of document.
A	2	08/10/2021	Added to page 41: "If the 'Large Tree Support' function is enabled, we recommend using the default parameters."
A	3	08/20/2021	Added information to Mode Table on page 8 and description on page 9.
A	4	09/02/2021	Deleted MRP commands
A	5	03/10/2022	Added information on LDAP Rolename, Radius Management Privilege Level & other minor changes. (Firmware version 3.1)
B	1	03/27/2023	Revised for new firmware V3.21; Add MRP.

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
ℹ	Note	Notes emphasize or supplement important points of the main text.
💡	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Warning	Warnings indicate that failure to take a specified action could result in damage to the device, or could result in serious bodily injury.

Contents

Introduction

SmartE Series

The SmartE series is a portfolio of hardened managed Ethernet switches. SmartE offers a key set of Layer 2 management features that are perfect for supporting network connectivity for edge applications even in extreme environments. With a wide range of models available in both Fast Ethernet and Gigabit Ethernet configurations, offering up to 16 Ethernet ports and 2 optional SFP ports for network expansion, the SmartE series provides a reliable and cost-effective network management solution for critical applications.

Before you install and use this product, please read this manual in detail.

Mode Setting

With mode setting, you can change the operating mode of the switch, without having access to one of the management interfaces.

Press the Mode button to enter mode setting, select the desired setting, and exit Mode setting. The four Mode LEDs indicate the setting that is currently selected, which will be applied when exiting mode setting.

The following setting options can be selected via Smart mode:

- Reset to factory default values
- Operate with a fixed IP address
- Reset the IP configuration
- Operate in unmanaged mode
- Exit mode selection without changes

Entering Mode Setting

At the bottom right of the front face there is a Mode button. To select an operating mode, power up the switch. When the LEDs of all ports go out, press the mode button for more than ten seconds. The four LEDs of ports 1 and 2 will flash, indicating that the device is ready for mode selection. The active state is then identified by the combination of the four flashing LEDs.

When the mode selection is started, the initial state is “Exit mode selection without changes.” Select the desired mode by pressing the mode button.

Mode	Description	Link/Act LED of Port 1	Link Speed LED of Port 1	Link/Act LED of Port 2	Link Speed LED of Port 2
Initial State	Exit mode selection without changes	On	Off	Off	Off
Mode 1	Reset to factory default values	Off	On	Off	Off
Mode 2	Operate with a fixed IP address	Off	On	On	Off
Mode 3	Reset the IP configuration	On	On	On	Off
Mode 4	Operate in unmanaged mode	Off	On	Off	On

To exit the selected mode, press and hold down the MODE button for at least five seconds. The selected operating mode will then be saved and activated as soon as you release the MODE button.

Mode descriptions:

Mode 1 – Reset to factory default values: When activated, all switch settings and configurations will be reset to factory defaults.

Mode 2 – Operate with a fixed IP address: This is the default setting for the switch. – DHCP server is activated to assign IP to connected PC, and device has a fixed IP: 192.168.0.254.

Mode 3 – Reset the IP configuration: Reset IP to default IP 192.168.1.10, subnet mask and default gateway to 0.0.0.0 only, but not reset stored configurations.

Mode 4 – Operate in unmanaged mode: The switch can be used without an IP address. The switch adopts the static IP address 0.0.0.0. The subnet mask and gateway are also 0.0.0.0. In this mode, web-based management can no longer be accessed, and the switch no longer sends BootP and DHCP requests.

The following main Layer 2 management features can be active in Unmanaged mode, but require a few configuration steps in the web GUI before setting the SmartE device to Unmanaged mode.

- Redundancy mechanisms (RSTP, LTS, FRD)
- Broadcast/multicast limiter
- IGMP snooping

ℹ Use of IGMP in Unmanaged mode is limited to IGMP snooping. The switch requires an IP address if the device is also to be used as an IGMP querier.

ℹ The device can only exit unmanaged mode by switching to a different mode or by resetting the switch to the factory default settings.

BootP

The device uses the BootP protocol for IP address assignment. Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment.

Notes on BootP

During initial startup, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests.

After a restart, the device sends three BootP requests and will only then adopt the old IP address if there is no BootP response.

Management Using the Web Interface

The web interface allows for remote monitoring, configuration, and control of the switch through any standard web browser. All switch features that can be configured through the Command Line Interface can also be configured through the web interface.

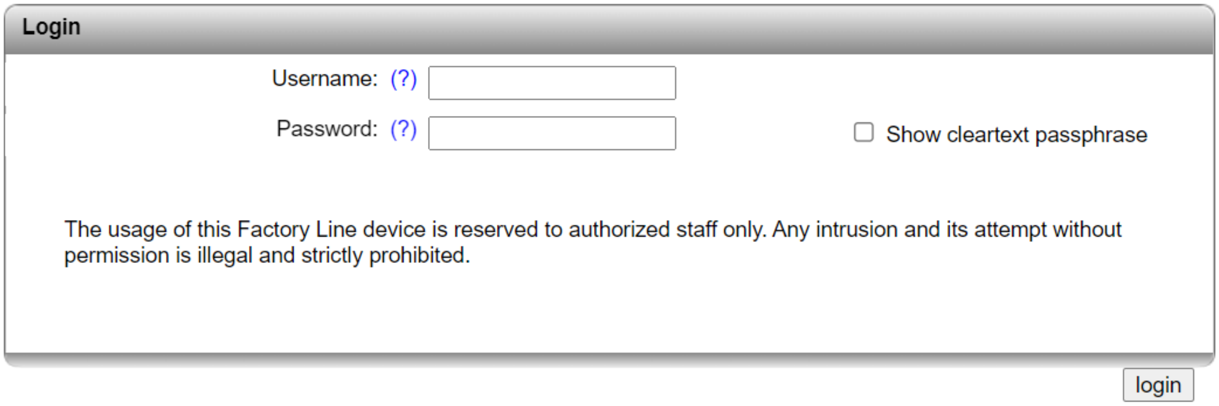
Default IP Address

The switch's default IP address is 192.168.1.10. The management computer must be set up so that it is on the same network as the switch. For example, the IP address of the management computer can be set to 192.168.1.100 with a subnet mask of 255.255.255.0. DHCP is disabled by default.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL into the address field of the browser and hit return.

- The Default Login is **root** (case sensitive)
- There is no password by default
- Enter the login name and click the Login button



The usage of this Factory Line device is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.

⚠ It is highly recommended that you change the default password when you first set up the switch. Use a secure password with adequate complexity.

ℹ Cookies must be enabled in the web browser in order to use web management.

ℹ Depending on the configuration of the device, a user account may be locked for a period of time after a certain number of failed login attempts. During this time, it is not possible to access web management, even if the correct user data is entered (see "User Management").

Layout of Web Management Interface

The web management interface is divided into three sections:

- Information: General device information
- Configuration: Device configuration
- Diagnostics: Device-specific diagnostics

The contents of each section are as follows:

Information

- Help & Documentation
- Device Status
- Local Diagnostic
- Alarm & Events
- Port Table
- MAC Address Table

Configuration

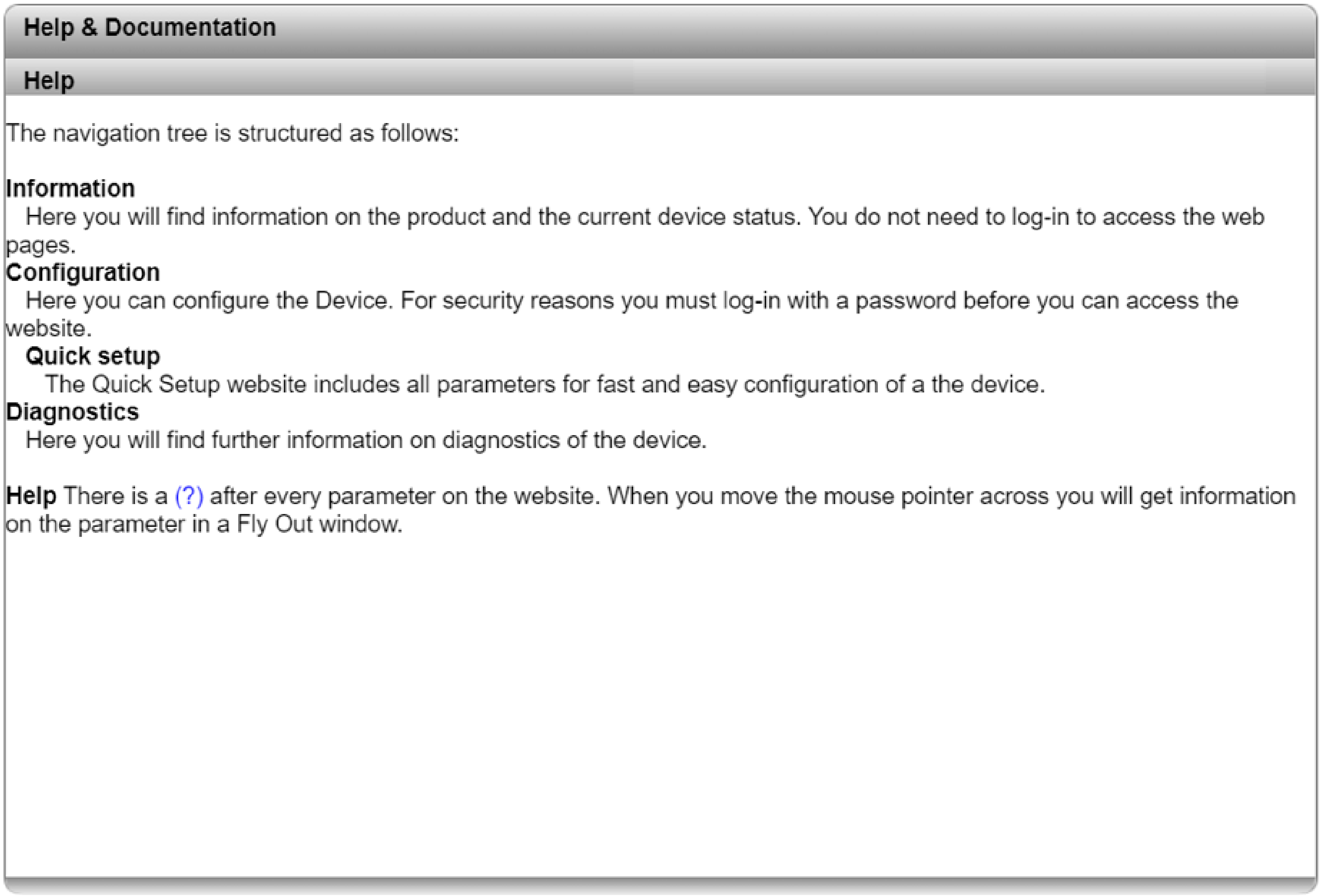
- My Profile
- User Management
- System
- Quick Setup
- Network
- Service
- Port Configuration
- VLAN Configuration
- Multicast Filtering
- Network Redundancy
- Security
- DHCP Service
- Local Events
- Quality of Service

Diagnostics

- LLDP Topology
- RSTP Diagnostic
- MRP Diagnostic
- Current VLANs
- Current Multicast Groups
- Port Mirroring
- Trap Manager
- Port Counter
- Port Utilization
- Snapshot
- Syslog
- SFP Diagnostics

Information - Help & Documentation

Here you will find useful information about using web-based management.



The navigation tree is structured as follows:

Information
Here you will find information on the product and the current device status. You do not need to log-in to access the web pages.

Configuration
Here you can configure the Device. For security reasons you must log-in with a password before you can access the website.

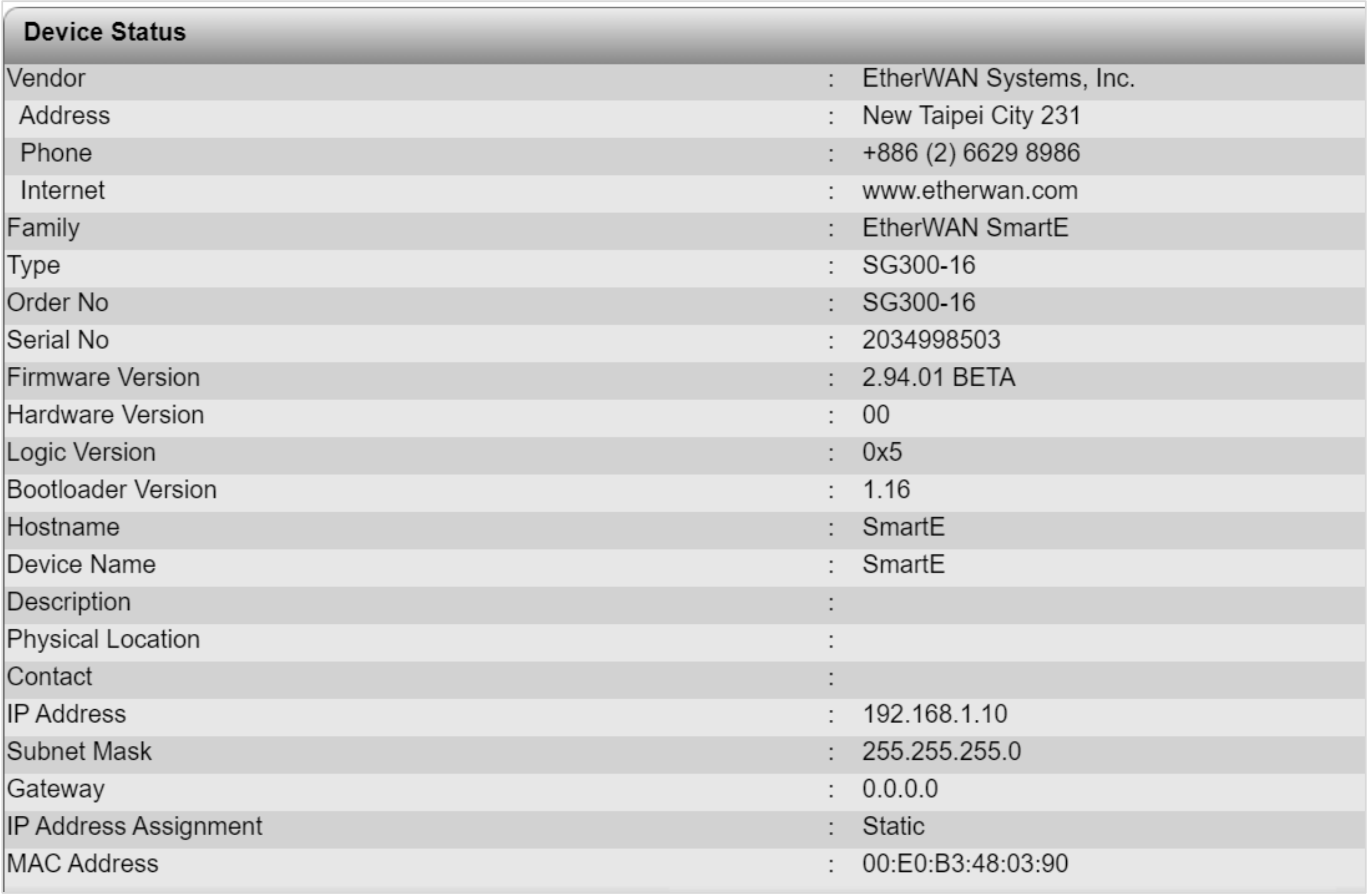
Quick setup
The Quick Setup website includes all parameters for fast and easy configuration of a the device.

Diagnostics
Here you will find further information on diagnostics of the device.

Help There is a (?) after every parameter on the website. When you move the mouse pointer across you will get information on the parameter in a Fly Out window.

Information – Device Status

Here you will find general information about your device, such as the serial number, firmware version, or hardware version.

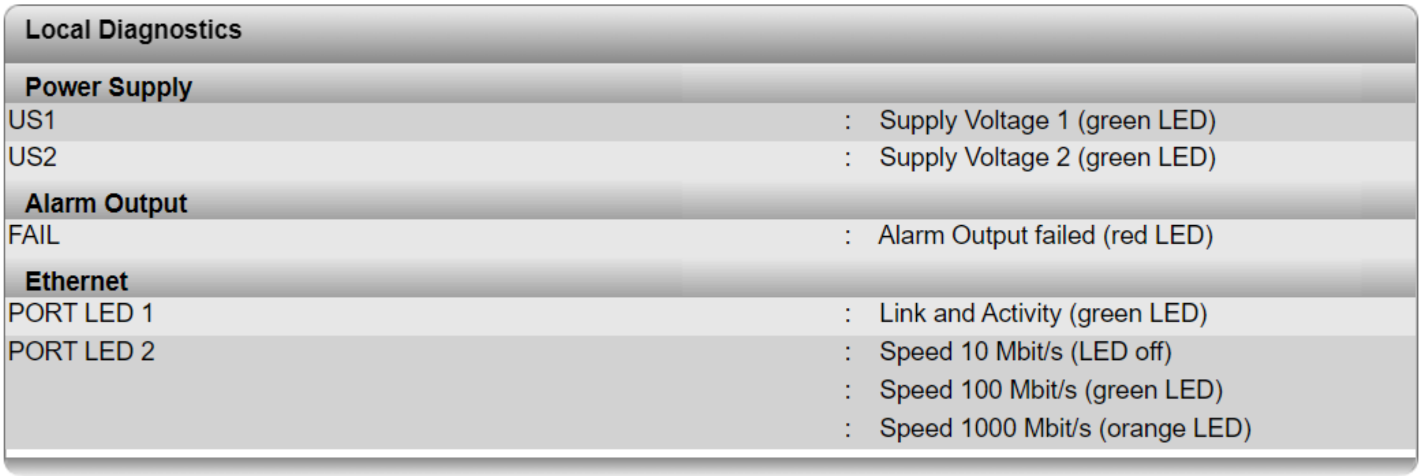


Device Status

Vendor	:	EtherWAN Systems, Inc.
Address	:	New Taipei City 231
Phone	:	+886 (2) 6629 8986
Internet	:	www.etherwan.com
Family	:	EtherWAN SmartE
Type	:	SG300-16
Order No	:	SG300-16
Serial No	:	2034998503
Firmware Version	:	2.94.01 BETA
Hardware Version	:	00
Logic Version	:	0x5
Bootloader Version	:	1.16
Hostname	:	SmartE
Device Name	:	SmartE
Description	:	
Physical Location	:	
Contact	:	
IP Address	:	192.168.1.10
Subnet Mask	:	255.255.255.0
Gateway	:	0.0.0.0
IP Address Assignment	:	Static
MAC Address	:	00:E0:B3:48:03:90

Information – Local Diagnostic

Here you will find a brief explanation of how to interpret the individual LEDs on the device.

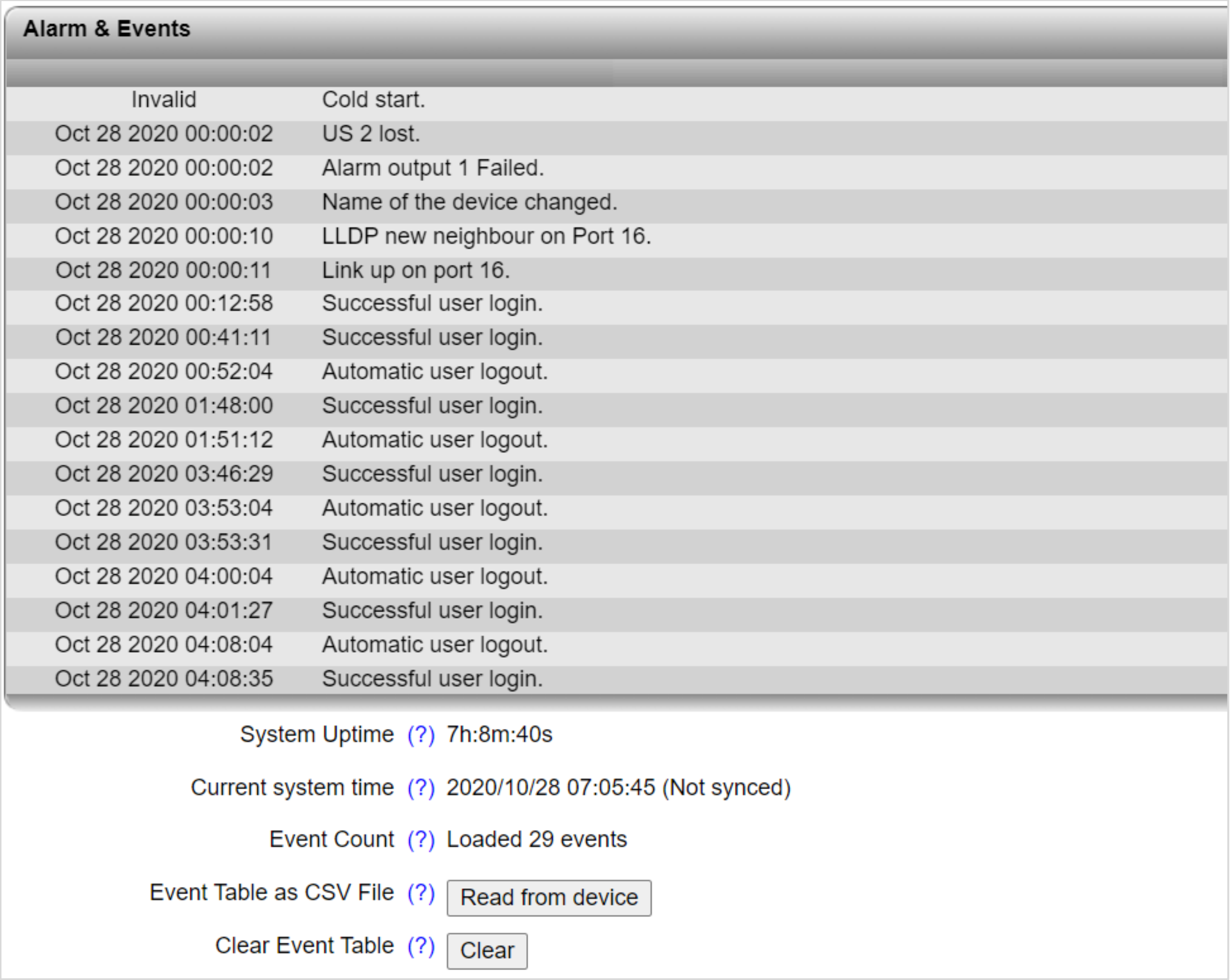


Local Diagnostics

Power Supply		
US1	:	Supply Voltage 1 (green LED)
US2	:	Supply Voltage 2 (green LED)
Alarm Output		
FAIL	:	Alarm Output failed (red LED)
Ethernet		
PORT LED 1	:	Link and Activity (green LED)
PORT LED 2	:	Speed 10 Mbit/s (LED off)
	:	Speed 100 Mbit/s (green LED)
	:	Speed 1000 Mbit/s (orange LED)

Information – Alarm & Events

This page displays a list of alarms and events in a table. You can save event table entries, so that they are also retained after the device is restarted. The event table can be downloaded from the device in CSV format.



Alarm & Events

Invalid	Cold start.
Oct 28 2020 00:00:02	US 2 lost.
Oct 28 2020 00:00:02	Alarm output 1 Failed.
Oct 28 2020 00:00:03	Name of the device changed.
Oct 28 2020 00:00:10	LLDP new neighbour on Port 16.
Oct 28 2020 00:00:11	Link up on port 16.
Oct 28 2020 00:12:58	Successful user login.
Oct 28 2020 00:41:11	Successful user login.
Oct 28 2020 00:52:04	Automatic user logout.
Oct 28 2020 01:48:00	Successful user login.
Oct 28 2020 01:51:12	Automatic user logout.
Oct 28 2020 03:46:29	Successful user login.
Oct 28 2020 03:53:04	Automatic user logout.
Oct 28 2020 03:53:31	Successful user login.
Oct 28 2020 04:00:04	Automatic user logout.
Oct 28 2020 04:01:27	Successful user login.
Oct 28 2020 04:08:04	Automatic user logout.
Oct 28 2020 04:08:35	Successful user login.

System Uptime (?) 7h:8m:40s

Current system time (?) 2020/10/28 07:05:45 (Not synced)

Event Count (?) Loaded 29 events

Event Table as CSV File (?) Read from device

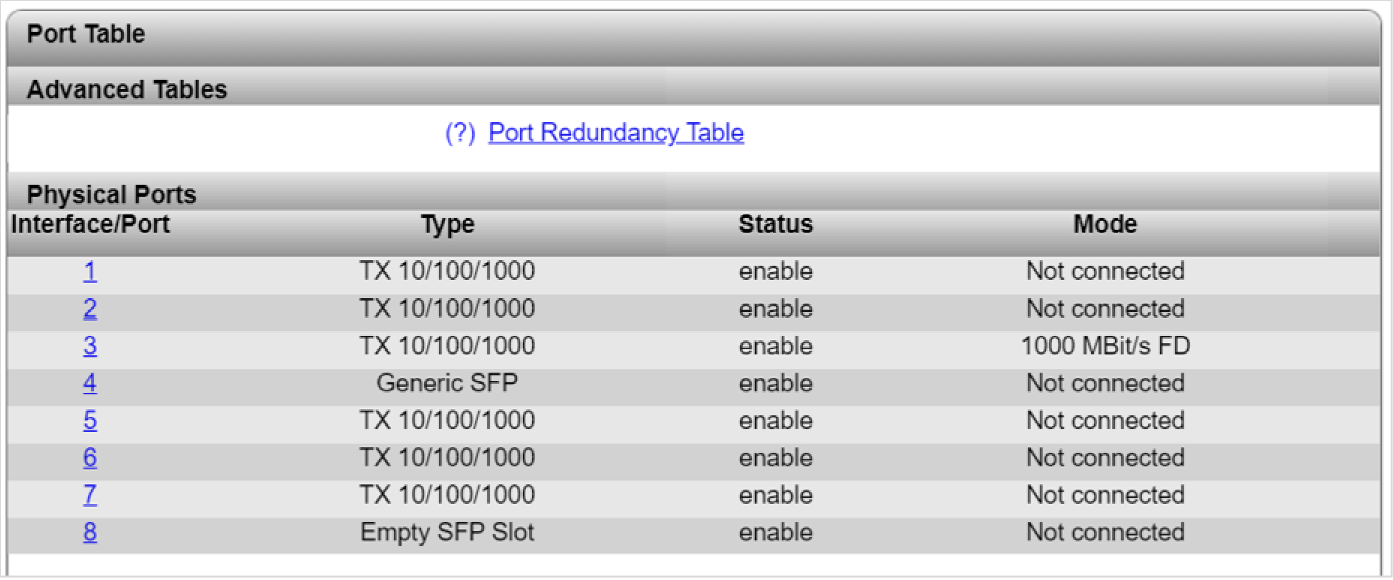
Clear Event Table (?) Clear

A maximum of 3000 entries can be stored in the event table. The oldest entries are then overwritten. If there is a large number of entries, it may take several seconds to load the Event Table.

The persistent storage of events is deactivated in the factory default state. The events are lost when the device is restarted. The function can be activated via the “Persistent Event Logging” item in the “Service”.

Information – Port Table

This page displays a list of the current states of the individual ports.



Port Table

Advanced Tables

(?) Port Redundancy Table

Physical Ports

Interface/Port	Type	Status	Mode
1	TX 10/100/1000	enable	Not connected
2	TX 10/100/1000	enable	Not connected
3	TX 10/100/1000	enable	1000 MBit/s FD
4	Generic SFP	enable	Not connected
5	TX 10/100/1000	enable	Not connected
6	TX 10/100/1000	enable	Not connected
7	TX 10/100/1000	enable	Not connected
8	Empty SFP Slot	enable	Not connected

Clicking on the “Port Redundancy Table” button opens a table containing information about the individual ports and their redundancy mechanism assignment.

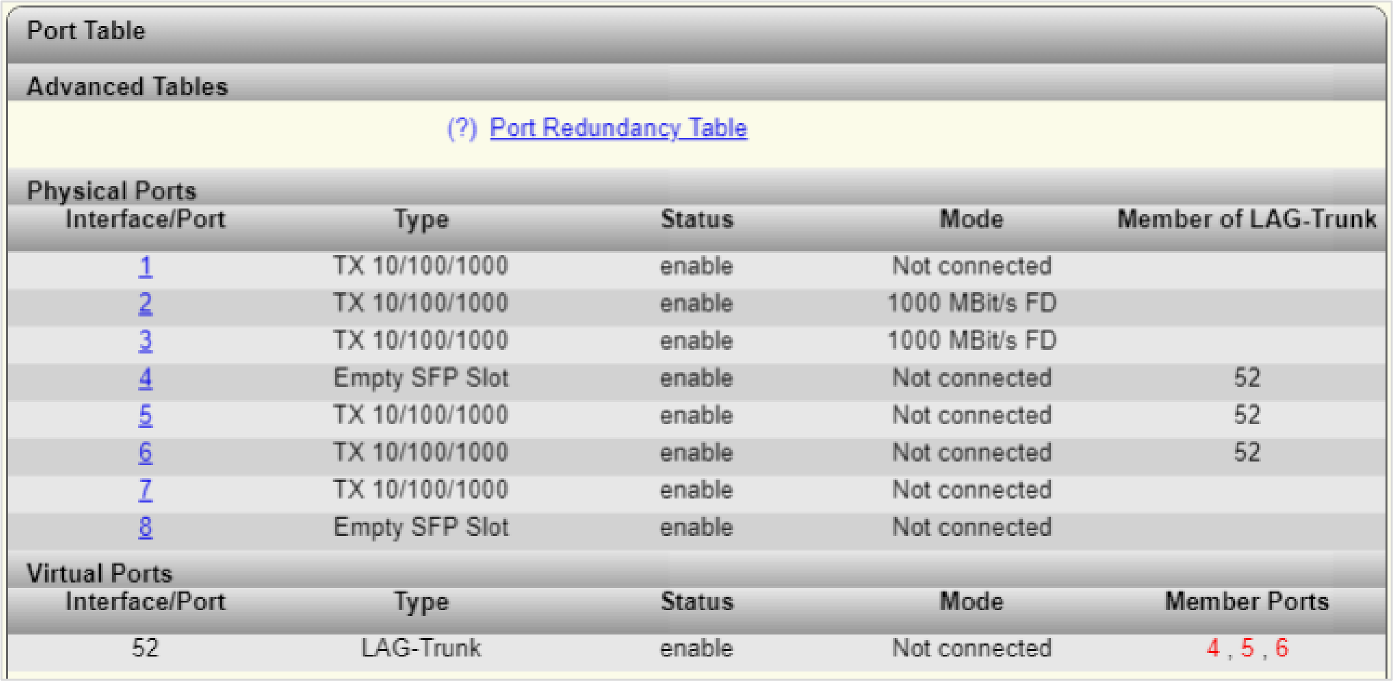
Interface/Port: Clicking on a port number in the “Interface/Port” column opens the “Port Configuration” page for the selected port.

Type: The “Type” column indicates whether it is a copper port (e.g., TX 10/100) or a fiberglass port (e.g., FX 100).

Status: The “Status” column shows whether the port is activated or deactivated.

Mode: The “Mode” column indicates the current connection status of the ports.

- Not connected: No active link at the port.
- 100 Mbps FD (or comparable status): Displays the transmission speed and duplex mode if there is an active link.
- Far-End Fault: Provides information about a fault on a fiber of a bi-directional fiberglass connection (e.g., due to a defective fiberglass cable). If the device at the other end also supports Far-End Fault, it
- detects a communication failure on its own receiver connection and sends a Far-End Fault signal pattern to the peer.



Port Table

Advanced Tables

(?) Port Redundancy Table

Physical Ports

Interface/Port	Type	Status	Mode	Member of LAG-Trunk
1	TX 10/100/1000	enable	Not connected	
2	TX 10/100/1000	enable	1000 MBit/s FD	
3	TX 10/100/1000	enable	1000 MBit/s FD	
4	Empty SFP Slot	enable	Not connected	52
5	TX 10/100/1000	enable	Not connected	52
6	TX 10/100/1000	enable	Not connected	52
7	TX 10/100/1000	enable	Not connected	
8	Empty SFP Slot	enable	Not connected	

Virtual Ports

Interface/Port	Type	Status	Mode	Member Ports
52	LAG-Trunk	enable	Not connected	4 , 5 , 6

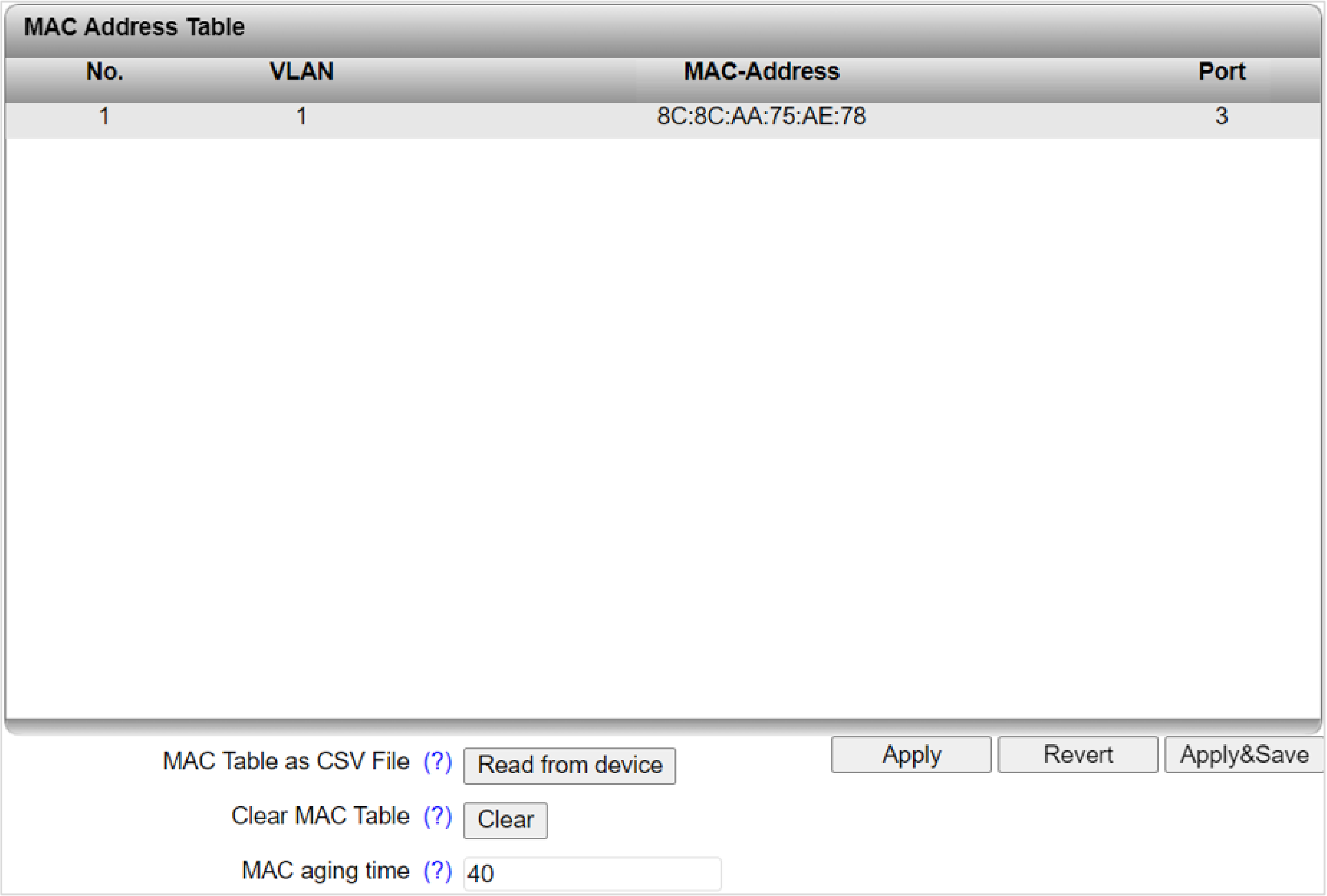
The “Member of LAG-Trunk” column and the “Virtual Ports” area only appear if trunks are configured via link aggregation on the device.

Member of LAG-Trunk: This column shows the assignment between the port and virtual trunk port.

Member Ports: This column shows the assignment between the port and virtual trunk port.

Information – MAC Address Table

On this page, you will find a list of the current devices in the network. You can download the list from the device in CSV format.



MAC Address Table

No.	VLAN	MAC-Address	Port
1	1	8C:8C:AA:75:AE:78	3

MAC Table as CSV File (?) Read from device

Clear MAC Table (?) Clear

MAC aging time (?) 40

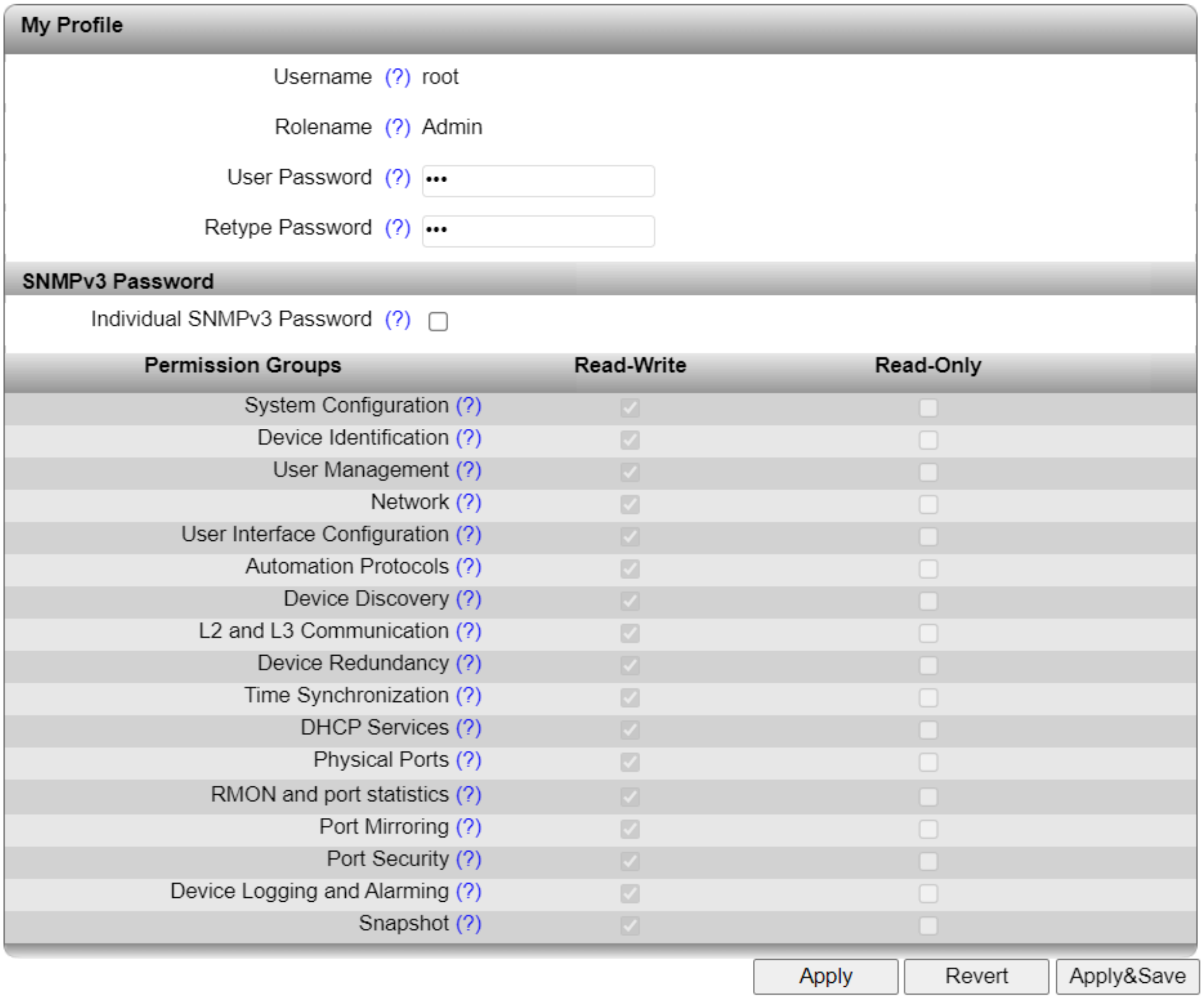
MAC Table as CSV File: Click on “Read from device” to download the current MAC address table from the device in CSV format.

Clear MAC Table: Click on “Clear” to clear the MAC address table.

MAC aging time: Enter the maximum time in seconds by that a device must report back again in order to remain in the table. The time can be between ten and 1000000 seconds (default: 40).

Configuration – My Profile

This page allows for the changing of the password of the root account, and the setting of an SNMPv3 password. The minimum SNMPv3 password length is eight characters.



My Profile

Username (?)	root
Rolename (?)	Admin
User Password (?)	•••
Retype Password (?)	•••

SNMPv3 Password

Individual SNMPv3 Password (?) □

Permission Groups	Read-Write	Read-Only
System Configuration (?)	☑	□
Device Identification (?)	☑	□
User Management (?)	☑	□
Network (?)	☑	□
User Interface Configuration (?)	☑	□
Automation Protocols (?)	☑	□
Device Discovery (?)	☑	□
L2 and L3 Communication (?)	☑	□
Device Redundancy (?)	☑	□
Time Synchronization (?)	☑	□
DHCP Services (?)	☑	□
Physical Ports (?)	☑	□
RMON and port statistics (?)	☑	□
Port Mirroring (?)	☑	□
Port Security (?)	☑	□
Device Logging and Alarming (?)	☑	□
Snapshot (?)	☑	□

Username: Your user name as the logged-in user is displayed here. You cannot change the name yourself.

Rolename: The role name to which your user is assigned is displayed here.

User Password: Enter the new password for your device access here. The new password must be between eight and 64 characters long. (For security reasons, the input fields do not display your password; “*********” is displayed instead.)

Retype Password: Enter the new password again here. The new password will be enabled after saving and logging out.

Individual SNMPv3 Password: Click the button to open two further input fields. Here you can configure a separate SNMPv3 password. The minimum password length is eight characters.

ℹ The “SNMPv3 Password” area is only available to the “admin” user account that was created in the factory default state.

SNMPv3 Password: This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Enter the desired SNMPv3 password in the input field. The password must be between eight and 64 characters long. For security reasons, your password is not displayed as plain text. If you do not assign an SNMPv3 password, the password of the “admin” user account will be used.

ℹ If you use this password, a user account with the name “snmpv3_user” will be created. The user is assigned read-only rights and cannot access the device via SNMPv3.

ℹ If you delete the user account “snmpv3_user”, the “Individual SNMPv3 Password” option is deactivated.

Retype SNMPv3 Password: This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Re-enter the new password.

Permission Groups: The table shows the rights of your own user account.

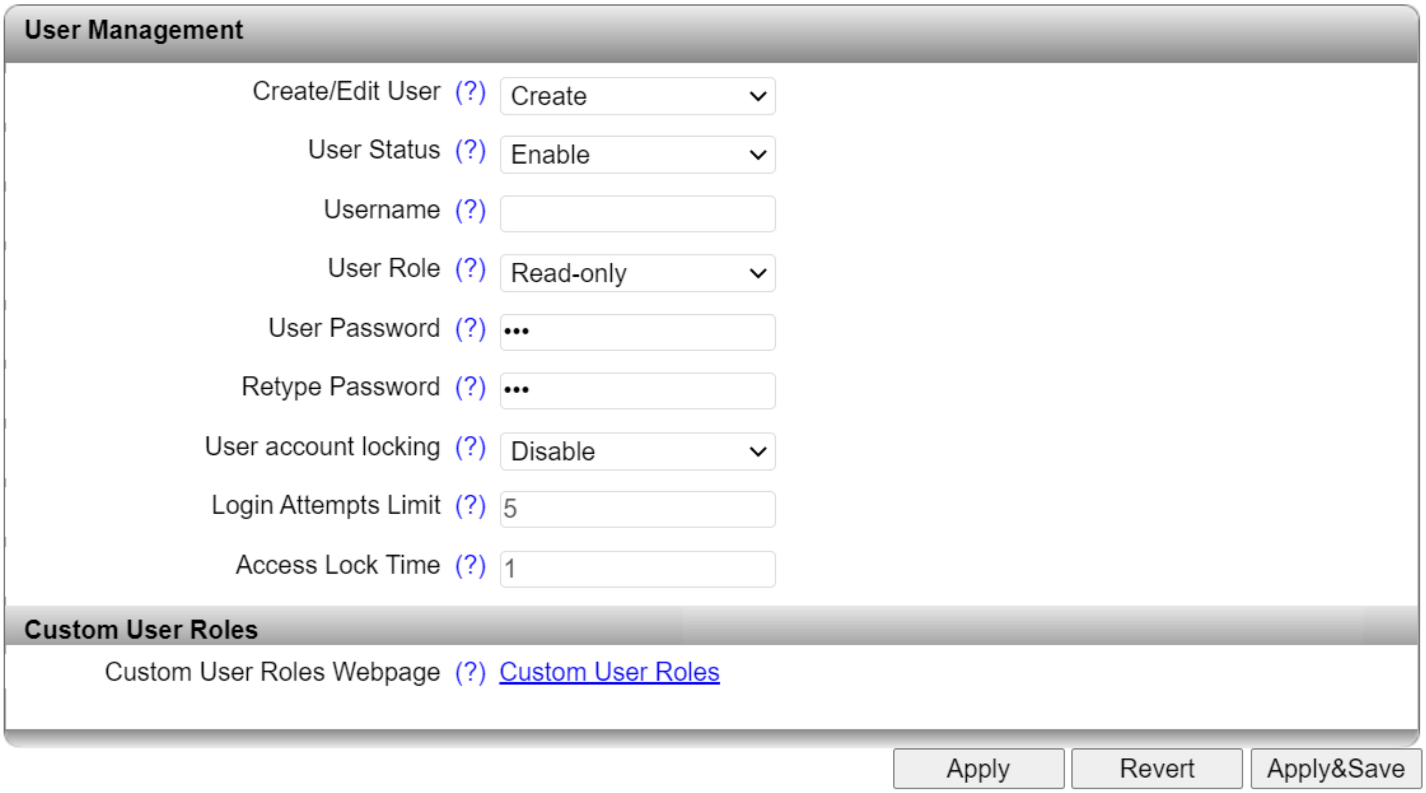
Configuration – User Management

Create and manage user accounts for the web-based management of the switch here. You can assign permissions to users via user roles.

ℹ The device also provides the option of server-based user authentication via LDAP or RADIUS. Configure the settings on the “Security”.

ℹ When a user logs in, the device always searches the local user accounts first. The server-based user authentication is only used if the user name is not available locally.

ℹ Up to ten users each can log in at the same time either via web-based management or CLI.



User Management

Create/Edit User (?)	Create
User Status (?)	Enable
Username (?)	
User Role (?)	Read-only
User Password (?)	•••
Retype Password (?)	•••
User account locking (?)	Disable
Login Attempts Limit (?)	5
Access Lock Time (?)	1

Custom User Roles

Custom User Roles Webpage (?) Custom User Roles

Create/Edit User: Select the user account that you wish to edit or delete. Select “Create” to create a new user account.

Delete button: Click here to delete the selected user account. The “root” account cannot be deleted.

User Status: Activate or deactivate the selected user account. When a user account is deactivated, access to the device is blocked, even if the correct login parameters are entered.

Username: Configure the user name. Once the user account is created, you will not be able to change the user name.

User Role: Assign a role to the selected account that defines the user rights. The following roles can be selected:

- Read-only: The user has read access to the device and therefore access to the web pages in the information and diagnostics areas. Furthermore, the user has permission to change their own access password.
- Expert: An expert user account has extensive read and write access to the device and can therefore modify a good portion of the configuration parameters. However, this excludes “User Management”.
- Admin: An admin user has unrestricted read and write access to the device.

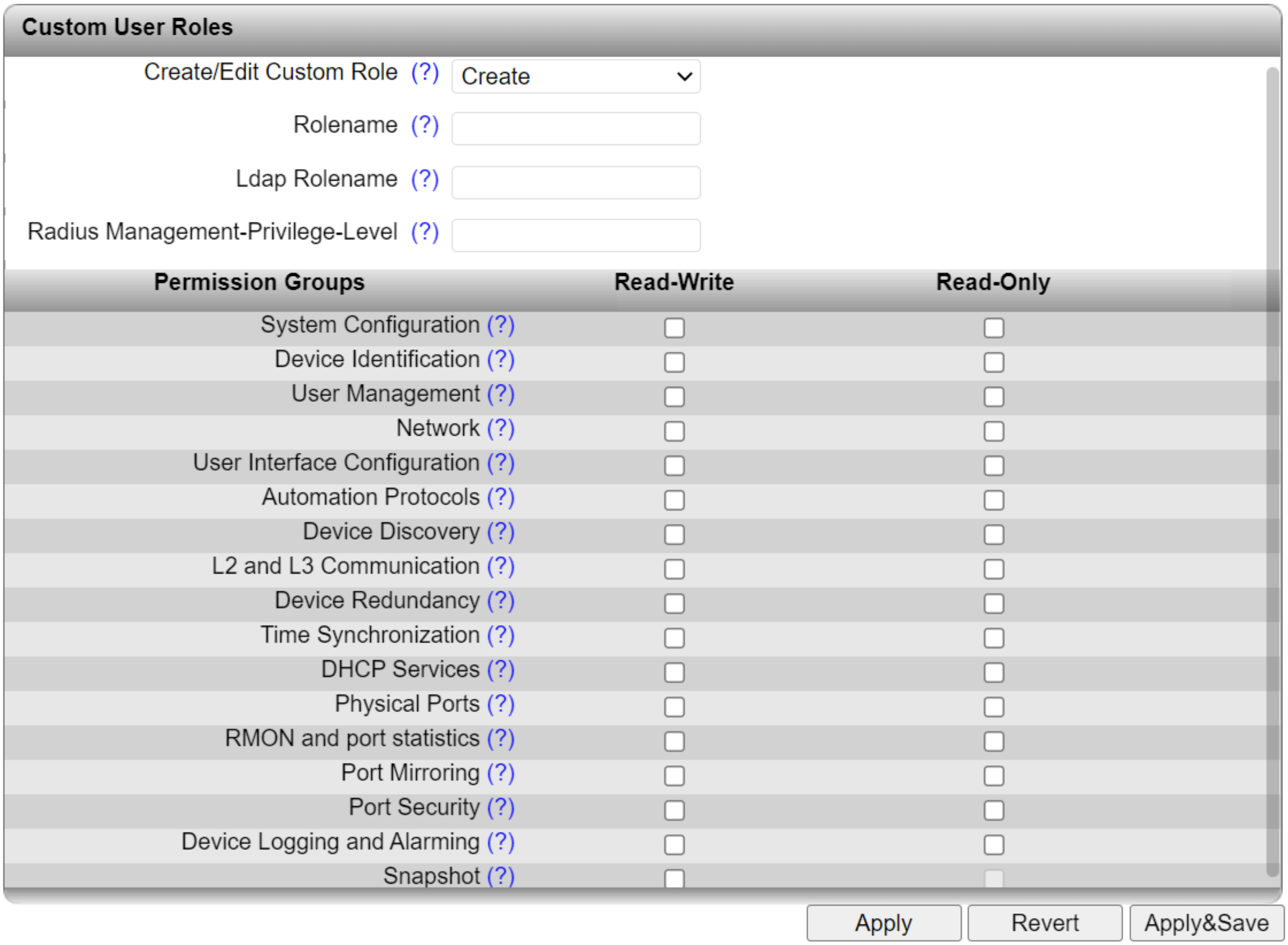
User Password / Retype Password: Here, you can configure the password for the selected user account. For a new user account, this password is also used for initial access to the device. Passwords must be between eight and 64 characters long.

User account locking: This function can be used to lock out a user for a certain period of time if they have repeatedly attempted to log in using the wrong password. It is not possible to access the device during this time, even if the correct access data is entered.

Login Attempts Limit: When the ‘User account locking” function is enabled, configure here the number of failed login attempts after which the user account is locked. The number must be between one and 100.

Access Lock Time: When the “User account locking” function is enabled, set the time (in minutes) for which a user account is locked if the “Login Attempts Limit” is exceeded. The time must be between one and 1440 minutes.

Custom User Roles: Clicking the Custom User Roles link opens a new page on which user roles can be created and edited. Create a new custom role by selecting "Create," or edit a role by selecting an existing role name. Role names can be up to 32 characters long. Once a role name is assigned, it cannot be edited. Use the check boxes in the table below to assign read-write or read-only rights to for the various permission groups.



Custom User Roles

Create/Edit Custom Role (?)	Create
Rolename (?)	
Ldap Rolename (?)	
Radius Management-Privilege-Level (?)	

Permission Groups	Read-Write	Read-Only
System Configuration (?)	□	□
Device Identification (?)	□	□
User Management (?)	□	□
Network (?)	□	□
User Interface Configuration (?)	□	□
Automation Protocols (?)	□	□
Device Discovery (?)	□	□
L2 and L3 Communication (?)	□	□
Device Redundancy (?)	□	□
Time Synchronization (?)	□	□
DHCP Services (?)	□	□
Physical Ports (?)	□	□
RMON and port statistics (?)	□	□
Port Mirroring (?)	□	□
Port Security (?)	□	□
Device Logging and Alarming (?)	□	□
Snapshot (?)	□	□

Create/Edit Custom Role: Create a new custom role by selecting **Create** or edit a role by selecting the Rolename.

Delete button: Click here to delete the selected user role. This action cannot be undone.

ℹ The preconfigured roles “Admin”, “Expert”, and “Read-only” cannot be deleted.

Rolename: Configure the Rolename of a new custom role. Once a custom role has been created, the Rolename cannot be changed anymore. It may be up to 32 characters long. Alphabetical characters, numerical digits and the following characters are permitted: - _ . @ .

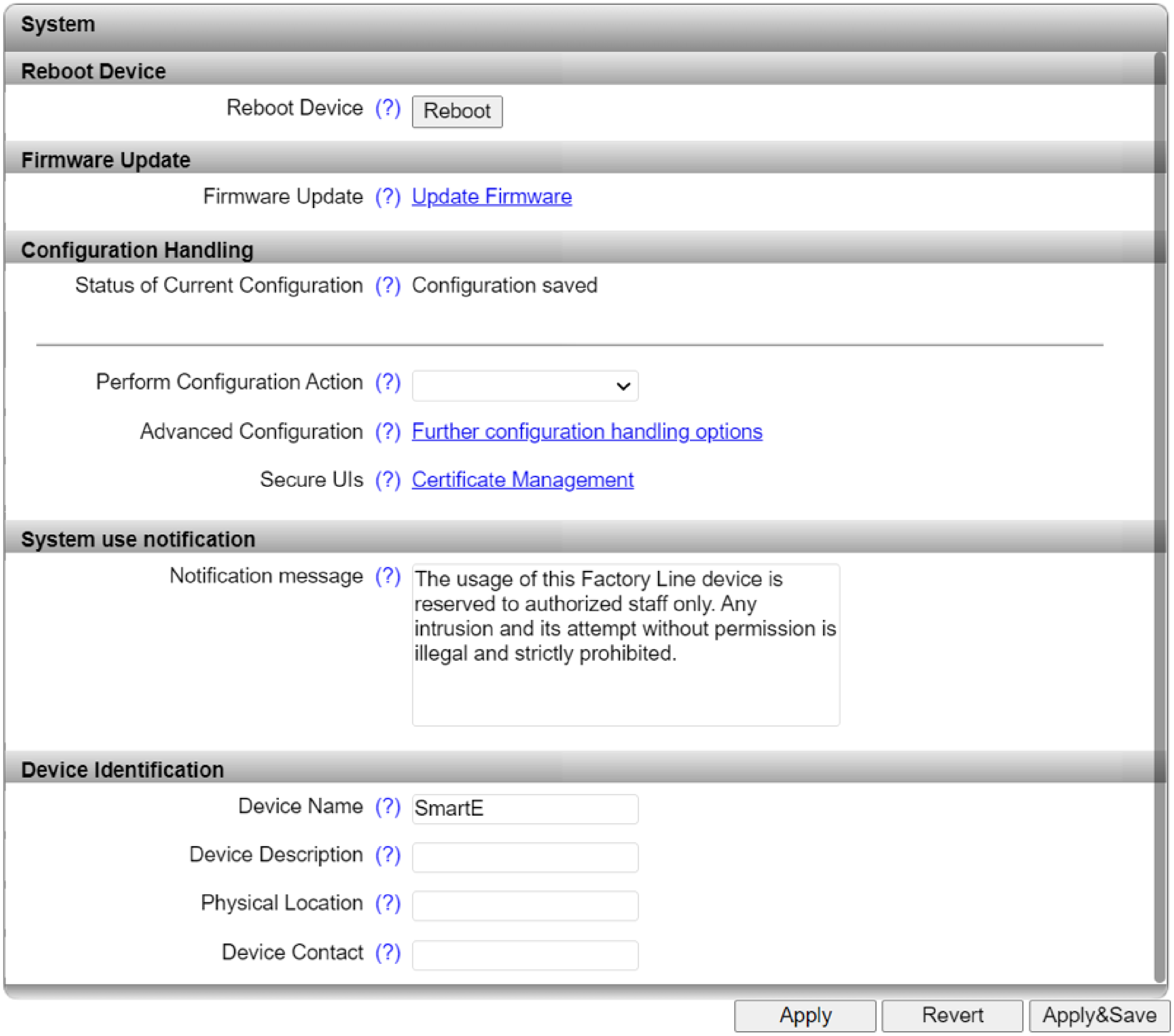
LDAP Rolename: The LDAP role name is made available to a user via the LDAP server. The role name is used to assign a user to a user role and therefore to assign permissions on the device. The LDAP role name is mapped to a local user role here.

Radius Management-Privilege-Level: Here you can configure a numerical value that is made available to a user via the RADIUS server during server-based authentication. This value is used to assign a user to a user role and therefore to assign permissions on the device. The management privilege level is mapped to a local user role here.

Permission Groups: In the table, you can assign and edit the read and write permissions for custom roles. The predefined permissions of the Admin", "Expert", and "Read-only" roles available by default cannot be changed.

- Read-Write: Clicking on the buttons assigns read and write permissions for the respective function group to the selected user role.
- Read-Only: Clicking on the buttons assigns read-only access for the respective function group to the selected user role.
- No selection: If you do not select either of the two check boxes for a function group, the user role will not be assigned permission for this function group.

Configuration – System



System

Reboot Device

Reboot Device (?)

Firmware Update

Firmware Update (?) Update Firmware

Configuration Handling

Status of Current Configuration (?) Configuration saved

Perform Configuration Action (?)

Advanced Configuration (?) Further configuration handling options

Secure UIs (?) Certificate Management

System use notification

Notification message (?) The usage of this Factory Line device is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.

Device Identification

Device Name (?) SmartE

Device Description (?)

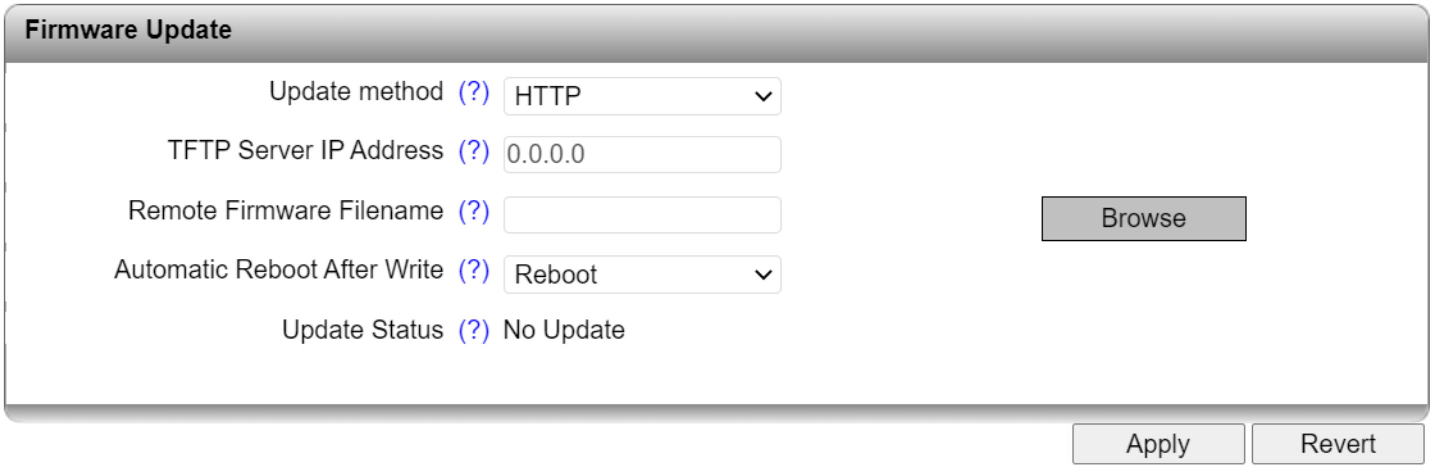
Physical Location (?)

Device Contact (?)

Reboot Device: Clicking on the “Reboot” button restarts the device. All unsaved parameters will be lost.

ℹ The connection to the device is interrupted for the boot phase.

Firmware Update: Clicking on the “Update Firmware” link opens a new window in which the parameters for the firmware update must be entered.



Firmware Update

Update method (?) HTTP

TFTP Server IP Address (?) 0.0.0.0

Remote Firmware Filename (?)

Automatic Reboot After Write (?) Reboot

Update Status (?) No Update

To update the firmware via HTTP:

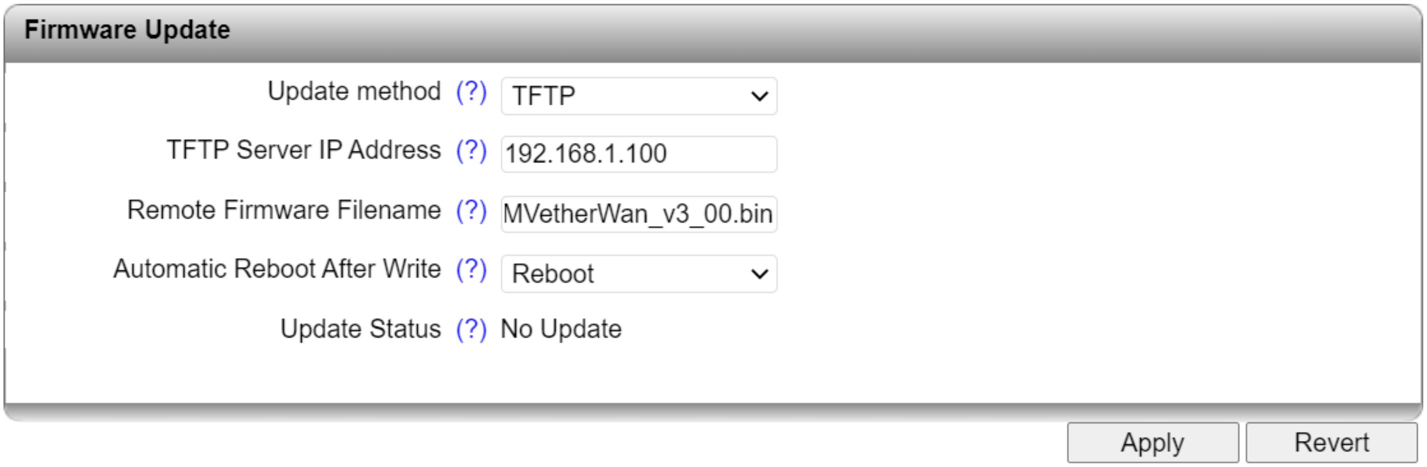
Browse: Clicking on the “Browse” button allows you to select the desired file on your PC.

Automatic Reboot After Write: Here, specify whether a reboot should be performed after the firmware update.

Click “Apply” to start the firmware update.

ℹ If you perform a firmware update without rebooting immediately, “Update Status” displays the message “Firmware Update successful”, which informs you that the firmware has been transferred to the device and will be activated on the next reboot.

To update the firmware via TFTP, select “TFTP” as the update method. Enter the IP address of the computer on which the TFTP server is active, and the filename. Click “Apply” to start the update.



Firmware Update

Update method (?) TFTP

TFTP Server IP Address (?) 192.168.1.100

Remote Firmware Filename (?) MVetherWan_v3_00.bin

Automatic Reboot After Write (?) Reboot

Update Status (?) No Update

Configuration Handling items

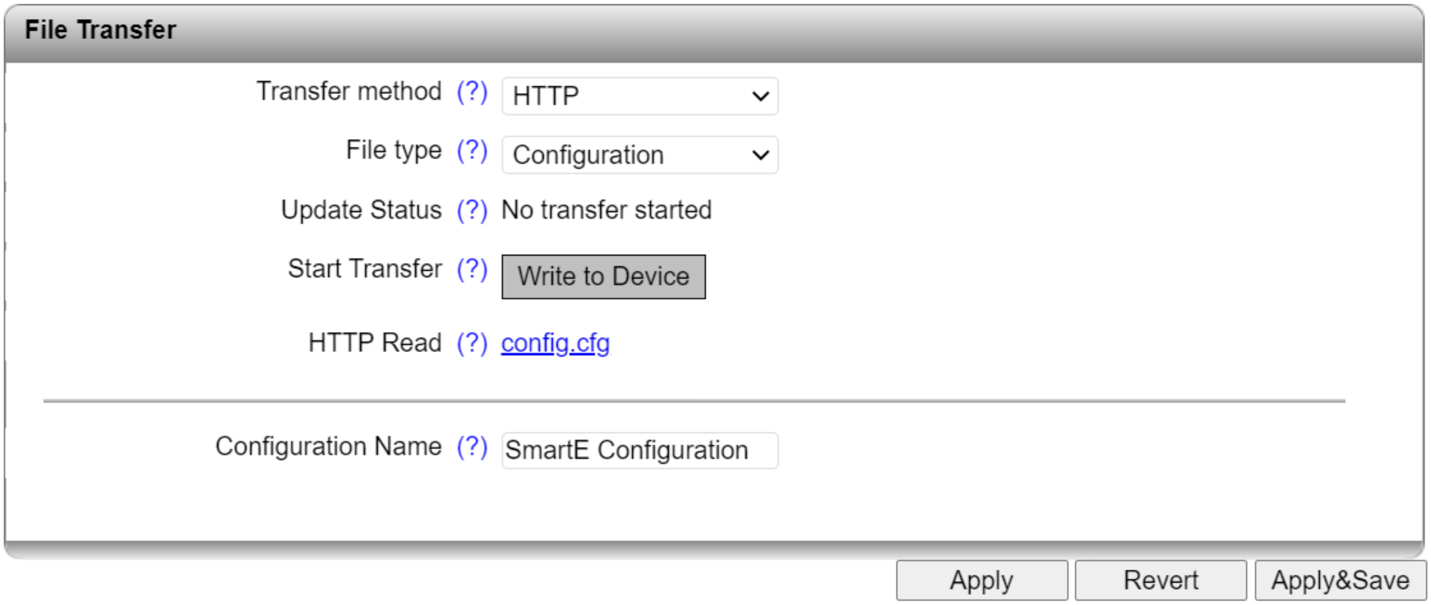
Status of Current Configuration: Shows the status of the active configuration.

- Configuration saved: The active configuration is saved to the device.
- Configuration modified but not saved: The active configuration has been changed, but not yet saved to the device. Click on “Apply & Save” to save the configuration to the device.

Perform Configuration Action: Select an action from the dropdown menu:

- Factory Default: Resets the device configuration to the delivery state.
- Save Configuration: Saves the active device configuration to Flash memory.
- Reload Configuration: Loads the configuration file from Flash memory and applies it. The device is then restarted.

Advanced Configuration: Clicking on the “Further configuration handling options” link opens a “File Transfer” window (see below). On that screen, enter the parameters for transferring a configuration file from the device to the PC (download) or from the PC to the device (upload).



File Transfer

Transfer method (?) HTTP

File type (?) Configuration

Update Status (?) No transfer started

Start Transfer (?) Write to Device

HTTP Read (?) config.cfg

Configuration Name (?) SmartE Configuration

Transfer Method: Select the transmission protocol you would like to use to transfer the file.

File Type: Select the file type to be transferred. It can be either a configuration file, a security context or a snapshot file.

Configuration Name: Enter the name under which you want to save the configuration on the PC. Any change to the configuration name only takes effect when you click on the “Apply & Save” button.

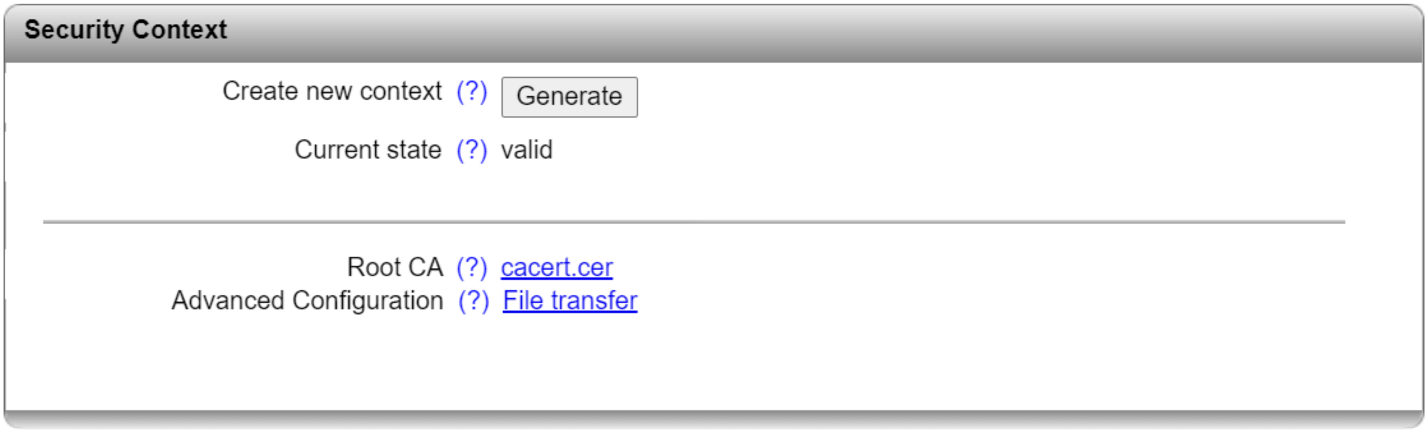
Update Status: Shows the current transfer status.

Start Transfer: Click on the “Write to device” button to select the file on your PC that is to be transferred to the switch.

HTTP Read: Click on the “config.cfg” link to download the active configuration directly to the connected PC. If transferring a snapshot file, click on the “snapshot.tar.gz” link to download the current snapshot file directly to your PC.

If transferring files via TFTP, enter the IP address of the computer on which the TFTP server is active, and the remote filename. Then select “Read from device” or “Write to device” in the **Direction** field. Click on the “Start” button to start the transfer of the file.

Secure UIs: Clicking on the “Security Context” link opens the “Security Context” screen.



Security Context

Create new context (?) Generate

Current state (?) valid

Root CA (?) cacert.cer

Advanced Configuration (?) File transfer

Create new context: Clicking on the “Generate” button creates all the necessary keys and certificates for operation with HTTPS and SSH.

Current state: Shows the status of the current availability of the security context.

Root CA: Clicking on the “cacert.cer” link loads the Root CA certificate for installation in the browser.

Advanced Configuration: Clicking on the “File transfer” link opens the “Advanced Configuration” window for file transfer with file type set to “Security Context”.

System use notification

Notification message: Enter the desired text to be displayed prior to login. The text is freely editable and can be up to 256 characters long.

Device Identification items

Information entered in this section is displayed on the “Device Status” page.

Device Name: Enter the device name.

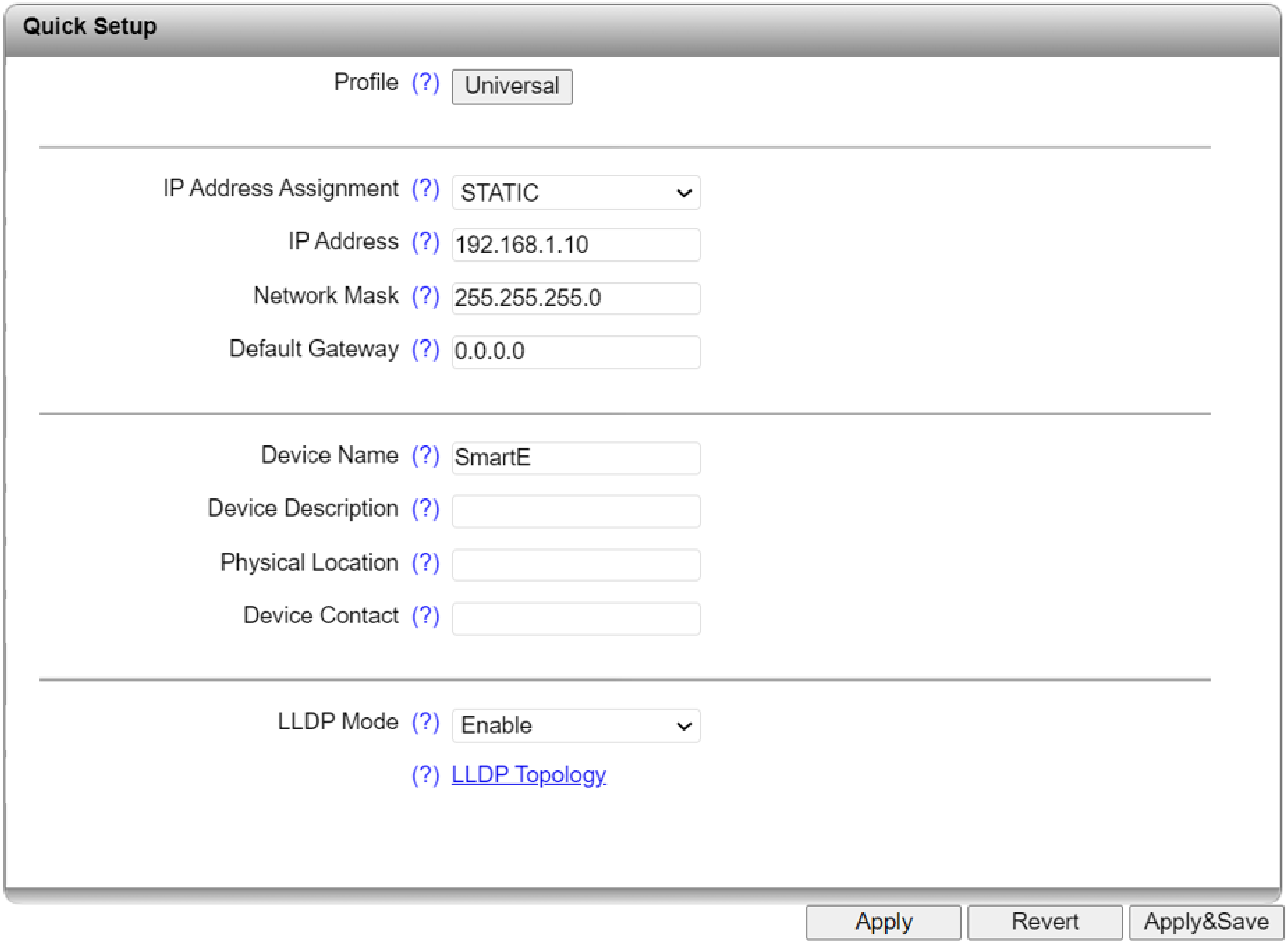
Device Description: Enter a device description. It may be up to 255 characters long.

Physical Location: Here, you can provide the location of the device, such as the building in which it is installed.

Device Contact: Here, you can enter a contact address.

Configuration – Quick Setup

Basic settings can be quickly configured in the Quick Setup area.



Quick Setup

Profile (?) Universal

IP Address Assignment (?) STATIC

IP Address (?) 192.168.1.10

Network Mask (?) 255.255.255.0

Default Gateway (?) 0.0.0.0

Device Name (?) SmartE

Device Description (?)

Physical Location (?)

Device Contact (?)

LLDP Mode (?) Enable

(?) LLDP Topology

Profile: Only one profile is available for this model – Universal. In Universal mode, BootP is activated for IP address assignment.

IP Address Assignment: Select the type of IP address assignment from the dropdown menu. The options are:

- STATIC: Static IP address
- BOOTP: Assignment via the Bootstrap protocol
- DHCP: Assignment via a DHCP server

IP Address: Set the desired IP address.

Network Mask: Set the desired subnet mask here.

Default Gateway: Set the desired default gateway here.

Device Name: Enter the device name of the switch.

Device Description: Enter a description for the device, up to 255 characters in length.

Physical Location: Enter a location for the device.

Device Contact: Here, you can enter the name of a contact person for the device.

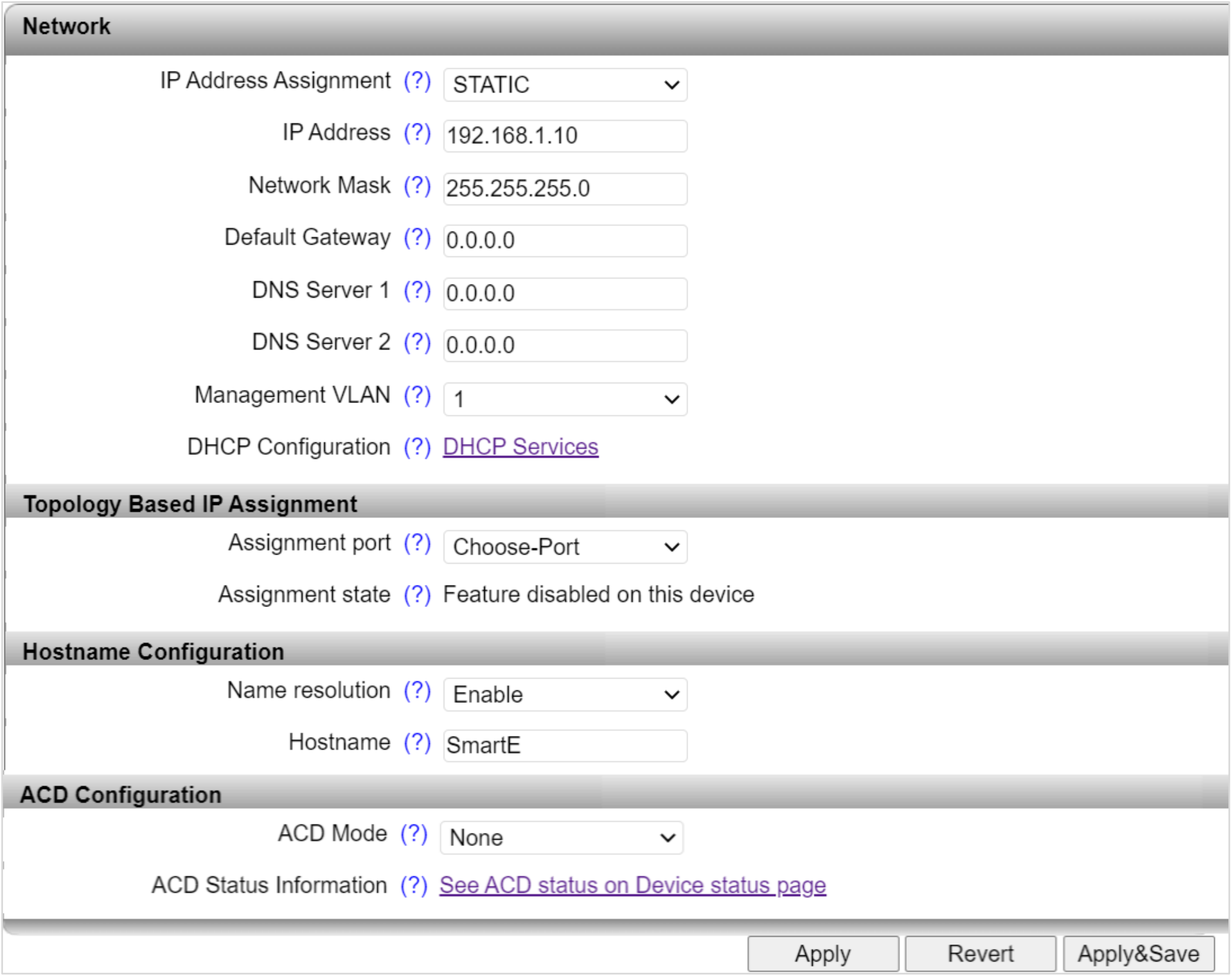
LLDP Mode: Enable or disable LLDP.

- Disable: LLDP is deactivated
- Enable: LLDP is activated
- Send only: Received LLDP BPDUs are ignored
- Receive only: No LLDP BPDUs are sent

The “LLDP Topology” link opens the corresponding page. This can also be accessed via the menu item of the same name.

Configuration – Network

Configure basic network settings on this page.



Network

IP Address Assignment (?)	STATIC
IP Address (?)	192.168.1.10
Network Mask (?)	255.255.255.0
Default Gateway (?)	0.0.0.0
DNS Server 1 (?)	0.0.0.0
DNS Server 2 (?)	0.0.0.0
Management VLAN (?)	1
DHCP Configuration (?)	DHCP Services

Topology Based IP Assignment

Assignment port (?)	Choose-Port
Assignment state (?)	Feature disabled on this device

Hostname Configuration

Name resolution (?)	Enable
Hostname (?)	SmartE

ACD Configuration

ACD Mode (?)	None
ACD Status Information (?)	See ACD status on Device status page

IP Address Assignment: Select the type of IP address assignment.

- STATIC: Static IP address
- BOOTP: Assignment via the Bootstrap protocol
- DHCP: Assignment via a DHCP server

For static IP addressing, complete the following fields:

- IP Address: Set the desired IP address.
- Network Mask: Set the desired subnet mask.
- Default Gateway: Set the desired default gateway.

DNS Server 1: Enter the IP address of the primary DNS server.

DNS Server 2: Enter the IP address of the secondary DNS server.

Management VLAN: Set the VLAN in which the web-based management can be accessed (default is “1”).

DHCP Configuration: Click the “DHCP Services” link to navigate to the DHCP Services page.

Topology Based IP Assignment allows for the assigning of blocks of IP addresses from an IP pool for different topological areas.

Topology Based IP Assignment items

Assignment port: Select the desired port from the dropdown menu. A device connected to the selected port requests incremented IP at DHCP server. Choosing a port disables the Accept BootP feature of the DHCP server settings.

Assignment state: Displays if the topology based IP assignment feature on this device is disabled, acting as root or acting as client.

Hostname Configuration items

Name resolution: Here, you can enable and disable DNS name resolution via mDNS and LLMNR. When the function is activated, you can also access the device via the host name (e.g., http://smarte.local).

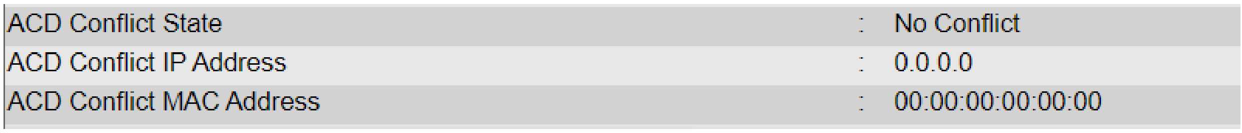
Hostname: Configure the DNS host name of the device here. The host name must be between two and 63 characters long. Alphanumeric characters and dashes are permitted. A host name must not start with a dash.

ℹ After deactivating DNS name resolution, it may take some time until the device can be accessed via the host name due to the DNS cache.

ACD (Address Conflict Detection) Configuration items

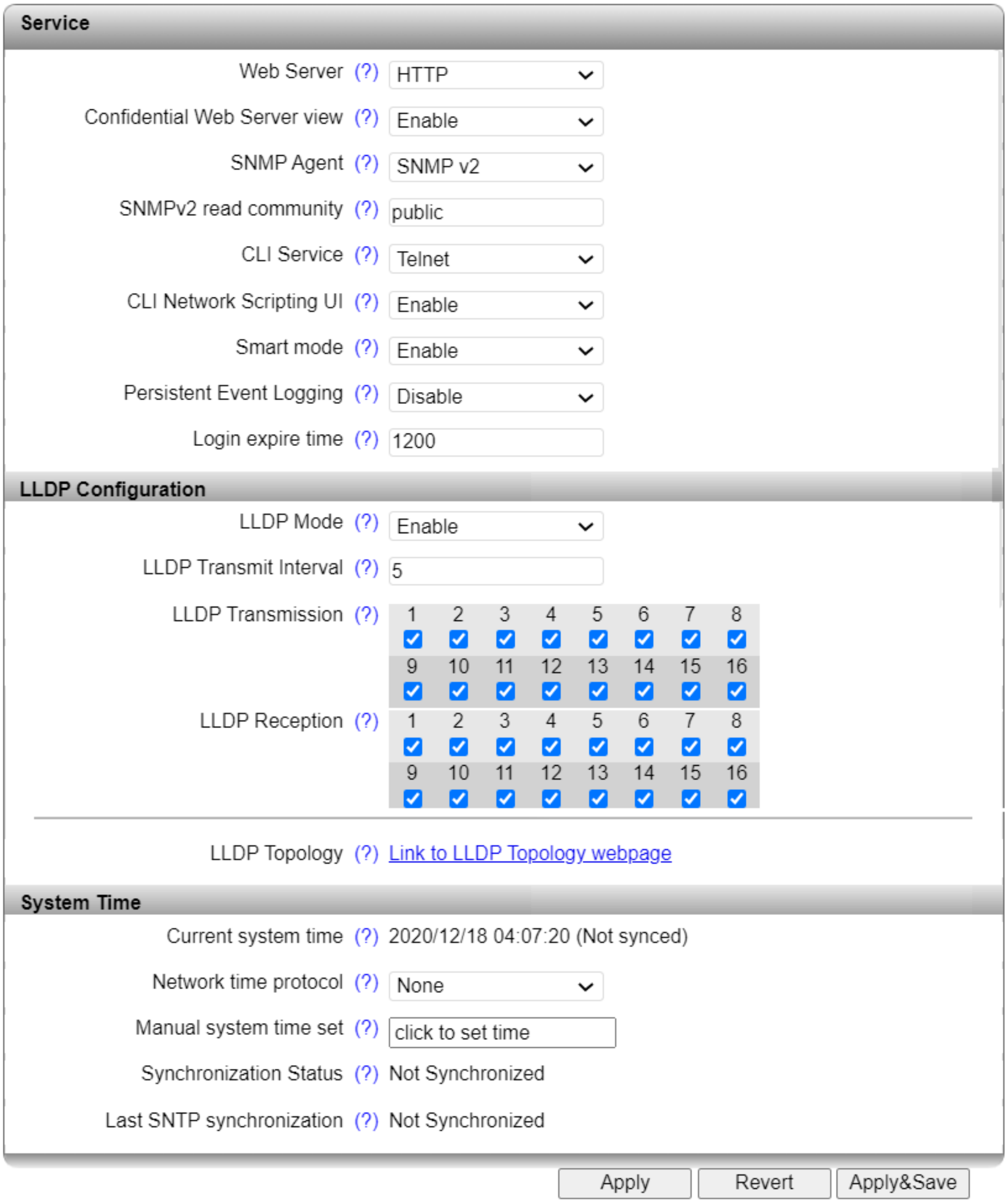
ACD Mode: Here, you can enable and disable the “Address Conflict Detection” function.

ACD Status Information: Clicking on the link opens the “Device Status” page.



ACD Conflict State	:	No Conflict
ACD Conflict IP Address	:	0.0.0.0
ACD Conflict MAC Address	:	00:00:00:00:00:00

Configuration – Service



Service

Web Server (?)	HTTP
Confidential Web Server view (?)	Enable
SNMP Agent (?)	SNMP v2
SNMPv2 read community (?)	public
CLI Service (?)	Telnet
CLI Network Scripting UI (?)	Enable
Smart mode (?)	Enable
Persistent Event Logging (?)	Disable
Login expire time (?)	1200

LLDP Configuration

LLDP Mode (?)	Enable
LLDP Transmit Interval (?)	5

LLDP Transmission (?)

1	2	3	4	5	6	7	8
☑	☑	☑	☑	☑	☑	☑	☑
9	10	11	12	13	14	15	16
☑	☑	☑	☑	☑	☑	☑	☑

LLDP Reception (?)

1	2	3	4	5	6	7	8
☑	☑	☑	☑	☑	☑	☑	☑
9	10	11	12	13	14	15	16
☑	☑	☑	☑	☑	☑	☑	☑

LLDP Topology (?) Link to LLDP Topology webpage

System Time

Current system time (?)	2020/12/18 04:07:20 (Not synced)
Network time protocol (?)	None
Manual system time set (?)	click to set time
Synchronization Status (?)	Not Synchronized
Last SNTP synchronization (?)	Not Synchronized

Web Server: Here, you can enable and disable the web server function and also select the mode (HTTP/HTTPS).

ℹ If you deactivate the web server, web-based management can no longer be accessed.

Confidential Web Server View: If this view is activated, no web pages in web-based management can be accessed without logging in first – this also applies to the web pages in the information area.

SNMP Agent: Enable and disable the SNMP server function and select the mode (SNMP v2, SNMP v3).

SNMPv2 read community: This option is only available if you selected “SNMP v2” for “SNMP Agent”. Here, enter the string for the SNMPv2 read community. This password must be entered for read access to objects.

CLI Service:

- Disable: The entry of CLI commands is deactivated.
- Telnet: The entry of CLI commands via Telnet is activated.
- SSH: The entry of CLI commands via Secure Shell (SSH) is activated.

Backspace Key CTRL-H: Select whether the key combination Ctrl+H should additionally be used as a backspace function. Some terminal programs use the backspace key as Delete. If you activate this option, you can instead use the key combination Ctrl+H in your terminal program to delete the last character.

CLI Network Scripting UI:

- Disable: The transmission of CLI commands via the network is deactivated.
- Enable: The transmission of CLI commands via the network is activated.

Smart mode: Here, you can enable and disable the Mode button.

⚠ If the Smart mode button is disabled and access is no longer possible via the Ethernet ports (e.g., due to incorrect configuration or forgotten access data), it is no longer possible to reset the device. The device must then be sent in to be reset by the manufacturer – this is subject to a fee.

Persistent Event Logging: Here, you can enable and disable the persistent storage of events. Persistent storage means that events are not deleted when the device is restarted.

Login expire time: Configure the duration until automatic logout (30 ... 3600 seconds, default is 1200 seconds). Entering 0 deactivates automatic logout.

LLDP Configuration items

LLDP Mode:

- Disable: LLDP is disabled
- Enable: LLDP is enabled
- Send only: Only LLDP BPDUs are sent.
- Receive only: Only LLDP BPDUs are received.

LLDP Transmit Interval: Set the interval at which LLDP telegrams are to be sent. The value must be between 5 and 32,786 seconds (default is 5 s).

LLDP Transmission: Enable and disable the forwarding of LLDP telegrams for specific ports.

LLDP Reception: Enable and disable the ignoring of LLDP telegrams for specific ports.

LLDP Topology: Clicking on the “Link to LLDP Topology webpage” link opens the page for “LLDP Topology”.

System Time items

Current system time: Displays the current system time. “Not synced” means that the system time has either been configured manually or it is not synchronized with an (S)NTP server.

Network time protocol: Activates synchronization via a web server. (None, Unicast, Broadcast)

- Primary SNTP server: IP address or DNS name of the primary SNTP server.
- Primary server description: Description of the primary SNTP server.
- Secondary SNTP server: IP address or DNS name of the secondary SNTP server.
- Secondary server description: Description of the secondary SNTP server.
- UTC offset: Selection of the time zone. The system time always refers to Greenwich Mean Time (standard time). The local time is based on the system time and the UTC offset. The time difference for summer and winter time must be taken into account, if required.

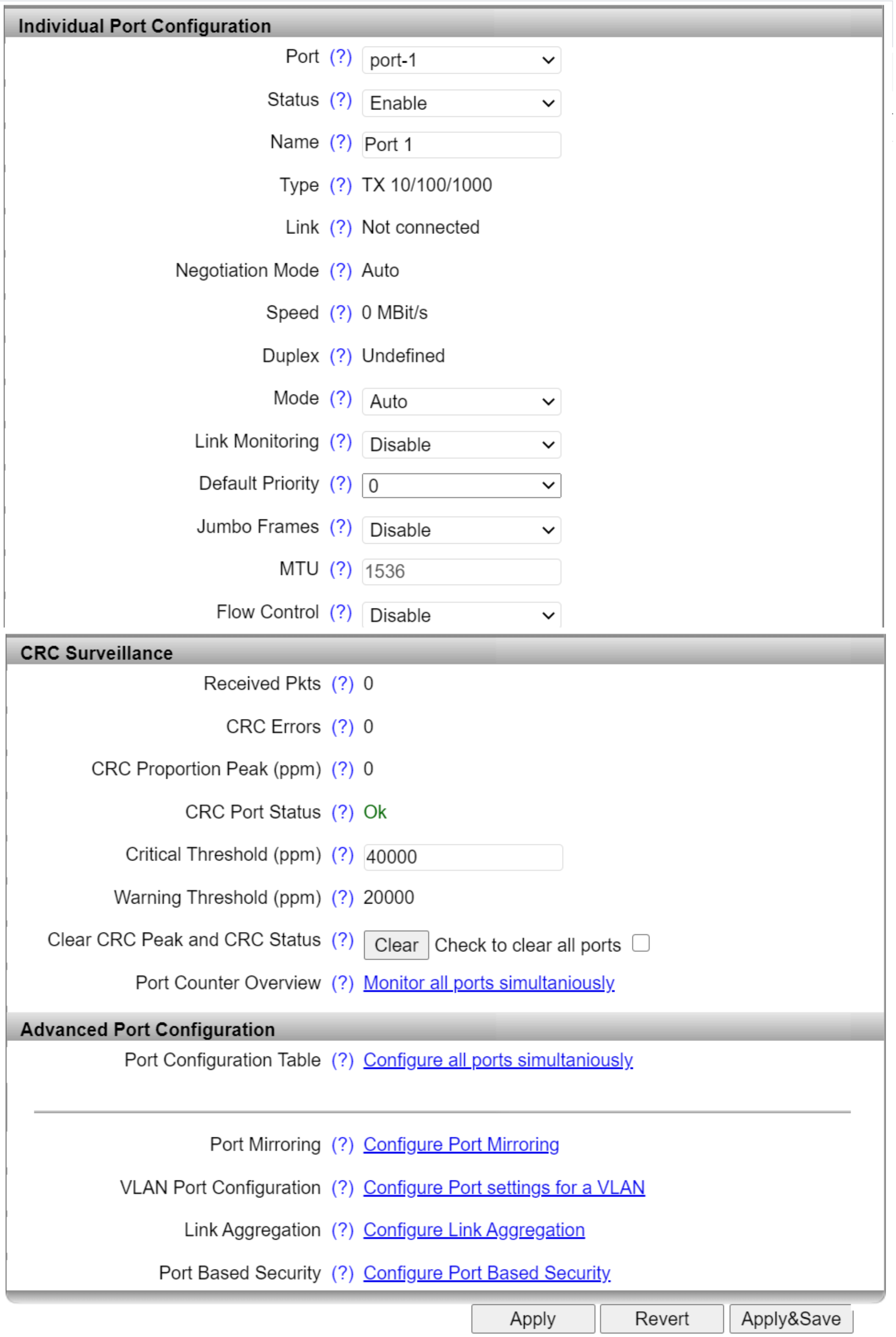
Manual system time set: Manual setting of the system time if no SNTP server is available.

ℹ The switch does not have a battery-backed real-time clock. If the time is entered manually, the time may deviate after the device is started.

Synchronization Status: Displays the current status of synchronization with the SNTP server.

Last SNTP synchronization: Displays the time of the last synchronization.

Configuration – Port Configuration



Individual Port Configuration

Port (?) port-1

Status (?) Enable

Name (?) Port 1

Type (?) TX 10/100/1000

Link (?) Not connected

Negotiation Mode (?) Auto

Speed (?) 0 MBit/s

Duplex (?) Undefined

Mode (?) Auto

Link Monitoring (?) Disable

Default Priority (?) 0

Jumbo Frames (?) Disable

MTU (?) 1536

Flow Control (?) Disable

CRC Surveillance

Received Pkts (?) 0

CRC Errors (?) 0

CRC Proportion Peak (ppm) (?) 0

CRC Port Status (?) Ok

Critical Threshold (ppm) (?) 40000

Warning Threshold (ppm) (?) 20000

Clear CRC Peak and CRC Status (?) Clear Check to clear all ports ☐

Port Counter Overview (?) Monitor all ports simultaniously

Advanced Port Configuration

Port Configuration Table (?) Configure all ports simultaniously

Port Mirroring (?) Configure Port Mirroring

VLAN Port Configuration (?) Configure Port settings for a VLAN

Link Aggregation (?) Configure Link Aggregation

Port Based Security (?) Configure Port Based Security

Port Configuration items

Port: Select the port that you want to configure individually.

Status: The port can be activated/deactivated here.

Name: You can assign a name to the port.

Type: Describes the physical properties of the port.

Link: Shows the current link status of the port.

Negotiation Mode: Shows the current auto negotiation status.

Speed: Displays the current transmission speed at which the port is operating.

Duplex: Displays the transmission mode of the port.

Mode: The port can be set to a fixed speed and transmission mode here.

- Auto: The transmission speed and mode are selected automatically.
- 10 Mbps Half Duplex: The port transmits at a speed of 10 Mbps in half-duplex mode.
- 10 Mbps Full Duplex: The port transmits at a speed of 10 Mbps in full-duplex mode.
- 100 Mbps Half Duplex: The port transmits at a speed of 100 Mbps in half-duplex mode.
- 100 Mbps Full Duplex: The port transmits at a speed of 100 Mbps in full-duplex mode.
- Fast Startup: This mode is reserved for future feature extensions, do not select it.

Link Monitoring: Specify whether the link behavior is to be monitored at the selected port.

Default Priority: Set the priority for incoming data packets to this port.

Jumbo Frames: Enable/disable the support of jumbo frames (>1518 bytes). The MTU size is set to 9600 bytes following activation.

ℹ The “Jumbo Frames” function is only available on SG300 Gigabit models.

MTU: Here, you can set the maximum transmission unit (MTU). Packet sizes between 1522 bytes and 9600 bytes are accepted.

Flow Control: Flow control for the selected port can be enabled and disabled here.

CRC Surveillance items

Received Pkts: Shows the number of packets received at the selected port since the last reboot or counter reset.

CRC Errors: Shows the number of CRC errors at the selected port since the last reboot or counter reset.

CRC Proportion Peak (ppm): Shows the highest proportion of CRC errors that occurred in a 30-second interval, relative to the total number of packets received in this interval since the last reboot or counter reset.

CRC Port Status: Shows the status of the current port.

Critical Threshold (ppm): Here, you can enter the threshold value at which the CRC Port Status switches to Critical (1000 ppm - 1,000,000 ppm are acceptable).

Warning Threshold (ppm): Shows the threshold value in ppm at which the CRC Port Status switches to Warning (50% of Critical Threshold).

Clear CRC Peak and CRC Status: Clicking the "Clear" button resets the CRC Peak and CRC Status.

Port Counter Overview: Clicking on the "Monitor all ports simultaneously" link takes you to the "Port Counter" page.

Advanced Port Configuration items

Port Configuration Table: Clicking on the "Configure all ports simultaneously" link takes you to the "Port Configuration Table" page. There, you can set the status, mode, link monitoring, jumbo frames, and flow control for all ports.

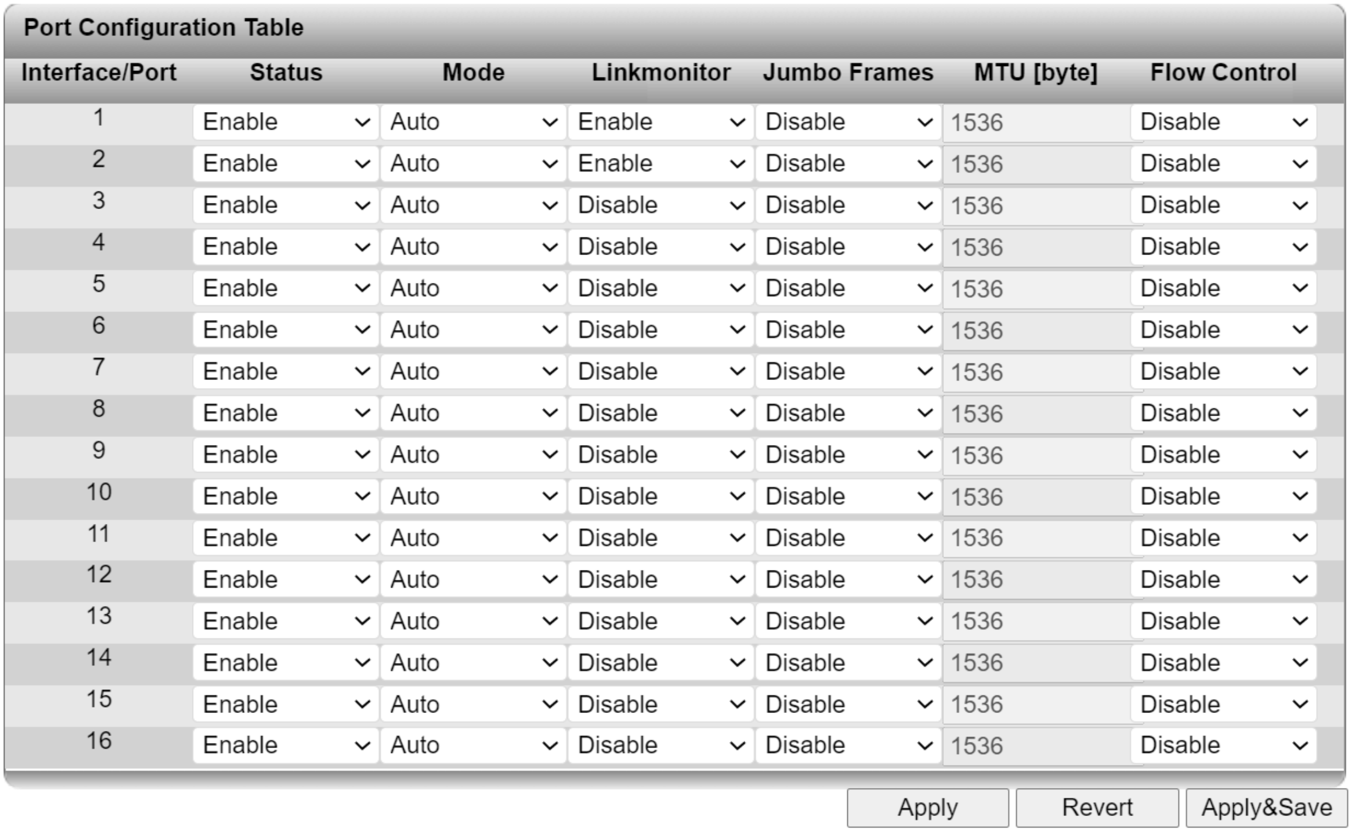
Port Mirroring: Clicking on the "Configure Port Mirroring" button takes you to the port mirroring configuration page.

VLAN Port Configuration: Clicking on the "Configure Port Settings for a VLAN" button takes you to the "VLAN Port Configuration" page.

Link Aggregation: Clicking on the "Configure Link Aggregation" button takes you to the "Link Aggregation" page.

Port Based Security: Clicking on the "Configure Port Based Security" button takes you to the "Port Based Security" page.

Port Configuration Table



Port Configuration Table

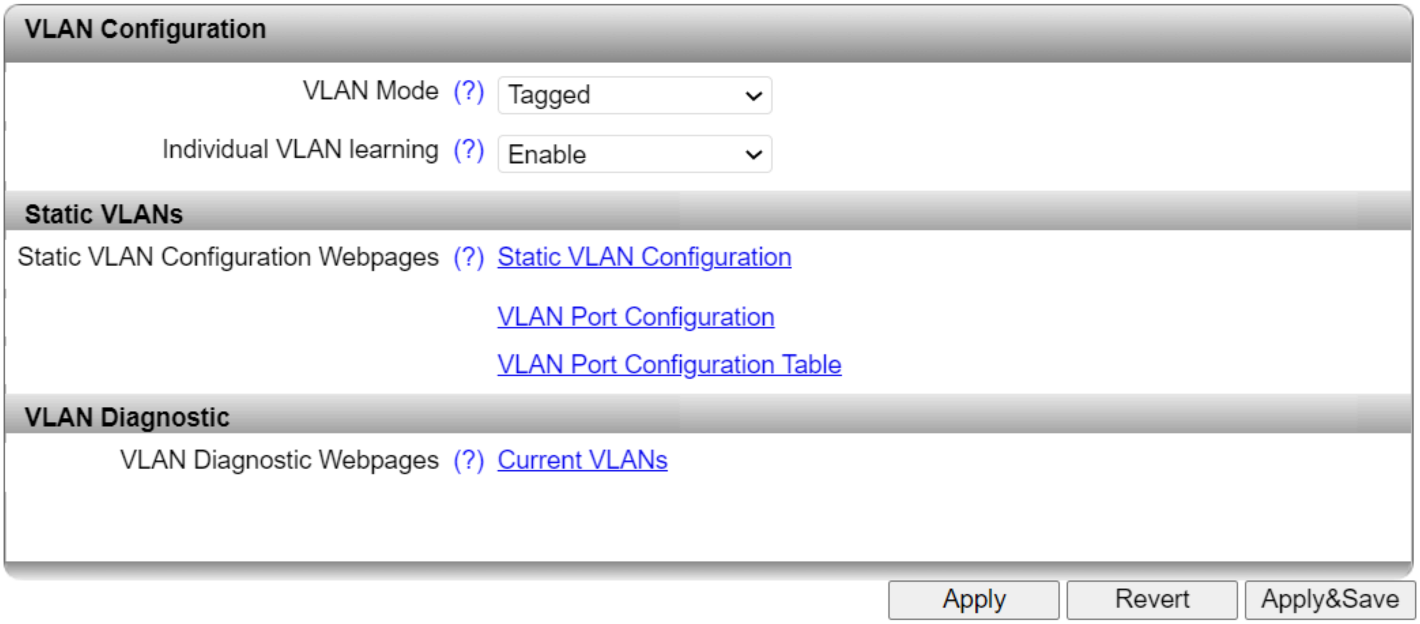
Interface/Port	Status	Mode	Linkmonitor	Jumbo Frames	MTU [byte]	Flow Control
1	Enable	Auto	Enable	Disable	1536	Disable
2	Enable	Auto	Enable	Disable	1536	Disable
3	Enable	Auto	Disable	Disable	1536	Disable
4	Enable	Auto	Disable	Disable	1536	Disable
5	Enable	Auto	Disable	Disable	1536	Disable
6	Enable	Auto	Disable	Disable	1536	Disable
7	Enable	Auto	Disable	Disable	1536	Disable
8	Enable	Auto	Disable	Disable	1536	Disable
9	Enable	Auto	Disable	Disable	1536	Disable
10	Enable	Auto	Disable	Disable	1536	Disable
11	Enable	Auto	Disable	Disable	1536	Disable
12	Enable	Auto	Disable	Disable	1536	Disable
13	Enable	Auto	Disable	Disable	1536	Disable
14	Enable	Auto	Disable	Disable	1536	Disable
15	Enable	Auto	Disable	Disable	1536	Disable
16	Enable	Auto	Disable	Disable	1536	Disable

Mode: The port can be set to a fixed speed and transmission mode here.
– Auto: The transmission speed and mode are selected automatically.
– 10 Mbps Half Duplex: The port transmits at a speed of 10 Mbps in half-duplex mode.
– 10 Mbps Full Duplex: The port transmits at a speed of 10 Mbps in full-duplex mode.
– 100 Mbps Half Duplex: The port transmits at a speed of 100 Mbps in half-duplex mode.
– 100 Mbps Full Duplex: The port transmits at a speed of 100 Mbps in full-duplex mode.
– Fast Startup: This mode is reserved for future feature extensions, do not select it.

Link Monitoring: Specify whether the link behavior is to be monitored at the selected port. An alarm message is then generated under “Alarm & Events”.

Flow Control: Flow control for the selected port can be enabled and disabled here.

Configuration – VLAN Configuration


VLAN Configuration

VLAN Mode (?) Tagged

Individual VLAN learning (?) Enable

Static VLANs

Static VLAN Configuration Webpages (?) Static VLAN Configuration

VLAN Port Configuration

VLAN Port Configuration Table

VLAN Diagnostic

VLAN Diagnostic Webpages (?) Current VLANs

VLAN Mode:

- Transparent: In “Transparent” mode, the switch processes the incoming data packets as described in the “Frame switching” section. Neither the structure nor the contents of the data packets are changed. The information about VLAN assignment from a tag that may be contained in the data packet is ignored.
- Tagged: In “Tagged” mode, the switch forwards the data packets based on the VLAN assignment.

Individual VLAN learning: Select whether Individual VLAN learning should be activated. If you deactivate this function, you can use asymmetric VLAN. The function can only be deactivated if you selected “Tagged” for “VLAN Mode”.

ℹ If you deactivate the function, you cannot use the MAC-based Port Security function.

Static VLANs

Static VLAN Configuration Webpages:

Clicking on the “Static VLAN Configuration” link takes you to the “Static VLAN Configuration” web page (see below). Up to 32 static VLANs can be set up here.

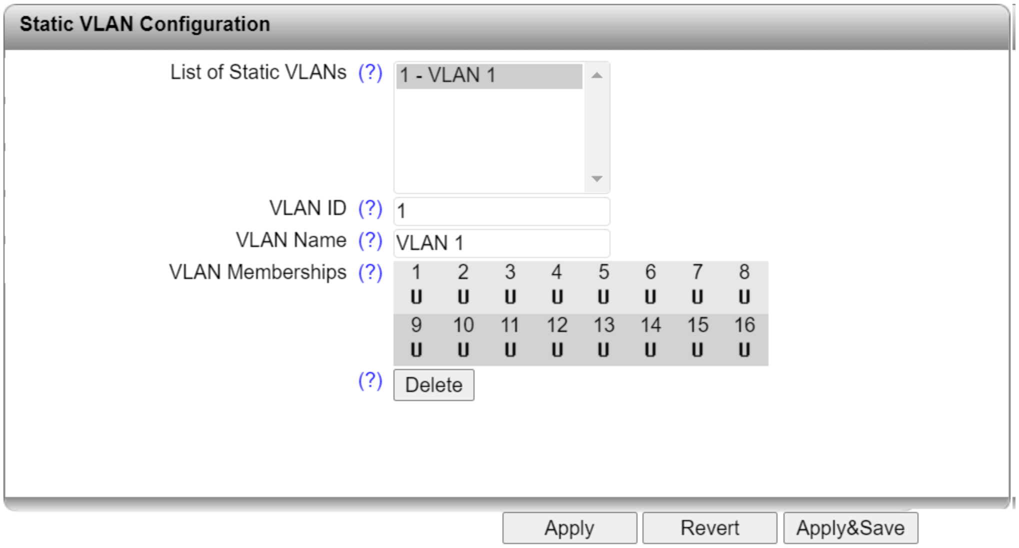
Clicking on the “VLAN Port Configuration” link takes you to the “VLAN Port configuration” web page.

Clicking on the “VLAN Port Configuration Table” link takes you to the VLAN port configuration table.

VLAN Diagnostic Webpages:

Clicking on the “Current VLANs” link opens the “Current VLANs” page as a pop-up.

Static VLAN Configuration



Static VLAN Configuration

List of Static VLANs (?) 1 - VLAN 1

VLAN ID (?) 1

VLAN Name (?) VLAN 1

VLAN Memberships (?)

1	2	3	4	5	6	7	8
U	U	U	U	U	U	U	U
9	10	11	12	13	14	15	16
U	U	U	U	U	U	U	U

List of Static VLANs: All VLANs created up to this point are displayed here.

VLAN ID: Set the VLAN ID you wish to assign to the new VLAN. The value must be between 2 and 4094.

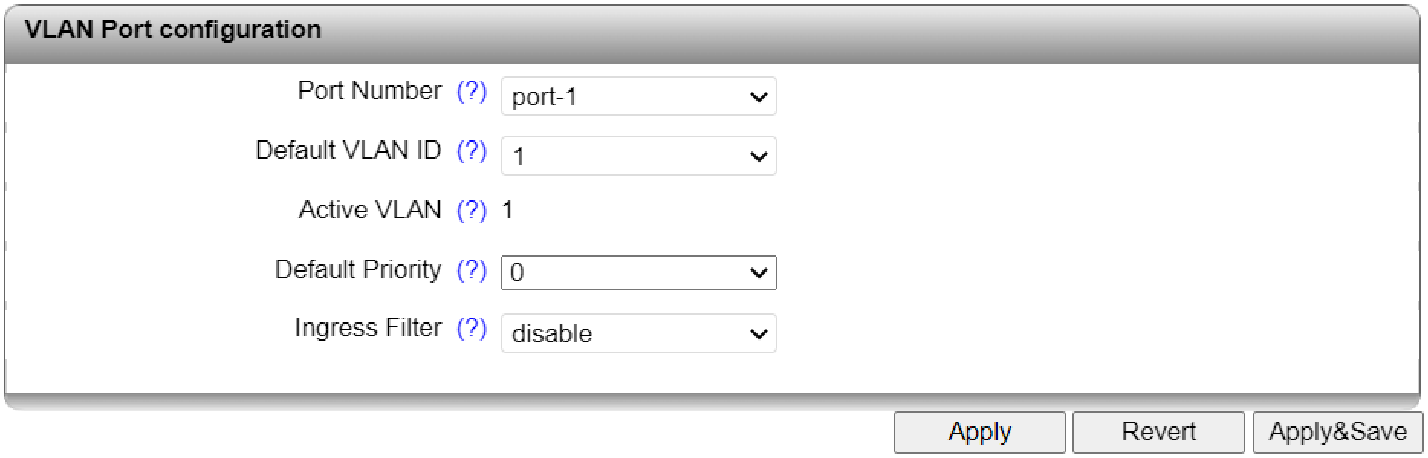
VLAN Name: Specify the VLAN name you wish to create.

VLAN Memberships: Specify which ports are to be located in the VLAN.

- T: Tagged port
- U: Untagged port
- -: Not a member of the VLAN

Use the “Delete” button to delete the VLAN selected in the list. VLAN 1 cannot be deleted.

VLAN Port configuration



VLAN Port configuration

Port Number (?)	port-1
Default VLAN ID (?)	1
Active VLAN (?)	1
Default Priority (?)	0
Ingress Filter (?)	disable

Port Number: Select the port for which you want to change the VLAN settings.

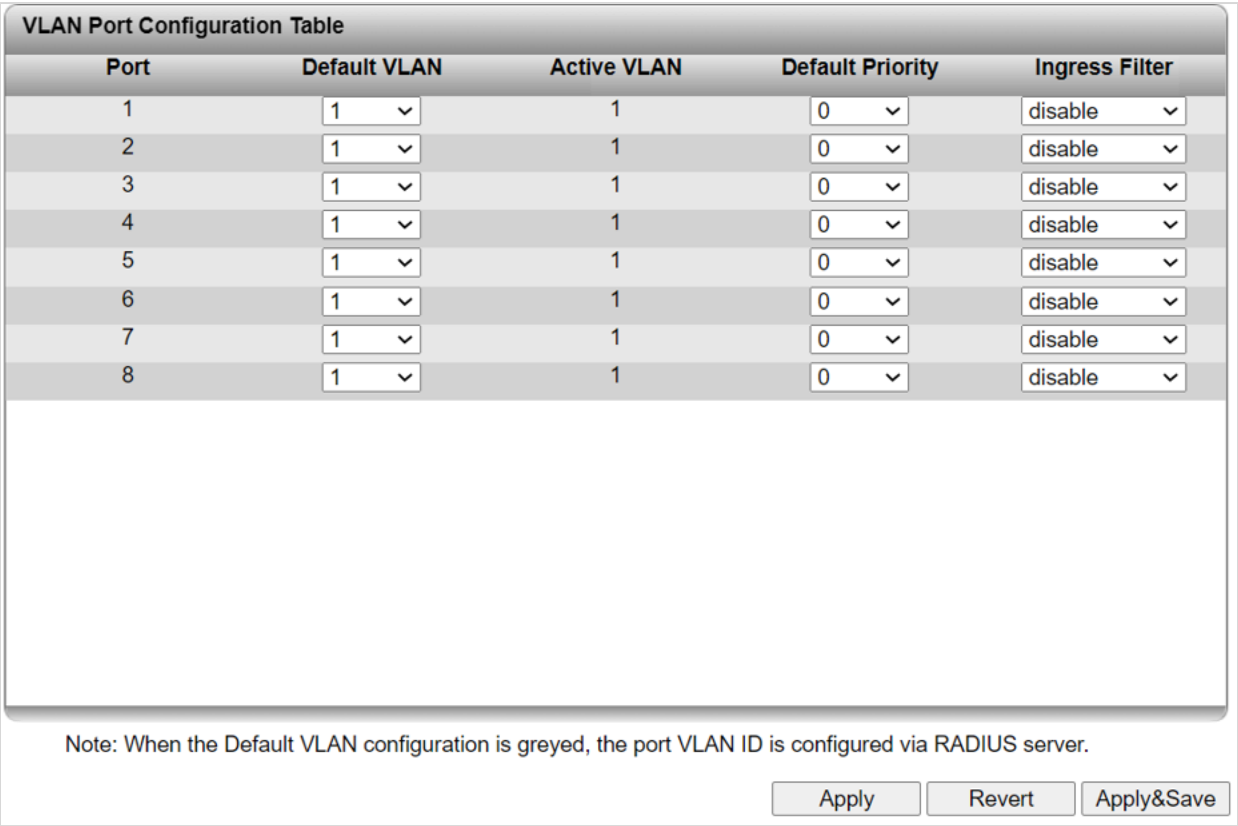
Default VLAN ID: Select the VLAN ID that is to be assigned to the port.

Active VLAN: If the port-specific VLAN ID is assigned via a RADIUS server, the “Active VLAN” display appears and the configured “Default VLAN ID” is grayed out. “Active VLAN” then shows the VLAN ID assigned to this port via the RADIUS server.

Default Priority: Set the VLAN priority for the selected port.

Ingress Filter: Specify whether the ingress filter should be activated. An ingress filter protects networks from unwanted incoming data traffic. Packets arriving with a VLAN ID that does not match the port membership will be filtered out.

VLAN Port Configuration Table



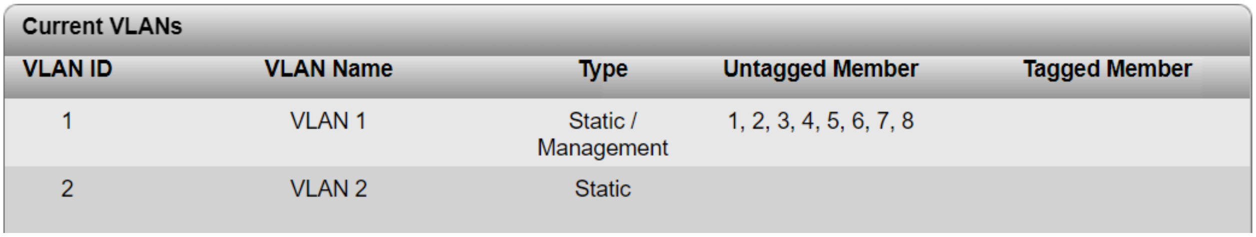
VLAN Port Configuration Table

Port	Default VLAN	Active VLAN	Default Priority	Ingress Filter
1	1	1	0	disable
2	1	1	0	disable
3	1	1	0	disable
4	1	1	0	disable
5	1	1	0	disable
6	1	1	0	disable
7	1	1	0	disable
8	1	1	0	disable

Note: When the Default VLAN configuration is greyed, the port VLAN ID is configured via RADIUS server.

Current VLANs

This page lists the current VLANs, their type, and the ports for each VLAN, which are either “Tagged” or “Untagged”.



Current VLANs

VLAN ID	VLAN Name	Type	Untagged Member	Tagged Member
1	VLAN 1	Static / Management	1, 2, 3, 4, 5, 6, 7, 8	
2	VLAN 2	Static		

VLAN ID: The VLAN ID is displayed here.

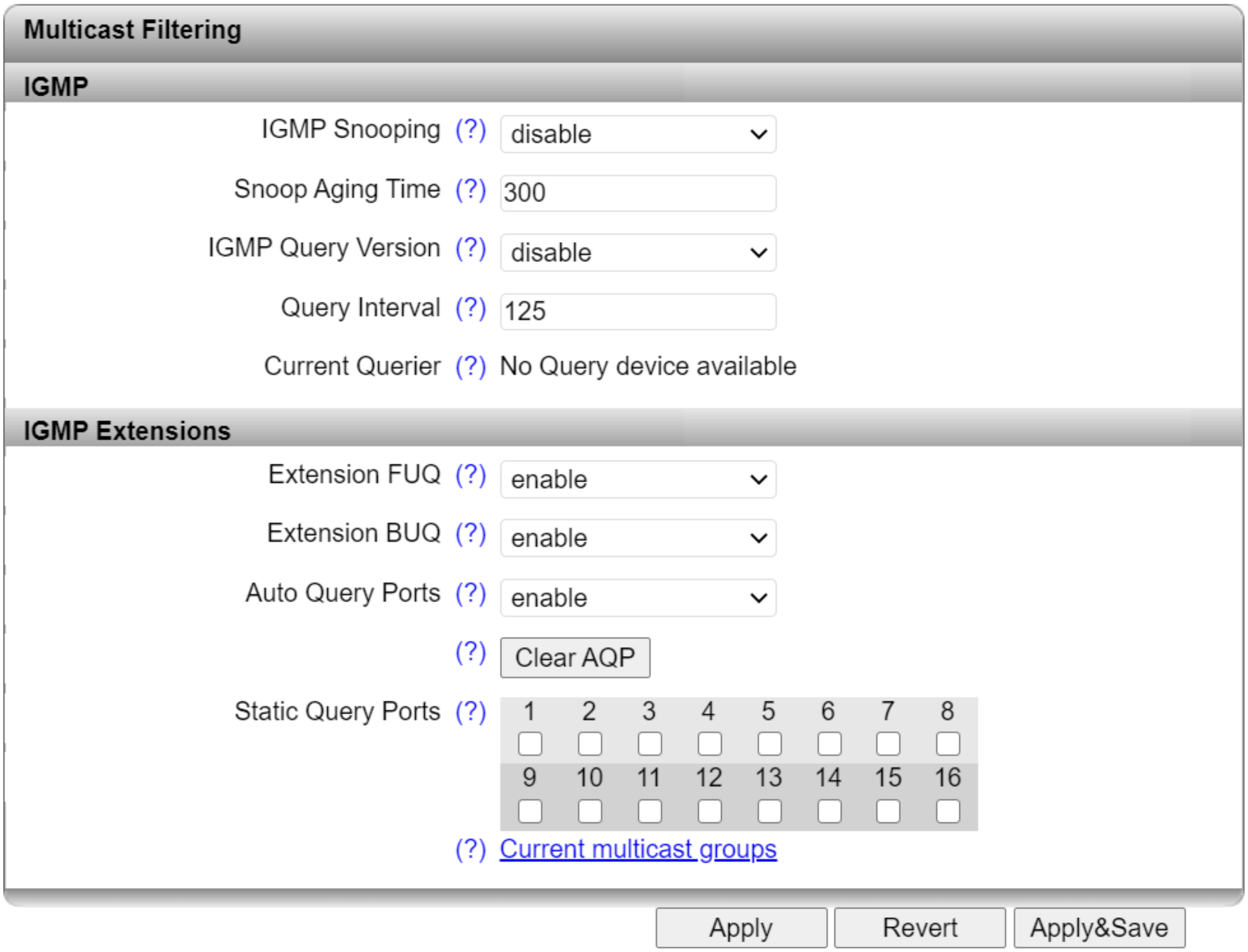
VLAN Name: The VLAN name is displayed here.

Type: The VLAN type is displayed here.

Untagged Member: The untagged members of the VLAN are displayed here.

Tagged Member: The tagged members of the VLAN are displayed here.

Configuration – Multicast Filtering



Multicast Filtering

IGMP

IGMP Snooping (?) disable

Snoop Aging Time (?) 300

IGMP Query Version (?) disable

Query Interval (?) 125

Current Querier (?) No Query device available

IGMP Extensions

Extension FUQ (?) enable

Extension BUQ (?) enable

Auto Query Ports (?) enable

(?) Clear AQP

Static Query Ports (?)

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□

(?) Current multicast groups

IGMP Snooping:

- disable: The “IGMP Snooping” function is disabled.
- enable: The “IGMP Snooping” function is enabled.

Snoop Aging Time: Set the snoop aging time. This is the time period during which membership reports are expected from the querier. If no membership reports are received during this time, the associated ports are deleted from the multicast groups. The value must be between 30 and 3600 (default is 300).

IGMP Query Version: Here, you can set the IGMP query version which the switch should use to send the queries. The switches support IGMP query versions v1 and v2. For Ethernet/IP applications, it is recommended that you activate version v2.

Query Interval: Here, you can set the interval at which the switch should send the queries. The value must be between ten and 3600 seconds.

Current Querier: Displays the IP address of the current querier in the network.

ℹ The IGMP querier function can only be used if the device has an IP address. Use of multicast filtering in Unmanaged mode is therefore limited to IGMP snooping.

Clicking on the “Current multicast groups” link opens the “Current Multicast Groups” page as a pop-up.

Extensions FUQ (Forward Unknown to Querier): Specify whether a multicast group should be created for unknown multicast packets, which forwards the packets in the direction of the querier.

Extension BUQ (Block Unknown at Querier): Specify whether unknown multicast packets should be blocked at the querier.

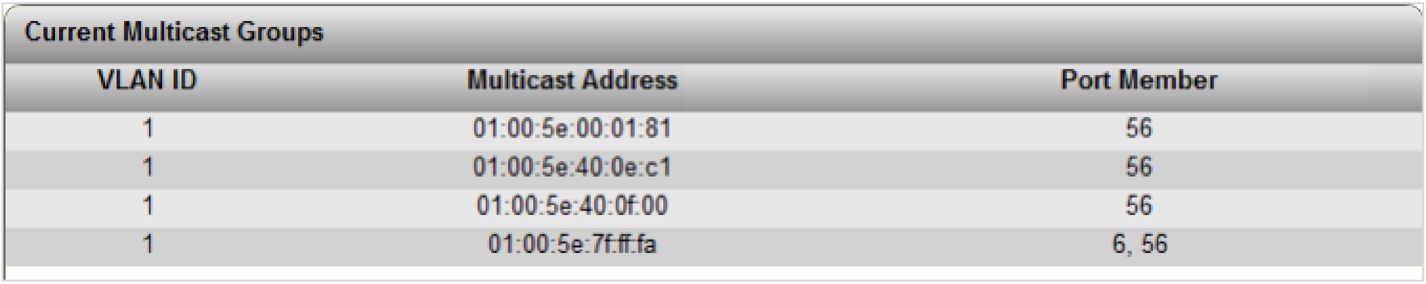
Auto Query Ports: Specify whether automatic selection of additional query ports is activated. Ports are automatically integrated in every multicast group. In the case of redundancy switch-over, the multicast packets are not blocked because the ports required are already members of the multicast group.

Clear AQP: Button for deleting the ports that are automatically assigned to the groups.

Static Query Ports: Select the ports that are static query ports.

ℹ The device can manage up to 50 dynamic multicast groups.

Click the **Current Multicast Groups** link to open a window that displays the current multicast groups:



Current Multicast Groups

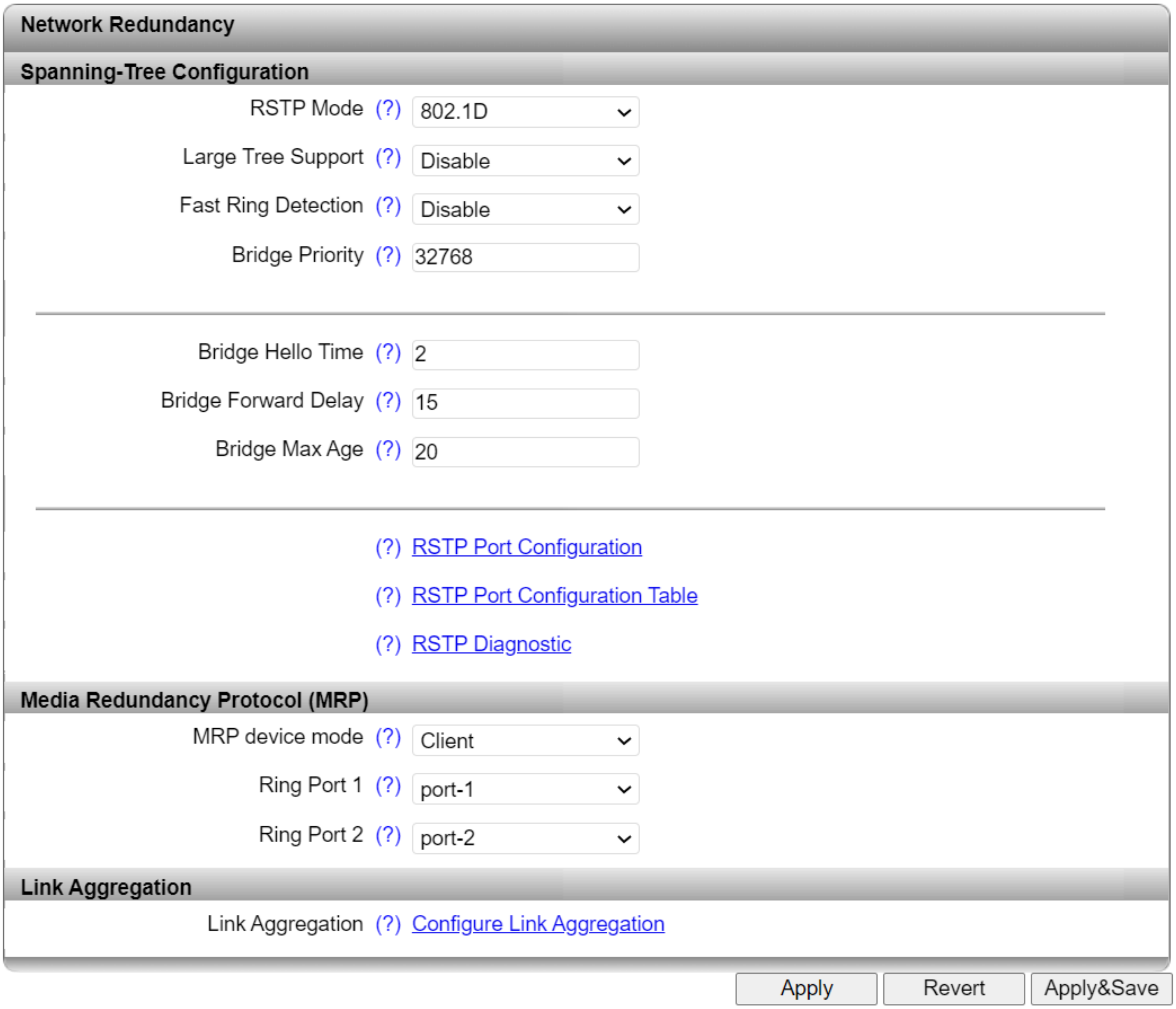
VLAN ID	Multicast Address	Port Member
1	01:00:5e:00:01:81	56
1	01:00:5e:40:0e:c1	56
1	01:00:5e:40:0f:00	56
1	01:00:5e:7f:ff:fa	6, 56

VLAN ID: The VLAN ID of the corresponding multicast group is displayed here.

Multicast Address: The MAC address of the multicast group is displayed here.

Port Member: The associated ports of the multicast group are displayed here.

Configuration – Network Redundancy



Network Redundancy

Spanning-Tree Configuration

RSTP Mode (?) 802.1D

Large Tree Support (?) Disable

Fast Ring Detection (?) Disable

Bridge Priority (?) 32768

Bridge Hello Time (?) 2

Bridge Forward Delay (?) 15

Bridge Max Age (?) 20

(?) RSTP Port Configuration

(?) RSTP Port Configuration Table

(?) RSTP Diagnostic

Media Redundancy Protocol (MRP)

MRP device mode (?) Client

Ring Port 1 (?) port-1

Ring Port 2 (?) port-2

Link Aggregation

Link Aggregation (?) Configure Link Aggregation

Spanning-Tree Configuration Items

RSTP Mode:

- Disable: The RSTP function is not activated
- 802.1D: The RSTP function is activated globally and working in accordance with standard IEEE802.1D-2004

The functions below are only available if “802.1D” is activated.

Large Tree Support: This option makes the ring topology suitable for 28 switches along the relevant path if RSTP is used. The Large Tree Support option could provide an RSTP ring topology with up to 57 devices. If the "Large Tree Support" function is enabled, it is recommended to use the default parameters. (see Appendix. Large Tree Support for more information.)

Fast Ring Detection: This function speeds up switch-over to a redundant path in the event of an error and enables easy diagnostics. RSTP Fast Ring Detection assigns an ID to each ring. This ID is communicated to every switch in the respective ring. One switch can belong to several different rings at the same time. (see Appendix. Fast Ring Detection for more information.)

Bridge Priority: The bridge and backup root can be specified via "Bridge Priority". Only multiples of 4096 are permitted. The value will be rounded automatically to the next multiple of 4096. When you click on "Apply & Save," the initialization mechanism is started (default is 32,768).

Bridge Hello Time: Specifies the time interval within which the root bridge regularly reports to the other switches via BPDU. The value must be between one and ten seconds.

ℹ This setting must only be made on the root bridge.

ℹ We recommend that you keep the default setting.

Bridge Forward Delay: The value indicates how long the switches are to wait for the port state in STP mode to change from "Discarding" to "Listening" and from "Listening" to "Learning" (2 x Forward Delay). The value must be between four and 30 seconds. The device only switches to the "Forwarding" status once this time has elapsed. In the "Listening" and "Learning" status, the device does not forward any user traffic and consequently prevents transient loops.

ℹ This setting must only be made on the root bridge.

ℹ We recommend that you keep the default setting.

Bridge Max Age: The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to ensure that each switch in the network has a constant value, which is used as the basis for testing the age of the saved configuration. The value must be between six and 40 seconds.

ℹ This setting must only be made on the root bridge.

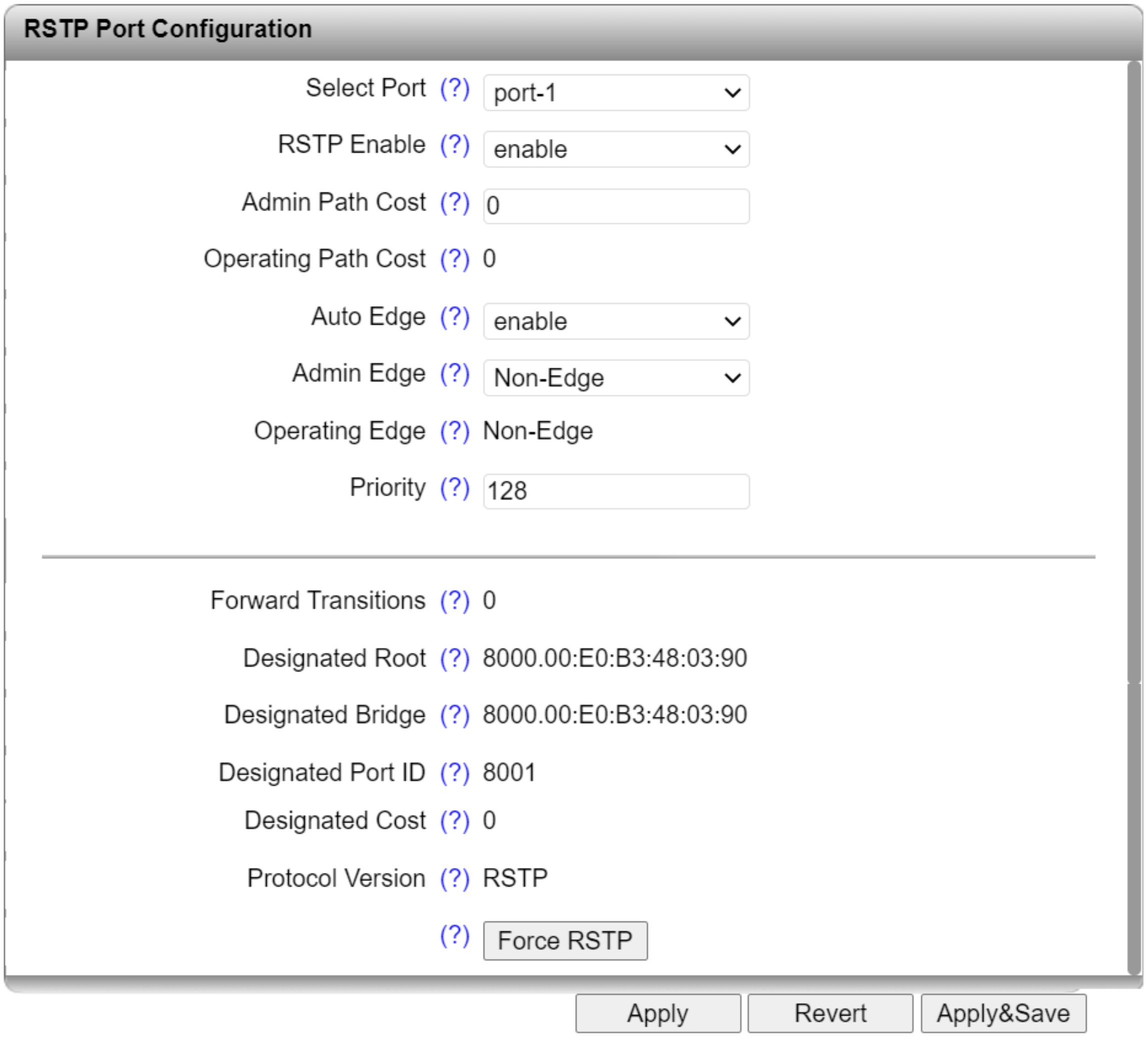
ℹ We recommend that you keep the default setting.

Clicking on the "RSTP Port Configuration" button takes you to the "RSTP Port Configuration" pop-up (see below).

Clicking on the "RSTP Port Configuration Table" button takes you to the "RSTP Port Configuration Table" pop-up.

Clicking on the "RSTP Diagnostics" button opens the "RSTP Diagnostics" page as a pop-up.

RSTP Port Configuration



RSTP Port Configuration

Select Port (?) port-1

RSTP Enable (?) enable

Admin Path Cost (?) 0

Operating Path Cost (?) 0

Auto Edge (?) enable

Admin Edge (?) Non-Edge

Operating Edge (?) Non-Edge

Priority (?) 128

Forward Transitions (?) 0

Designated Root (?) 8000.00:E0:B3:48:03:90

Designated Bridge (?) 8000.00:E0:B3:48:03:90

Designated Port ID (?) 8001

Designated Cost (?) 0

Protocol Version (?) RSTP

Select Port: Select the port for which you want to change the RSTP settings.

RSTP Enable:

- Enable: RSTP is activated for the port
- Disable: RSTP is deactivated for the port

Admin Path Cost: Enter the path costs set for this port. The value must be between zero and 200000000. A path cost equal to “0” activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).

Operating Path Cost: Displays the path costs used for this port.

Auto Edge: Specify whether to automatically switch from non-edge port to edge port after a link up.

Admin Edge: Specify whether this port is to be operated as an edge port (default setting), if possible.

Operating Edge: Shows whether this port is operated as an edge port or a non-edge port.

Priority: Enter the priority set for this port. The value must be between zero and 140. Multiples of 16 are permitted. The entered value is automatically rounded to the next multiple of 16 (default: 128).

Forward Transitions: Indicates the number of times the port has switched from the “Discarding” state to the “Forwarding” state.

Designated Root: Shows the root bridge for this spanning tree.

Designated Bridge: Indicates the switch from which the port receives the best BPDUs.

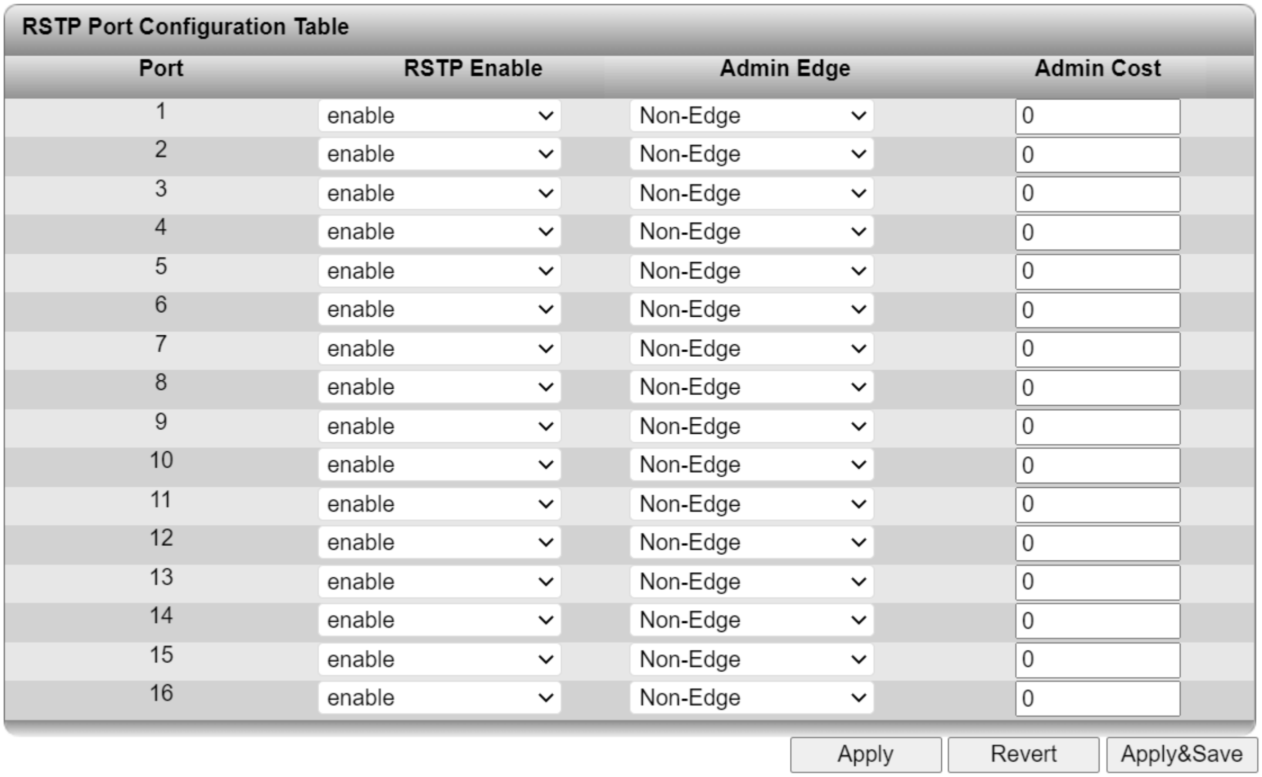
Designated Port ID: Indicates the port via which the BPDUs are sent from the designated bridge. The value is based on the port priority (2 digits) and the port number. The value is displayed in hexadecimal numbers.

Designated Cost: Shows the path costs of this segment to the root switch.

Protocol Version: Shows the protocol version.

Force RSTP: Clicking on the “Force RSTP” button activates RSTP for the port as long as it has been operated in STP mode beforehand.

RSTP Port Configuration Table



RSTP Port Configuration Table

Port	RSTP Enable	Admin Edge	Admin Cost
1	enable	Non-Edge	0
2	enable	Non-Edge	0
3	enable	Non-Edge	0
4	enable	Non-Edge	0
5	enable	Non-Edge	0
6	enable	Non-Edge	0
7	enable	Non-Edge	0
8	enable	Non-Edge	0
9	enable	Non-Edge	0
10	enable	Non-Edge	0
11	enable	Non-Edge	0
12	enable	Non-Edge	0
13	enable	Non-Edge	0
14	enable	Non-Edge	0
15	enable	Non-Edge	0
16	enable	Non-Edge	0

Port: Shows the ports for which RSTP is available.

RSTP Enable: Activate or deactivate RSTP for each port individually.

Admin Edge: Specify whether this port is to be operated as an edge port (default setting), if possible.

Admin Cost: Enter the path costs set for this port. A path cost equal to “0” activates cost calculation according to the transmission speed (10 Mbps = 2,000,000; 100 Mbps = 200,000).

Media Redundancy Protocol (MRP)

A ring can be created in the network using MRP in accordance with IEC 62439, thus providing a redundant connection.

A ring may contain a maximum of 50 switches, one of which is defined as the MRP manager. All other devices in the ring must support the MRP client function. The ring is created using dedicated ports. The MRP ports are configured in the management for the respective switch. When configure correctly, MRP offers a guaranteed maximum switch-over time of 200 ms.

ℹ The MRP function is only available on firmware versions 3.20 or later.

MRP device mode:

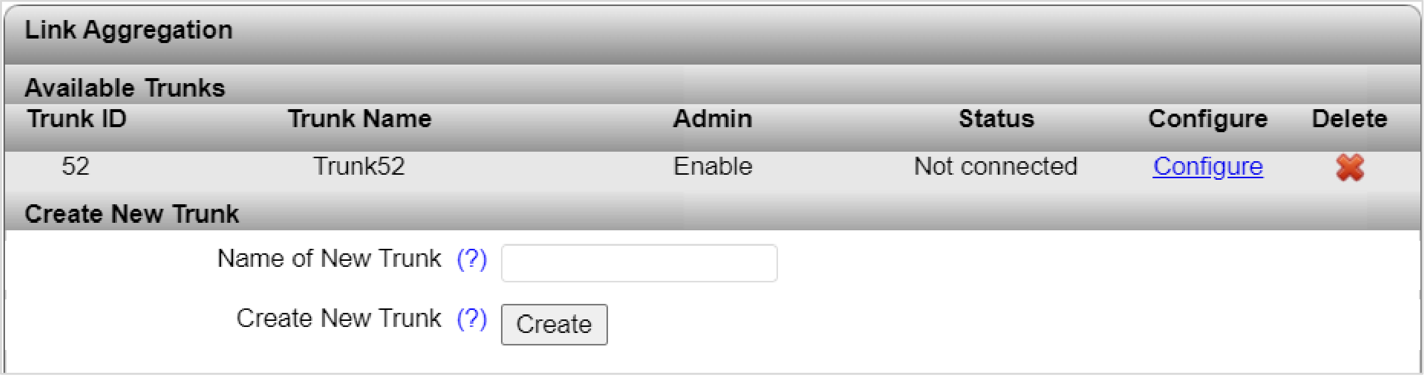
- Disable: The MRP function is not activated.
- Client: The MRP function is activated. The switch is an MRP client.
- Manager: The MRP function is activated. The switch is the ring manager.

Ring Port 1: Select the first MRP ring port here.

Ring Port 2: Select the second MRP ring port here.

Link Aggregation

Clicking on the “Link Aggregation” link takes you to the configuration page for link aggregation:



Link Aggregation

Available Trunks

Trunk ID	Trunk Name	Admin	Status	Configure	Delete
52	Trunk52	Enable	Not connected	Configure	✖

Create New Trunk

Name of New Trunk (?)

Create New Trunk (?) Create

Trunk ID: This column shows the trunk ID.

Trunk Name: This column shows the trunk name.

Admin: This column shows whether the trunk is enabled for administration.

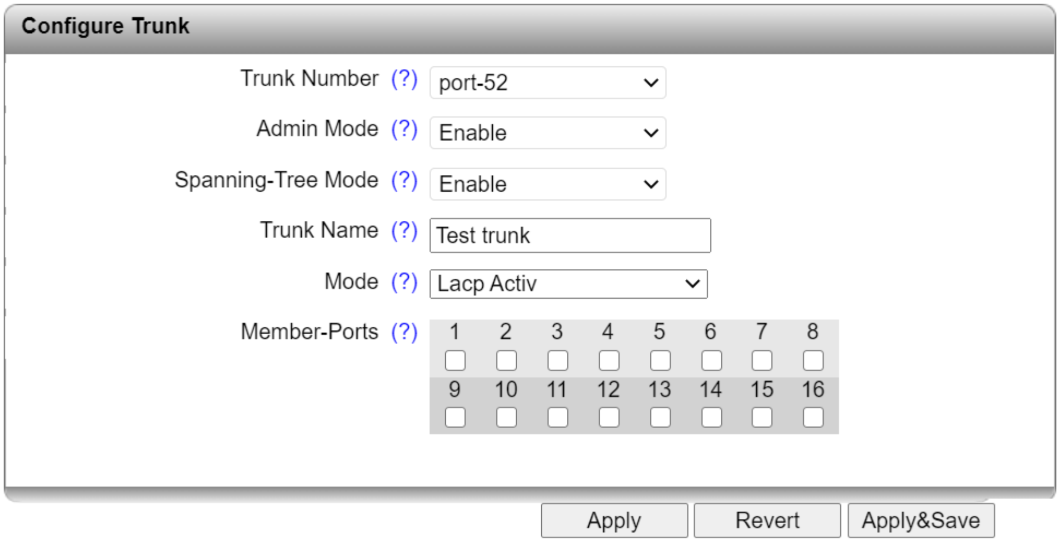
Status: This column shows the trunk connection status.

Configure: Clicking on the “Configure” link in the table containing all the created trunks opens the configuration page for the respective trunk.

Delete: Click on the red “X” to delete the selected trunk.

Name of New Trunk: Enter a name for a new trunk.

Create New Trunk: Click on the “Create” button to create a new empty trunk.



Configure Trunk

Trunk Number (?) port-52

Admin Mode (?) Enable

Spanning-Tree Mode (?) Enable

Trunk Name (?) Test trunk

Mode (?) Lacp Activ

Member-Ports (?)

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□

Trunk Number: Select the trunk to be configured by entering its ID.

Admin Mode: Enable or disable a trunk.

Spanning-Tree Mode: Here, select whether the RSTP protocol is to be enabled for this trunk.

Trunk Name: Here, you can change the name of the trunk.

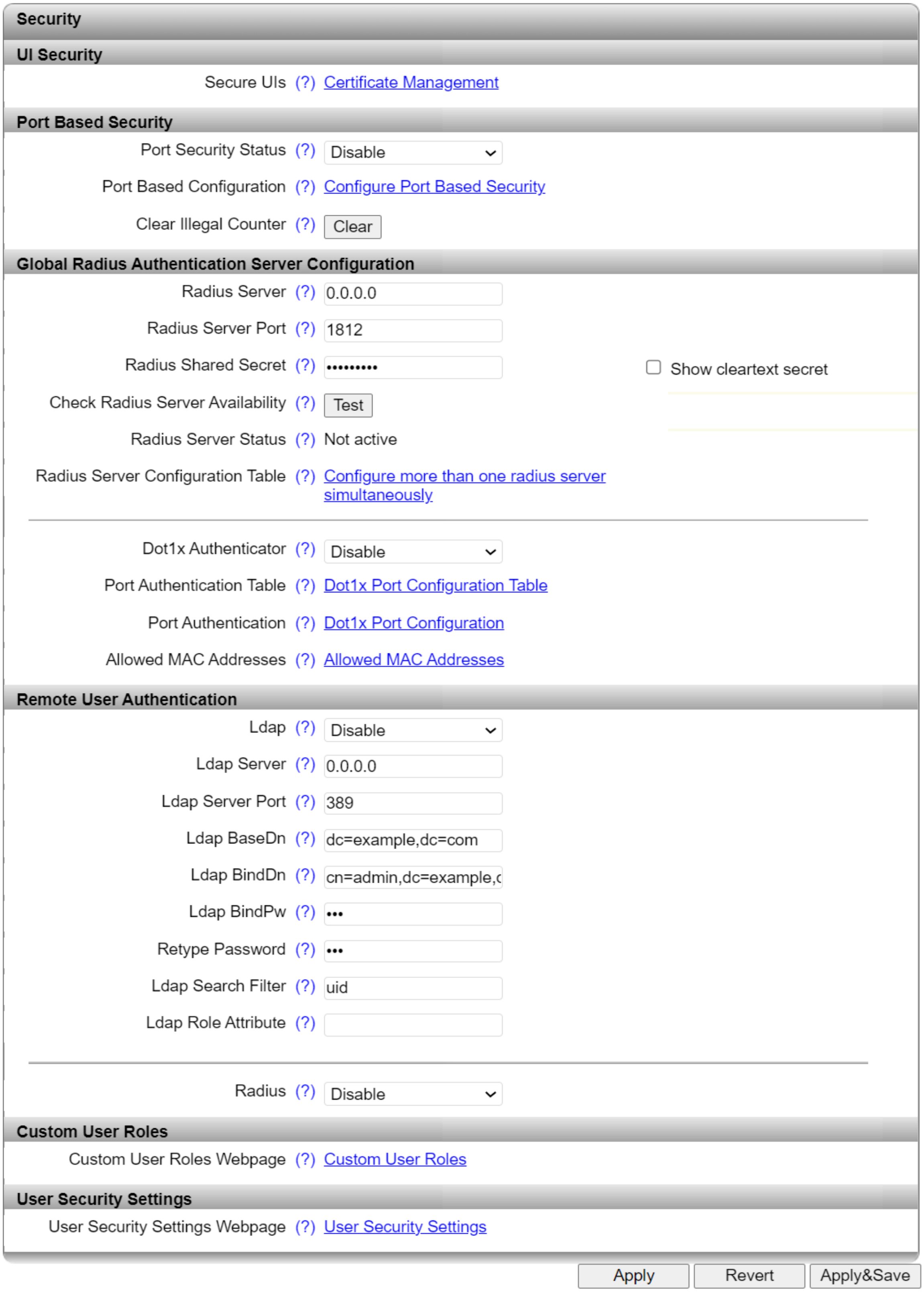
Mode: Here, you can specify how ports are to be added to the trunk.

- Static: The ports are immediately added to the trunk.
- When “LACP Active/Passive” is selected, the two members of a link aggregation first exchange information via LACPDUs:
    - With “Active”, this is regardless of whether the peer also has LACP.
    - With “Passive”, this only occurs after LACPDUs have been received by the peer.

ℹ If the switch is used as an MRP client and if a trunk port was selected for at least one ring port, increased recovery times may be required in the MRP ring if “LACP Active/Passive” is activated. In this case, it is therefore recommended to select “Static” mode.

Member-Ports: Select up to four ports that are to belong to the trunk.

Configuration – Security



Security

UI Security

Secure UIs (?) Certificate Management

Port Based Security

Port Security Status (?) Disable

Port Based Configuration (?) Configure Port Based Security

Clear Illegal Counter (?) Clear

Global Radius Authentication Server Configuration

Radius Server (?) 0.0.0.0

Radius Server Port (?) 1812

Radius Shared Secret (?) ••••••••• □ Show cleartext secret

Check Radius Server Availability (?) Test

Radius Server Status (?) Not active

Radius Server Configuration Table (?) Configure more than one radius server simultaneously

Dot1x Authenticator (?) Disable

Port Authentication Table (?) Dot1x Port Configuration Table

Port Authentication (?) Dot1x Port Configuration

Allowed MAC Addresses (?) Allowed MAC Addresses

Remote User Authentication

Ldap (?) Disable

Ldap Server (?) 0.0.0.0

Ldap Server Port (?) 389

Ldap BaseDn (?) dc=example,dc=com

Ldap BindDn (?) cn=admin,dc=example,c

Ldap BindPw (?) •••

Retype Password (?) •••

Ldap Search Filter (?) uid

Ldap Role Attribute (?)

Radius (?) Disable

Custom User Roles

Custom User Roles Webpage (?) Custom User Roles

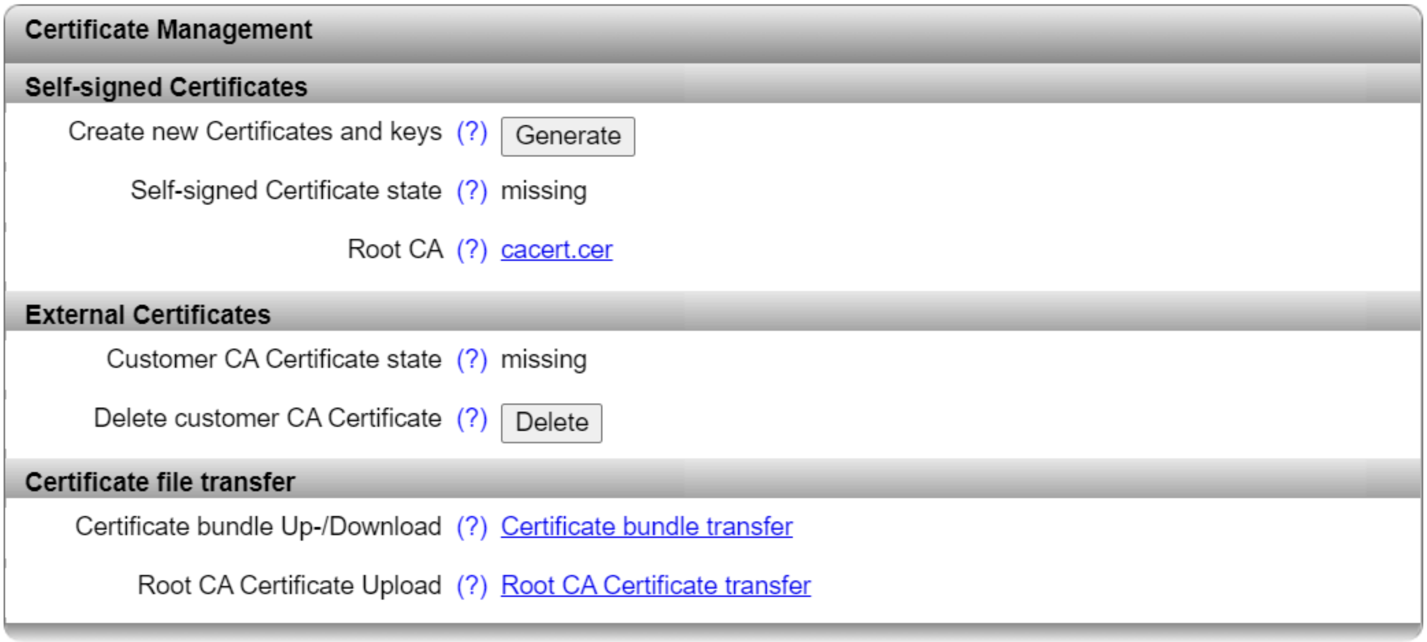
User Security Settings

User Security Settings Webpage (?) User Security Settings

UI Security Items

Secure UIs: Clicking on the “Certificate Management” link opens the pop-up of the same name.

Pop-up window of “Certificate Management”



Certificate Management

Self-signed Certificates

Create new Certificates and keys (?) Generate

Self-signed Certificate state (?) missing

Root CA (?) cacert.cer

External Certificates

Customer CA Certificate state (?) missing

Delete customer CA Certificate (?) Delete

Certificate file transfer

Certificate bundle Up-/Download (?) Certificate bundle transfer

Root CA Certificate Upload (?) Root CA Certificate transfer

Create new Certificates and keys: Click on “Generate” to create all the necessary keys and certificates for operation with HTTPS and SSH.

Self-signed Certificate state: The current availability of the self-signed certificate is displayed here.

Root CA: Click on “cacert.cer” to download the created root CA certificate for the installation from the device.

Customer CA Certificate state: The current status of the customer CA certificate is displayed here. You can provide your own signed certificate. Your browser’s security warnings will then no longer be triggered.

Delete customer CA Certificate: Click on “Delete” to delete your own signed certificate.

Certificate bundle Up-/Download: Click on “Certificate bundle transfer” to open the “File Transfer” pop-up window (see “File Transfer”).

Root CA Certificate Upload: Click on “Root CA Certificate transfer” to open the “File Transfer” pop-up window (see “File Transfer”).

Port Based Security Items

Port Security Status: Here, you can globally enable and disable port-based security.

Port Based Configuration: Clicking on the "Configure Port Based Security" link takes you to the configuration page for port-based security (see below).

Clear Illegal Counter: Clicking on the "Clear" button sets the illegal access counter for all of the ports to zero.

Global Radius Authentication Server Configuration Items

Radius Server: Here, you can set the IP address of the RADIUS authentication server.

Radius Server Port: Here, you can set the UDP port of the RADIUS server (default is 1812).

Radius Shared Secret: Here, you can set the shared secret required for encrypted communication with the RADIUS authentication server. The shared secret must have between eight and 64 characters..

Check Radius Server Availability: Clicking on the "Test" button checks whether the configured RADIUS server is reachable.

Radius Server Status: The status of the RADIUS server that can be checked via "Check Radius Server Availability" is displayed here.

Radius Server Configuration Table: Click on "Configure more than one radius server simultaneously" to open the "Radius Server Configuration Table" window.

Dot1x Authenticator: Here, you can specify whether the device should be an 802.1x authenticator or not.

ℹ One end device can be authenticated via 802.1x per port.

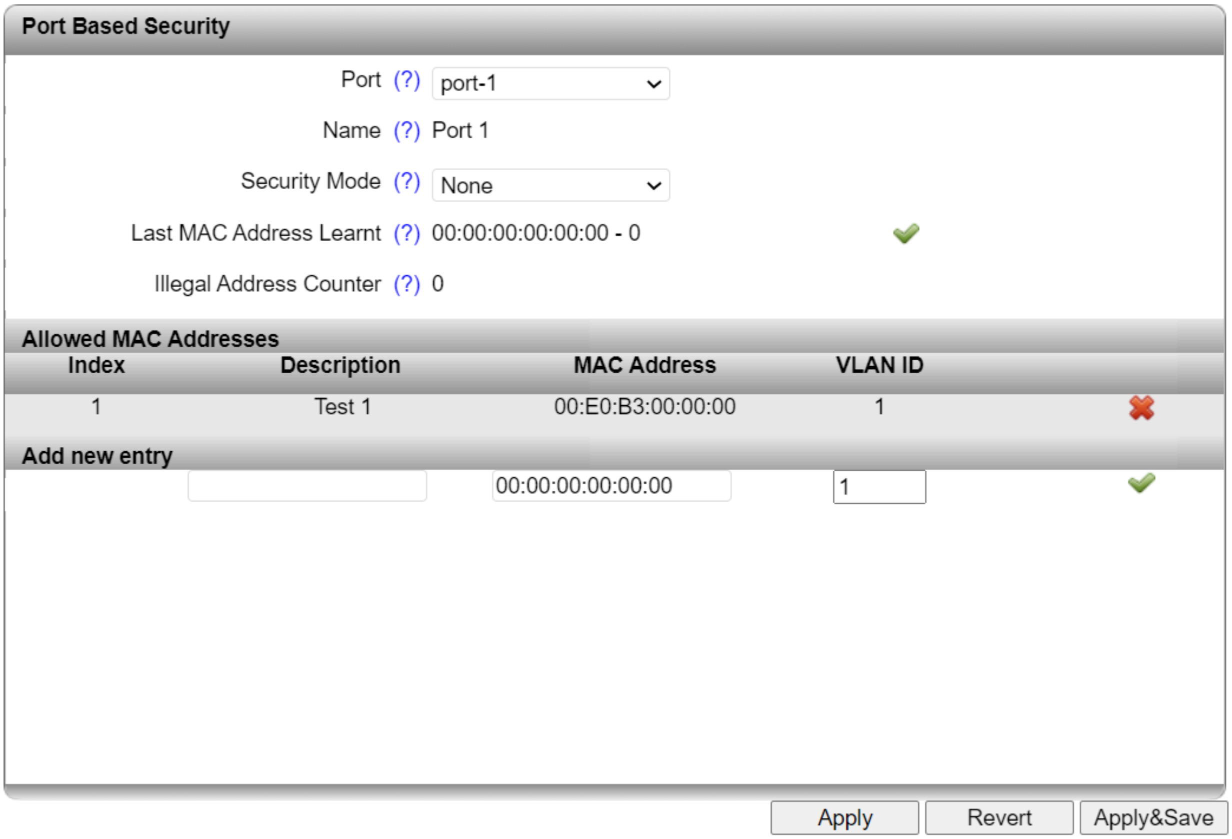
Port Authentication Table: Clicking on the "Dot1x Port Configuration Table" link takes you to the table-based configuration page for RADIUS authentication.

Port Authentication: Clicking on the "Dot1x Port Configuration" link takes you to the port-based configuration page for RADIUS authentication.

Allowed MAC Addresses: Clicking on the "Allowed MAC Addresses" link to open a list of all MAC addresses currently permitted.

Pop-up Window of “Configure Port Based Security”

All of the configurations on the “Port Based Security” webpage only take effect if the “Port Security Status” function is activated on the “Security” webpage.



Port Based Security

Port (?) port-1

Name (?) Port 1

Security Mode (?) None

Last MAC Address Learnt (?) 00:00:00:00:00:00 - 0 ✓

Illegal Address Counter (?) 0

Allowed MAC Addresses

Index	Description	MAC Address	VLAN ID	
1	Test 1	00:E0:B3:00:00:00	1	✖

Add new entry

		00:00:00:00:00:00	1	✓

Port: Select the port for which the security settings should be made.

Name: Displays the name of the selected port.

Security Mode: Here, set what happens if a MAC address that is not permitted is detected by the device.

- None: No security settings for this port.
- Trap: If a MAC address that is not permitted is detected at the port, a trap is sent to the defined SNMP trap server. The packets are not blocked.
- Block: If a MAC address that is not permitted is detected at the port, all packets are blocked at the port and a trap is sent to the defined SNMP trap server. The packets at this port remain blocked until a permitted MAC address is detected.

Last MAC Address Learnt: Displays the MAC address of the last connected device. By clicking on the green checkmark, this MAC address can be added to the list of permitted MAC addresses.

Illegal Address Counter: Displays the number of times a port has been accessed illegally. Each initial access by a MAC address is counted. Repeated access by known MAC addresses are counted twice if a different MAC address has accessed the port in the meantime.

Allowed MAC Addresses Items

Up to 50 MAC addresses are permitted per port. Each MAC address can only be permitted at one port. MAC addresses that are permitted at one port also cannot be dynamically learned at other ports. The web-based management or network cannot be accessed via a MAC address that is permitted at another port.

Index: Displays the index of the permitted MAC addresses.

Description: Here, you can provide a description for a permitted MAC address.

MAC Address: Enter a MAC address for which you want to allow access. Alternatively, you can select the green checkmark to the right of the "Last MAC Address Learned" field to use the last MAC address that was learned.

VLAN ID: Enter the VLAN where the device with the permitted MAC address is located.

Delete: Clicking on the red "X" to the right of this column deletes the permitted MAC address for this port.

Add new entry Items

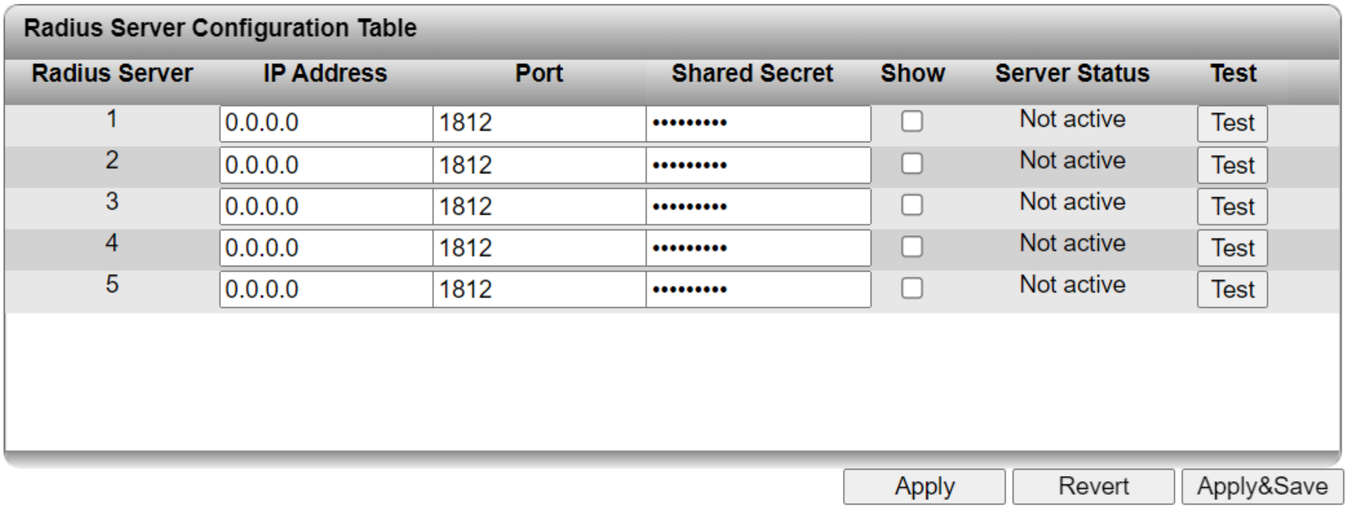
Description: Here, enter a description for an allowed MAC address.

MAC Address: Enter a MAC address for which you wish to allow access. Alternatively, click on the green check mark next to "Last MAC Address Learnt" to accept this MAC address.

VLAN ID: Enter the VLAN where the device with the allowed MAC address is located.

Confirm: Click on the green check mark to add an allowed MAC address.

Pop-up window of “Configure more than one radius server simultaneously”



Radius Server Configuration Table

Radius Server	IP Address	Port	Shared Secret	Show	Server Status	Test
1	0.0.0.0	1812	•••••••••	□	Not active	Test
2	0.0.0.0	1812	•••••••••	□	Not active	Test
3	0.0.0.0	1812	•••••••••	□	Not active	Test
4	0.0.0.0	1812	•••••••••	□	Not active	Test
5	0.0.0.0	1812	•••••••••	□	Not active	Test

Radius Server Configuration Table Items

Radius Server: The ID of the RADIUS server is displayed here.

IP Address: Here, enter the IP address of the RADIUS server.

Port: Here, enter the port of the RADIUS server.

Shared Secret: Here, enter the shared secret that is required for encrypted communication with the RADIUS server. The shared secret must have between eight and 64 characters.

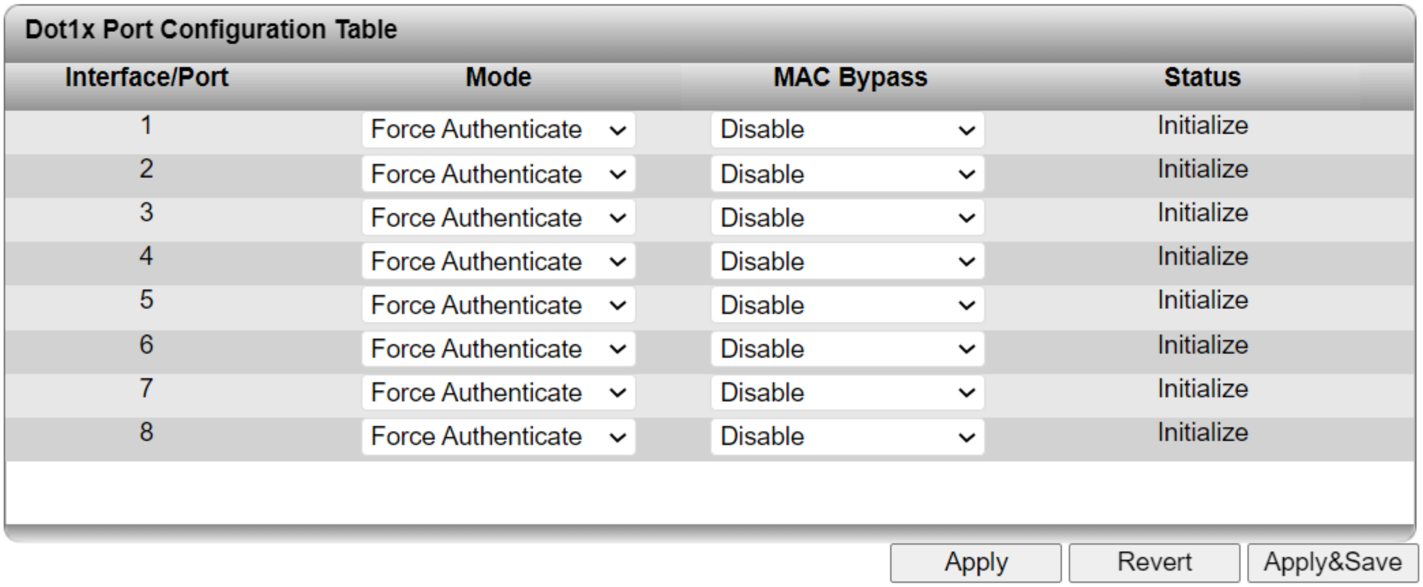
Show: Activate the check box to display the shared secret.

Server Status: The status of the RADIUS server that can be tested via “Test” is displayed here.

Test: Click on “Test” to check whether the configured RADIUS server is reachable.

If more than one RADIUS server is configured and RADIUS server 1 is not available, it can take up to 30 seconds for the page to load.

Dot1x Port Configuration Table Page



Dot1x Port Configuration Table

Interface/Port	Mode	MAC Bypass	Status
1	Force Authenticate	Disable	Initialize
2	Force Authenticate	Disable	Initialize
3	Force Authenticate	Disable	Initialize
4	Force Authenticate	Disable	Initialize
5	Force Authenticate	Disable	Initialize
6	Force Authenticate	Disable	Initialize
7	Force Authenticate	Disable	Initialize
8	Force Authenticate	Disable	Initialize

Interface/Port: Displays the port number.

Mode: Here, you can set the authentication mode for the port.

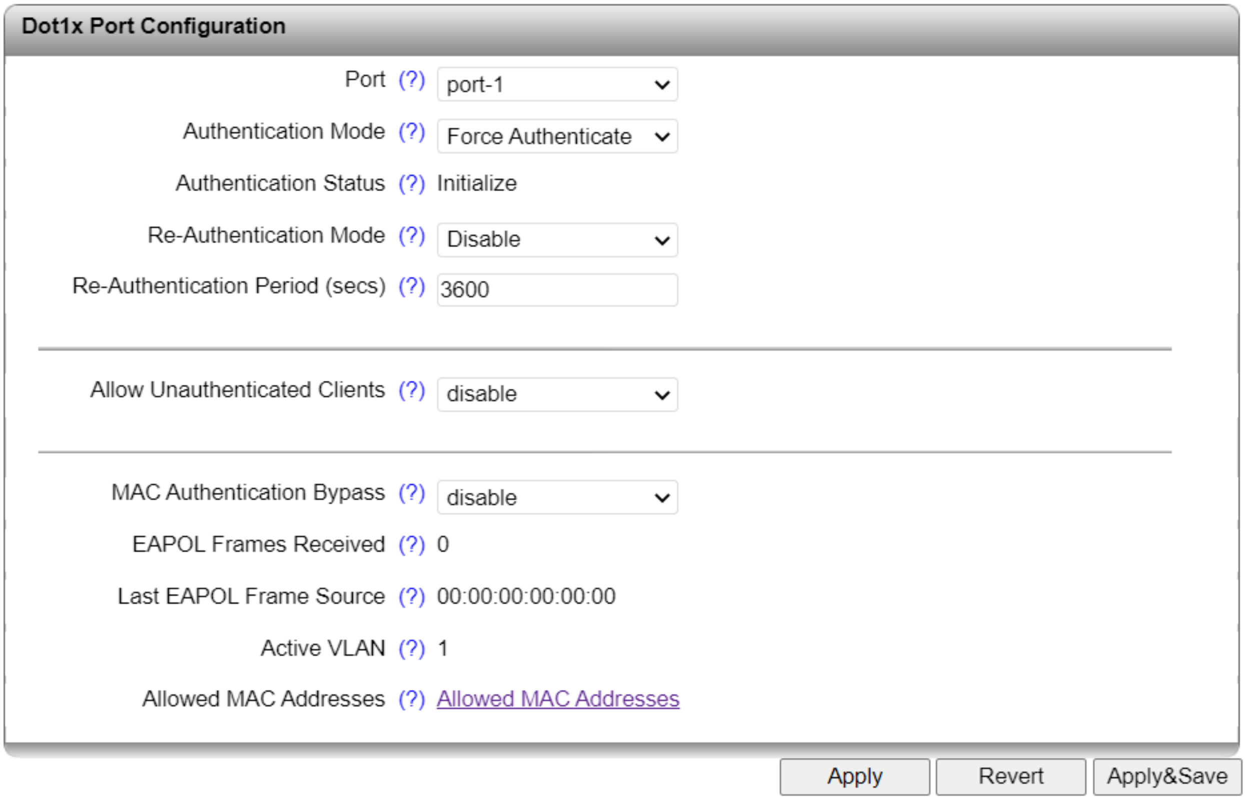
- Auto: Devices connected to the port are authenticated via 802.1x. The “Dot1x Authenticator” must be activated for this.
- Force Authenticate: All of the devices connected to the port are authenticated.
- Force Unauthenticate: None of the devices connected to the port are authenticated.

MAC Bypass: Here you can enable and disable the “MAC Authentication Bypass” (MAB) function for the port. The authentication is performed based on the MAC address of the connected device. The MAC address is automatically detected.

NOTE: Threat to network security
Activating the “MAC Bypass” function poses a threat to your network security.

Status: Displays the authentication status of the port.

Dot1x Port Configuration Page



Dot1x Port Configuration

Port (?)	port-1
Authentication Mode (?)	Force Authenticate
Authentication Status (?)	Initialize
Re-Authentication Mode (?)	Disable
Re-Authentication Period (secs) (?)	3600
Allow Unauthenticated Clients (?)	disable
MAC Authentication Bypass (?)	disable
EAPOL Frames Received (?)	0
Last EAPOL Frame Source (?)	00:00:00:00:00:00
Active VLAN (?)	1
Allowed MAC Addresses (?)	Allowed MAC Addresses

Port: Here, select the port for which you wish to carry out RADIUS configuration.

Authentication Mode: Here, you can set the authentication mode for the port.

- Auto: Devices connected to the port are authenticated via 802.1x. The “Dot1x Authenticator” must be activated for this.
- Force Authenticate: All of the devices connected to the port are authenticated.
- Force Unauthenticate: None of the devices connected to the port are authenticated.

Authentication Status: Displays the authentication status of the port.

Re-Authentication Mode: Here, you can specify whether a client should be re-authenticated at a regular interval.

Re-Authentication Period (secs): Set the interval at which a client should be re-authenticated (1 ... 65,535 seconds).

Failed Authentication Handling: Select what should happen if non-authenticated clients are rejected by the RADIUS server.

- Disable: Non-authenticated clients are rejected.
- Guest-VLAN: Non-authenticated clients are assigned to a guest VLAN.

- Port Disable: If a non-authenticated client is rejected by the RADIUS server, the port in question is disabled for a set time.

This option is only available if you selected “Guest-VLAN” for “Failed Authentication Handling”:

Guest VLAN: Select the guest VLAN to which clients should be assigned if they cannot be authenticated via the RADIUS server. The assignment then takes place automatically.

These two options are only available if you selected “Port Disable” for “Failed Authentication Handling”:

Port Re-Enable Timer: Enter the time in seconds for which the port should remain deactivated after an unauthenticated connection attempt. The value must be between one and 3600 seconds.

Port Re-Enable Timer Status: This shows whether the port is currently deactivated and the timer is running.

MAC Authentication Bypass: elect whether the “MAC Authentication Bypass” (MAB) function should be activated for the port. The clients that are not certified with EAPOL can be authenticated by the RADIUS server via their MAC address.

MAB Authentication Status: The MAB authentication status is displayed here.

EAPOL Frames Received: Displays the received EAPOL packets.

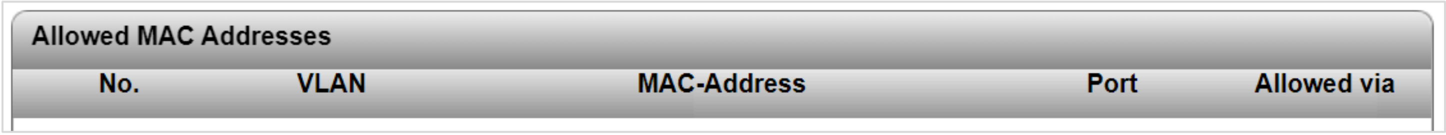
Last EAPOL Frame Source: Displays the last MAC address from which an EAPOL packet was received at the port.

Active VLAN: Shows the port-based VLAN ID assigned by the RADIUS server.

Allowed MAC Addresses: Click on “Allowed MAC Addresses” to open the “Allowed MAC Addresses” pop-up window.

Pop-up window of “Allowed MAC Addresses”

Link goes to a table listing of all the MAC addresses that are allowed access via dot1x, MAB or Guest VLAN.



Allowed MAC Addresses

No.	VLAN	MAC-Address	Port	Allowed via

No.: A serial number that numbers the allowed MAC addresses consecutively is displayed here.

VLAN: The VLAN to which the MAC address is assigned is displayed here.

MAC-Address: The MAC address is displayed here.

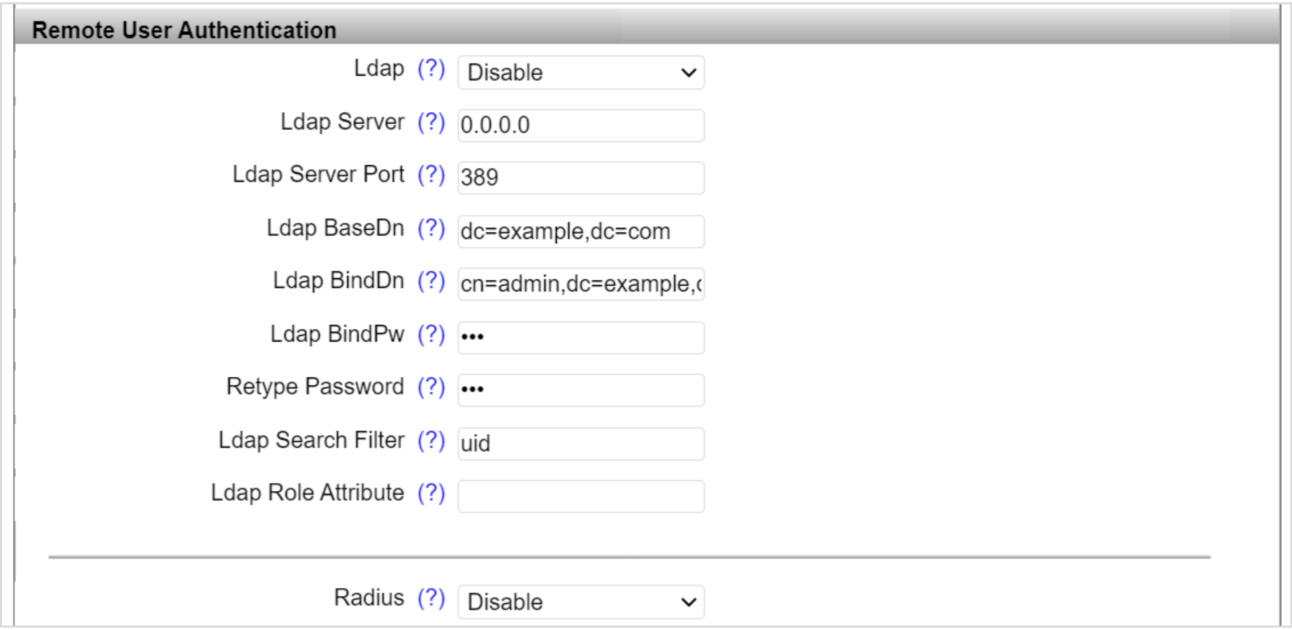
Port: The port number via which the MAC address is connected to the device is displayed here.

Allowed via: This shows whether the MAC address was allowed via Dot1x or MAB.

Remote User Authentication

Configure LDAP (Lightweight Directory Access Protocol) parameters on this page.

ℹ When a user logs in, databases are searched for a valid user name and password combination, where the user rights are also correctly assigned. The local database is searched first. Then, the LDAP is searched (if enabled), followed by the RADIUS database (if enabled). If a valid combination is found, the search is terminated and the user is logged in.



Remote User Authentication

Ldap	(?)	Disable
Ldap Server	(?)	0.0.0.0
Ldap Server Port	(?)	389
Ldap BaseDn	(?)	dc=example,dc=com
Ldap BindDn	(?)	cn=admin,dc=example,(
Ldap BindPw	(?)	•••
Retype Password	(?)	•••
Ldap Search Filter	(?)	uid
Ldap Role Attribute	(?)	
Radius	(?)	Disable

Ldap: Select whether LDAP server-based user authentication should be activated.

Ldap Server: Here, enter the address of the LDAP server as an IP address or DNS name.

Ldap Server Port: Configure the TCP port for connection with the LDAP server here (default: 389).

ℹ An encrypted connection to the LDAP server (e.g., via SSL/TLS and Port 636) is not currently supported by the device.

Ldap BaseDn: Here, enter the LDAP Base Distinguished Name. The BaseDN describes the base address or the storage location under which the user data is stored in the directory on the LDAP server.

Ldap BindDn: Here, enter the LDAP Bind Distinguished Name. The BindDn is the user name for logging the device into the LDAP server in order to be able to perform operations on the LDAP server such as browsing user data.

Ldap BindPw: Here, enter the LDAP Bind Password. The Bind password is required for authenticating the device on the LDAP server. This password is linked to the BindDn.

Retype Password: Re-enter the Bind password here.

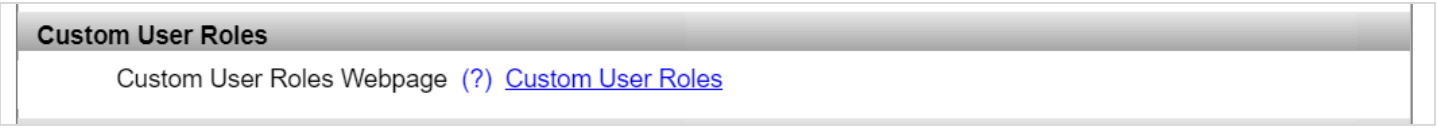
Ldap Search Filter: Here you can configure the server attribute under which the user name is to be found when logging into the server.

Optional: With the wildcard operator {0}, you can define the part of the attribute that is to be entered during login (e.g., mail={0}@example.com).

Ldap Role Attribute: Here, configure the attribute under which the designation and the user roles are stored on the LDAP server. This attributed is mapped on the device with a local role designation so that rights can be assigned to a user. To do this, on the “Custom User Roles” webpage, you can map the LDAP role name from the server to a local user role under “Ldap Rolename”.

Radius: Here you can enable and disable user authentication via RADIUS. To establish a connection to the RADIUS server, the settings described above on the “Security” webpage under “Global Radius Authentication Server Configuration” are used.

Custom User Roles

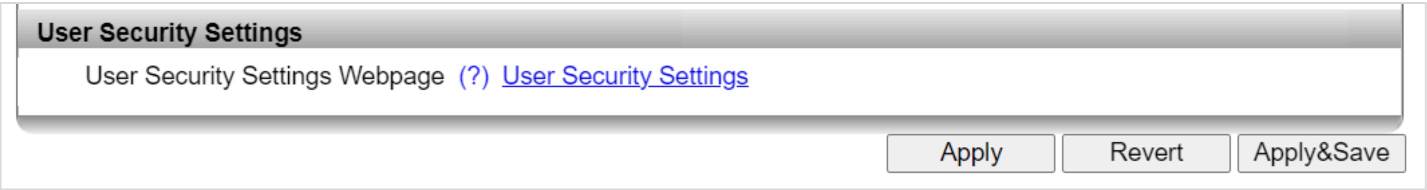


Custom User Roles

Custom User Roles Webpage (?) Custom User Roles

Custom User Roles Webpage: Click on “Custom User Roles” to open the “Custom User Roles” pop-up window.

User Security Settings

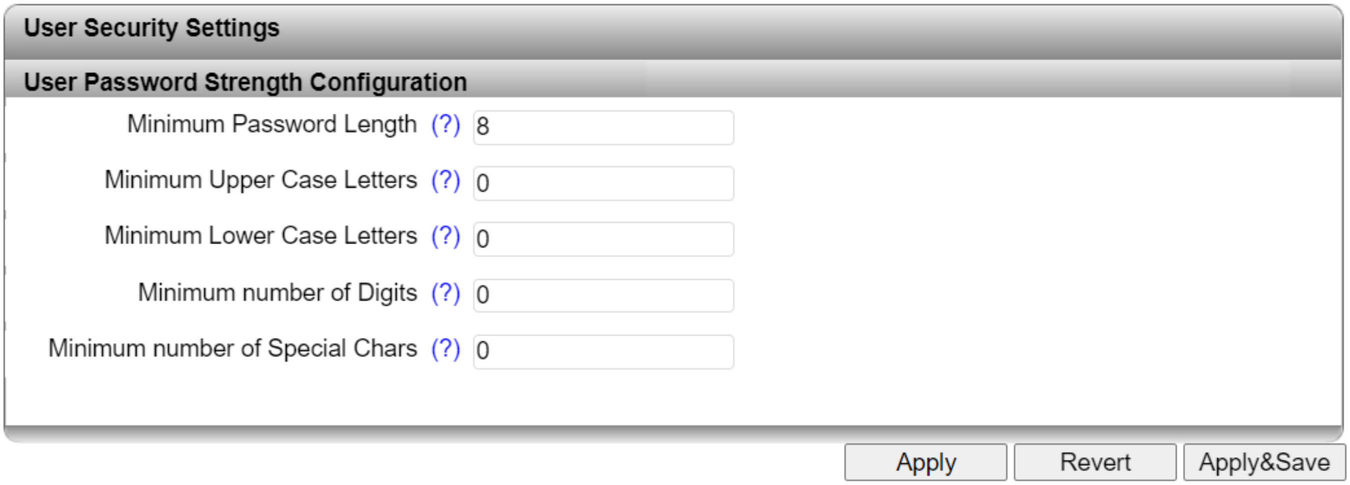


User Security Settings

User Security Settings Webpage (?) User Security Settings

User Security Webpage: Click on “User Security Settings” to open the “User Security Settings” pop-up window.

Pop-up window of “User Security Settings”



User Security Settings

User Password Strength Configuration

Minimum Password Length (?)	8
Minimum Upper Case Letters (?)	0
Minimum Lower Case Letters (?)	0
Minimum number of Digits (?)	0
Minimum number of Special Chars (?)	0

Minimum Password Length: Here, enter the desired minimum length for passwords. The value can have between eight and 64 characters (default: 8).

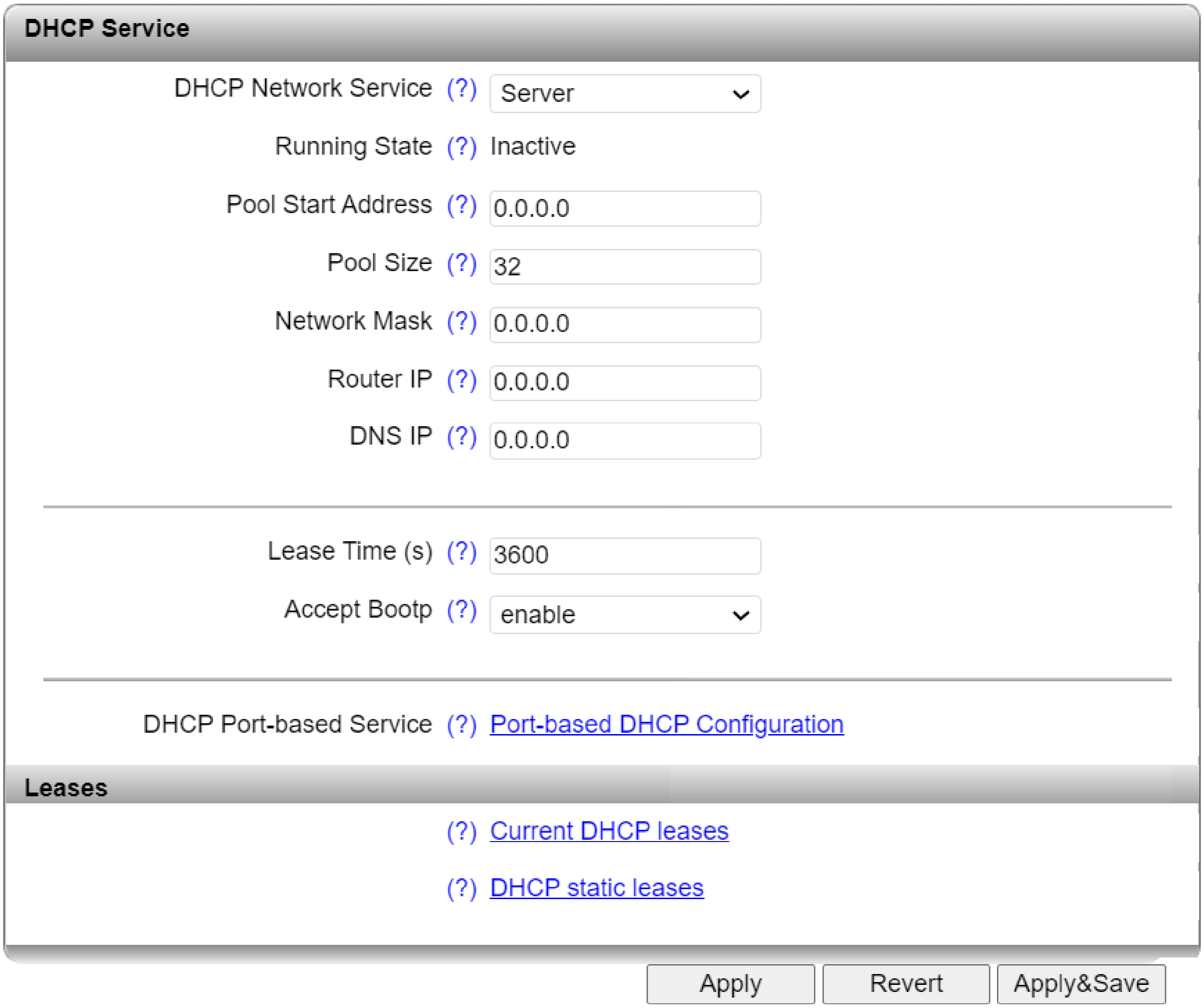
Minimum Upper Case Letters: Here, enter the desired minimum number of uppercase letters (A–Z). The value can have between zero and eight characters (default: 0).

Minimum Lower Case Letters: Here, enter the desired minimum number of lowercase letters (a–z). The value can have between zero and eight characters (default: 0).

Minimum number of Digits: Here, enter the desired minimum number of digits (0–9). The value can have between zero and eight characters (default: 0).

Minimum number of Special Characters: Here, enter the desired minimum number of special characters (e.g., .#:!?). The value can have between zero and eight characters (default: 0).

Configuration – DHCP Service



DHCP Service

DHCP Network Service (?)	Server
Running State (?)	Inactive
Pool Start Address (?)	0.0.0.0
Pool Size (?)	32
Network Mask (?)	0.0.0.0
Router IP (?)	0.0.0.0
DNS IP (?)	0.0.0.0
Lease Time (s) (?)	3600
Accept Bootp (?)	enable
DHCP Port-based Service (?)	Port-based DHCP Configuration

Leases

(?) Current DHCP leases

(?) DHCP static leases

DHCP Network Service: Select the DHCP service you wish to use.

- None: No DHCP service will be used on the switch.
- Relay Agent: The DHCP relay agent (DHCP option 82) is enabled.
- Server: The switch will be used as the DHCP server. This can only be activated if the IP Address Assignment mode is set to “STATIC”.

When “Relay Agent” is selected as the DHCP network service, the following fields become available:

Option 82 Remote ID: Here, select the address that should be used as the remote ID.

- IP: Uses the IP address of the switch as the remote ID.
- MAC: Uses the MAC address of the switch as the remote ID.
- STRING: The string in the “Option82 Unique String” field is used as the remote ID.

Remote ID Unique String: This option is only available if you selected “STRING” for “Option 82 Remote ID”. Enter a unique string that is used as the remote ID.

Server IP Address: Here, set the IP address of the DHCP server in your network.

Port Mode: Here, select the ports for which the DHCP relay agent should be activated.

When “Server” is selected as the DHCP network service, the following fields become available:

Running State: Shows the current status of the DHCP server. The status is “Inactive” if some setting options are incorrect.

Pool Start Address: Set the first IP address of the DHCP server address pool.

Pool Size: Set the number of IP addresses in the DHCP server address pool. Please note that the number of IP addresses must match the configured subnet.

Network Mask: Set the subnet mask that is assigned to the DHCP clients.

Router IP: Here, set the router/default gateway IP address that is assigned to the DHCP clients.

DNS IP: Here, set the DNS IP address that is assigned to the DHCP clients.

Lease Time (s): Here, you can set the time that the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2,592,000 seconds; “0” is interpreted as an infinite time (default is 3600).

Accept Bootp: Here, you can specify whether the switch acting as the DHCP server accepts BootP requests. If this function is activated, an IP address with an infinite lease time is assigned to the requesting DHCP clients.

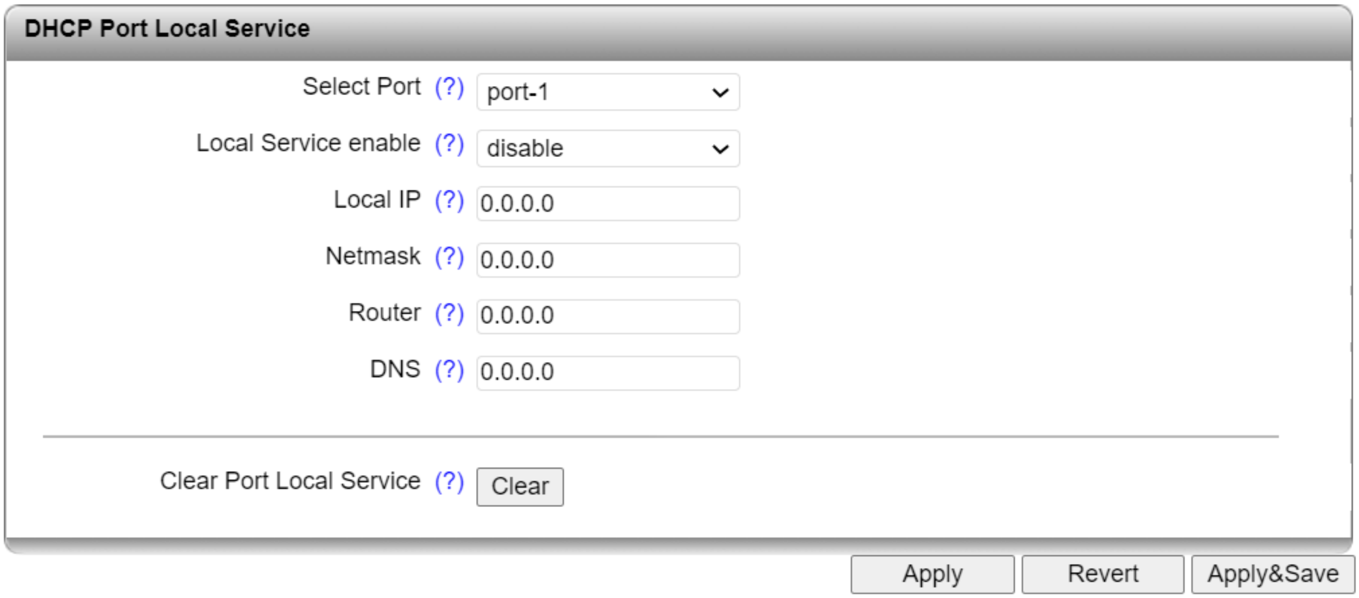
DHCP Port-based Service: Clicking on the “Port-based DHCP Configuration” link opens the “Port-based DHCP Configuration” window (See below).

Leases

Clicking on the “Current DHCP leases” link opens the “Current DHCP leases” window where the IP addresses that are currently assigned are displayed.

Clicking on the “DHCP static leases” link opens the “DHCP Static Leases” window for configuring static IP address assignments.

Port-based DHCP Configuration



DHCP Port Local Service

Select Port (?)	port-1
Local Service enable (?)	disable
Local IP (?)	0.0.0.0
Netmask (?)	0.0.0.0
Router (?)	0.0.0.0
DNS (?)	0.0.0.0
Clear Port Local Service (?)	Clear

Select Port: Select the port for which you wish to carry out port-based DHCP server configuration.

Local Service enable: Here, activate the port-based DHCP server function for the selected port.

Local IP: Enter the IP address that is assigned to the client at the selected port.

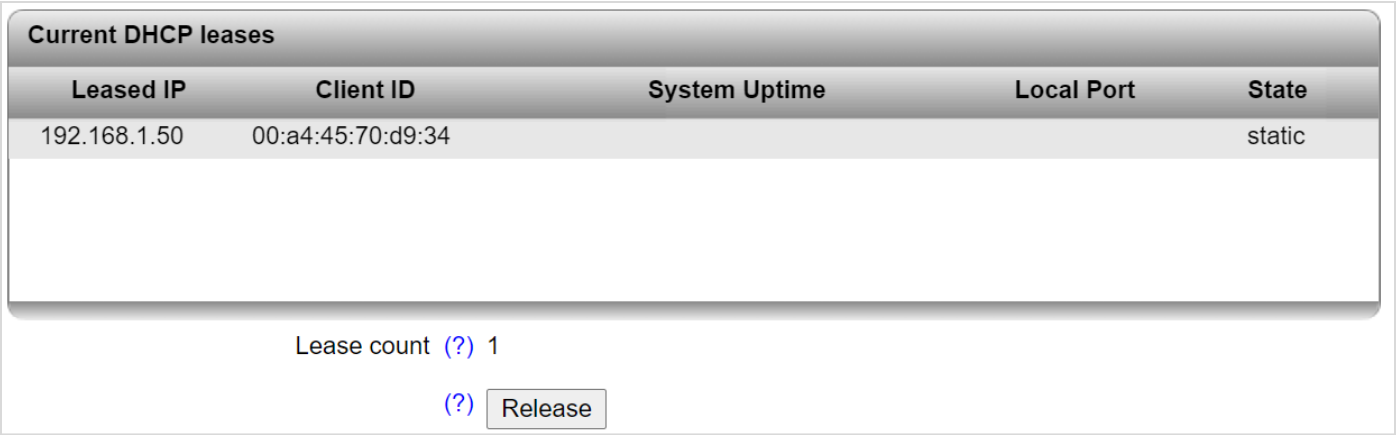
Netmask: Here, enter the subnet mask that is assigned to the client at the selected port.

Router: Here, enter the gateway address that is assigned to the client at the selected port.

DNS: Here, enter the DNS address that is assigned to the client at the selected port.

Clear Port Local Service: Clicking on the “Clear” button deletes the port-based DHCP configurations of all ports.

Current DHCP Leases



Current DHCP leases

Leased IP	Client ID	System Uptime	Local Port	State
192.168.1.50	00:a4:45:70:d9:34			static

Lease count (?) 1

Leased IP: Displays the assigned IP addresses.

Client ID: Displays the MAC address of the client to which the IP address is assigned.

System Uptime: Displays the time that has elapsed since the IP address was assigned to the client.

Local Port: Displays the port to which the client is connected.

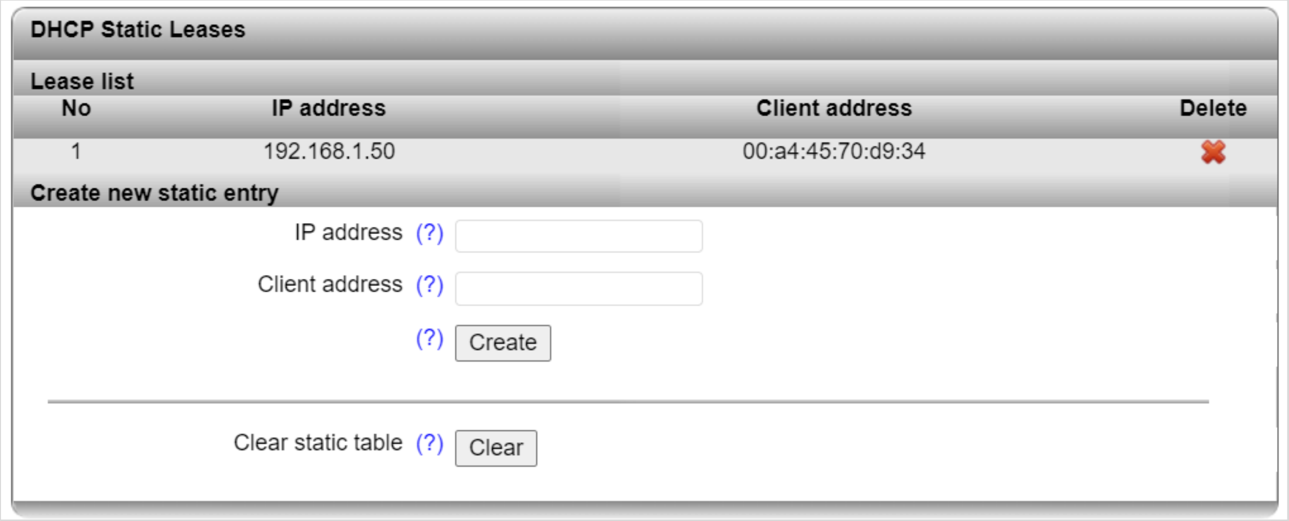
State: Displays the status of the client.

Lease count: Displays the number of assigned IP addresses.

Release: Clicking on the “Release” button releases unused entries again.

DHCP Static Leases

In addition, you can create new static IP assignments by assigning a fixed IP address to MAC addresses.



DHCP Static Leases

Lease list

No	IP address	Client address	Delete
1	192.168.1.50	00:a4:45:70:d9:34	✖

Create new static entry

IP address (?)

Client address (?)

(?) Create

Clear static table (?) Clear

Lease list Items

No: This column numbers the entries consecutively.

IP address: Displays the static IP address that is assigned.

Client address: Displays the MAC address of the client.

Delete: Clicking on the red “X” in the “Delete” column deletes the entry.

Create new static entry items

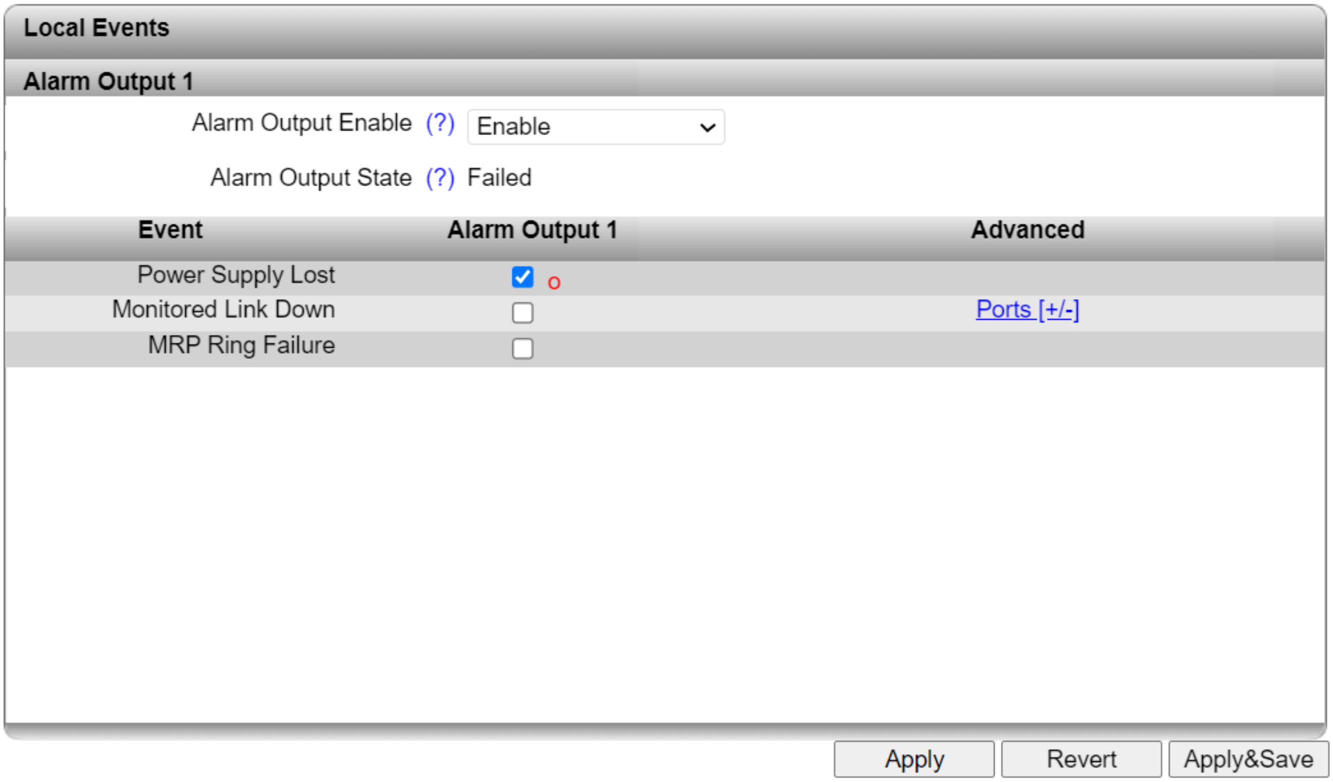
IP address: Enter the static IP address that you wish to assign.

Client address: Enter the MAC address to which you wish to assign a static IP address.

Create: Click on the “Create” button to perform the static assignment.

Clear static table: Click on the “Clear” button to delete all the static DHCP leases.

Configuration – Local Events



Local Events

Alarm Output 1

Alarm Output Enable (?) Enable

Alarm Output State (?) Failed

Event	Alarm Output 1	Advanced
Power Supply Lost	☑ o	
Monitored Link Down	□	Ports [+/-]
MRP Ring Failure	□	

Alarm output 1

Here, you can activate the digital alarm output and read the current status (if a red “o” is present, this event has occurred).

Alarm Output Enable: Select whether the digital alarm output as well as the alarm message via the FAIL LED on the device should be activated.

Alarm Output State: The current alarm message status is displayed here.

Events

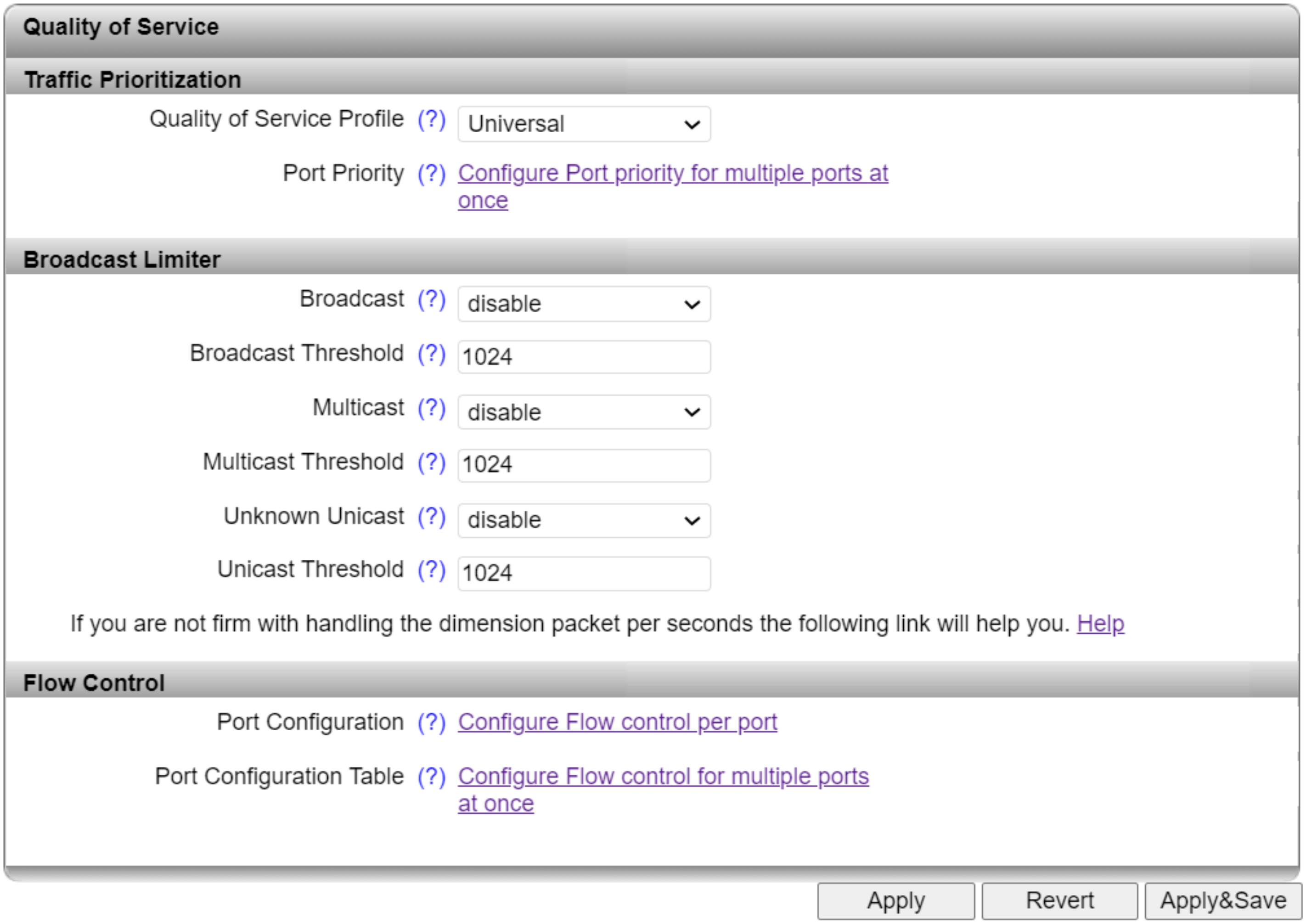
Specify the conditions under which the digital alarm output should report an error.

Power Supply lost: An error message is generated if supply voltage PWR1 or PWR2 is lost.

Monitored link down: Under “Advanced”, select the ports to which link down behavior should be reported.

MRP Ring Failure: The device outputs an error message if an MRP ring error occurs.

Configuration – Quality of Service



Quality of Service

Traffic Prioritization

Quality of Service Profile (?) Universal

Port Priority (?) Configure Port priority for multiple ports at once

Broadcast Limiter

Broadcast (?) disable

Broadcast Threshold (?) 1024

Multicast (?) disable

Multicast Threshold (?) 1024

Unknown Unicast (?) disable

Unicast Threshold (?) 1024

If you are not firm with handling the dimension packet per seconds the following link will help you. Help

Flow Control

Port Configuration (?) Configure Flow control per port

Port Configuration Table (?) Configure Flow control for multiple ports at once

Traffic Prioritization

The switch has eight priority queues into which incoming data traffic is sorted according to specific criteria. These queues are processed in descending order of priority. High-priority data traffic is therefore always forwarded first.

Quality of Service Profile: Select the pre-defined profile for prioritizing data traffic.

- Universal: This profile is the factory setting on standard versions. Class of Service (VLAN tag priority) is activated for data prioritization.
- EtherNet/IP: In this profile, prioritization via DSCP values and TCP/UDP ports is enabled in addition to Class of Service. This means that preferential treatment is given to EtherNet/IP data traffic. Only control packets of redundancy protocols (RSTP and MRP) are given even higher priority.

- EtherNet/IP_L4PortOnly: in this profile, EtherNet/IP data traffic (e.g., CIP Motion, CIP Safety) is prioritized based on TCP/UDP ports.
- CC-Link: This profile prioritizes packets with CC-Link and time synchronization packets in accordance with 802.1AS.

Port Priority: Clicking on the link takes you directly to the configuration page for the default priority. Incoming data traffic on the device that does not have a priority tag is marked according to the setting and is assigned to a priority queue. To activate these settings, the VLAN mode of the device must also be set to “Tagged”.

Broadcast Limiter items

In this area, you can set threshold values in data packets or frames per second for different data streams. This allows you to protect your network against overload.

Broadcast: Activate or deactivate the broadcast limiter.

Broadcast Threshold: Set the threshold value in frames per second for the broadcast limiter. The value entered is rounded down to the next valid value.

Multicast: Activate or deactivate the multicast limiter.

Multicast Threshold: Set the threshold value in frames per second for the multicast limiter. The value entered is rounded down to the next valid value.

Unknown Unicast: Here, you can activate or deactivate the limiter for unknown unicasts. Unicasts of a MAC address that have been learned by the switch are not affected.

Unicast Threshold: Here, set the threshold value in frames per second for the limiter of unknown unicasts. The value entered is rounded down to the next valid value.

Help: Click on “Help” to open the “Storm Control Help” window.

Flow Control items

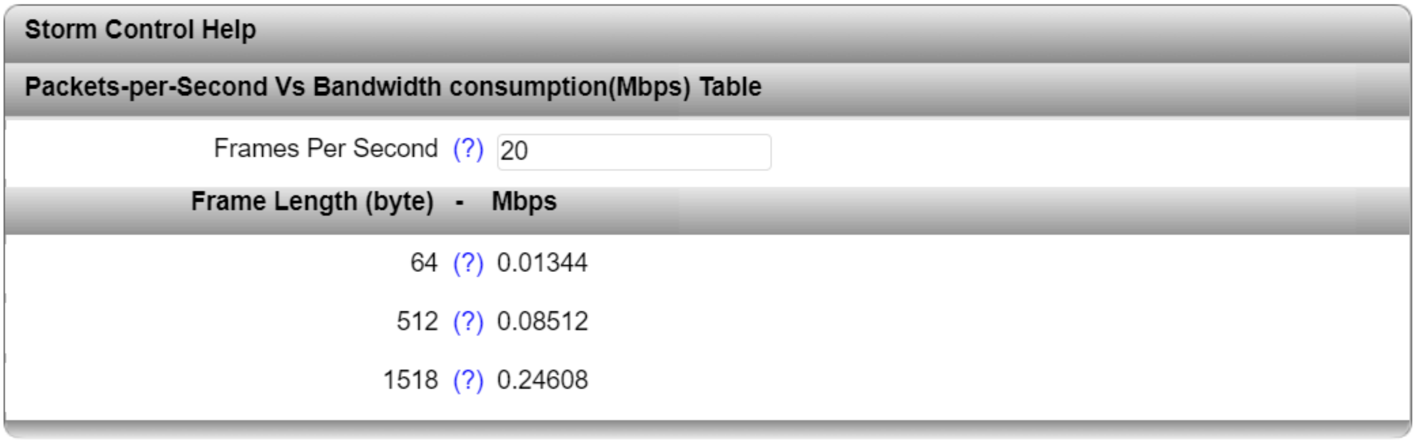
If you activate the flow control function on a port, there are two types of reactions:

- If the device detects a data overload at this port, a pause frame is sent to the connected device. This corresponds to the request to pause the sending of packets.
- If the device receives a pause frame on this port, the sending of packets is briefly interrupted.

Port Configuration: Clicking on the “Configure Flow Control per port” link opens the “Port Configuration” page, which contains the configuration options for flow control.

Port Configuration Table: Clicking on the “Configure Flow control for multiple ports at once” link opens the “Port Configuration Table” page where flow control can be configured for all ports.

Pop-up window of “Storm Control Help”



Storm Control Help

Packets-per-Second Vs Bandwidth consumption(Mbps) Table

Frames Per Second (?) 20

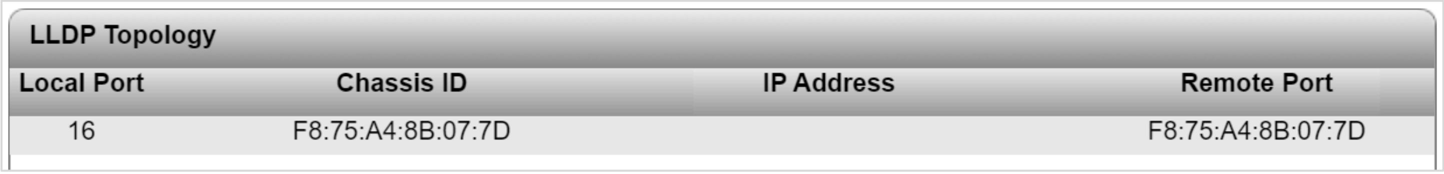
Frame Length (byte)	-	Mbps
64	(?)	0.01344
512	(?)	0.08512
1518	(?)	0.24608

Frames Per Second: Enter the desired number of frames per second and press the Enter key.

Frame Length (byte): This column shows three sample frame lengths in bytes.

Mbps: This column shows you the required Mbps, based on the number of frames per second and the frame length.

Diagnostics – LLDP Topology



LLDP Topology

Local Port	Chassis ID	IP Address	Remote Port
16	F8:75:A4:8B:07:7D		F8:75:A4:8B:07:7D

Local Port: Contains the port number of the local switch that is used to connect a neighbor to this switch.

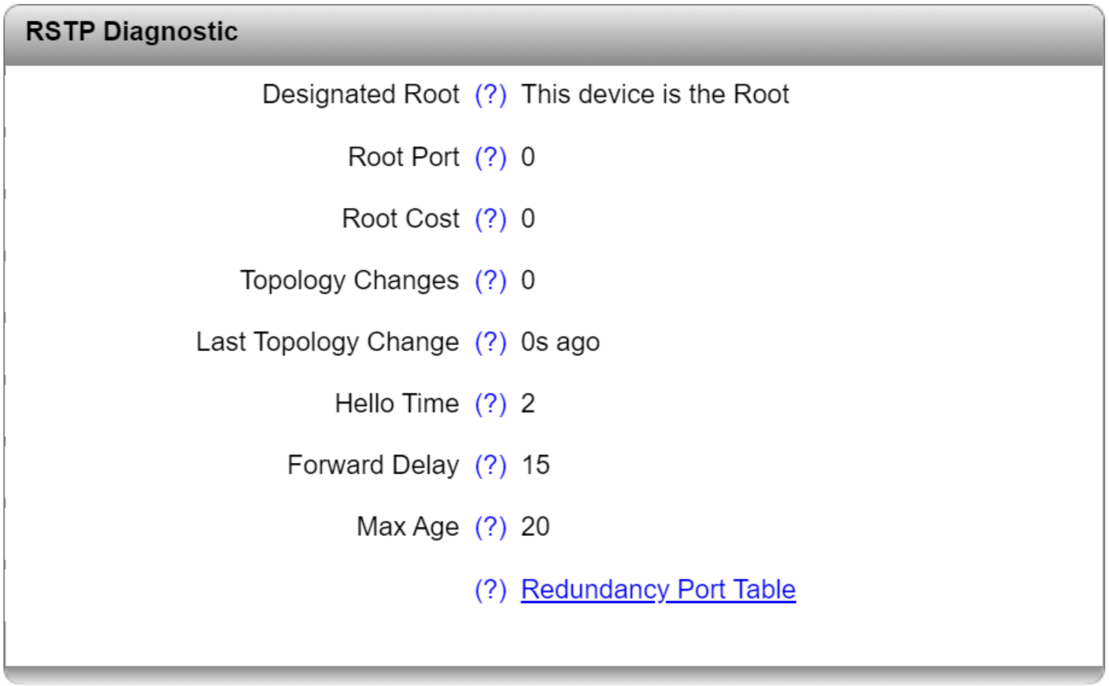
Chassis ID: MAC address of the connected neighboring device.

IP Address: Management IP address for the neighbor.

Remote Port: Port number of the neighboring switch that is used to connect the neighbor to the local switch.

ℹ The switch manages a maximum of 50 items of neighbor information. Any information beyond this is ignored.

Diagnostics – RSTP Diagnostic



RSTP Diagnostic

Designated Root	(?)	This device is the Root
Root Port	(?)	0
Root Cost	(?)	0
Topology Changes	(?)	0
Last Topology Change	(?)	0s ago
Hello Time	(?)	2
Forward Delay	(?)	15
Max Age	(?)	20
	(?)	Redundancy Port Table

Designated Root: Shows the root bridge for this spanning tree.

Root Port: Displays the port to which the root is connected. If the root is not directly connected, it shows the direction of the root.

Root Cost: Displays the total path costs for the root.

Topology Changes: Displays the number of topology changes.

Last Topology Change: Displays when the last topology changes took place.

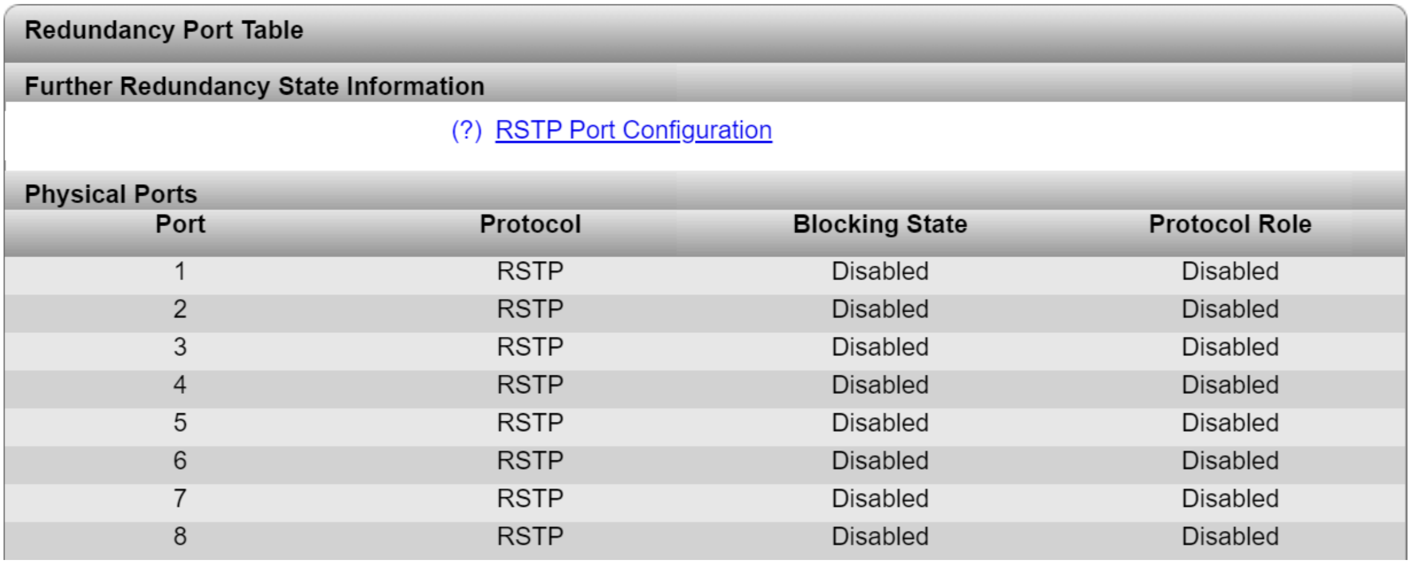
Hello Time: Shows the hello time set at the root.

Forward Delay: Shows the forward delay set at the root.

Max Age: Shows the maximum age time set at the root.

Clicking on the “Redundancy Port Table” button opens a table containing information about the individual ports and their redundancy mechanism assignment:

Pop-up window of “Redundancy Port Table”



Redundancy Port Table

Further Redundancy State Information

(?) RSTP Port Configuration

Physical Ports

Port	Protocol	Blocking State	Protocol Role
1	RSTP	Disabled	Disabled
2	RSTP	Disabled	Disabled
3	RSTP	Disabled	Disabled
4	RSTP	Disabled	Disabled
5	RSTP	Disabled	Disabled
6	RSTP	Disabled	Disabled
7	RSTP	Disabled	Disabled
8	RSTP	Disabled	Disabled

RSTP Port Configuration: Click on “RSTP Port Configuration” to open the “RSTP Port Configuration” window. Here, you can make your RSTP settings for the individual ports.

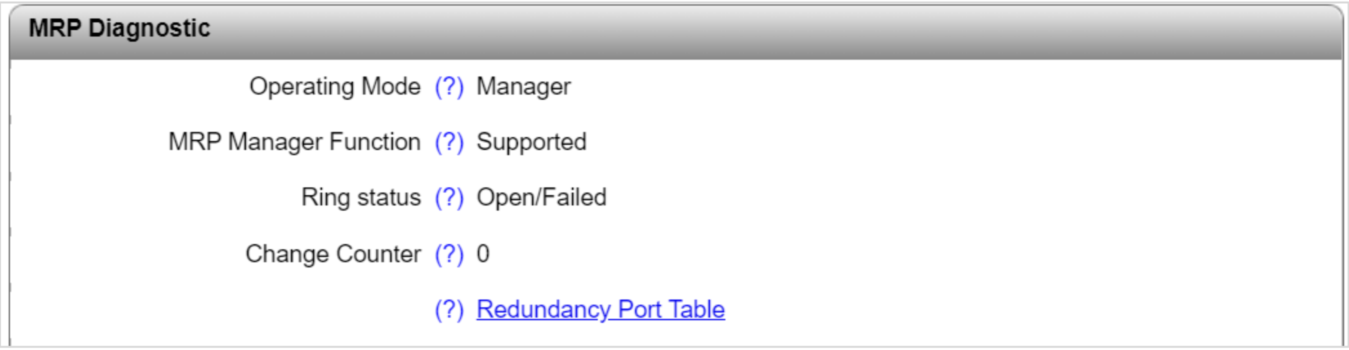
Port: This column shows the respective port.

Protocol: This column shows the redundancy protocol selected for this port.

Blocking State: This column shows how the protocol deals with incoming data packets.

Protocol Role: This column shows whether the data packets are sent towards or away from the root.

Diagnostics – MRP Diagnostic



MRP Diagnostic

Operating Mode (?) Manager

MRP Manager Function (?) Supported

Ring status (?) Open/Failed

Change Counter (?) 0

(?) Redundancy Port Table

Operating Mode: The current MRP device status is displayed here.

MRP Manager Function: This shows whether the MRP manager function is supported on the device.

Ring status: This option is only available if you selected “Manager” for the operating mode of the MRP (see “Network Redundancy: Media Redundancy Protocol (MRP)”). The current MRP ring status is displayed here.

Change Counter: This option is only available if you selected “Manager” for the operating mode of the MRP (see “Network Redundancy: Media Redundancy Protocol (MRP)”). The number of status changes in the MRP ring is displayed here.

Redundancy Port Table: Click on “Redundancy Port Table” to open the “Redundancy Port Table” pop-up window. It contains a table with the individual ports and their assignment to redundancy mechanisms.

Diagnostics – Current VLANs

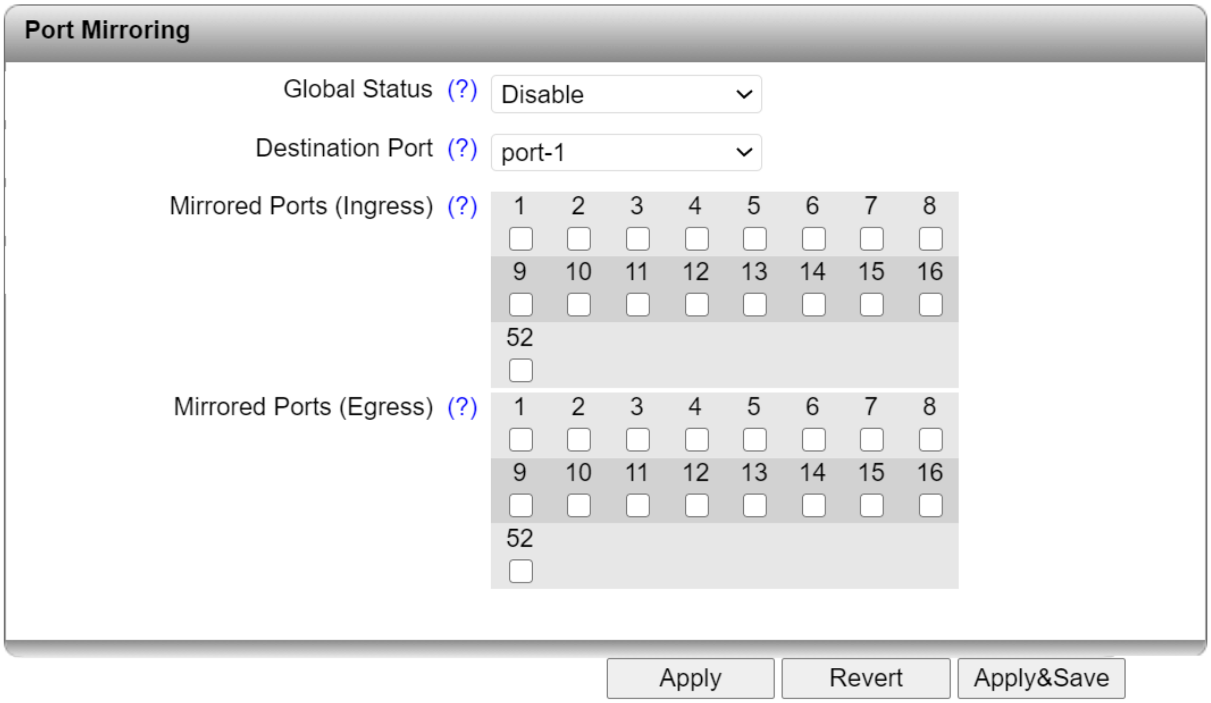
Refer to Configuration – VLAN Configuration – Current VLANs

Diagnostics – Current Multicast Groups

Refer to Configuration – Multicast Filtering – Current Multicast Groups

Diagnostics – Port Mirroring

The port mirroring function allows you to mirror the incoming and outgoing data traffic of individual ports to one port where it can be analyzed using a connected diagnostic device or tool.



Port Mirroring

Global Status (?) Disable

Destination Port (?) port-1

Mirrored Ports (Ingress) (?)

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□
52							
□							

Mirrored Ports (Egress) (?)

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□
52							
□							

Global Status:

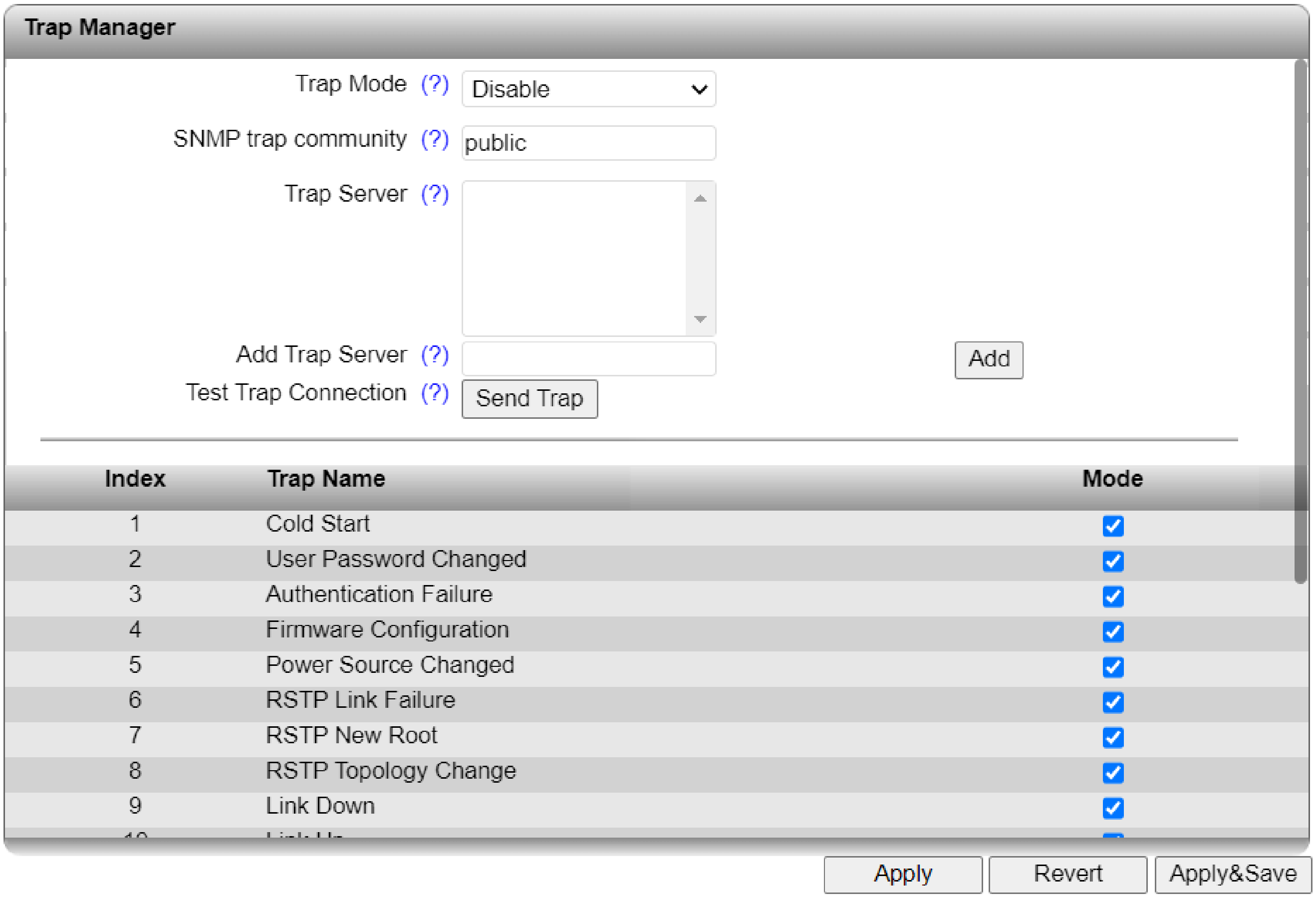
- Enable: Port mirroring is activated globally
- Disable: Port mirroring is deactivated globally

Destination Port: Select the port to which the diagnostic device or tool is connected.

Mirrored Ports (Ingress): Specify the ports from which the incoming data traffic should be mirrored.

Mirrored Ports (Egress): Specify the ports from which the outgoing data traffic should be mirrored.

Diagnostics – Trap Manager



Trap Manager

Trap Mode (?) Disable

SNMP trap community (?) public

Trap Server (?)

Add Trap Server (?) Add

Test Trap Connection (?) Send Trap

Index	Trap Name	Mode
1	Cold Start	☑
2	User Password Changed	☑
3	Authentication Failure	☑
4	Firmware Configuration	☑
5	Power Source Changed	☑
6	RSTP Link Failure	☑
7	RSTP New Root	☑
8	RSTP Topology Change	☑
9	Link Down	☑
10	Link Up	☑

Trap Mode:

- Enable: The sending of SNMP traps is enabled
- Disable: The sending of SNMP traps is disabled

SNMP trap community: Here you can change the name or string of the SNMP trap community.

Trap Server: All trap servers that are to receive SNMP traps from this device are displayed here.

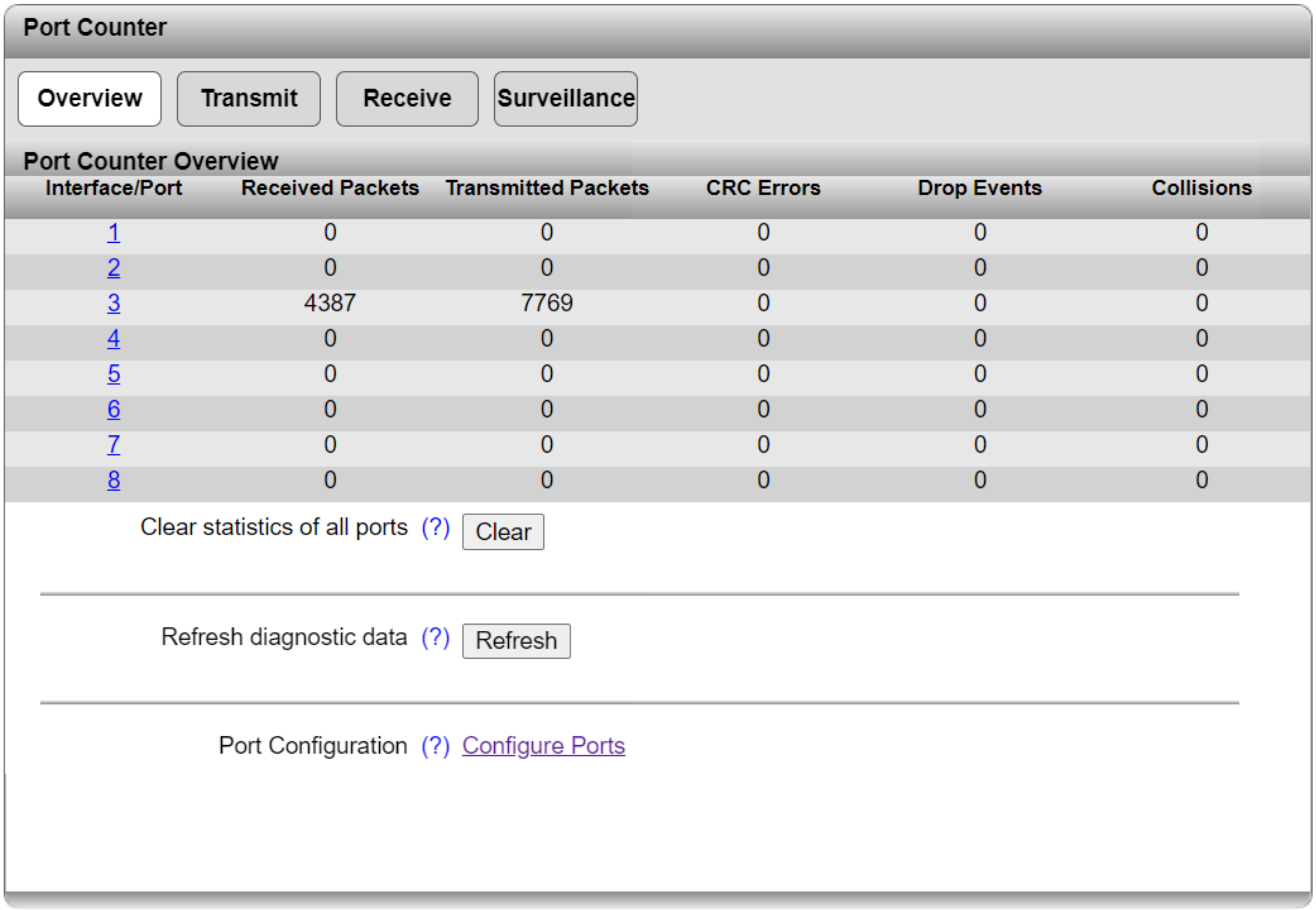
Add Trap Server: Enter the IP address or DNS name of a trap server and click on “Apply & Save” to create this trap server.

Test Trap Connection: Click on the “Send Trap” button to test the connection to the trap server.

The table lists the SNMP traps that the device can send. Select the actions for which SNMP traps should be sent by clicking the corresponding check boxes.

Diagnostics – Port Counter

This page provides an overview of the port statistics for the device. Four views provide an overview of the general, sent and received packets, errors, and collisions on the individual ports.



Port Counter

Port Counter Overview

Interface/Port	Received Packets	Transmitted Packets	CRC Errors	Drop Events	Collisions
1	0	0	0	0	0
2	0	0	0	0	0
3	4387	7769	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0

Clear statistics of all ports (?) Clear

Refresh diagnostic data (?) Refresh

Port Configuration (?) Configure Ports

Interface/Port: Clicking on one of the port numbers in the "Interface/Port" column takes you to the Port Details page. Here, you can view detailed statistics about the sent and received data packets for every port. In addition, the current and maximum port utilization is displayed as a percentage.

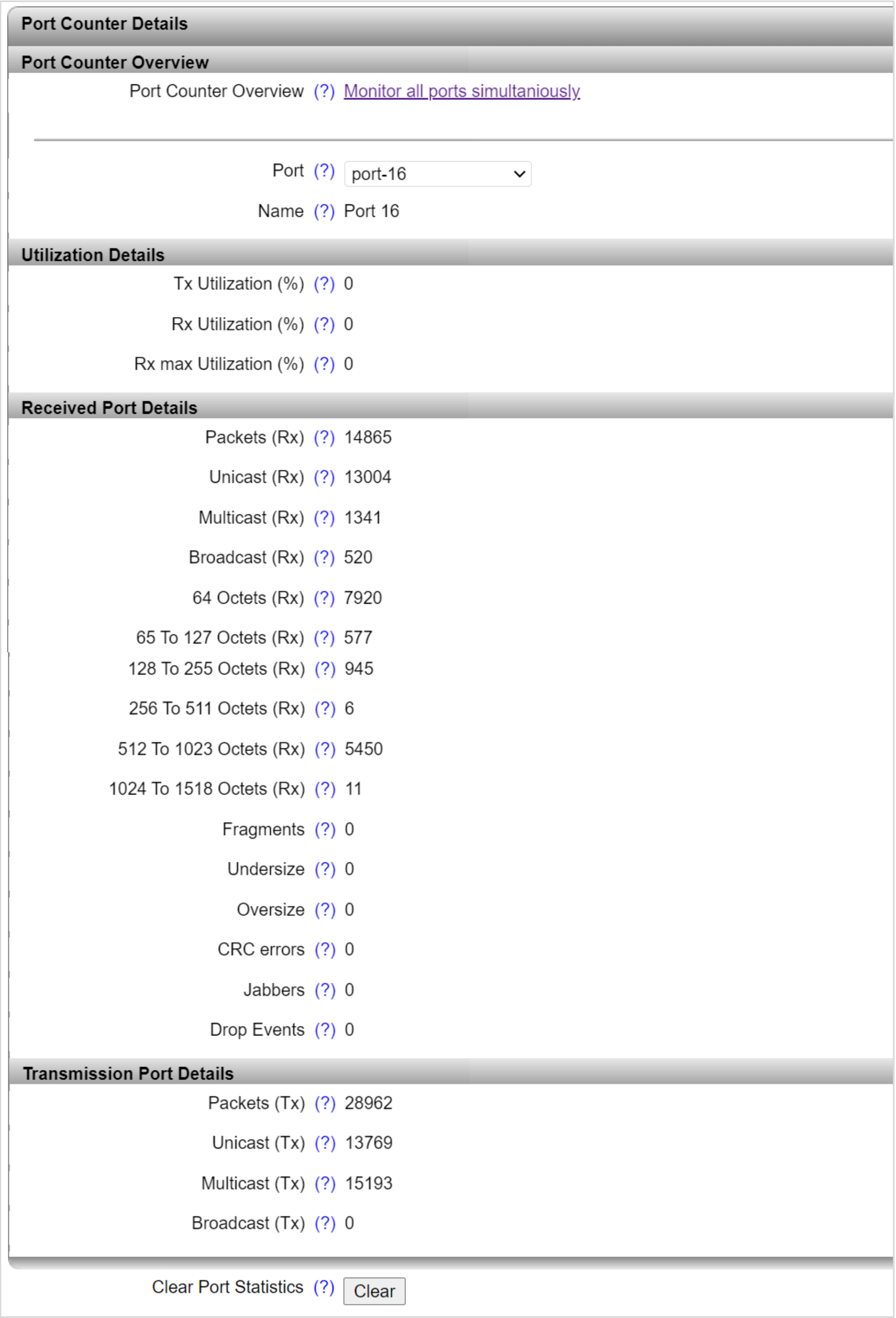
Clear statistics of all ports / Clear CRC Peak and CRC status: Clicking on the "Clear" button resets all of the port counters in the Overview, Transmit, and Receive views to zero.

In Surveillance view, click the button to reset the CRC Proportion Peak and CRC Status of all ports.

Refresh diagnostic data: Clicking on the "Refresh" button to update the port counter statistics.

Port Configuration: Clicking on the "Configure Ports" link opens the "Port Configuration" page.

Port Details Page



Port Counter Details

Port Counter Overview

Port Counter Overview	(?)	Monitor all ports simultaniously
Port	(?)	port-16
Name	(?)	Port 16

Utilization Details

Tx Utilization (%)	(?)	0
Rx Utilization (%)	(?)	0
Rx max Utilization (%)	(?)	0

Received Port Details

Packets (Rx)	(?)	14865
Unicast (Rx)	(?)	13004
Multicast (Rx)	(?)	1341
Broadcast (Rx)	(?)	520
64 Octets (Rx)	(?)	7920
65 To 127 Octets (Rx)	(?)	577
128 To 255 Octets (Rx)	(?)	945
256 To 511 Octets (Rx)	(?)	6
512 To 1023 Octets (Rx)	(?)	5450
1024 To 1518 Octets (Rx)	(?)	11
Fragments	(?)	0
Undersize	(?)	0
Oversize	(?)	0
CRC errors	(?)	0
Jabbers	(?)	0
Drop Events	(?)	0

Transmission Port Details

Packets (Tx)	(?)	28962
Unicast (Tx)	(?)	13769
Multicast (Tx)	(?)	15193
Broadcast (Tx)	(?)	0

Clear Port Statistics	(?)	Clear

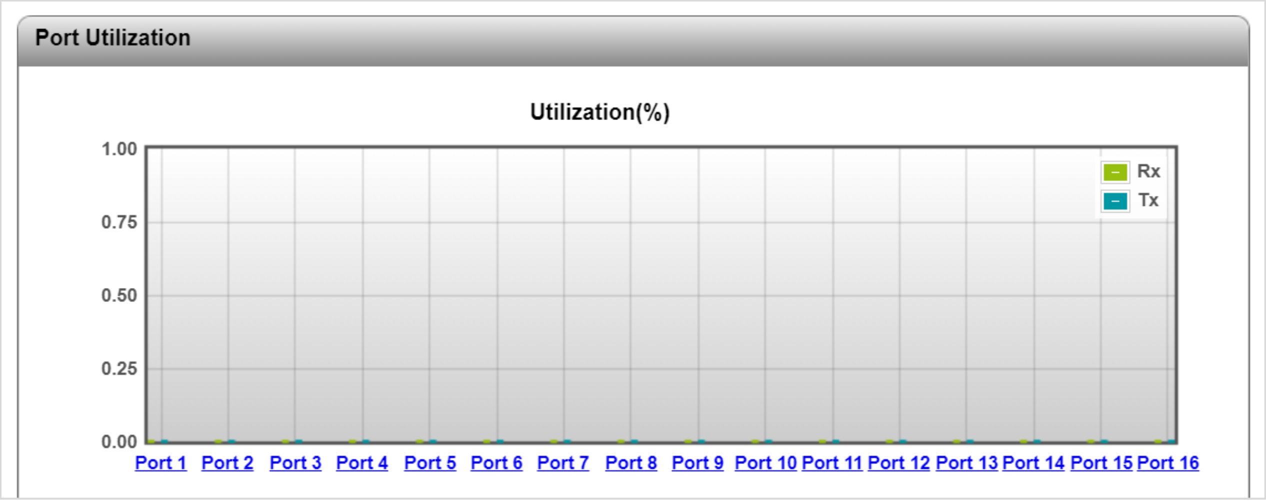
Port Counter Overview: Clicking on the “Monitor all ports simultaneously” link takes you back to the “Port Counter” overview page.

Clear Port Statistics: Clicking on the “Clear” button resets all of the counters for the currently displayed port to zero.

Refresh diagnostic data: Clicking on the “Refresh” button to update the page.

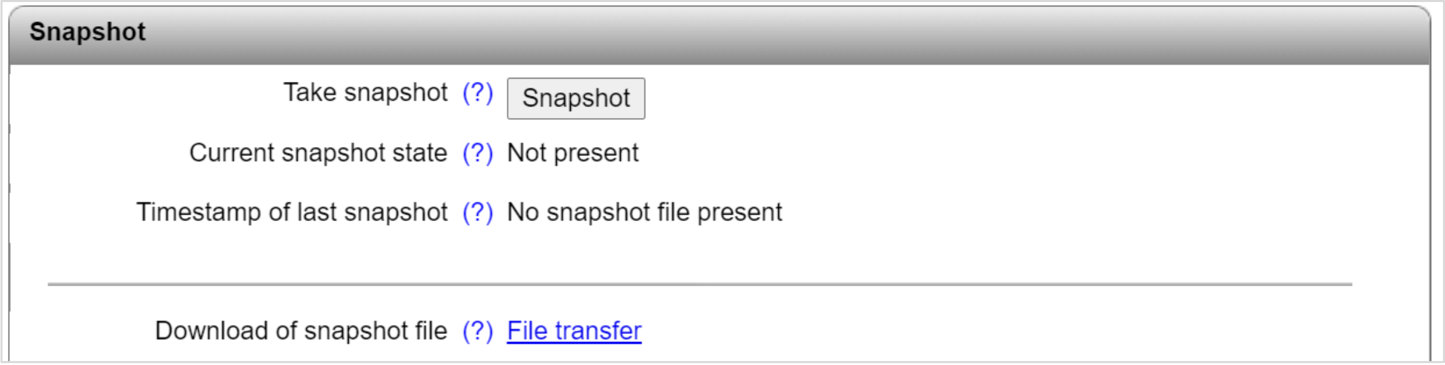
Diagnostics – Port Utilization

Here you will find an overview of the percentage port utilization for this device. For a detailed overview, click on the graph of an individual port.



Diagnostics – Snapshot

You can use the snapshot function to capture and download all parameters relevant to the runtime (e.g., configuration, events, etc.) and provide them to a service technician.



Snapshot

Take snapshot	(?)	Snapshot
Current snapshot state	(?)	Not present
Timestamp of last snapshot	(?)	No snapshot file present
Download of snapshot file	(?)	File transfer

Take snapshot: Click the “Snapshot” button to take a snapshot.

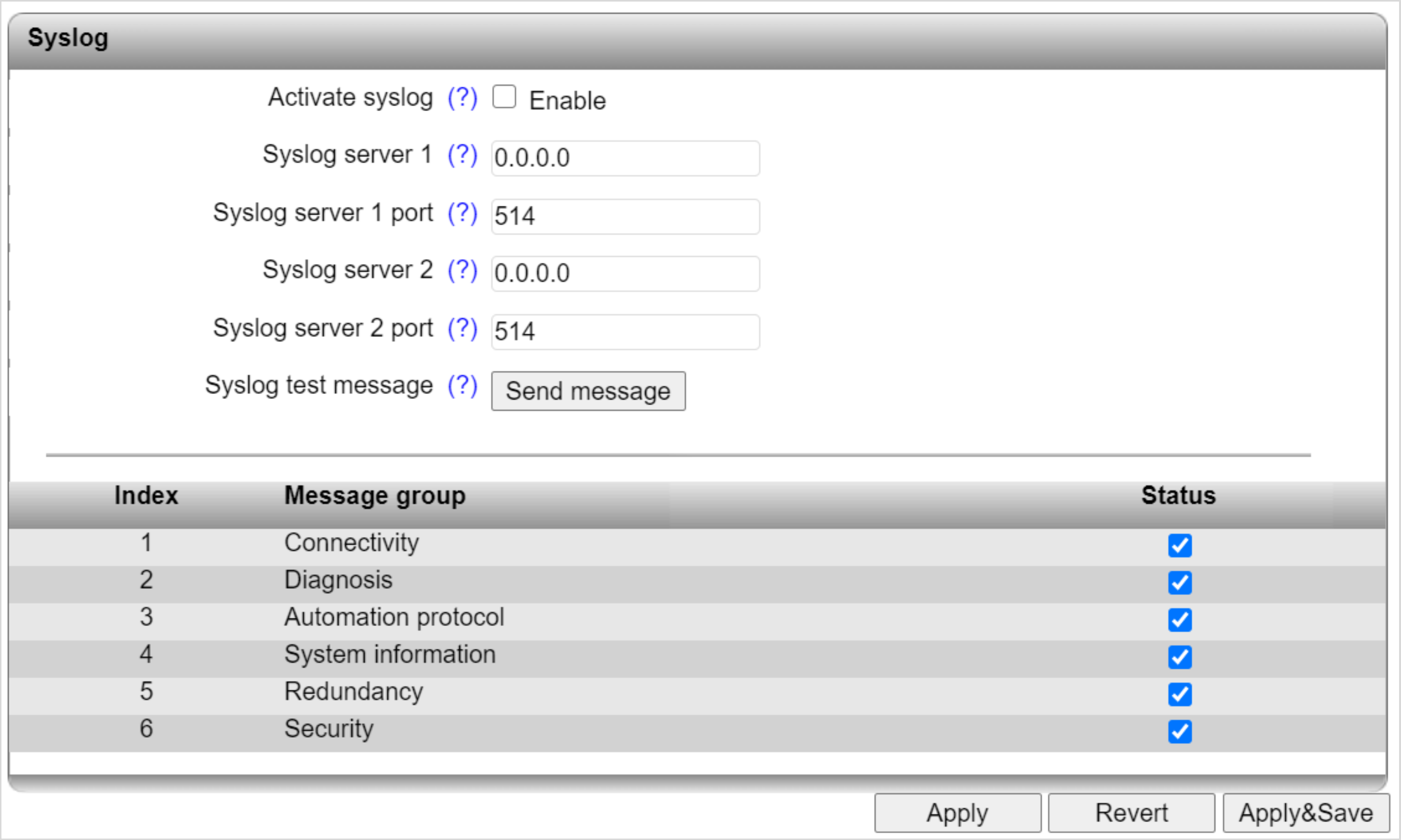
Current snapshot state: Indicates whether the snapshot is available, is currently being generated or does not exist.

Timestamp of last snapshot: Displays the time at which the last snapshot was generated.

Download of snapshot file: Clicking on the “File transfer” link opens the window for manual file download.

Diagnostics – Syslog

The Syslog function enables messages or events to be transmitted to one or more servers via UDP. In the event that two Syslog servers have been configured, the switch sends all messages/events to both servers.



Syslog

Activate syslog (?)	□ Enable
Syslog server 1 (?)	0.0.0.0
Syslog server 1 port (?)	514
Syslog server 2 (?)	0.0.0.0
Syslog server 2 port (?)	514
Syslog test message (?)	Send message

Index	Message group	Status
1	Connectivity	☑
2	Diagnosis	☑
3	Automation protocol	☑
4	System information	☑
5	Redundancy	☑
6	Security	☑

Activate syslog: Activate or deactivate the Syslog function here.

Syslog server 1: Set the IP address or DNS name of the first Syslog server here.

Syslog server 1 port: Set the UDP port of the first Syslog server here (default: 514).

Syslog server 2: Set the IP address or DNS name of the second Syslog server here.

Syslog server 2 port: Set the UDP port of the second Syslog server here (default: 514)

Syslog test message: Click on the “Send message” button to test the connection to the Syslog server. With Syslog, message reception is not confirmed by the server. Therefore the connection status can only be checked on the server, and not in the web-based management of the switch.

Status: Use the check boxes in the “Status” column to select the categories whose events are to be sent to the Syslog server.

The table below provides an overview of the specific events in the respective categories.

Connectivity	IP conflict detected
	TFTP connection failed
	ACDconflict detected IP
	LLDP new neighbor on port
	LLDP neighbor information changed on port
	Link monitor alarm raises on port
	IP address changed on interface
	Port Link up/down
	SFP module plugged on Port
	ACD device has no IP
	MTU size changed
Diagnosis	CRC status and peak on port reset
	CRC status on port changed to ok
	CRC status on port changed to critical
	CRC thresholds on port changed by user
	Alarm output failed
	CRC status on port changed to warning
System information	System time synchronized
	Pluggable memory removed
	Update firmware successful
	Configuration saved/loaded on/from pluggable memory
	Update failed
	Configuration difference detected
	Configuration saved/loaded successfully

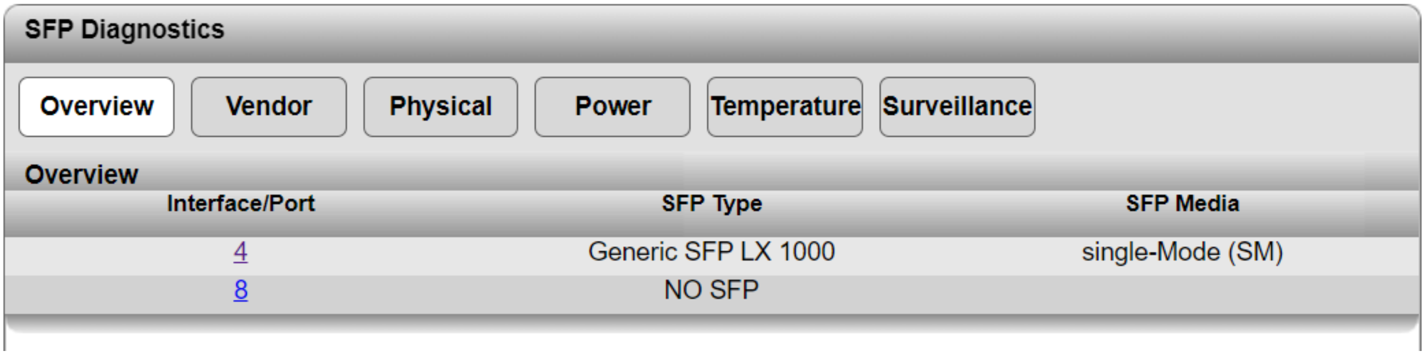
System information	Configuration parameter changed
	Smart Mode entered
	Smart Mode button enabled/disabled
	Error in configuration file
	Pluggable memory cleared
	New interface created
	Power supply lost
	Name of the device changed
	Parameter has been changed by the user
	FW image not valid
	Update processing
	Write to flash memory
	Wrong update image
	IGMP Snooping mode changed
	IGMP Snooping aging time changed
	Syslog test message
	Start FW update
	Write FW image into flash
Redundancy	RSTP ring detected
	RSTP topology changed
	RSTP root changed
	RSTP ring failed
	MRP client/manager activated
	MRP ring failed
	MRP link failed at port
Security	Port access violation on Port
	Radius Authentication Server shared secret changed
	Port successfully authenticated
	Password changed
	User authentication failed
	Radius authentication server IP/UDP address changed
	User configuration changed
	User login/logout
	Unauthorized access

Diagnostics – SFP Diagnostics

You will find detailed information on the SFP ports on this webpage.

The various “Overview”, “Vendor”, “Physical”, “Power”, and “Temperature” buttons provide various diagnostic data points that are made available by the respective SFP modules used. The data provided largely follows the Digital Diagnostic Monitoring Interface (DDMI) in accordance with SFF-8472 Rev 9.3.

This page is only available on devices with SFP ports.
Not every SFP module makes all of the data requested from the switch available.



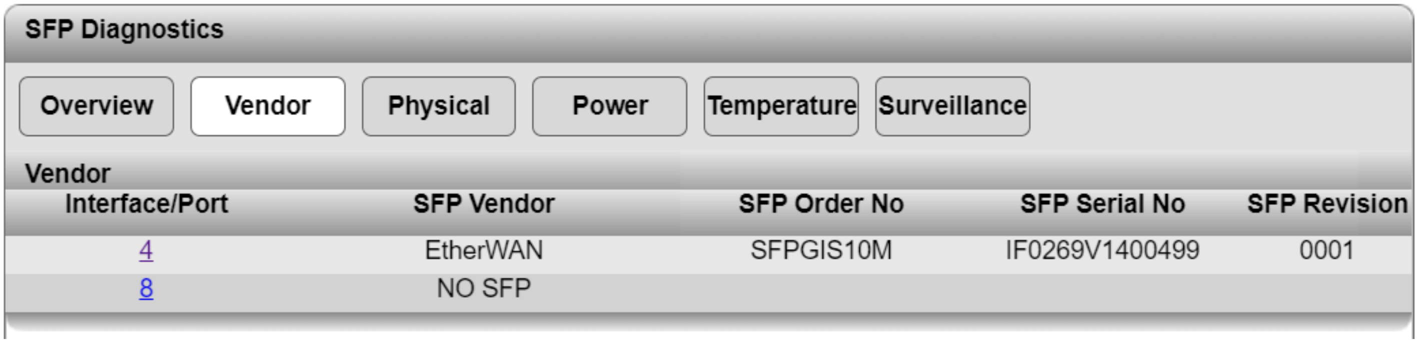
Overview

Interface/Port	SFP Type	SFP Media
4	Generic SFP LX 1000	single-Mode (SM)
8	NO SFP	

Overview
Interface/Port: The ports that can be used with SFP modules are displayed here. Clicking on the port number opens the “SFP Diagnostics Details” webpage for this port. This webpage shows all of the SFP information at a glance.

SFP Type: The type of SFP module used is displayed here. If no SFP module is inserted, “NO SFP” is displayed.

SFP Media: This column shows whether a multimode or singlemode SFP module is present.



Vendor

Interface/Port	SFP Vendor	SFP Order No	SFP Serial No	SFP Revision
4	EtherWAN	SFPGIS10M	IF0269V1400499	0001
8	NO SFP			

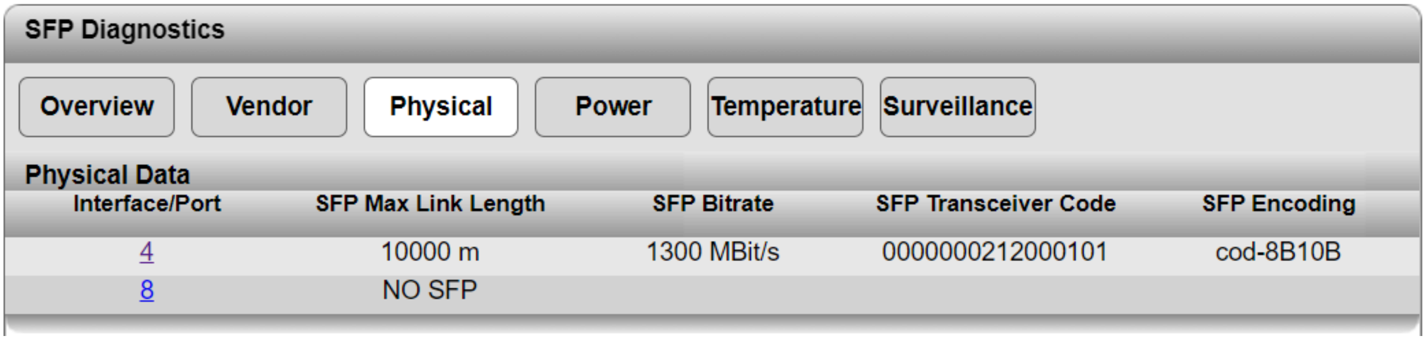
Vendor
Interface/Port: The ports that can be used with SFP modules are displayed here. Clicking on the port number opens the “SFP Diagnostics Details” webpage for this port. This webpage shows all of the SFP information at a glance.

SFP Vendor: The manufacturer of the SFP module is displayed here. If no SFP module is inserted, “NO SFP” is displayed.

SFP Order No: The order number of the SFP module used is displayed here.

SFP Serial No: This column shows the serial number of the SFP module used.

SFP Revision: The item revision of the SFP module used is displayed here.



Physical Data

Interface/Port	SFP Max Link Length	SFP Bitrate	SFP Transceiver Code	SFP Encoding
4	10000 m	1300 MBit/s	0000000212000101	cod-8B10B
8	NO SFP			

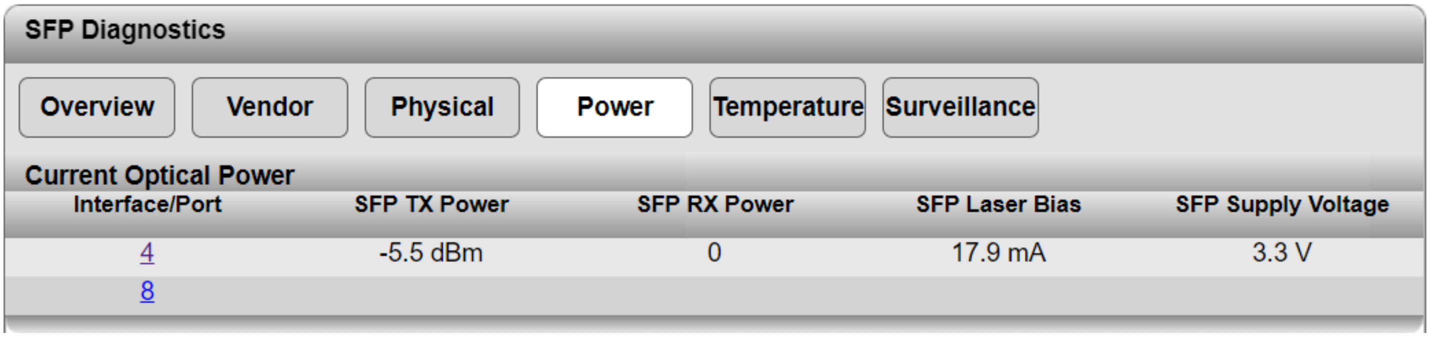
Physical Data
Interface/Port: The ports that can be used with SFP modules are displayed here. Clicking on the port number opens the “SFP Diagnostics Details” webpage for this port. This webpage shows all of the SFP information at a glance.

SFP Max Link Length: The maximum supported SFP module link length is displayed here in meters. If no SFP module is inserted, “NO SFP” is displayed.

SFP Bitrate: The nominal bit rate of the SFP module is displayed here. The bit rate includes the bits that are required for coding and delimiting the signal and the bits that carry data information. Therefore, it explicitly does not refer to the transmission speed available on the port.

SFP Transceiver Code: The transceiver code describes the electronic or optical interfaces that are supported by the transceiver. For optical receivers, values such as the fiber channel speed, transmission media, transmitter technology, and distance capability should be indicated.

SFP Encoding: The serial encryption mechanism is displayed in this column.



Current Optical Power

Interface/Port	SFP TX Power	SFP RX Power	SFP Laser Bias	SFP Supply Voltage
4	-5.5 dBm	0	17.9 mA	3.3 V
8				

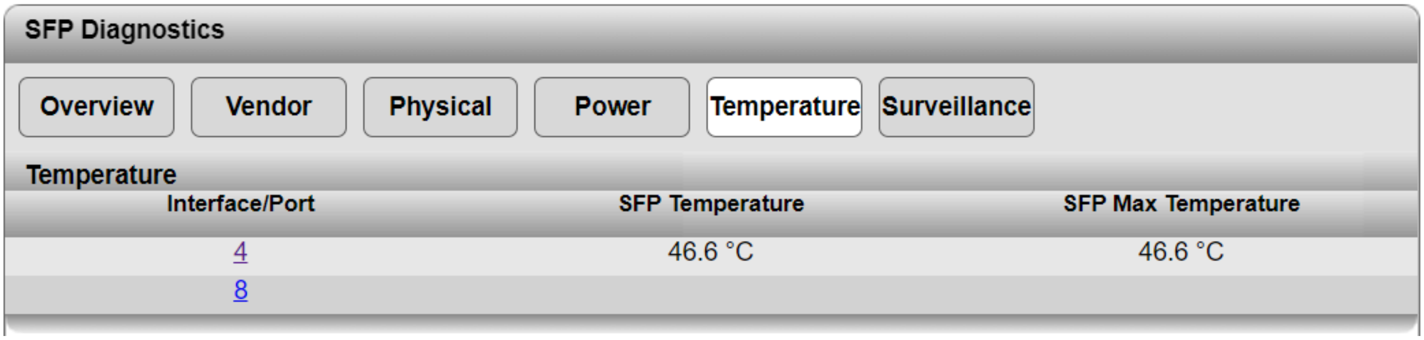
Current Optical Power
Interface/Port: The ports that can be used with SFP modules are displayed here. Clicking on the port number opens the “SFP Diagnostics Details” webpage for this port. This webpage shows all of the SFP information at a glance.

SFP TX Power: The current outgoing power level is displayed in dBm here.

SFP RX Power: The current incoming power level is displayed in dBm here.

SFP Laser Bias: The current laser bias current strength of the SFP module used is displayed in mA here.

SFP Supply Voltage: The current power supply of the SFP module used is displayed in V here.



Temperature

Interface/Port	SFP Temperature	SFP Max Temperature
4	46.6 °C	46.6 °C
8		

Temperature
Interface/Port: The ports that can be used with SFP modules are displayed here. Clicking on the port number opens the “SFP Diagnostics Details” webpage for this port. This webpage shows all of the SFP information at a glance.

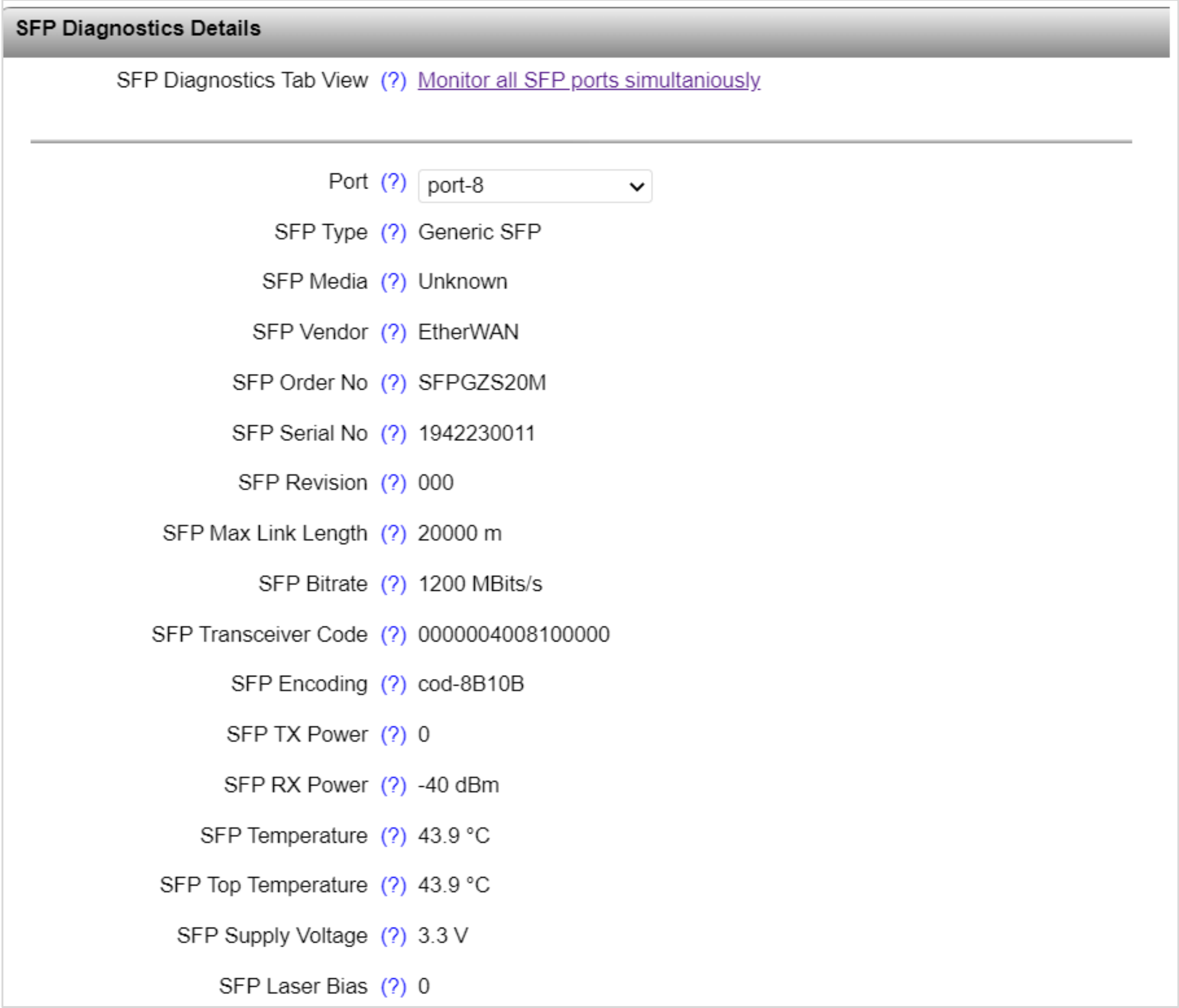
SFP Temperature: The current temperature measured in the SFP module is displayed in °C here.

SFP Top Temperature: The maximum temperature of any inserted SFP module inserted on this port since the switch was last restarted is displayed in °C here.

The SFP Top Temperature on a port can only be reset via a switch restart. Replacing an SFP module on a port does not cause the SFP Top Temperature value to be reset either.

SFP Diagnostics Details items

The SFP Diagnostics Details page provides a summary of all diagnostics information on the SFP module used.



SFP Diagnostics Details

SFP Diagnostics Tab View	(?)	Monitor all SFP ports simultaniously
Port	(?)	port-8
SFP Type	(?)	Generic SFP
SFP Media	(?)	Unknown
SFP Vendor	(?)	EtherWAN
SFP Order No	(?)	SFPGZS20M
SFP Serial No	(?)	1942230011
SFP Revision	(?)	000
SFP Max Link Length	(?)	20000 m
SFP Bitrate	(?)	1200 MBits/s
SFP Transceiver Code	(?)	0000004008100000
SFP Encoding	(?)	cod-8B10B
SFP TX Power	(?)	0
SFP RX Power	(?)	-40 dBm
SFP Temperature	(?)	43.9 °C
SFP Top Temperature	(?)	43.9 °C
SFP Supply Voltage	(?)	3.3 V
SFP Laser Bias	(?)	0

SFP Diagnostics Tab View: Click on the “Monitor all SFP ports simultaneously” link to return to the overview.

Port: Select the port you wish to configure.

SFP Type: The Gigabit Ethernet conformity type of the selected port is displayed here.

SFP Media: The media type that should be used with this SFP module is displayed here.

SFP Vendor: The name of the SFP module manufacturer is displayed here.

SFP Order No: The order number of the SFP module is displayed here.

SFP Serial No: The serial number of the SFP module is displayed here.

SFP Revision: The revision number of the SFP module is displayed here.

SFP Max Link Length: The maximum link length in meters supported by this SFP module is displayed here.

SFP Bitrate: The nominal bit rate of the SFP module is displayed here.

SFP Transceiver Code: A code in hexadecimal format for the electronic or optical compatibility is displayed here.

SFP Encoding: The encoding mechanism of the SFP module is displayed here.

SFP TX Power: The current optical power of the transmission unit is displayed here in increments of 0.1 dBm.

SFP RX Power: The current optical power that is received is displayed here in increments of 0.1 dBm.

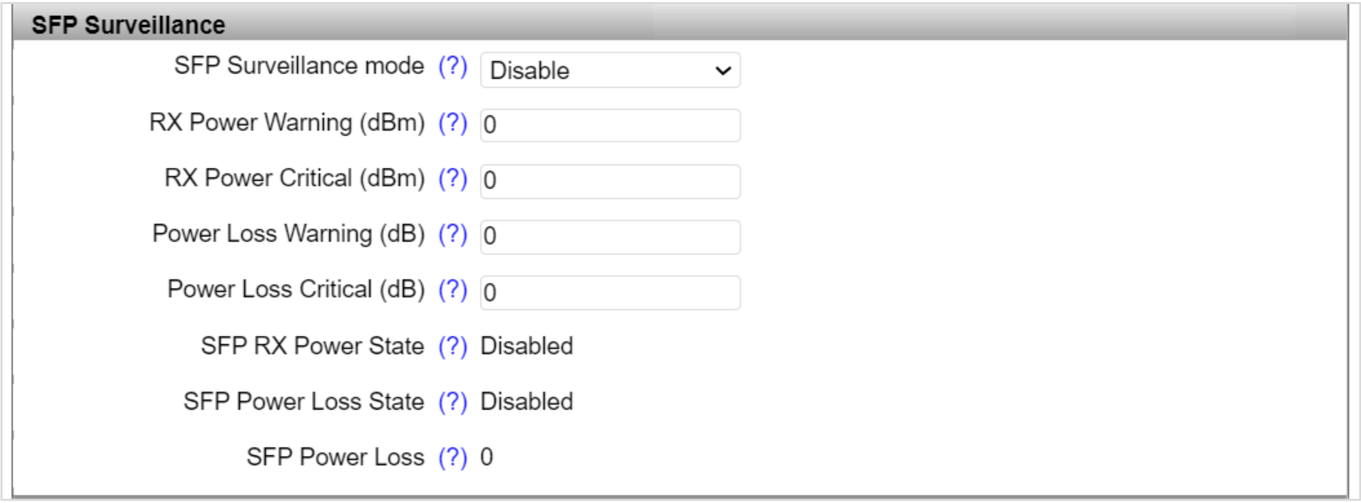
SFP Temperature: The current temperature in °C measured in the SFP module is displayed here.

SFP Top Temperature: The maximum temperature in °C measured in the SFP module since the last switch restart is displayed here.

SFP Supply Voltage: The current supply voltage of the SFP module in V is displayed here.

SFP Laser Bias: The current laser bias current of the SFP module in mA is displayed here.

SFP Surveillance items



SFP Surveillance

SFP Surveillance mode (?)	Disable
RX Power Warning (dBm) (?)	0
RX Power Critical (dBm) (?)	0
Power Loss Warning (dB) (?)	0
Power Loss Critical (dB) (?)	0
SFP RX Power State (?)	Disabled
SFP Power Loss State (?)	Disabled
SFP Power Loss (?)	0

SFP Surveillance mode: Select whether surveillance mode should be activated for the selected port.

RX Power Warning (dBm): Enter a value in dBm at which a warning about incoming voltage will be displayed. Enter “0” to deactivate surveillance of the threshold value.

RX Power Critical (dBm): Enter a value in dBm at which a warning about incoming voltage will be displayed. Enter “0” to deactivate surveillance of the threshold value.

Power Loss Warning (dB): Enter a value in dB at which a warning will be displayed. Enter “0” to deactivate surveillance of the threshold value.

Power Loss Critical (dB): Enter a value in dB at which a warning will be displayed. Enter “0” to deactivate surveillance of the threshold value.

SFP RX Power State: The current status of the optical power is displayed here.

SFP Power Loss State: The current status of the power loss is displayed here.

SFP Power Loss: The current power loss is displayed here in increments of 0.1 dB.

Appendix.

Fast Ring Detection

You can enable the “Fast Ring Detection” function in the web-based management under “Network Redundancy”.

This function speeds up the switch-over to a redundant path in the event of an error and enables easy diagnostics. Fast Ring Detection assigns an ID to each ring. This ID is communicated to every switch in the respective ring. One switch can belong to several different rings at the same time.

ℹ The “Fast Ring Detection” function is proprietary. It can only be used if all devices in the structure support this function.

The ring ID consists of the port number of the blocking port and the MAC address of the corresponding switch.

Advantages of the ring ID:

- Redundant paths are identified more easily
- Blocking ports are found more easily
- It is possible to check whether the desired topology corresponds to the actual topology

When using Fast Ring Detection, note the following:

- With RSTP Fast Ring Detection, only use devices that support this function.
- Enable RSTP Fast Ring Detection on all devices.
- All data paths must be in full duplex mode.

Fast Ring Detection switch-over times

With the maximum permissible number of switches in a ring, typical switch-over times range from 100 ms to 300 ms with Fast Ring Detection.

ℹ It is only possible to access the maximum number of switches when “Large Tree Support” is enabled at the same time.

Large Tree Support

The “Large Tree Support” function increases the maximum possible number of switches in an RSTP topology.

ℹ The “Large Tree Support” function is proprietary. It can only be used if all devices in the structure support this function.

When using Large Tree Support, note the following:

- Only use devices in the topology that support Large Tree Support.
- Enable Large Tree Support on all devices.
- We recommend that you only enable Large Tree Support when your network has more switches than possible for the standard RSTP.

Topology sizes

The RSTP protocol permits the setup of redundant networks and enables simple ring topologies as well as meshed structures. To prevent failures, you have to observe the following maximum values during planning and setup.

1. Ring topologies with “Large Tree Support” disabled
   - With default parameters (especially MaxAge = 20): Maximum 20 devices in the ring
   - With adapted MaxAge = 40: Maximum 40 devices in the ring

2. Ring topologies with “Large Tree Support” enabled
   - With default parameters (especially MaxAge = 20): Maximum 70 devices in the ring

3. Meshed topologies with “Large Tree Support” disabled
   - With default parameters (especially MaxAge = 20): Maximum distance to root bridge (intermediate data paths): 9 hops
   - With adapted MaxAge = 40: Maximum distance to root bridge: 19 hops

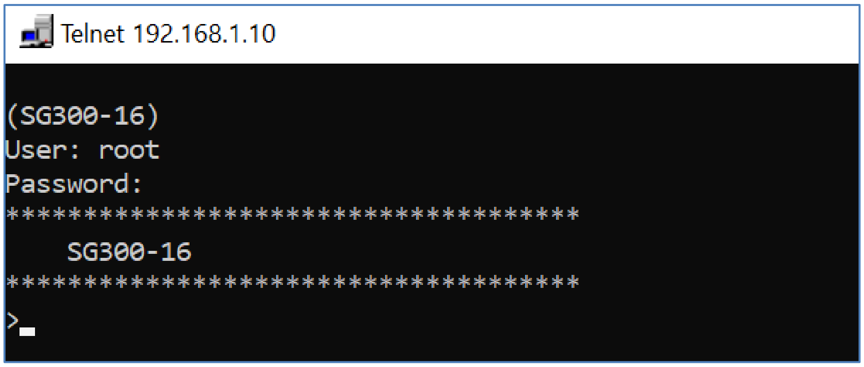
4. Meshed topologies with “Large Tree Support” enabled
   - With default parameters (especially MaxAge = 20): Maximum distance to root bridge (intermediate data paths): 34 hops

CLI (Command Line Interface)

Using the Command Line Interface (CLI)

The CLI is a text-based tool that can be used to configure the switch. The CLI is accessed by means of a connection via Telnet (factory default) or SSH. A third-party program such as PuTTY can also be used for connection.

Connect to the IP address of the switch and enter the username (default is **root**) and password (default is blank). The switch model/SKU number will be displayed.



Telnet 192.168.1.10

```
(SG300-16)
User: root
Password:
*************************************
    SG300-16
*************************************
>
```

Basic Principles of CLI Commands

In this manual, **CLI command names** are in bold. *CLI parameters* are in italics and must be replaced by appropriate values (e.g., names or numbers). If a command has several parameters, the order of these must be strictly observed.

The parameters of a command may be mandatory, optional or a selection of values (see Command Syntax table below).

Command Syntax Symbols

The following symbols are used to describe the values and arguments for command entries in the CLI.

<angle brackets>	Variable or value that must be specified.
[square brackets]	Optional parameters or arguments.
optionA | optionB	Vertical bar. Separates multiple exclusive items in a list of options.
{braces}	Denotes the mandatory selection of a value from a given list of values
[{}] Braces within square brackets	Denotes a selection within an optional parameter

Command Syntax

A command consists of one or more terms which can be followed by one or more parameters. These parameters can be mandatory or optional values.

Some commands, e.g., **show network** or **clear config**, do not require parameters. Other commands, e.g., **network parms**, require values to be specified after the command name. The parameters must be entered in the specified order, whereby optional parameters always follow mandatory parameters.

The following example illustrates the syntax using the **network parms** command:

network parms <ipaddr> <netmask> [gateway]

network parms is the command name. <ipaddr> and <netmask> are parameters and represent mandatory values, which must be specified after entering the command name. [gateway] is an optional parameter, which means that a value does not have to be specified.

The following examples illustrate the *correct* syntax for entering the **network parms** command:

network parms 192.168.10.42 255.255.255.0

network parms 192.168.10.42 255.255.255.0 192.168.10.0

The following examples illustrate *incorrect* syntax for entering the network parms command:

network parms 192.168.10.42 - missing mandatory parameter network parms 255.255.255.0 - missing mandatory parameter

network parms 255.255.255.0 192.168.10.42 - incorrect parameter sequence

Using the CLI Help

Entering a question mark (?) in the command prompt displays a list of all the commands currently available together with a brief description. Typing a question mark (?) after each entry displays all the available command names or parameters from that point on.

Auto Completion of Commands

The auto completion command is an additional way of writing a command, provided enough letters have already been entered to clearly identify the command name. As soon as enough letters have been entered, press space or TAB to automatically complete the words.

Using the CLI Network Scripting UI

The CLI network scripting UI enables CLI commands from scripts to be loaded into the device via the network. This means that the device can be configured and diagnosed using a URL via a PC or from a controller. Each command that is entered is confirmed by the device, either with OK (config commands) or by outputting the device data (show commands).

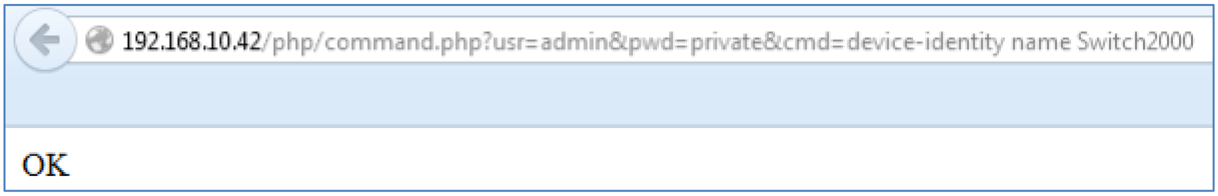
The command entry must follow a specific syntax:

http://ipaddress/php/command.php?usr=username&pwd=password&cmd=cli_command_1 | cli_command_2 | ....

The following examples illustrate the correct syntax for entering commands via the CLI network scripting UI:

Example: changing the device name

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=device-identity name SmartE

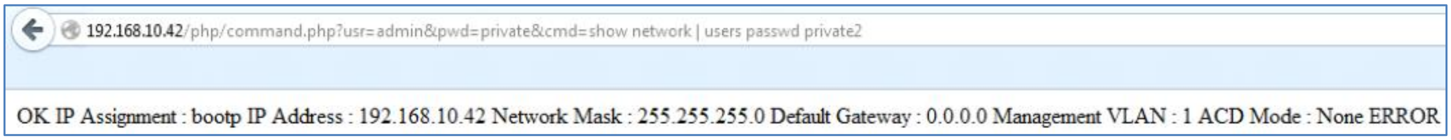


```
192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=device-identity name Switch2000
```

```
OK
```

Example: displaying the network parameters and changing the user password

http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network | users passwd private2



```
192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network | users passwd private2
```

```
OK IP Assignment : bootp IP Address : 192.168.10.42 Network Mask : 255.255.255.0 Default Gateway : 0.0.0.0 Management VLAN : 1 ACD Mode : None ERROR
```

CLI Commands

General Commands

Command	Value range	Default
reload		
Description	Restart the device	
Example	reload	

Command	Value range	Default
logout		
Description	Exit the CLI session (unsaved changes will be lost).	
Example	logout	

Command	Value range	Default
help		
Description	Open the CLI help	
Example	help	

Command	Value range	Default
quit		
Description	Exit the CLI session (unsaved changes will be lost).	
Example	quit	

Command	Value range	Default
show tech-support		
Description		
Example	show tech-support	

Command	Value range	Default
clear config		
Description	Reset configuration to factory default.	
Example	clear config	

Command	Value range	Default
write <configuration-name>	Max. 256 chars	
Description	Save the device configuration.	
Example	write prodconfig	

Command	Value range	Default
show configuration-status		
Description	Displays the following items: Configuration Name Configuration Status (modified, saved, not saved, etc.) Configuration Source	
Example	show configuration-status	

Command	Value range	Default
users create {username} {password} {repeat-password}	Password 8 – 64 characters	
Description	Create a new user	
Example	users create kautsky password123	

Command	Value range	Default
users delete {username}		
Description	Delete a user	
Example	users delete kautsky	

Command	Value range	Default
users passwd <username> <old-password> <new-password> <repeat-new-password>	New password (8 - 64 chars)	
Description	Change a user password	
Example	users passwd admin1 oldpass Switch123	

Command	Value range	Default
users roles create <rolename>		
Description	Create a new rolename	
Example	users roles create testrole	

Command	Value range	Default
users roles delete <rolename>		
Description	Delete a rolename	
Example	users roles delete testrole	

Command	Value range	Default
users role <username> {admin | expert | read-only}		
Description	Set user role.	
Example	Users role gandalf admin	

Command	Value range	Default
users status <username> {enable | disable}		
Description	Enable or disable a user account. A disabled user cannot login to the device anymore.	
Example	users status noobuser enable	

Command	Value range	Default
users lock-status <username> {enable | disable}		
Description	Enable or disable the mode that a user access to the device is denied if the configured number of consecutive invalid login attempts has been reached.	
Example	users lock-status newuser1 disable	

Command	Value range	Default
users lock-limit <username> <lock-limit>	(1 – 100)	
Description	Set user lock limit	
Example	users lock-limit userbob 5	

Command	Value range	Default
users lock-timeout <username> <value>	1-1440 minutes	
Description	Set user lock timeout	
Example	users lock-timeout userbob 5	

Command	Value range	Default
users roles add-group-ro {rolename} {system | ident | user | network |ui | automation | discovery | l2l3 | redundancy | timesynch | dhcp | port-cfg | rmon | port-mirr | port-sec | routing | logging}		
Description	Add permission group to role with read-only capabilities	
Example	users roles add-group-ro testgroup ui	

Command	Value range	Default
users roles add-group-rw {rolename} {system | ident | user | network |ui | automation | discovery | l2l3 | redundancy | timesynch | dhcp | port-cfg | rmon | port-mirr | port-sec | routing | logging}		
Description	Add permission group to role with read-write capabilities	
Example	users roles add-group-rw testgroup ui	

Command	Value range	Default
users roles remove-group <rolename> <permissiongroup>		
Description	Remove permission group from role	
Example	users roles remove-group testrole discovery	

CRC Surveillance Commands

Command	Value range	Default
show surveillance crc port-no <port>		
Description	Displays the CRC information of the selected port.	
Example	show surveillance crc port-no 5	

Command	Value range	Default
show surveillance crc all		
Description	Shows the CRC information of all ports.	
Example	show surveillance crc all	

Command	Value range	Default
show port-info port-no <port>		
Description	Displays port information of the selected port, including the CRC status.	
Example	show port-info port-no 5	

Command	Value range	Default
show snmp-trap		
Description	Shows all SNMP traps, including the CRC trap (ok / warning / critical).	
Example		

Command	Value range	Default
clear crc-surveillance port-no <port>		
Description	Sets the CRC error counter of the selected port to 0 and the CRC error status to OK.	
Example	clear crc-surveillance port-no 5	

Command	Value range	Default
clear crc-surveillance all		
Description	Sets the CRC error counter of all ports to 0 and the CRC error status to OK	
Example		

Command	Value range	Default
port <port> crc-threshold <threshold>	1000 ppm to 1000000 ppm	40000
Description	Sets the CRC threshold for the selected port	
Example	port 5 crc-threshold 50000	

Port Security Commands

Command	Value range	Default
port-security status {enable | disable}		disable
Description	Enable or disable port security	
Example	port-security status enable	

Command	Value range	Default
port-security port <port-no> status <status>	{none | trap | block}	
Description	Set port security mode for a specific port **none**: no security function **trap**: send trap when a new device/new MAC address is detected **block**: block everything except the exceptions entered (whitelist)	
Example	port-security port 1 status trap	

Command	Value range	Default
port-security port <port-no> add-mac <MAC> <VLAN>	MAC: (xx:xx:xx:xx:xx:xx)	
Description	Create new filter entry An entry consists of MAC and VLAN. Always use “VLAN 1” for WLAN. Note: the command “port-security port 10 configure” can be used to add a description.	
Example	port-security port 10 add-mac 00:A0:45:DD:5E:8C 1	

Command	Value range	Default
port-security port <port-no> remove-mac <MAC> <VLAN>	MAC: (xx:xx:xx:xx:xx:xx) VLAN: for WLAN: 1	
Description	Remove filter entry. The entry is specified via MAC and VLAN.	
Example	port-security port 10 remove-mac 00:a0:45:dd:5e:8c 1	

Command	Value range	Default
port-security port <port-no> configure <MAC> <VLAN> description <description>	description: (15 characters)	
Description	Add or edit description for filter entry. The entry is specified via MAC and VLAN.	

Example	port-security port 10 configure 00:a0:45:dd:5e:8c 1 description “Testdesc1”

Command	**Value range**	**Default**
show port-security port <port-no>	Port: (1…| all)	
Description	Show all current security settings for the port: Security mode Last MAC Address Learned Illegal Address Counter Allowed MAC Address table with columns (description, MAC-address, VLAN ID)	
Example	show port-security port 1	

Command	**Value range**	**Default**
show port-security global		
Description	Shows the global port security settings	
Example	show port-security global	

Command	**Value range**	**Default**
port-security clear-illegal-cntr		
Description	Clear port security illegal counters.	
Example	port-security clear-illegal-cntr	

Radius Commands

Command	**Value range**	**Default**
users radius auth-server_Id <Id> name		
Description	Configure the name of the authentication server	
Example	users radius auth-server_Id 1 name testname	

Command	**Value range**	**Default**
users radius auth-server_Id <Id> shared-secret		
Description	Shared secret (password) for login to Radius server	
Example	users radius auth-server_Id 1 shared-secret “MySecret”	

Command	**Value range**	**Default**
users radius auth-server_Id <Id> udp-port		
Description	Radius server port	
Example	users radius auth-server_Id 1 udp-port 8888	

Command	Value range	Default
users radius auth-server_Id <Id> ip-address		
Description	IP address of the Radius server Only “1” may be used as the Id at present.	
Example	users radius auth-server_Id 1 ip-address 192.168.0.250	

Dot1x Authentication Commands

Command	Value range	Default
show dot1x-authenticator global		
Description	Displays the global dot1x mode.	
Example	show dot1x-authenticator global	

Command	Value range	Default
show dot1x-authenticator port <port-no>		
Description	Shows the following parameters for dot1x on a selected port: Control Mode, Guest VLAN, Re-Authentication Mode, Re-Authentication Timeout, Last EAPOL MAC Address, Status	
Example	show dot1x-authenticator port 5	

Command	Value range	Default
dot1x-authenticator port <port-no> reauthenticate		
Description	Reauthenticate the client on the given port.	
Example	dot1x-authenticator port 10 reauthenticate	

Command	Value range	Default
dot1x-authenticator port <port-no> reauthentication-period <value>	1 - 65535 seconds	
Description	Re-Authenticate client at regular interval defined by the period.	
Example	dot1x-authenticator port 10 reauthentication-period 100	

Command	Value range	Default
dot1x-authenticator port <port-no> reauthentication-mode {enable | disable}		
Description	Enable Re-Authentication mode to authenticate the client at regular interval defined by Re-Authentication Period.	
Example	dot1x-authenticator port reauthentication-mode enable	

Command	Value range	Default
dot1x-authenticator port <port-no> control-mode {auto | force-authenticate | force-unauthenticate}		
Description	Configure 802.1x on this port. Force Authenticate: Authenticate all the devices on this port. (Disable 802.1x) Force Unauthenticate: Do not authenticate any device on this port.	
Example	dot1x-authenticator port 10 control-mode force-authenticate	

Command	Value range	Default
dot1x-authenticator global {enable | disable}		
Description	Enable or Disable dot1x authenticator globally.	
Example	dot1x-authenticator global enable	

System Commands

Command	Value range	Default
show version		
Description	Display the device description and hardware information: Serial number Hardware version Firmware version Bootloader version	
Example	show version	

Command	Value range	Default
show sys-info		
Description	Display the system information: Device name Object ID Device description Contact person Device location	
Example	show sys-info	

Command	Value range	Default
device-identity name <name>	<name> max. 256 chars	SmartE
Description	Change the device name	
Example	device-identity name Switch-xyzzy	

Command	Value range	Default
device-identity description <description>	<description> max. 256 chars	
Description	Change the device description	
Example	device-identity description Switch dilvish	

Command	Value range	Default
device-identity location <location>	<location> max. 256 chars	
Description Change the device location		
Example device-identity location Nakatomi tower		

Command	Value range	Default
device-identity contact <contact>	<contact> max. 256 chars	
Description Change the contact person for the device		
Example device-identity contact Thomas A. Anderson		

Command	Value range	Default
snapshot trigger		
Description Trigger the snapshot function to capture the current runtime parameters.		
Example snapshot trigger		

Command	Value range	Default
show snapshot status		
Description Shows the status of the Snapshot file (not present / busy / present / error).		
Example show snapshot status		

Command	Value range	Default
show snapshot timestamp		
Description Shows the timestamp of the last snapshot.		
Example show snapshot timestamp		

Command	Value range	Default
show transfer-status		
Description Shows the status of the currently running snapshot transfer		
Example show transfer-status		

Command	Value range	Default
snapshot trigger		
Description Creates a snapshot with the currently applied parameters.		
Example snapshot trigger		

Command	Value range	Default
file-transfer <method> read-from-device snapshot <ipaddress> <file-name>		
Description	Starts the download of the snapshot from the device	
Example	file-transfer tftp read-from-device snapshot 192.168.1.40 Snap1	

Command	Value range	Default
show syslog message-group		
Description	Shows the activation status of the group messages.	
Example	show syslog message-group	

Command	Value range	Default
show syslog status		
Description	Shows the activation status of the syslog function on the switch.	
Example	show syslog status	

Command	Value range	Default
show syslog server		
Description	Shows the syslog server parameters	
Example	show syslog server	

Command	Value range	Default
syslog status {enable | disable}		
Description	Activate or deactivate the syslog function. The deactivated syslog prevents any communication to a syslog server.	
Example	syslog status enable	

Command	Value range	Default
syslog server <value> ip-address <ip address>		
Description	Configure the IP address of the syslog server.	
Example	syslog server 1 ip-address 192.168.1.200	

Command	Value range	Default
syslog server <value> udp-port <port>		
Description	Configure the UDP port of the syslog server.	
Example	syslog server 1 udp-port 10	

Command	Value range	Default
syslog send-test-message		
Description	Send a test message to test the configuration.	
Example	syslog send-test-message	

Command	Value range	Default
syslog message-group <value> {enable | disable}	1 Connectivity 2 Diagnosis 3 Automation protocol 4 System information 5 Redundancy 6 Security	
Description	Enable / disable a message group	
Example	syslog message-group 1 disable	

Event Table Commands

Command	Value range	Default
show event-table		
Description	Display the event table with the following columns: Index Event Device runtime	
Example	show event-table	

Command	Value range	Default
clear event-table		
Description	Delete/clear the event table	
Example	clear event-table	

MAC Address Table Commands

Command	Value range	Default
show mac-address-table		
Description	Display the MAC address table	
Example	show mac-address-table	

Command	Value range	Default
clear mac-address-table		
Description	Clear the MAC address table.	
Example	clear mac-address-table	

FW Image Handling Commands

Command	Value range	Default
file-transfer tftp write-to-device firmware <ip-address> <filename>	<ip-address> IP address (xxx.xxx.xxx.xxx)	
Description	Transfer of a firmware image file to the device. The firmware update is performed immediately, the device then restarts and the CLI connection is terminated.	
Example	file-transfer tftp write-to-device firmware 192.168.0.1 SMARTE_v1_00.bin	

Script Handling Commands

Command	Value range	Default
show script		
Description		
Example	show script	

Network Commands

Command	Value range	Default
show network		
Description	Display the current network parameters: IP address assignment (static, BootP, DHCP) IP address Network mask Default gateway Management VLAN Address Conflict Detection (ACD) mode	
Example	show network	

Command	Value range	Default
network parms <ip-address> <netmask> [gateway]	<ip-address> (xxx.xxx.xxx.xxx) <netmask> (xxx.xxx.xxx.xxx) [gateway] (xxx.xxx.xxx.xxx)	0.0.0.0 0.0.0.0 0.0.0.0
Description	Change the network parameters: IP address Network mask Default gateway	
Example	network parms 192.168.0.150 255.255.255.0	

Command	Value range	Default
network protocol {bootp | dhcp | none}		bootp
Description	Change the IP address assignment	
Example	network protocol dhcp	

Command	Value range	Default
network mgmt-vlan <vlan-id>	VLAN ID (1 - 4000)	1
Description	Change the management VLAN	
Example	network mgmt-vlan 2	

Command	Value range	Default
network acd-mode {acd | none}		None
Description	Change the ACD (Address Conflict Detection) mode	
Example	network acd-mode acd	

Command	Value range	Default
network dns-server <1 | 2> <IP address>	<1 | 2> Primary or secondary DNS server (xxx.xxx.xxx.xxx)	
Description	Configure the DNS server	
Example	network dns-server 1 192.168.1.250	

Command	Value range	Default
network hostname resolution {enable | disable}		enable
Description	Activate / deactivate host name resolution.	
Example	network hostname resolution disable	

Command	Value range	Default
network hostname name <hostname>		
Description	Configure the host name of the device.	
Example	network hostname name Glamdring	

Command	Value range	Default
lldp initial-ip-port		
Description	Configure topology based initial IP port.	
Example	lldp initial-ip-port	

Services Commands

Command	Value range	Default
show service {sntp | general}		
Description	Status indicator for all of the following services: Sntp Network time protocol Primary SNTP server Primary server description Primary server name Secondary SNTP server Secondary server description Secondary server name UTC offset Synchronization Status Last SNTP synchronization General Web server SNMP server CLI service CLI network scripting UI (CLI command entry via URL)	
Example	show service sntp	

Command	Value range	Default
service cli-service {telnet | ssh | disable}		Telnet
Description	Change the CLI service protocol.	
Example	service cli-service telnet	

Command	Value range	Default
service cli-network-script-ui {enable | disable}		enable
Description	Activation/deactivation of the CLI network scripting UI (CLI command entry via URL)	
Example	service cli-network-script-ui disable	

Command	Value range	Default
service web-server {disable | http | https}		http
Description	Change the web server protocol	
Example	service web-server https	

Command	Value range	Default
service snmp-agent {disable | snmp-v2 | snmp-v3}		snmp-v2
Description	Change the SNMP server	
Example	service snmp-agent snmp-v2	

Command	Value range	Default
service login-expire <time>	60 – 3600 seconds	1200
Description	Configure login expire time.	
Example	service login-expire 3600	

Command	Value range	Default
service snmpv2-read-comm {tx}	Max. 255 characters	
Description	Configure SNMPv2 read community.	
Example	service snmpv2-read-comm 100	

Command	Value range	Default
service confidential-web-view {enable | disable}		
Description	Enable|Disable a required user login for the web site access.	
Example	service confidential-web-view enable	

Command	Value range	Default
service smart-mode {enable | disable}		
Description	Enable|Disable smart mode (mode button).	
Example	service smart-mode disable	

Command	Value range	Default
service persistent-evt-log {enable | disable}		enable
Description	Enable|Disable persistent storage of event-table.	
Example	service persistent-evt-log enable	

Command	Value range	Default
service sntp status {enable | disable}		disable
Description	Activate / deactivate the global SNTP status.	
Example	service sntp status enable	

Command	Value range	Default
service sntp mode {unicast | broadcast}		
Description	Set the SNTP mode.	
Example	service sntp mode broadcast	

Command	Value range	Default
service sntp primary-server <ip-address>	(xxx.xxx.xxx.xxx)	
Description	Set the IP address of the SNTP server.	
Example	service sntp primary-server 192.168.20.50	

Command	Value range	Default
service sntp primary-server description <description>	Max. 256 characters	
Description	Set the description of the SNTP server.	
Example	service sntp primary-server description alphaserver	

Command	Value range	Default
service sntp backup-server <ip-address>	(xxx.xxx.xxx.xxx)	
Description	Set the IP address of the backup SNTP server.	
Example	service sntp backup-server 192.168.15.100	

Command	Value range	Default
service sntp backup-server description <description>		
Description	Set the description of the backup SNTP server.	
Example	service sntp backp-server description betaserver	

Command	Value range	Default
service system-time <"YYYY/MM/DD hh:mm:ss">		
Description	Set the local system time.	
Example	service system-time "2021/01/26 14:51:01"	

LLDP Services Commands

Command	Value range	Default
show lldp topology all		
Description	Tabular display of the LLDP topology with the following columns: Local port Chassis ID of the connected device IP address of the connected device Remote port of the connected device Description of the remote port on the connected device	
Example	show lldp topology all	

Command	Value range	Default
show lldp global		
Description	Display the configuration parameters: LLDP status LLDP transmission interval LLDP transmit port LLDP receive port	
Example	show lldp global	

Command	Value range	Default
show lldp topology port-no <port-no>		
Description	Display the topology information at a port: Complete chassis ID Complete port name System name System description	
Example	show lldp topology port-no 3	

Command	Value range	Default
lldp status {enable | disable}		enable
Description	Change the LLDP status	
Example	lldp status enable	

Command	Value range	Default
lldp tx-interval <value>	Interval in seconds (5 - 32768)	5
Description	Change the LLDP transmission interval	
Example	lldp tx-interval 10	

Command	Value range	Default
lldp port-tx enable <port-list>	Comma-separated list of port numbers	All enable
Description	Activation of the LLDP transmit ports	
Example	lldp port-tx enable 3,4,8	

Command	Value range	Default
lldp port-tx disable <port-list>	Comma-separated list of port numbers	No disable
Description	Deactivation of the LLDP transmit ports	
Example	lldp port-tx disable 3,4,8	

Command	Value range	Default
lldp port-rx enable <port-list>	Comma-separated list of port numbers	All enable
Description	Activation of the LLDP receive ports	
Example	lldp port-rx enable 3,4,8	

Command	Value range	Default
lldp port-rx disable <port-list>	Comma-separated list of port numbers	No disable
Description	Deactivation of the LLDP receive ports	
Example	lldp port-rx disable 3,4,8	

Port Features Commands

Command	Value range	Default
show port-info all		
Description	Display the basic parameters of all ports: Port number Port name Port type Port status Port mode	
Example	show port-info all	

Command	Value range	Default
show port-info port-no <port-no>		
Description	Display the basic parameters of one port: Port number Port name Port type Port status Port mode Status flow control Status link monitoring	
Example	show port-info port-no 3	

Command	Value range	Default
show port-stat port-no <port-no>		
Description	Display the port statistics of one port	
Example	show port-stat port-no 5	

Command	Value range	Default
show port-util port-no <port-no>		
Description	Display the RX and TX utilization of one port	
Example	show port-util port-no 1	

Command	Value range	Default
show port-util all		
Description	Display the RX and TX utilization of all ports	
Example	show port-util all	

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> admin-mode {enable | disable}</td><td></td><td>all enable</td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of a port</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 admin-mode disable</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> modus autoneg</td><td></td><td></td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of auto-negotiation on one port</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 modus autoneg</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> modus auto10_100</td><td></td><td></td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of auto-negotiation on one port (only 10/100 Mbps, not 1000 Mbps)</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 modus auto10_100</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> modus speed <speed> {half-duplex | full-duplex}</td><td><speed> Transmission speed in Mbps {10 | 100 | 1000})</td><td></td></tr>
<tr><td><b>Description</b></td><td colspan="3">Change the transmission speed and duplex mode on one port</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 modus speed 100 half-duplex</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> modus faststartup</td><td></td><td></td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of Fast Startup mode on one port.</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 modus faststartup</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> description <text></td><td>(0 - 31 chars)</td><td></td></tr>
<tr><td><b>Description</b></td><td colspan="3">Change the port name</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 description RingPortGrue</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> link-monitoring {enable | disable}</td><td></td><td>all disable</td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of link monitoring on one port</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 link-monitoring disable</td></tr>
</table>

<table>
<tr><th colspan="2">Command</th><th>Value range</th><th>Default</th></tr>
<tr><td colspan="2">port <port-no> flow-control {enable | disable}</td><td></td><td>All disable</td></tr>
<tr><td><b>Description</b></td><td colspan="3">Activation/deactivation of flow control on one port</td></tr>
<tr><td><b>Example</b></td><td colspan="3">port 3 flow-control disable</td></tr>
</table>

Command	Value range	Default
port <port-no> jumbo-frames {enable | disable}		disable
Description	Enable or disable Jumbo frames.	
Example	port 5 jumbo-frames enable	
Command	**Value range**	**Default**
port <port-no> mtu <value>	Number of bytes 1522 to 9600	1536
Description	Set the maximum jumbo frame size in bytes.	
Example	port 4 mtu 1522	

Command	Value range	Default
port <port-no> crc-threshold <value>		40000
Description	Set the threshold for CRC errors on the selected port.	
Example	port 2 crc-threshold 30000	

Command	Value range	Default
clear port-stat port-no <port-no>		
Description	Resets the port statistics counters for the selected port back to 0.	
Example	clear port-stat port-no 3	

Command	Value range	Default
clear port-stat all		
Description	Resets the port statistics counters for all ports to 0	
Example	clear port-stat all	

Port Mirroring Commands

Command	Value range	Default
show port-mirror		
Description	Display the port mirroring parameters: Global status Receive port (mirroring port) Mirrored ports (incoming traffic) Mirrored ports (outgoing traffic)	
Example	show port-mirror	

Command	Value range	Default
port-mirror status {enable | disable}		disable
Description	Activation/deactivation of the global port mirroring status	
Example	port-mirror status enable	

Command	Value range	Default
port-mirror dest <port-no>		1
Description	Change the receive port (mirroring port)	
Example	port-mirror dest 8	

Command	Value range	Default
port-mirror ingress enable <port-list>	Comma-separated list of port numbers	all disable
Description	Activation of RX port mirroring (incoming traffic) on multiple ports	
Example	port-mirror ingress enable 3,4,8	

Command	Value range	Default
port-mirror ingress disable <port-list>	Comma-separated list of port numbers	all disable
Description	Deactivation of RX port mirroring (incoming traffic) on multiple ports	
Example	port-mirror ingress disable 3,4,8	

Command	Value range	Default
port-mirror egress enable <port-list>	Comma-separated list of port numbers	all disable
Description	Activation of TX port mirroring (outgoing traffic) on multiple ports	
Example	port-mirror egress enable 3,4,8	

Command	Value range	Default
port-mirror egress disable <port-list>	Comma-separated list of port numbers	all disable
Description	Deactivation of TX port mirroring (outgoing traffic) on multiple ports	
Example	port-mirror egress disable 3,4,8	

VLAN Commands

Command	Value range	Default
show vlan global		
Description	Display the current VLAN mode	
Example	show vlan global	

Command	Value range	Default
show vlan static-table		
Description	Display the static VLAN table: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	
Example	show vlan static-table	

Command	Value range	Default
show vlan current-table		
Description	Display the current VLAN table: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	
Example	show vlan current-table	

Command	Value range	Default
show vlan port-table		
Description	Display the port-based static VLAN table for all ports: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	
Example	show vlan port-table	

Command	Value range	Default
show vlan port <port-no>		
Description	Display the port-based static VLAN table for one port: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	
Example	show vlan port 3	

Command	Value range	Default
show vlan vlan-id <vlan-id>	(1 - 4000)	
Description	Display the VLAN information for a VLAN: VLAN ID VLAN name Device ports (untagged) Device ports (tagged)	
Example	show vlan vlan-id 3	

Command	Value range	Default
vlan status {transparent | tagged}		transparent
Description	Change the VLAN mode	
Example	Vlan status tagged	

Command	Value range	Default
vlan create <vlan-id>	(1 - 4000)	
Description	Create a new static VLAN	
Example	Vlan create 5	

Command	Value range	Default
vlan delete <vlan-id>	(1 - 4000)	
Description	Delete a static VLAN	
Example	vlan delete 5	

Command	Value range	Default
vlan static <vlan-id> name <vlan-name>	(1 - 4000), (0 - 31 chars)	
Description	Change the name of a static VLAN	
Example	vlan static 5 name VLAN_5	

Command	Value range	Default
vlan static <vlan-id> tagged-mem-ports <port-list>	(1 - 4000) Comma-separated list of port numbers	
Description	Assignment of device ports (tagged) to a VLAN	
Example	vlan static 5 tagged-mem-ports 2,5	

Command	Value range	Default
vlan static <vlan-id> untagged-mem-ports <port-list>	(1 - 4000) Comma-separated list of port numbers	
Description	Assignment of device ports (untagged) to a VLAN	
Example	vlan static 5 untagged-mem-ports 2,5	

Command	Value range	Default
vlan static <vlan-id> no-member <port-list>	(1 - 4000) Comma-separated list of port numbers	
Description	Removal of device ports from a VLAN	
Example	vlan static 5 no-member 3,5	

Command	Value range	Default
vlan port <port-no> vlan <vlan-id>	(1 - 4000)	
Description	Assignment of a default VLAN ID to a port	
Example	vlan port 3 vlan 5	

Command	Value range	Default
vlan port <port-no> priority <value>	(0 - 7)	0
Description	Assignment of a default priority to a port	
Example	vlan port 3 priority 7	

Command	Value range	Default
vlan port <port-no> ingress-filter {enable | disable}		all disable
Description	Activation/deactivation of the ingress filter at a port	
Example	vlan port 3 ingress-filter disable	

Command	Value range	Default
vlan routing add <vlan-id> <interface-no>		
Description	Creates a routing VLAN from a VLAN and assigns this to a Layer 3 interface.	
Example	vlan routing add 200 2	

Command	Value range	Default
vlan routing delete <vlan-id>		
Description	Removes the routing VLAN and makes it a Layer 2 VLAN.	
Example	vlan routing delete 200	

Multicast Commands

Command	Value range	Default
show multicast igmp		
Description	Display the IGMP snooping information: Status IGMP Snooping Snoop Aging Time IGMP Query Version Query interval Status of IGMP extension FUQ Status of IGMP extension BUQ Status of IGMP extension auto query port List of static query ports	
Example	show multicast igmp	

Command	Value range	Default
show multicast static-groups		
Description	Tabular display of the static multicast groups with the following columns: Multicast address VLAN ID Member ports including status	
Example	show multicast static-groups	

Command	Value range	Default
show multicast current-groups		
Description	Tabular display of the current multicast groups with the following columns: VLAN ID Multicast address Port member	
Example	show multicast current-groups	

Command	Value range	Default
multicast igmp snoop status {enable | disable}		disable
Description	Activation/deactivation of IGMP snooping	
Example	multicast igmp snoop status enable	

Command	Value range	Default
multicast igmp snoop aging <value>	Aging time in seconds (30 - 3600)	300
Description	Change the aging time	
Example	multicast igmp snoop aging 100	

Command	Value range	Default
multicast igmp querier version {disable | v1 | v2}		disable
Description	Change the querier version	
Example	multicast igmp querier version v2	

Command	Value range	Default
multicast igmp querier interval <value>	Querier interval in seconds (10 - 3600)	125
Description	Change the querier interval	
Example	multicast igmp querier interval 500	

Command	Value range	Default
multicast igmp extension fuq {enable | disable}		enable
Description	Activation/deactivation of the IGMP extension FUQ	
Example	multicast igmp extension fuq enable	

Command	Value range	Default
multicast igmp extension buq {enable | disable}		enable
Description	Activation/deactivation of the IGMP extension BUQ	
Example	multicast igmp extension buq enable	

Command	Value range	Default
multicast igmp extension auto-query {enable | disable}		enable
Description	Activation/deactivation of the IGMP extension auto query port	
Example		

Command	Value range	Default
multicast igmp extension clear-auto-query		
Description	Delete all auto query ports	
Example	multicast igmp extension clear-auto-query	

Command	Value range	Default
multicast igmp extension static-query-port add <port-list>	Comma-separated list of port numbers	
Description	Add static query ports	
Example	multicast igmp extension static-query-port add 2,4	

Command	Value range	Default
mutlicast igmp extension static-query-port remove <port-list>	Comma-separated list of port numbers	
Description	Delete static query ports	
Example	multicast igmp extension static-query-port remove	

Command	Value range	Default
multicast static create <mac-address> <vlan-id>		
Description	Generate a new static multicast group	
Example	multicast static create 01:00:5e:00:18:0e 1	

Command	Value range	Default
multicast static delete <mac-address> <vlan-id>		
Description	Delete an existing static multicast group	
Example	multicast static delete 01:00:5e:00:18:0e 1	

Command	Value range	Default
multicast static configure <mac-address> <vlanid> static-mem-ports <port-list>	<port-list> Comma-separated list of port numbers	
Description	Add ports to a static multicast group	
Example	multicast static configure 01:00:5e:00:18:0e 1 static-mem-ports 3,5,8	

Command	Value range	Default
multicast static configure <mac-address> <vlanid> forbidden-mem-ports <port-list>	<port-list> Comma-separated list of port numbers	
Description	Forbid membership of ports in a static multicast group	
Example	multicast static configure 01:00:5e:00:18:0e 1 forbidden-mem-ports 3,5,8	

Command	Value range	Default
multicast static configure <mac-address> <vlanid> no-member <port-list>	<port-list> Comma-separated list of port numbers	
Description	Delete ports from a static multicast group	
Example	multicast static configure 01:00:5e:00:18:0e 1 no-member 3,5,8	

RSTP Commands

Command	Value range	Default
show spanning-tree global		
Description	Display the RSTP information: Status RSTP Mode Status Large Tree Support Status Fast Ring Detection Bridge Priority Bridge Hello Time Bridge Forward Delay Bridge Max Age MAC address of the root Root Port Root Cost Number of topology changes Last topology change Hello Time Forward Delay Max Age	
Example	show spanning-tree global	

Command	Value range	Default
show spanning-tree port port-no <port-no>		
Description	Display the RSTP information for a specific port: Status RSTP Mode Admin Path Cost Operating Path Cost Status Auto Edge Status Admin Edge Status Operating Edge Priority Number of forward transitions MAC address of the root MAC address of the bridge Port ID Cost	
Example	show spanning-tree port port-no 10	

Command	Value range	Default
show spanning-tree port all		
Description	Tabular display of the RSTP information for a specific port with the following columns: Port number Status RSTP Mode Path Cost Operating Edge Blocking State Protocol Role	
Example	show spanning-tree port all	

Command	Value range	Default
spanning-tree status {disable | 802.1w}		802.1w
Description	Activation/deactivation of RSTP	
Example	spanning-tree status 802.1w	

Command	Value range	Default
spanning-tree lts {enable | disable}		disable
Description	Activation/deactivation of Large Tree Support	
Example	spanning-tree lts enable	

Command	Value range	Default
spanning-tree frd {enable | disable}		disable
Description	Activation/deactivation of Fast Ring Detection	
Example	spanning-tree frd enable	

SmartE Series

Command	Value range	Default
spanning-tree bdg-prio <value>	(0 - 61440 in increments of 4096)	32768
Description	Change the Bridge Priority	
Example	spanning-tree bdg-prio 4096	

Command	Value range	Default
spanning-tree hello-time <value>	Hello time in seconds (1 - 10)	2
Description	Change the Bridge Hello Time	
Example	spanning-tree hello-time 3	

Command	Value range	Default
spanning-tree fwd-delay <value>	Bridge Forward Delay in seconds (4 - 30)	15
Description	Change the Bridge Forward Delay	
Example	spanning-tree fwd-delay 20	

Command	Value range	Default
spanning-tree max-age <value>	Bridge Max Age in seconds (6 - 40)	20
Description	Change the Bridge Max Age	
Example	spanning-tree max-age 25	

Command	Value range	Default
spanning-tree port <port-no> status {enable | disable}		all enable
Description	Activation/deactivation of RSTP for a specific port	
Example	spanning-tree port 3 status disable	

Command	Value range	Default
spanning-tree port <port-no> path-ost <value>	Path cost (0 = automatic detection based on the current port speed; 1 - 200000000 = manual setting)	0
Description	Change the path cost for a specific port	
Example	spanning-tree port 3 path-cost 20000	

Command	Value range	Default
spanning-tree port <port-no> auto-edge {enable | disable}		all enable
Description	Activation/deactivation of Auto Edge for a specific port	
Example	spanning-tree port 3 auto-edge enable	

Command		Value range	Default
spanning-tree port <port-no> admin-edge {edge | non-edge}			all non-edge
Description	Activation/deactivation of Admin Edge for a specific port		
Example	spanning-tree port 3 admin-edge non-edge		

Command		Value range	Default
spanning-tree port <port-no> priority <value>		Priority (0 - 240 in increments of 16)	128
Description	Change the priority for a specific port		
Example	spanning-tree port 3 priority 192		

Command		Value range	Default
spanning-tree port <port-no> force-rstp			
Description	Force change from STP to RSTP for a specific port		
Example	spanning-tree port 3 force-rstp		

MRP Commands

Command		Value range	Default
show mrp			
Description	Display the MRP information: Domain name MRP UUID MRP device status Status of MRP manager function MRP VLAN ID Ring port 1 Ring port 2 MRP manager priority level Ring status Counter for status change in the ring Last status change in the ring		
Example	show mrp		

Command		Value range	Default
mrp mode {none | client | manager}			
Description	Change the MRP device status		
Example	mrp mode client		

SmartE Series

Command	**Value range**	**Default**
mrp ports <mrp-port1> <mrp-port2>	<mrp-port1> Port number for MRP port 1 <mrp-port2> Port number for MRP port 2	<mrp-port1> = 1 <mrp-port2> = 2
Description	Change the MRP ports	
Example	mrp ports 3 4	

Command	**Value range**	**Default**
mrp vlan <vlan-id>	VLAN ID (1 - 4000)	<vlan-id> = 1
Description	Change the MRP VLAN ID	
Example	mrp vlan 2	

Command	**Value range**	**Default**
mrp uuid <UUID-string>	<UUID-string> MRP UUID (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)	<UUID-string> = ffffffff-ffff-ffff-ffff-ffffffffffff
Description	Change the MRP UUID	
Example	mrp uuid ffffffff-ffff-ffff-ffff-ffffffffffff	

Command	**Value range**	**Default**
mrp domain-name <string>	<string> MRP domain name (max. 256 chars)	
Description	Change the MRP domain name	
Example	mrp domain-name mrpdomain2	

Command	**Value range**	**Default**
mrp manager-priority <value>	<value> MRP manager priority (0 - 61439 in increments of 4096)	<value> = 32768
Description	Change the MRP manager priority	
Example	mrp manager-priority 4096	

Port Channel Commands

Command	**Value range**	**Default**
show port-channel trunk-id <name>		
Description	Displays the trunk ID, trunk name, admin mode, spanning tree mode, algorithm and associated ports for the selected trunk.	
Example	show port-channel trunk-id Redtrunk1	

Command	**Value range**	**Default**
show port-channel all		
Description	Shows all trunks in a table with trunk ID, trunk name, admin mode and status.	
Example	show port-channel all	

Command	Value range	Default
port-channel create <name>		
Description	Create a trunk with the configured name.	
Example	port-channel create Portch1	

Command	Value range	Default
port-channel delete <name>		
Description	Delete a trunk with the configured name.	
Example	port-channel delete Portch1	

Command	Value range	Default
port-channel config <name> admin-mode {enable | disable}		
Description	Configuration of the port channel admin mode.	
Example	port-channel config PortCh1 admin-mode enable	

Command	Value range	Default
port-channel config <name> spann-tree {enable | disable}		
Description	Configuration of the Port Channel Spanning Tree mode.	
Example	port-channel config PortCh1 spann-tree enable	

Command	Value range	Default
port-channel config <name> chg-name <name>		
Description	Change a port channel name	
Example	port-channel config PortCh1 chg-name PortCh2	

Command	Value range	Default
port-channel config <name> member-port add <port-list>		
Description	Add member ports to the port channel. Ports are listed in a comma separated list.	
Example	port-channel config PortCh2 member-port add 1,2,8	

Command	Value range	Default
port-channel config <name> member-port del <port-list>		
Description	Delete member ports from the port channel. Ports are listed in a comma separated list.	
Example	port-channel config PortCh2 member-port del 1,2	

Command	Value range	Default
port-channel config <name> trunk-mode mode {LIST-OF-MODES}	Static, lacp-active and lacp-passive	lacp-active
Description	Configuration of the port selection for the selected port channel. Static, lacp-active and lacp-passive are supported.	
Example	port-channel config PortCh2 trunk-mode mode static	

Command	Value range	Default
port-channel global-algorithm algorithm {LIST-OF-ALGORITHMS}	Src MAC, Dst MAC, Src and Dst MAC, Src/Dst IP and TCP/UDP port, Src/Dst MAC, IP and TCP/UDP port	Src/Dst MAC, IP and TCP/UDP port
Description	Configuration of the load balancing algorithm for all port channels of the device.	
Example	port-channel global-algorithm algorithm Src and Dst MAC	

Security Context Commands

Command	Value range	Default
show sec-context		
Description	Display the security context status	
Example	show sec-context	

Command	Value range	Default
sec-context generate		
Description	Generate a security context	
Example	sec-context generate	

Command	Value range	Default
file-transfer {tftp | http} {write-to-device | read-from-device} sec-context <ip-ad-dress> <filename>	(xxx.xxx.xxx.xxx)	
Description	Transfer of a root CA certificate file to the device or from the device to the PC.	
Example	file-transfer tftp write-to-device sec-context 192.168.0.1 cacert.cer	

DHCP Commands

Command	Value range	Default
show dhcp global		
Description	Display the global DHCP status	
Example	show dhcp global	

Command	Value range	Default
show dhcp server current-lease		
Description	Tabular display of the current DHCP leases (assigned IP addresses): Number Assigned IP address MAC address of the device Local port Status	
Example	show dhcp server current-lease	

Command	Value range	Default
show dhcp server static-lease		
Description	Tabular display of the current static DHCP leases (assigned IP addresses): Number Assigned IP address MAC address of the device	
Example	show dhcp server static-lease	

Command	Value range	Default
show dhcp server port-local <port-no>		
Description	Display the port-based DHCP server information: Port Status of the port-based DHCP server IP address Subnet mask Default gateway DNS server	
Example	show dhcp server port-local 3	

Command	Value range	Default
dhcp-service service {none | relay-agent | server}		
Description	Set the operating mode of the DHCP server	
Example	dhcp-service service server	

Command	Value range	Default
dhcp-service relay-agent remote-id {ip | mac}		ip
Description	Change the relay agent remote ID	
Example	dhcp-service relay-agent remote-id mac	

Command	Value range	Default
dhcp-service relay-agent server <ip-address>		0.0.0.0
Description	Change the DHCP server in relay agent mode	
Example	dhcp-service relay-agent server 192.168.0.2	

Command	Value range	Default
dhcp-service relay-agent port-mode enable <port-list>	Comma-separated list of port numbers	
Description	Activation of the relay agent on multiple ports	
Example	dhcp-service relay-agent port-mode enable 3,4,8	

Command	Value range	Default
dhcp-service relay-agent port-mode disable <port-list>	Comma-separated list of port numbers	
Description	Deactivation of the relay agent on multiple ports	
Example	dhcp-service relay-agent port-mode disable 3,4,8	

Command	Value range	Default
dhcp-service server pool-start-addr <ip-ddress>		0.0.0.0
Description	Change the start address of the DHCP pool	
Example	dhcp-service server pool-start-addr 192.168.0.3	

Command	Value range	Default
dhcp-service server pool-size <size>	DHCP pool size (depends on subnet)	32
Description	Change the maximum number of IP addresses specified by the DHCP server (size of the address pool)	
Example	dhcp-service server pool-size 20	

Command	Value range	Default
dhcp-service server net-mask <net-mask>		0.0.0.0
Description	Change the subnet mask that is assigned to the DHCP clients	
Example	dhcp-service server net-mask 255.255.255.0	

Command	Value range	Default
dhcp-service server router-ip <ip-address>		0.0.0.0
Description	Change the default gateway that is assigned to the DHCP clients	
Example	dhcp-service server router-ip 192.168.0.1	

Command	Value range	Default
dhcp-service server dns-ip <ip-address>		0.0.0.0
Description	Change the DNS server that is assigned to the DHCP clients	
Example	dhcp-service server dns-ip 192.168.10.10	

Command	Value range	Default
dhcp-service server lease-time <value>	DHCP lease time in seconds (300 - 2592000)	3600
Description	Change the DHCP lease time (validity of the IP address assignment)	
Example	dhcp-service server lease-time 3600	

Command	Value range	Default
dhcp-service server accept-bootp {enable | disable}		enable
Description	Activation/deactivation of the acceptance of BootP requests by the DHCP server	
Example	dhcp-service server accept-bootp enable	

Command	Value range	Default
dhcp-service server static-lease create <ip-address> <client-mac-address>		
Description	Create a static IP assignment (DHCP lease) for a defined client address (MAC address)	
Example	dhcp-service server static-lease create 192.168.0.20 XX:XX:XX:6C:D2:05	

Command	Value range	Default
dhcp-service server static-lease delete <ip-address>		
Description	Delete a statically assigned IP address (DHCP lease)	
Example	dhcp-service server static-lease delete 192.168.0.20	

Command	Value range	Default
dhcp-service server static-lease clear		
Description	Delete all static IP assignments (DHCP lease)	
Example	dhcp-service server static-lease clear	

Command	Value range	Default
dhcp-service server port-local <port-no> status {enable | disable}		all disable
Description	Activation/deactivation of a port-based DHCP server	
Example	dhcp-service server port-local 3 status enable	

Command	Value range	Default
dhcp-service server port-local <port-no> local-ip <ip-address>		0.0.0.0
Description	Change an IP address assigned by a port-based DHCP server	
Example	dhcp-service server port-local 3 local-ip 192.168.0.30	

Command	Value range	Default
dhcp-service server port-local <port-no> net-mask <net-mask>		0.0.0.0
Description	Change a subnet mask assigned by a port-based DHCP server	
Example	dhcp-service sercer port-local 3 net-mask 255.255.255.0	

Command	Value range	Default
dhcp-service server port-local <port-no> router-ip <ip-address>		0.0.0.0
Description	Change a default gateway address assigned by a port-based DHCP server	
Example	dhcp-service server port-local 3 router-ip 192.168.0.1	

Command	Value range	Default
dhcp-service server port-local <port-no> dns-ip <ip-address>		0.0.0.0
Description	Change a DNS server address assigned by a port-based DHCP server	
Example	dhcp-service server port-local 3 dns-ip 192.168.10.10	

Command	Value range	Default
dhcp-service server port-local-clear		
Description	Delete all port-based DHCP servers	
Example	dhcp-service server port-local-clear	

Alarm Output Commands

Command	Value range	Default
show alarm-output <output-no>	Alarm contact number	
Description	Display the alarm contact information: Alarm contact status Alarm contact output status (error state) Event status power supply interrupted Event status link down	
Example	show alarm-output 1	

Command	Value range	Default
alarm-output <output-no> global {enable | disable}		enable
Description	Change alarm contact status	
Example	alarm-output 1 global enable	

Command	Value range	Default
alarm-output <output-no> pow-supply-lost enable | disable}		enable
Description	Change event status power supply interrupted	
Example	alarm-output 1 pow-supply-lost enable	

Command	Value range	Default
alarm-output <output-no> link-down {enable | disable}		disable
Description	Change event status link down	
Example	alarm-output 1 link-down enable	

Command	Value range	Default
alarm-output <output-no> mrp {enable | disable}		disable
Description	Change event status MRP ring error	
Example	alarm-output 1 mrp enable	

Command	Value range	Default
alarm-output <output-no> plug-mem-miss {enable | disable}		disable
Description	Change event status configuration memory missing	
Example	alarm-output 1 plug-mem-miss enable	

QoS Commands

Command	Value range	Default
show broadcast-limiter		
Description	Display the broadcast limiter information: Status of the broadcast limiter Broadcast threshold value Status of the multicast limiter Multicast threshold value Status of the unknown unicast limiter Unknown unicast threshold value	
Example	show broadcast-limiter	

Command	Value range	Default
show quality-of-service profile		
Description	Shows the Quality of Service information.	
Example	show quality-of-service profile	

Command	Value range	Default
quality-of-service profile {universal | ethernet-ip}		universal
Description	Set predifined priority mapping and queue usage for certain traffic class.	
Example	quality-of-service profile universal	

Command	Value range	Default
broadcast-limiter broadcast status {enable | disable}		disable
Description	Change the broadcast limiter status	
Example	broadcast-limiter broadcast status enable	

Command	Value range	Default
broadcast-limiter broadcast threshold <value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024
Description	Change the broadcast limiter threshold	
Example	broadcast-limiter broadcast threshold 2048	

Command	Value range	Default
broadcast-limiter multicast status {enable | disable}		disable
Description	Change the multicast limiter status	
Example	broadcast-limiter multicast status enable	

Command	Value range	Default
broadcast-limiter multicast threshold <value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024
Description	Change the multicast limiter threshold	
Example	broadcast-limiter multicast threshold 2048	

Command	Value range	Default
broadcast-limiter unicast status {enable | disable}		disable
Description	Change the unknown unicast limiter status	
Example	broadcast-limiter unicast status enable	

Command	Value range	Default
broadcast-limiter unicast threshold <value>	Threshold value in frames per second (0 - 1048576 in increments of 1024)	1024
Description	Change the broadcast limiter threshold	
Example	broadcast-limiter unicast threshold 2048	

Trap Manager Commands

Command	Value range	Default
show snmp-trap		
Description	Tabular display of the SNMP trap states with the following columns: Trap Name Status	
Example	show snmp-trap	

Command	Value range	Default
snmp-trap status {enable | disable}		disable
Description	Change the global SNMP status	
Example	snmp-trap status enable	

Command	Value range	Default
snmp-trap server add <ip-address>		
Description	Add an SNMP trap server	
Example	snmp-trap server add 192.168.0.50	

Command	Value range	Default
snmp-trap server remove <ip-address>		
Description	Delete an SNMP trap server	
Example	snmp-trap server remove 192.168.0.50	

Command	Value range	Default
snmp-trap trap <trap> {enable | disable}	Traps separated by comma: user-config-chg - User config change event-tbl-oflow - Event Table Overflow crc-peak-increase - CRC proportion peak increased crc-status-critical - CRC status change to critical crc-status-warning - CRC status change to warning crc-status-ok - CRC status change to ok mrp - Set MRP ring change ip-conflict - Set IP conflict presisted dlr-ring-chg - DLR ring change fw-status-chg - firmware status changed port-sec-violation - Port security violation link-up - Link Up link-down - Link Down rstp-top-chg - RSTP Topology Change rstp-new-root - RSTP New Root rstp-link-fail - RSTP Link Failure pow-src-chg - Power source changed fw-config - Firmware configuration auth-fail - Authentication failure user-pwd-chg - User password changed config-diff - Configuration differ warm-start - Warm start cold-start - Cold start	all enable
Description	Change the SNMP trap states	
Example	snmp-trap trap link-up,auth-fail,warm-start enable	

Command	Value range	Default
snmp-trap send-test-trap		
Description	Send a test trap	
Example	snmp-trap send-test-trap	

Contact Information

EtherWAN System, Inc.
www.etherwan.com

USA Office

2301 E. Winston Road
Anaheim, CA 9280
Tel: +1-714-779-3800
Email: info@etherwan.com

Pacific Rim Office

8F., No.2, Alley 6, Lane 235, Baoqiao Rd.
Xindian District, New Taipei City 231
Taiwan
Tel: +886 -2- 6629-8986
Email: info@etherwan.com.tw

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

SmartE Series
March 27, 2023