WyreStorm

NHD-128-NDI-TRX
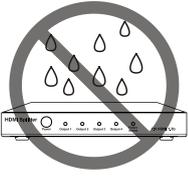
NDI to NetworkHD Transceiver
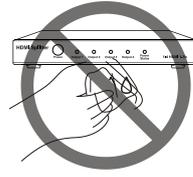
Important Safety Instructions

1. Do not expose this apparatus to rain, moisture, dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the apparatus.
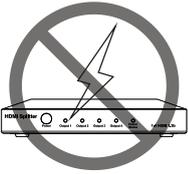
2. Do not install or place this unit in a bookcase, built-in cabinet or in another confined space. Ensure the unit is well ventilated.

3. To prevent risk of electric shock or fire hazard due to overheating, do not obstruct the unit's ventilation openings with newspapers, tablecloths, curtains, and similar items.

4. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.

5. Do not place sources of naked flames, such as lighted candles, on the unit.

6. Clean this apparatus only with dry cloth.

7. Unplug this apparatus during lightning storms or when unused for long periods of time.
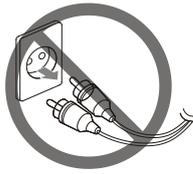
8. Protect the power cord from being walked on or pinched particularly at plugs.

9. Only use attachments / accessories specified by the manufacturer.

10. Refer all servicing to qualified service personnel.

Table of Contents

Introduction

Overview

The NDI-NHD transceiver is a flexible solution designed to bridge NDI sources and receivers with NHD encoders and decoders. It features a modular system with up to eight independent virtual modules for receiving NDI streams, as well as one virtual module for receiving an NHD stream, each with a unique IP address and MAC address. The transceiver can convert NDI streams to NHD and NHD streams to NDI, enabling seamless distribution across the network. This dual functionality allows smooth integration of both legacy and modern video systems, ensuring interoperability between NDI and NHD workflows and compatibility with the existing NHD systems.

Features

Modular System
- Provides up to eight modules for receiving NDI streams and one virtual module for receiving an NHD stream, each with a unique IP address and MAC address, each NDI module providing a stream preview.
- Intuitive management via Web UI, enabling precise configuration and routing of NDI and IP streams.

NDI/NHD Source Selection and Routing
- Allows each virtual module to independently select an NDI/NHD stream from the network.

Protocol Conversion
- Converts selected NDI streams into NHD video for compatibility with NHD decoders.
- Converts a selected NHD video stream into an NDI stream for distribution to NDI receivers, allowing IP-based content to be displayed on NDI platforms (Teams, NDI tool, etc.).

Seamless Integration
- Ensures smooth interoperability between NDI and NHD streams, guaranteeing seamless communication across different video systems.

PoE Support

Package Contents

1x NHD-128-NDI-TRX Gateway
4x Wall Mounting Ears (Plastic)
2x Rack Mounting Ears for NHD-000-RACK4 (Vertical Installation)
1x Quickstart Guide

Specifications

Audio and Video	
Video Input Port	**LAN:** 1x RJ-45 Female Connector
Video Input Type	**NHD:** H.264/H.265, RTP/UDP, Multicast **NDI:** NDI HX (NDI 6), RUDP/TCP, Multicast
Input Resolutions	**NHD:** Up to 4K@30Hz **NDI Main Stream:** Up to 4K@30Hz **Preview Stream:** Up to 480P@60Hz
Input Bitrate	**NHD:** Up to 16Mpbs **NDI Main Stream:** Up to 16Mpbs **Preview Stream:** Up to 1Mbps
Video Output	**LAN:** 1x RJ-45 Female Connector
Video Output Type	**NHD:** H.264/H.265, RTP/UDP, Multicast **NDI Main Stream:** NDI HX (NDI 6), RUDP/TCP, Multicast **Preview Stream:** MJPEG, HTTP
Output Resolutions	**NHD:** Up to 4K@30Hz **NDI Main Stream:** Up to 4K@30Hz **Preview Stream:** CIF (360 x 240) @30Hz
Output Encoding Rate	**NHD:** Up to 16Mpbs **NDI Main Stream:** Up to 20Mpbs **Preview Stream:** Up to 512Kbps
Control Method	Front panel LED screen Rear panel RESET button LAN-based control (Web UI and NHD-CTL-PRO controller)
Power	
Power	12V DC 1A, PoE
ESD Protection	Human body model: ±12kV (air-gap discharge) / ±8kV (contact discharge)
Environmental	
Operating Temperature	32°F to 113°F (0°C to 45°C), 10% to 90%, non-condensing
Storage Temperature	-4°F to 158°F (-20°C to 70°C), 10% to 90%, non-condensing

Dimensions and Weight	
Width x Height x Depth	6.89" x 0.98" x 3.94" (175mm x 25mm x 100.2mm)
Net Weight	1.14lbs (0.52kg)
Regulatory	
Safety and Emission	CE	FCC	RoHS	RCM	EAC	UKCA

Panel Description
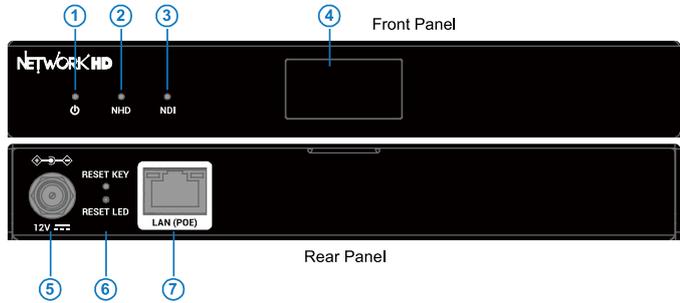
#	Name	Description
1	**Power LED**	**On:** The device is powered on. **Off:** The device is powered off.
2	**NHD LED**	**On:** The device is receiving video streams from an NHD series transmitter. **Blinking Slowly:** The device is connected to the system but doesn't receive any NHD video streams. **Blinking Quickly:** "Find Me" mode is activated.
3	**NDI LED**	**On:** The device is receiving video streams from NDI video source(s). **Blinking Slowly:** The device is connected to the system but doesn't receive any NDI video streams. **Blinking Quickly:** "Find Me" mode is activated.
4	**LED Screen**	Displays the device's IP address and firmware version, or logo. The display content on the screen can be configured through the device's web UI. Example: IP Address: 169.254.10.169 255.255.0.0 Version: V1.0.06
5	**12V**	Connect to a 12V DC 1A power adapter (not included).
6	**RESET KEY and LED**	Press and hold the RESET key for at least 5 seconds until the RESET LED lights solid blue, then release the key, the device will be reset to the factory defaults.
7	**LAN (POE)**	Connect to a gigabit Ethernet switch for video streaming, device management and/or power input via PoE. **Note:** Default IP addressing mode of the device is DHCP.

Installation

Note: Before installation, please ensure the device is disconnected from the power source.

To mount the device on a suitable location:

1. Attach the two wall mount brackets to one side of the device using the screws provided in the package as illustrated below.
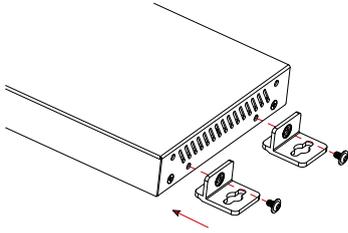
2. Repeat step 1 for the opposite side of the device.
3. Mount the device onto the desired surface using appropriate screws (not included).

To mount the device on a rack:

1. Attach the rack mount bracket to one side of the unit using the included screws, as illustrated below.
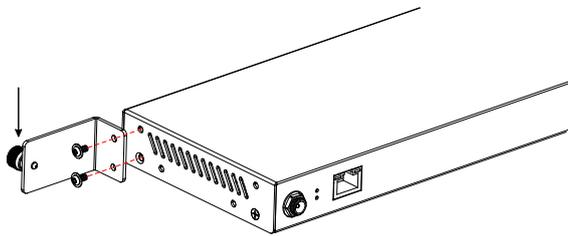
2. Repeat step 1 for the other side of the device.
3. Secure the device to the rack by rotating the spring-loaded captive screw clockwise on the rack bracket until fully locked.

Typical Application
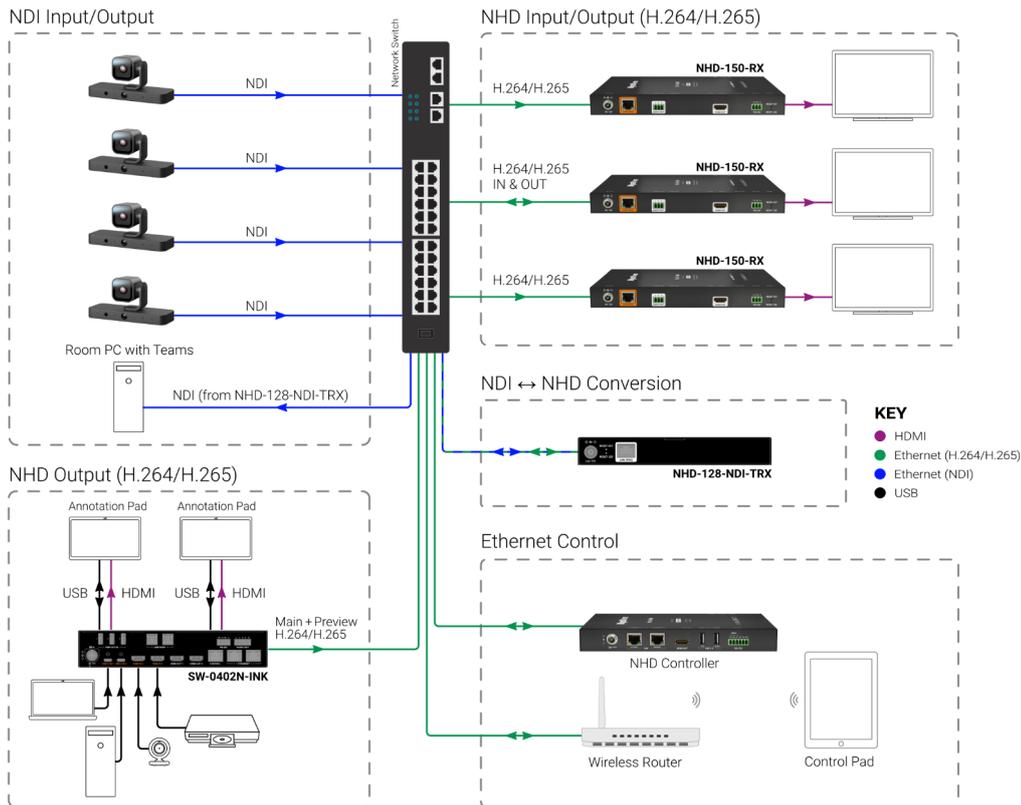
Notes: The NHD-128-NDI can receive up to eight NDI streams and convert them into NHD streams. It can also convert IP-based video streams (from NHD encoders) into NDI streams. In addition to decoding, the NHD-150-RX supports encoding and delivering the NHD stream in multi-view to the network.

Configuring the Web UI

The web UI is an intuitive software interface that enables users to easily manage and control the device via a browser. It is recommended to use Chrome, Safari, Microsoft Edge or Firefox browser for the best experience.

Accessing the Web UI

By default, the IP addressing mode for the device is DHCP.

To access the Web UI of the device:

1. Connect the LAN port of the device to a local area network equipped with a DHCP server. This allows the device to acquire a valid IP address.

2. Connect your PC to the same network as the device.

3. Check the device's IP address through the OLED screen on the front panel.

4. Input the device's IP address in the browser and press Enter. The Login page appears.
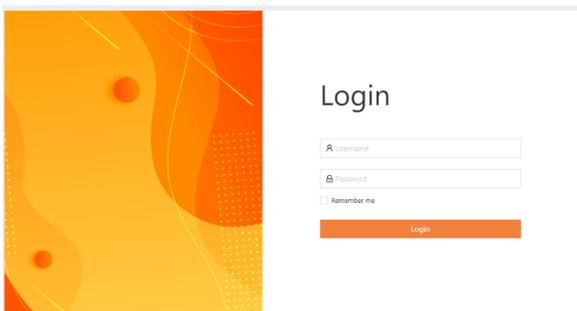
5. Input the login name and password, then press Enter. The login name and default password are both set to admin. Upon the first login, you will be prompted to change the password. Enter a new one and click Apply to complete the update.

    Note: The new password must contain at least one uppercase letter, one lowercase letter, one number and one special character, and be 8 to 16 characters long.
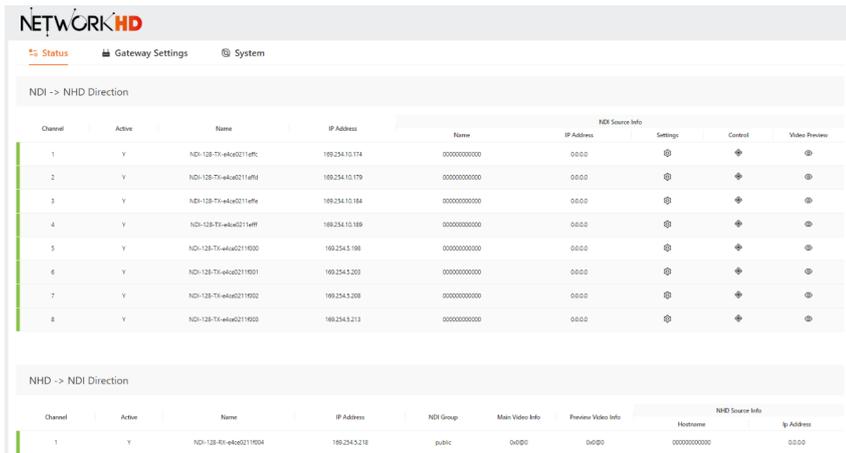

6. The main page opens. Click a tab on the top navigation pane to enter the corresponding page.

The web interface includes three tabs:
*   **Status:** Displays the status of the device.
*   **Gateway Settings:** Allows you to configure NDI and IP stream routing.
*   **System:** Provides options for configuring IP settings, web services, security, login password, LED screen's display content, as well as performing firmware upgrades and system settings.

The device supports two signal conversion pathways:
*   NDI streams to NHD (H.264/H.265) streams
*   NHD (H.264/H.265) streams to NDI streams

Follow the instructions below to configure each feature based on your system requirements.

Signal Conversion from NDI to NHD

This function allows the transceiver to receive up to eight channels of NDI streams and convert them into NHD streams, making them compatible with NHD decoders and existing H.264/H.265-based systems.

Process Overview

1. **Introduce NDI sources**

    Log on to the web interface of the transceiver, navigate to the Gateway Settings tab, and then go to the NDI-> NHD Direction section. Click the NDI Source Management button to open a window that displays the detected NDI sources.
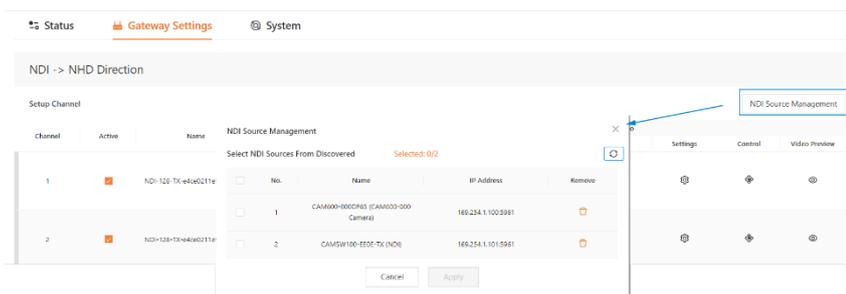
Select the desired NDI source(s) from the device list to make them visible and routable to the transceiver. After selecting the sources, click Apply to save the settings.

2. **Route NDI sources to the NDI receiving channels**

From the Name dropdown menu, select an available NDI source to assign it to an NDI receiving channel. For example, select CAMSW100-EE0E-TX as the source for the NDI-128-TX-e4ce0211effc channel.

Additionally, you can preview the video stream in real time by clicking the Video Preview icon associated with the channel.

3. **Route the channel of the transceiver to an NHD decoder**

The transceiver can be routed to an NHD decoder via the web UI configuration on the NHD controller.

Routing via the NHD controller

Log on to the web interface of the NHD controller, go to the Matrix Status tab, and under the Matrix section, click the corresponding circle button (which will turn from white to solid green) to route the NDI-128-TX-e4ce0211effc channel to an NHD decoder (for example, NHD-120-RX-341B22094004).

After completing these steps, the NDI sources will display on the screen connected to the NHD decoder.

Signal Conversion from NHD to NDI

This function allows the transceiver to convert IP-based video streams (from NHD encoders) into NDI streams, facilitating easy integration and distribution to NDI receivers across the network.

Process Overview

1. **Introduce NHD sources**
   Log on to the web interface of the transceiver, navigate to the Gateway Settings tab, and then go to the NHD -> NDI Direction section. Click the NHD Source Management button to open a window displaying the discovered NHD sources.
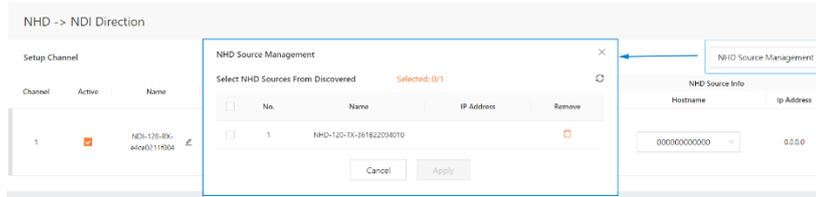
   Select the desired NHD source(s) from the device list to make them visible and routable to the NHD receiving channel of the transceiver, then click Apply to save the settings.
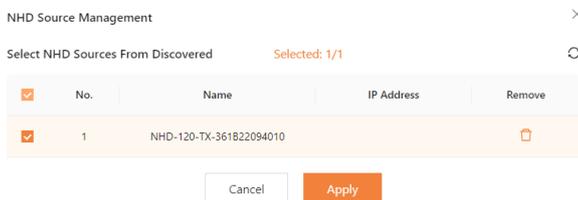

2. **Route the NHD source to the channel.**
   From the Name dropdown menu, select the available NHD source to assign to the channel. For example, route the NHD-120-TX-361B22094010 to the channel.

3. Route the channel of the transceiver to an NDI receiver (such as NDI Tool) through the receiver's specific configuration. Once the configuration is complete, the NDI receiver will output the NHDsource to the connected display.

# Viewing NDI and NHD Setting Details
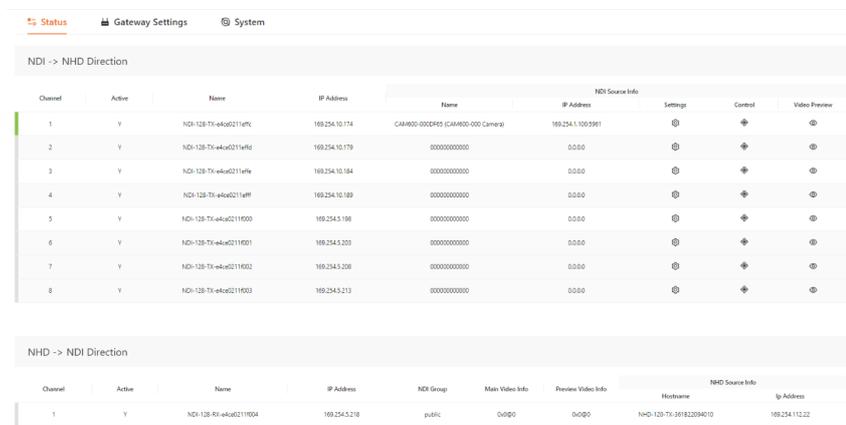
The Status tab provides status of NDI-to-NHD and NHD-to-NDI routing, including the information of NDI sources, NDI receiving channels, NHD sources, and NHD receiving channel, as well as the NDI source preview.

System Settings

The System tab allows you to configure IP address settings, manage services, adjust security settings, change the login password and modify the content displayed on the LED screen. You can also perform firmware updates, reset or reboot the device, and export system in this tab.

IP Address Settings
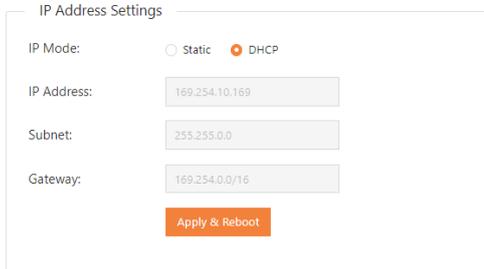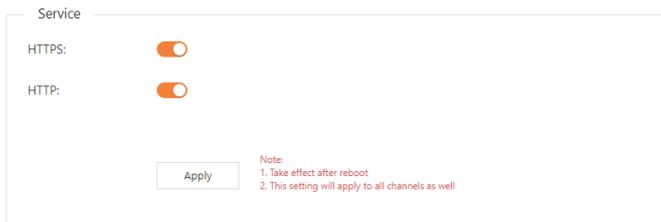

This section allows you to configure either a static IP address or DHCP for the device.

By default, the device operates in DHCP mode. If it fails to acquire a valid IP address due to the absence of a DHCP server, it will automatically assign itself an IP itself in the range of 169.264.x.x with a subnet mask of 255.255.0.0.

• Apply & Reboot: Click to apply the settings and reboot the device.
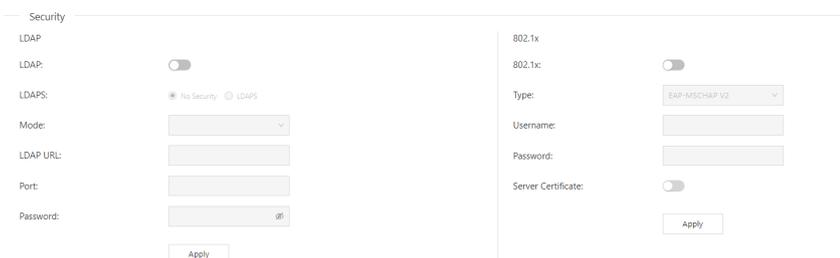
Service Settings

This section allows you to configure the web protocol settings for the device.

• **HTTPS:** To toggle HTTPS (HyperText Transfer Protocol Secure) on or off. HTTPS ensures a secure communication channel, encrypting data transmitted between the device and the user's browser.
Default setting: On

• **HTTP.** To toggle HTTP (HyperText Transfer Protocol) on or off.
HTTP is a standard, unsecured protocol for data transfer. Disabling HTTP and enabling only HTTPS enhances security.
Default setting: On

• **Apply:** To apply settings.
Note: The setting will take effect after the device reboots.
The settings will be applied to both the eight NDI receiving channels and the one NHD receiving channel.

Security Considerations

• By default, HTTPS is enabled to provide secure communication between the device and user browsers, ensuring that sensitive data is transmitted in an encrypted format.

• While HTTP can be enabled for compatibility reasons, it does not encrypt the data being transferred, which may expose the device to security risks.

• For enhanced security, it is recommended to disable HTTP and enables HTTPS only. This ensures that all communications are encrypted and helps prevent unauthorized access and data interception during transmission.

Security

This section allows you to configure the security protocol settings for the device.

LDAP

- **LDAP:** To toggle LDAP service on or off for the device.
  When enabled, the device will authenticate user credentials against the LDAP server upon login attempts. If the credentials match the records in the LDAP directory, access is granted; otherwise, access is denied.

  Example of LDAP application: In an office environment, LDAP is commonly integrated with an Active Directory to control user access to systems such as ticketing systems, email accounts, Wi-Fi, etc.

  Default setting: Off

- **LDAPS:** To select the security level for LDAP communication.

  LDAPS: Requires the user to upload a signed certificate for secure authentication with the LDAP server over SSL/TLS. This ensures encrypted communication between the device and LDAP server.

  No Security: LDAP communication is not encrypted. This means data, including user credentials, is transmitted in plaintext. This setting is typically used in trusted internal networks or for non-sensitive applications.

- **Mode:** To select the authentication mode.

  DN (Distinguished Name): Requires the user to enter both the BIND.
  DN (the distinguished name of a user or service account with sufficient permissions to perform LDAP operations) and Password for authentication.

  UID (User Identifier): Requires the user to enter UID (the unique identifier for the user), BASE DN (the distinguished name indicating the starting point of the search in the LDAP directory), and Password for authentication.

LDAP:	⬤━
LDAPS:	⦿ No Security ○ LDAPS
Mode:	UID ▾
LDAP URL:	
Port:	
UID:	
BASE DN:	
Password:	⌀

Apply

- **LDAP URL:** To enter the LDAP server's URL. This can either be an IP address or a fully qualified domain name (FQDN), along with the appropriate protocol (e.g. ldap://your-ldap-server.com or ldaps://your-ldap-server.com).

- **Port:** To enter the port number for the LDAP server. Common default ports are:
  389 for standard LDAP
  636 for LDAPS (LDAP over SSL)

802.1x

802.1X is a port-based network access control protocol that uses a RADIUS server for authenticating devices connected to the network, ensuring that only authenticated devices are granted access. It provides an additional layer of security by enforcing device authentication before allowing network access.

- **802.1x:** To toggle 802.1X authentication service on or off for the device.
  When enabled, the device will authenticate using one of the two supported methods: EAP-MSCHAP V2 or EAP-TLS.
  Default setting: Off

- **Type:** To select between the two available authentication types:

  EAP-MSCHAP V2: Performs authentication based on a username and password. This method is widely supported but offers less security compared to certificate-based methods.

802.1x:	⬤━
Type:	EAP-MSCHAP V2 ▾
Username:	
Password:	

  EAP-TLS: Performs authentication using a client certificate, private key and private key password. The private key is optional but recommended for added security.

  EAP-TLS is more secure as it uses mutual certificate-based authentication, making it more difficult for attackers to impersonate or spoof a device. This method is recommended for high-security environments where device identity needs to be verified thoroughly.

802.1x:	⬤━
Type:	EAP-TLS ▾
Username:	
Client Certificate:	Select the Client Certificate files
Private Key:	Select the Private Key files
Private Key Password:	⌀

- **Server Certificate:** To toggle server certificate authentication on or off for the device.
  When set to On, the RADIUS server verifies the device's identity by using a server certificate. Only upon successful authentication will the device be allowed to access the network. This feature is recommended for environments with high security requirements to ensure that both the client nd server identities are properly authenticated before granting network access.

  Default setting: Off

Admin Password

This section allows you to change the login password for the device.

Default login password is admin.

Note: The new password must contain at least one uppercase letter, one lowercase letter, one number and one special character, and be 8 to 16 characters long.

LED Screen

This section allows you to configure the content shown on the LED screen on the device's front panel.

• **IP & Version:** To display the IP address, subnet mask and firmware version of the device on the LED screen.

• **Logo:** To display the logo on the LED screen.

• **Off:** To turn off the LED screen display function.
Default setting: IP & Version

System Reboot & Reset

This section allows you to reboot or reset the device to its factory default settings.

• **Reboot:** To restart the device without affecting any of its configurations. This is useful for applying certain changes or troubleshooting without losing data.

• Reset to Factory: To restore the device to its original factory settings, erasing all configurations and custom data. This action is irreversible, so ensure that you have backed up any important configurations before proceeding.

Firmware Update

This section allows you to perform a firmware update for the device.

Follow these steps to update the firmware:

1. Click Select the firmware files to choose the firmware file (.bin) from your local PC.

2. Click Upgrade & Reboot to start the update process. The update will take approximately 2 minutes to complete, after which the device will automatically reboot. Refresh the web interface to regain access.

Log Export

Log	
System Log:	Export

This section allows you to download the system logs to your local computer.

To export the logs, simply click the Export button. The logs will be saved to your computer in the .logz format.