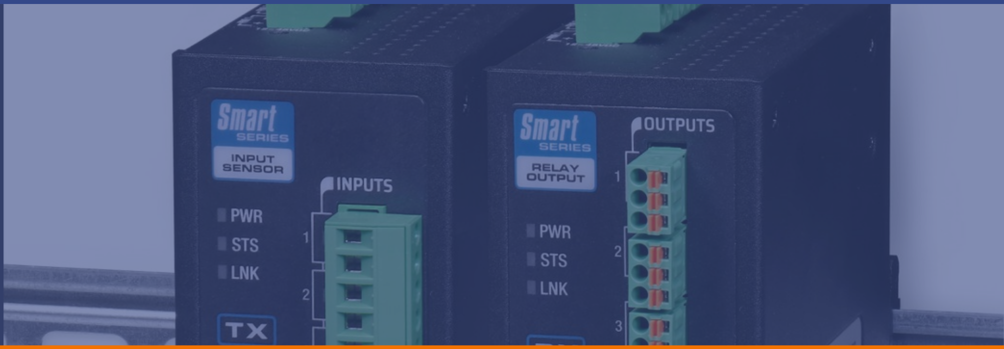
RLH Industries, Inc.



Smart 8 Input Sensor
Smart 8 Relay Output

Software Manual

www.fiberopticlink.com

MD-068 2025A-1107

Every effort has been made to ensure that the information in this document is accurate. RLH is not responsible for printing or clerical errors. Because we are constantly seeking ways to improve our products, specifications and information contained in this document are subject to change without notice.

RLH Industries, Inc.
936 North Main Street
Orange,CA 92867
USA

Ph. +1 714 532-1672
email: info@fiberopticlink.com
www.fiberopticlink.com

Contents

System Configuration

Device Access 5

Web Interface

Overview Dashboard 6
Title Bar / Header 7
Navigation Panel 8
I/O Summary Table 9
Event Log Snapshot 10

Configuration Panel

Overview 11
Input [1-8] (Input [n] Configuration) 12
Dependencies, Validation, & Troubleshooting 13
Relay [1-8] (Relay Configuration Window) Overview 14
Relay Configuration Window (SNMPv1) Configuration 16
System Pairing 18
System Pairing (Smart 8 Input Sensor) Configuration 19
System Pairing (Smart 8 Input Sensor) Topologies 20
System Pairing (Smart 8 Relay Output) Configuration 23
System Pairing (Smart 8 Relay Output) Topologies 24

Event Log

Overview 27

Admin Panel

Network Panel **29**
Overview 29
Network Details 30
Network Hostname 31
Network Fiber Port 32
Network Copper Port 33
Network Fiber/Copper Port - IEEE 802.1X Configuration 34
Network Fiber/Copper Port - IEEE 802.1X: EAP-TLS Configuration 35
Network Fiber/Copper Port - IEEE 802.1X: EAP-TTLS Configuration 36
Network (Fiber/Copper Port) IEEE 802.1X: EAP-PEAP Configuration 37
Network (Fiber/Copper Port) IEEE 802.1X: EAP-MD5 Configuration 38
Web (HTTP/HTTPS) Configuration **39**
Web (Access Method) Configuration 40
Web (Local User) Accounts Configuration 41
Web (Radius Centralized) RADIUS Server Client Configuration 42
Web (Date & Time) System Clock Configuration 43
Web (Email Notifications) SMTP Server Configuration 44
Web (Email Notifications) SMTP Server Configuration 45
MQTT (Navigation Panel) Overview 46

Contents

MQTT (Broker) Configuration 47
[Admin] MQTT (Broker) - MQTT over TLS (MQTTS) Broker Configuration 48
MQTT (Publisher) Configuration 49
MQTT (Publisher) Configuration 50
MQTT (Publisher) Publish Message Format Configuration 51
MQTT (Subscriber) Overview 52
MQTT (Subscriber) Configuration 53
MQTT (Publisher/Subscriber) Debug Messages Overview 54
MQTT (Publisher/Subscriber) MQTTS Configuration 55
Modbus TCP Slave Overview 56
Modbus TCP Slave Configuration 57
DNP TCP (DNP3 Outstation) Overview: Smart 8 Relay Output 58
DNP TCP (DNPv3 Outstation) Smart 8 Relay Output Configuration 59
DNP3/TCP Object Implementation Table - Smart 8 Input Sensor 60
DNP TCP - DNP3 Outstation Configuration: Smart 8 Relay Output 61
MQTT (DNP TCP) DNPv3 Outstation Configuration: Smart 8 Relay Output 62

DNP3/TCP Object Implementation Table - Smart 8 Relay Output 63

SNMP (Navigation Panel) Overview 65

SNMP (SNMP Enable) Configuration 66
SNMP (SNMP View Config) Configuration 67
SNMP (SNMPv1/v2c Config) Configuration 68
SNMP (SNMPv3 User Config) Overview 69
SNMP (SNMPv3 User Config) Configuration 70
SNMP (Trap Notifications) Configuration: SNMPv2c 71
SNMP Traps Configuration: SNMPv3 72
SNMPv1/v2c/v3 Traps Receiver Overview 73
SNMPv1/v2c/v3 Traps Receiver Configuration 74
Certificates - Certs Management 75
Certificates - TLS/SSL Certificate Management Store 76
TLS/SSL Certificate Management Store - Download 77

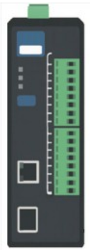
Maintenance (Navigation Panel) Overview 78

Maintenance (Configuration) Management 79
Maintenance (Restart Device) - Restart 80

System Configuration

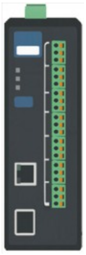
Device Access

The system is accessible by entering its IP address into the URL address bar of your web browser. This login page is not restricted to any particular web browser; it can be accessed successfully for example via Microsoft Edge, Google Chrome, Mozilla Firefox, and others. Listed below are the default IP parameters of each system:



(Smart 8 Input Sensor)

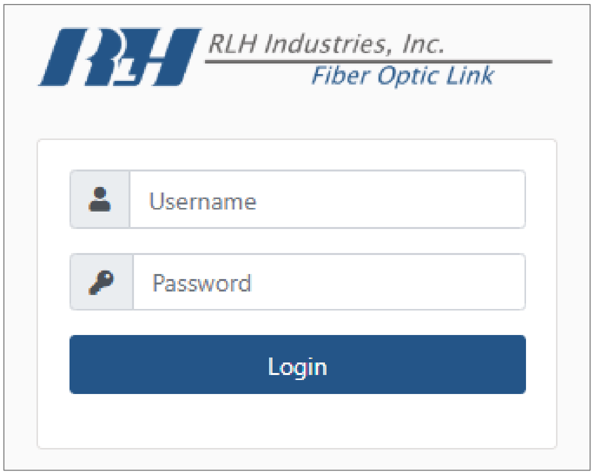
- **IP Address (RJ45)**: 192.168.1.201
- **IP Address (SFP)**: 192.168.2.202
- **Subnet Mask**: 255.255.255.0
- **Username**: admin
- **Password**: admin



(Smart 8 Relay Output)

- **IP Address (RJ45)**: 192.168.1.201
- **IP Address (SFP)**: 192.168.2.202
- **Subnet Mask**: 255.255.255.0
- **Username**: admin
- **Password**: admin

After entering the IP address into the address bar, the login portal should open with the below prompt. Use the default Username and Password listed above, and select the "Login" button to access the system's Overview dashboard.



Web Management Portal Login Prompt

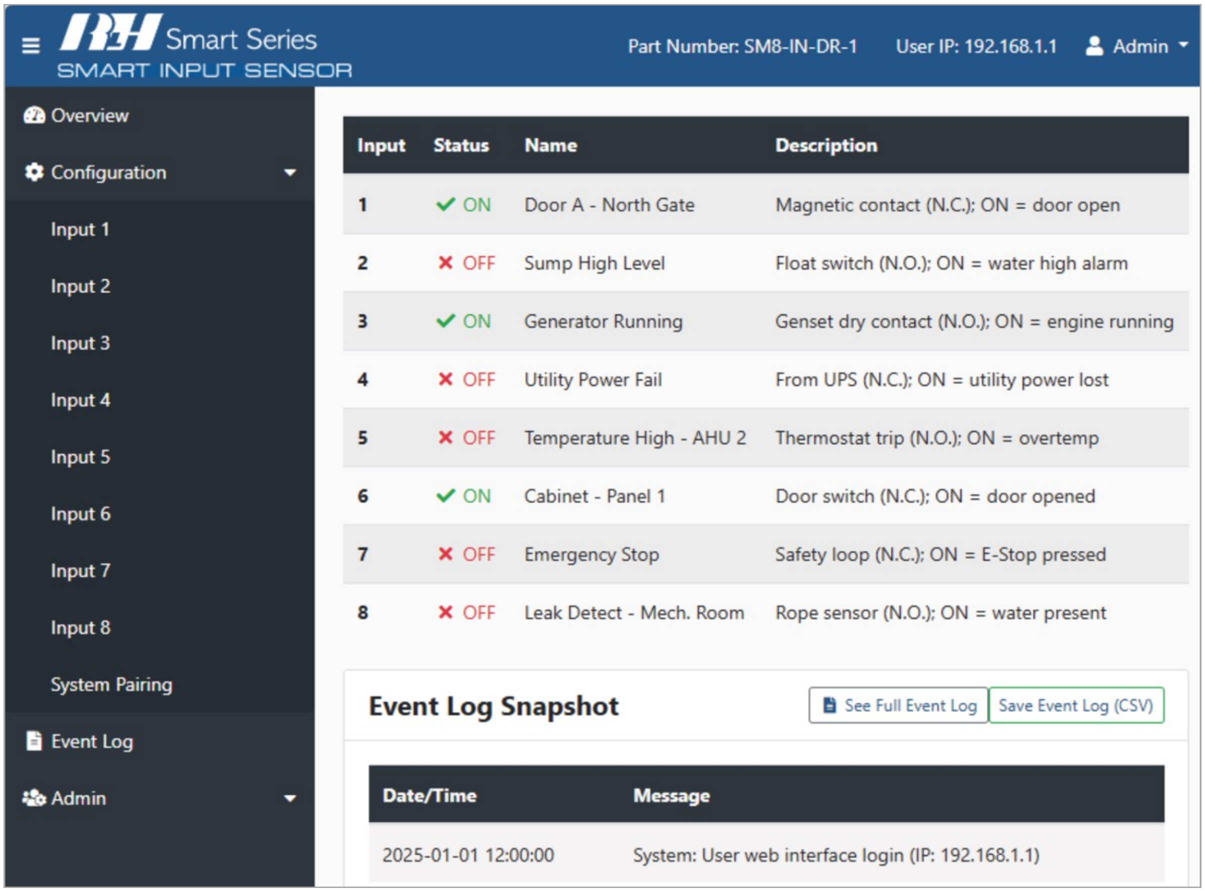
Once the user has logged in, an idle timeout period of 10 minutes will initiate. If no user actions are facilitated (e.g., selecting a feature on the Navigation Panel, saving a configuration change, etc.) within that 10-minute timeout period, the user will be logged out from the system upon initiating any subsequent action in the web interface, returning to the Portal Login displayed above.

Web Interface

Overview Dashboard

Identified by a dashboard icon, the Overview dashboard provides a summary of the system's Digital Input (Smart 8 Input Sensor) or Relay Output (Smart 8 Relay Output) channels, and a rolling snapshot of recent system events. Reference this page directly for quick health checks, verification of I/O state changes, rapid access to the full Event Log, performing system configuration changes, and reviewing hardware/model versions.

Note that the width of the interface is adaptable to the user's screen resolution, and can collapse further via a Navigation Toggle feature. By default, the Configuration Navigation Panel will be open, allowing for instant access to viewing or modifying particular I/O channels and the system's active System Pairing configuration.



Part Number: SM8-IN-DR-1 User IP: 192.168.1.1

Input	Status	Name	Description
1	✓ ON	Door A - North Gate	Magnetic contact (N.C.); ON = door open
2	✗ OFF	Sump High Level	Float switch (N.O.); ON = water high alarm
3	✓ ON	Generator Running	Genset dry contact (N.O.); ON = engine running
4	✗ OFF	Utility Power Fail	From UPS (N.C.); ON = utility power lost
5	✗ OFF	Temperature High - AHU 2	Thermostat trip (N.O.); ON = overtemp
6	✓ ON	Cabinet - Panel 1	Door switch (N.C.); ON = door opened
7	✗ OFF	Emergency Stop	Safety loop (N.C.); ON = E-Stop pressed
8	✗ OFF	Leak Detect - Mech. Room	Rope sensor (N.O.); ON = water present

Event Log Snapshot

Date/Time	Message
2025-01-01 12:00:00	System: User web interface login (IP: 192.168.1.1)

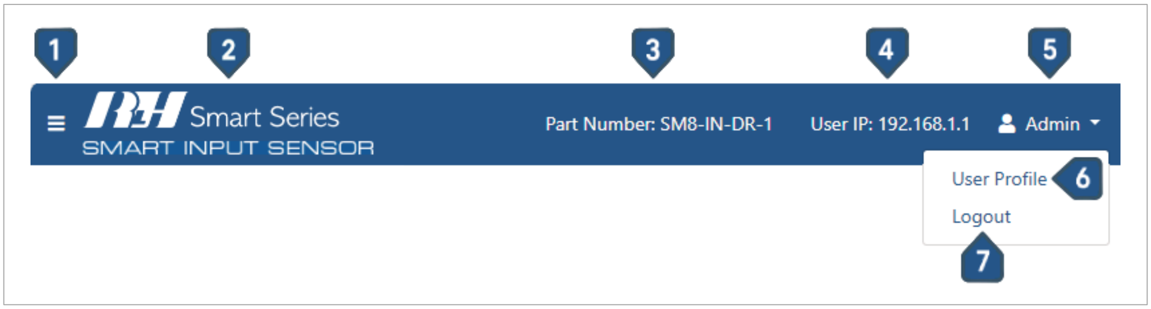
Overview Dashboard (Smart 8 Input Sensor)

Notable differences between the Smart 8 Input Sensor's interface and the Smart 8 Relay Output are that the "Input" column changes to "Output", Configuration->Input [#] changes to Configuration->Output [#], the title header is listed as Smart Relay Output, and the Part Number field will be hard-set to "SM8-OUT-1".

Title Bar / Header

The Header is persistent across the web interface, providing context for the specific unit the user is connected to. It includes the model name and Part Number, the user's client IP (User IP) within the current session, and a User Account menu. At the far left is a Navigation Toggle (≡) for collapsing, or expanding, the left Navigation Panel hosting each feature window.

Use the header to confirm you're on the intended unit before making changes, access profile/sign-out controls, and quickly show or hide the Navigation Panel as needed for maximizing the working area of the page.

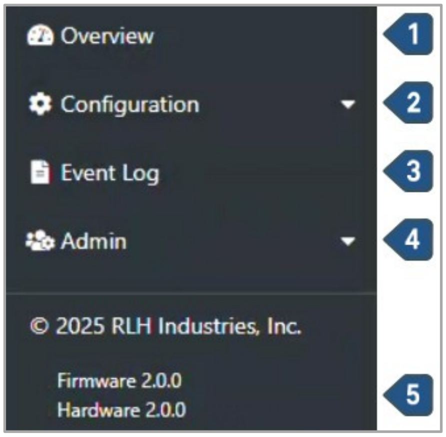


Header Layout

Item	Parameter	Description
1	`Navigation Toggle (≡)`	Identifies the Port Number referenced
2	`Model Name`	Up - The link is active / Down - The link is not active
3	`Part Number`	10/100/1000Mbps
4	`User IP`	Port is operating as Half Duplex
5	`User Account`	Port is operating at full duplex
6	`User Profile`	Displays the number of received bytes
7	`Logout`	Displays the number of transmitted bytes

Navigation Panel

The Navigation Panel is the primary way to move through the system's different features. It groups pages by the following functions: Overview, Configuration, Event Log, and Admin. It can also collapse via the Navigation Toggle (≡) to keep rarely used items out of the way. A footer shows firmware and hardware versions of the running build.



© 2025 RLH Industries, Inc.

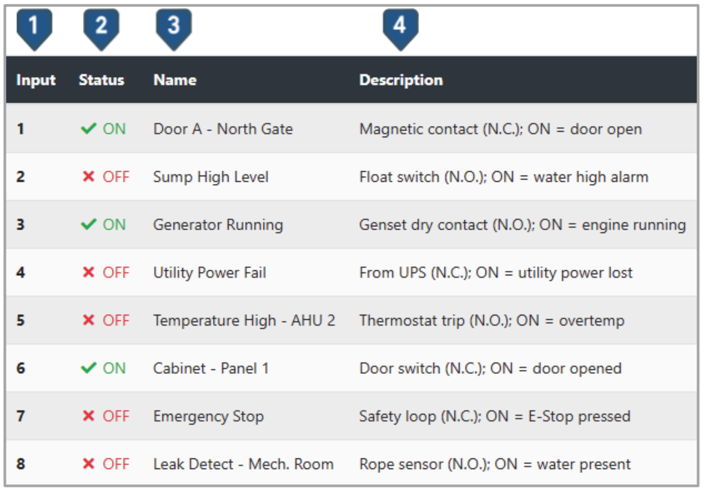
Firmware 2.0.0
Hardware 2.0.0

Navigation Panel

Item	Parameter	Description
1	`Overview`	Opens the Overview Dashboard
2	`Configuration`	Expands the Configuration panel for I/O channel and System Pairing settings
3	`Event Log`	Opens the Event Log window
4	`Admin`	Expands the Admin Panel for system-wide configuration: networking, web access/auth, timekeeping, notifications, protocols, certificates, and maintenance
5	`System Build`	Displays the Firmware/Hardware versions

I/O Summary Table

The I/O Summary Table lists all of the system’s channels and their current status and is the central portion of the Overview Dashboard. It enumerates each Digital Input (Smart 8 Input Sensor) or Relay Output (Smart 8 Relay Output), and shows at a glance whether it is active (ON) or inactive (OFF). This immediate visual status overview is crucial during system commissioning and troubleshooting, as it confirms all inputs/outputs are functioning as expected, and can reveal any active alarms.



Input	Status	Name	Description
1	✓ ON	Door A - North Gate	Magnetic contact (N.C.); ON = door open
2	✗ OFF	Sump High Level	Float switch (N.O.); ON = water high alarm
3	✓ ON	Generator Running	Genset dry contact (N.O.); ON = engine running
4	✗ OFF	Utility Power Fail	From UPS (N.C.); ON = utility power lost
5	✗ OFF	Temperature High - AHU 2	Thermostat trip (N.O.); ON = overtemp
6	✓ ON	Cabinet - Panel 1	Door switch (N.C.); ON = door opened
7	✗ OFF	Emergency Stop	Safety loop (N.C.); ON = E-Stop pressed
8	✗ OFF	Leak Detect - Mech. Room	Rope sensor (N.O.); ON = water present

I/O Summary Table (Smart 8 Input Sensor)

Each row in the I/O summary table corresponds to a particular channel and includes additional identifying information, as outlined below.

Item	Parameter	Description
1	`Input/Output`	Displays an index (1-8) for each Digital Input or Relay Output channel
2	`Channel Status`	A color-coded indicator declaring each I/O state as ON (green) or OFF (red) ON (Active): Digital Input signal detected, or Relay Output is energized OFF (Inactive): Digital Input signal absent, or Relay Output is de-energized
3	`Channel Name`	User-defined label for the channel (blank by default)
4	`Channel Description`	User-defined notes for the channel (blank by default)

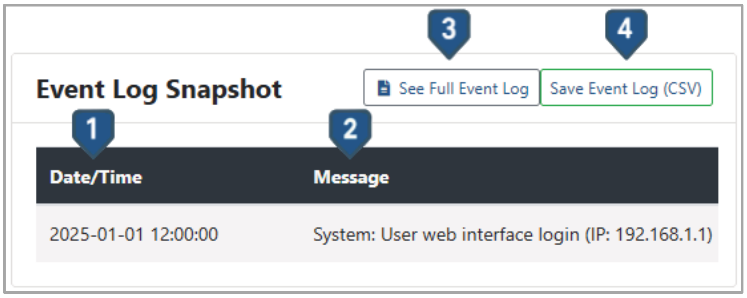
I/O Summary Table (Smart 8 Input Sensor) Description

Common uses of this table include:

- Validate a field device's commissioning by toggling it and subsequently refreshing the page to observe if the corresponding I/O channel's state changes
- Verifying the accuracy of the naming and descriptions of I/O channels
- Troubleshoot an issue quickly; a channel stuck in the OFF state may indicate a wiring fault, or a network fault if System Pairing is configured

Event Log Snapshot

At the bottom of the Overview Dashboard is the Event Log Snapshot, a panel displaying the most recently recorded system events. Each entry includes the date and time of the event, and a brief message describing what occurred. This snapshot includes up to ten of the latest event entries so users can immediately review the system's latest activity without leaving the Overview Dashboard.



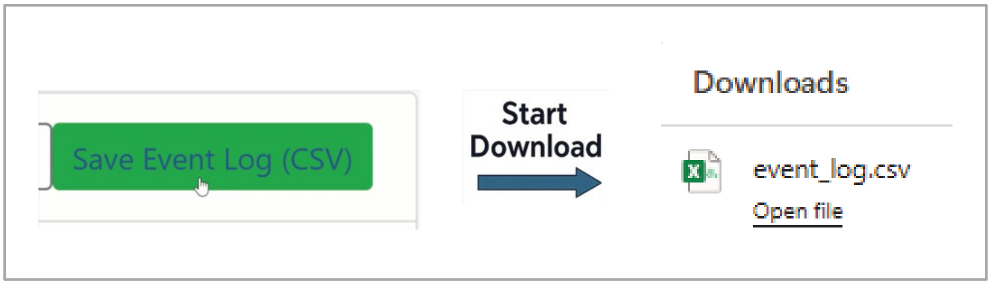
Event Log Snapshot

Date/Time	Message
2025-01-01 12:00:00	System: User web interface login (IP: 192.168.1.1)

Event Log Snapshot

Item	Parameter	Description
1	`Date/Time`	Displays the timestamp associated with an event in the following format: [Year-Month-Day Hour:Minute:Second] / [YYYY-MM-DD HH:MM:SS]
2	`Message`	Displays the event's description (e.g., logins, I/O status, configuration)
3	`See Full Event Log`	Opens the Event Log window
4	`Save Event Log (CSV)`	Initiates a download containing all events present in the Event Log

For a more in-depth review of all the system's events, select the "See Full Event Log" button present on the Event Log Snapshot's header, or select "Event Log" from the left-hand Navigation Panel. The Event Log Snapshot also includes an "Save Event Log (CSV)" button for users to initiate a one-click export and download of the entire Event Log's event history data as a comma-separated values (CSV) file.



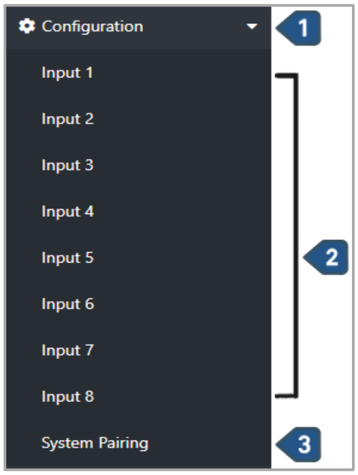
Save Event Log (CSV) Selected

Event Log exported

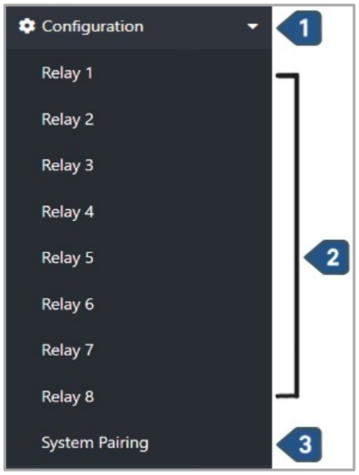
Configuration Panel

Overview

The Configuration panel, identified by a Gear icon, provides access to I/O channel settings and System Pairing options. On the Smart 8 Input Sensor model, this menu will list configuration panels for Inputs 1–8, whereas the Smart 8 Relay Output model will conversely list Relays 1–8. For both models, the Configuration panel is expanded by default, displaying the configuration panels for each I/O channel and System Pairing. Selecting an I/O channel (Input[#] or Relay[#])'s configuration panel opens the configuration window for that particular channel, while System Pairing opens the configuration window for linking together Smart 8 Input Sensors with Smart 8 Relay Outputs.



(Smart 8 Input Sensor)



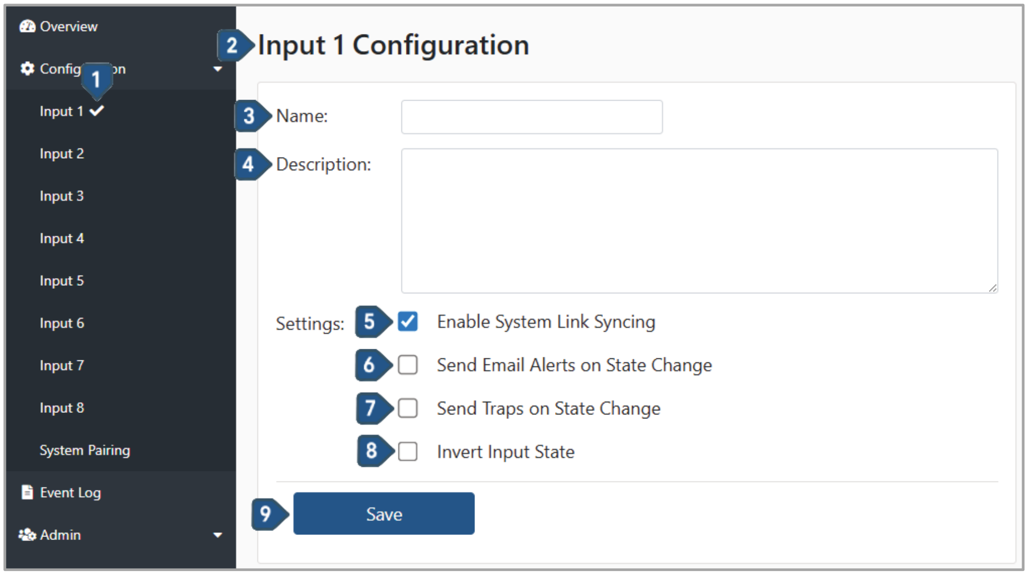
(Smart 8 Relay Output)

Item	Parameter	Description
1	`Navigation Toggle (≡)`	Lists the configuration panels for each I/O channel, and System Pairing (Collapsed by default on the Overview Dashboard)
2	`Model Name`	Opens the configuration window for that particular I/O channel [1-8]
3	`Part Number`	Opens the System Pairing configuration window

The I/O channel and System Pairing configuration windows that these sections of the Configuration Panel provide access to will slightly vary in appearance, and their scope of functionality, between the Smart 8 Input Sensor with Smart 8 Relay Output models. This will be expanded upon further in the subsequent pages; integrators should accordingly review each section carefully, as certain features pertaining to I/O channel and System Pairing configuration changes will differ depending on the model in use.

Input [1-8] (Input [n] Configuration)

The Input [1-8] Configuration window is the per-channel control interface for a Digital Input channel. It enables integrators to define and document the channel's function, bind it to conditional downstream processes (relay pairing, notifying operators/NMS), and re-defining state interpretation logic.



Input 1 Configuration

Name:

Description:

Settings: ☑ Enable System Link Syncing

☐ Send Email Alerts on State Change

☐ Send Traps on State Change

☐ Invert Input State

Save

Input [1-8] Configuration Window

Item	Parameter	Description
1	`Check Mark (✓)`	Identifies the selected Digital Input channel on the Configuration Panel
2	`Input [1-8] Configuration`	The page title, identifying the selected Digital Input channel
3	`Name`	A short label for the Digital Input channel (Character Limit: 50)
4	`Description`	A supplemental notes section with a resize grip ( ) at the bottom-right corner of the text input field (Character Limit: 280)
5	`Enable System Link Syncing`	Publishes the Digital Input's state (ON/OFF) to one or more paired Smart 8 Relay Outputs; no effect if System Pairing is disabled or disconnected
6	`Send Email Alerts on State Change`	Generates and distributes an email after each state transition (ON↔OFF); no effect if the system's SMTP server is disabled or misconfigured
7	`Send Traps on State Change`	Emits an SNMP trap after each state transition (ON↔OFF); no effect if the system's SNMP Trap Notification settings are disabled or misconfigured
8	`Invert Input State`	Inverts the system's Digital Input state interpretation logic; ON becomes OFF, and OFF becomes ON, without any changes to the channel's wiring
9	`Save`	Commits and immediately applies all changes to the Digital Input channel

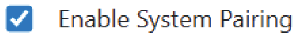
*By default, only Enable System Link Syncing is enabled

Dependencies, Validation, & Troubleshooting

Some of these downstream input-level notification and transmission setting options are contingent upon the working operation of other system-level services, which are configured outside of this window. Please review the prerequisites of these features below to ensure that all underlying dependencies are enabled, configured, and verified before presuming that the mechanisms are active.

System Link Syncing:

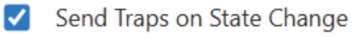
(Configuration->System Pairing)

- System Pairing must be enabled, and maintaining an active System Pairing session:
  - Enable System Pairing: Enabled  ☑ Enable System Pairing
  - System Pairing Status: Connected **System Pairing Status:** Connected
- If the System Pairing Status is Disconnected, review and troubleshoot the System Pairing configuration on the Smart 8 Input Sensor, and Smart 8 Relay Output(s)
- If the System Pairing Status is Connected, but Digital Input states aren't transferred, reassess whether the correct Digital Input channel(s) have Syncing enabled

Email Alerts: ☑ Send Email Alerts on State Change

(Admin->Email Notifications)

- Email Notifications must be enabled, and configured with an operational SMTP server:
  - Enable Email Notifications: Enabled ☑ Enable Email Notifications
  - Configure SMTP server, user account, and sender/recipient address parameters
  - Verify settings with "Send Test Email (on save)": ☑ Send Test Email (on save)
- Use the "Invert Input State" feature on each channel with Email Alerts configured to validate that the intended recipient(s) will receive Email Alerts during state changes

SNMP Traps:  ☑ Send Traps on State Change

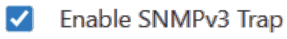
(Admin->SNMP->Trap Notifications)

- At least one SNMP Trap version (SNMPv2c and/or SNMPv3) must be enabled, with its Host Server(s) configured correctly for the traps to be properly received:

(SNMPv2c):

  - Enable SNMPv2c Trap: Enabled ☑ Enable SNMPv2c Trap
  - Configure Host Server(s), Port, and Community

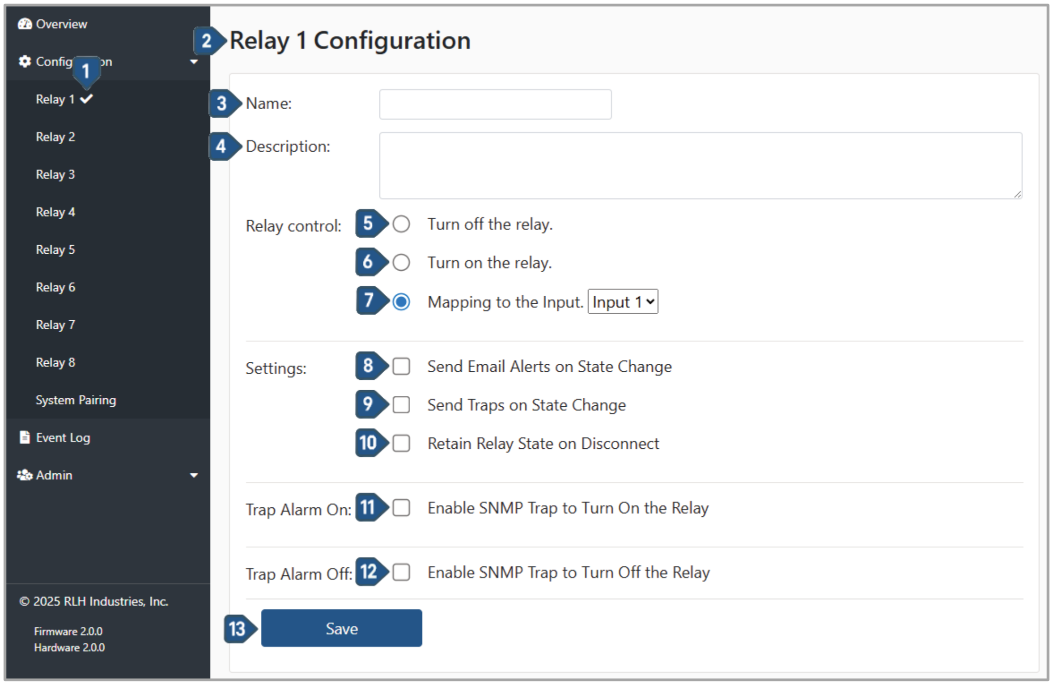
(SNMPv3):

  - Enable SNMPv3 Trap: Enabled  ☑ Enable SNMPv3 Trap
  - Configure Host Server, Port, USM User, Security Level, and Engine ID

- The Host Server(s) should receive a coldStart trap once the configuration is saved
- Use the "Invert Input State" feature on each channel with SNMP Traps configured to validate that the Host Server(s) will receive SNMP Traps during state changes

Relay [1-8] (Relay Configuration Window) Overview

The Relay [1-8] Configuration window is the per-channel control interface for a Relay Output channel. It enables integrators to define and document the relay's function, statically assign its state, and bind it to conditional upstream (input pairing, trap triggering) or downstream processes (notifying operators/NMS).



Relay 1 Configuration

Name:

Description:

Relay control: ○ Turn off the relay.
○ Turn on the relay.
● Mapping to the Input. Input 1

Settings: □ Send Email Alerts on State Change
□ Send Traps on State Change
□ Retain Relay State on Disconnect

Trap Alarm On: □ Enable SNMP Trap to Turn On the Relay

Trap Alarm Off: □ Enable SNMP Trap to Turn Off the Relay

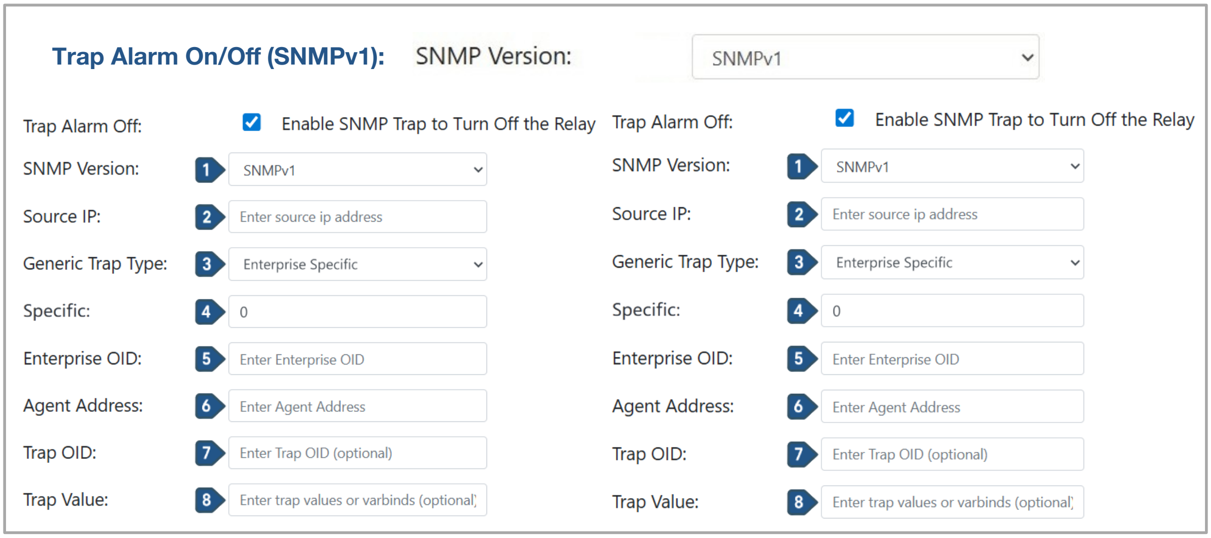
Relay [1-8] Configuration Window

Item	Parameter	Description
1	`Check Mark (✔)`	Identifies the selected Relay Output channel on the Configuration Panel
2	`Relay [1-8] Configuration`	The page title, identifying the selected Relay Output channel
3	`Name`	A short label for the Relay Output channel (Character Limit: 50)
4	`Description`	A supplemental notes section with a resize grip ( ) at the bottom-right (Character Limit: 200)
5	`Turn off the relay`	Statically assigns the Relay Output to an OFF state
6	`Turn on the relay`	Statically assigns the Relay Output to an ON state
7	`Mapping to the Input.`	Dynamically assigns the Relay Output to an ON or OFF state based on the Digital Input it is mapped to, per the Input [1-8] drop-down menu. This feature is enabled by default, and requires a System Pairing connection.
8	`Send Email Alerts on State Change`	Generates and distributes an email after each state transition (ON↔OFF); no effect if the system's SMTP server is disabled or misconfigured
9	`Send Traps on State Change`	Emits an SNMP trap after each state transition (ON↔OFF); no effect if the system's SNMP Trap Notification settings are disabled or misconfigured
10	`Retain Relay State on Disconnect`	If an active System Pairing connection is lost, the Relay Output will remain in the last state (ON/OFF) acquired from its mapped Digital Input
11/12	`Enable SNMP Trap to Turn On/Off the Relay`	Allows the Relay Output to change its state after receiving an SNMP trap; enabling either reveals additional settings that the following page will clarify
13	`Save`	Commits and immediately applies all changes to the Relay Output channel

Relay Configuration Window (SNMPv1) Configuration

When configured as an SNMP Trap Receiver, the Smart 8 Relay Output can energize (ON) or de-energize (OFF) a relay when it receives a trap matching the conditions defined in the "Trap Alarm" settings. Each Relay Output channel supports up to two Trap Alarm rules: "Trap Alarm On", which energizes the relay, and "Trap Alarm Off", which de-energizes the relay. Both rules can be enabled simultaneously on the same Relay Output channel, and each channel maintains its own independent Trap Alarm configuration.

If both rules are triggered by identical trap conditions, the Relay Output will alternate its current energization (ON/OFF) state. Trap Alarm rules process traps as either SNMPv1, or SNMPv2c/SNMPv3, since SNMPv1 uniquely includes two version-specific parameters: Enterprise OID, and Agent Address.



Trap Alarm On/Off (SNMPv1): SNMP Version: SNMPv1

Trap Alarm Off: ☑ Enable SNMP Trap to Turn Off the Relay
SNMP Version: 1 SNMPv1
Source IP: 2 Enter source ip address
Generic Trap Type: 3 Enterprise Specific
Specific: 4 0
Enterprise OID: 5 Enter Enterprise OID
Agent Address: 6 Enter Agent Address
Trap OID: 7 Enter Trap OID (optional)
Trap Value: 8 Enter trap values or varbinds (optional)

Trap Alarm Off: ☑ Enable SNMP Trap to Turn Off the Relay
SNMP Version: 1 SNMPv1
Source IP: 2 Enter source ip address
Generic Trap Type: 3 Enterprise Specific
Specific: 4 0
Enterprise OID: 5 Enter Enterprise OID
Agent Address: 6 Enter Agent Address
Trap OID: 7 Enter Trap OID (optional)
Trap Value: 8 Enter trap values or varbinds (optional)

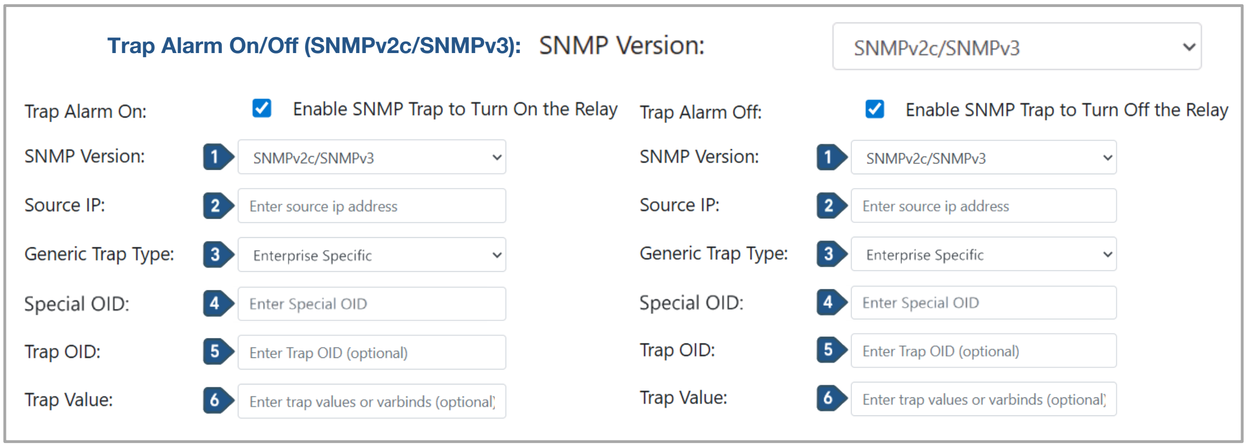
Trap Alarm On / Off (SNMPv1) Configuration Window

Item	Parameter	Description
1	`SNMP Version`	Specifies the SNMP Version (SNMPv1, or SNMPv2c/SNMPv3). This rule expects for incoming traps. SNMPv1 uniquely includes the Enterprise OID and Agent Address parameters. By default, this field is set to SNMPv1.
2	`Source IP`	The rule's permitted source IP address, corresponding to the IP header of a data packet carrying the trap. Usually identical to the Agent Address, unless the packet is forwarded through an SNMP proxy agent or translated by NAT.
3	`Generic Trap Type`	Matches the trap to an RFC 1215-standard type (Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, EGP Neighbor Loss), or instead to a non-standard Enterprise Specific type used by vendor-defined traps.
4	`Specific`	The OID reported in the SNMPv1 trap's enterprise field. Identifies a vendor's IANA registered OID subtree, and is required for Enterprise Specific traps.
5	`Enterprise OID (SNMPv1 Only)`	The OID reported in the SNMPv1 trap's enterprise field. Identifies a vendor's IANA-registered OID subtree, and is required for Enterprise Specific traps. Example: 1.3.6.1.4.1.38714 (Enterprise OID for RLH Industries Inc.)
6	`Agent Address (SNMPv1 Only)`	The IPv4 address reported in the SNMPv1 trap's agent-addr field. Identifies the SNMP agent that originated the trap, and is a field unique to SNMPv1.
7	`Trap OID`	Specifies a varbind OID that the trap must contain for the rule to trigger. If the Trap Value is blank, the rule will accept any varbind value for this OID.
8	`Trap Value`	Specifies a varbind value that the trap must contain for the rule to trigger. If the Trap OID is blank, the rule will accept any varbind OID with this value.

SNMPv2 / SNMPv3 Configuration

The Trap Alarm configuration for SNMPv2c/SNMPv3 follows the same functional design as SNMPv1, but the newer protocols' structure eliminates the need for separate Enterprise OID and Agent Address parameters. This reflects a fundamental change in SNMPv2c/SNMPv3, where a trap's notification OID is conveyed through the snmpTrapOID.0 varbind, replacing dedicated SNMPv1 fields such as enterprise and agent-addr.

As a result, the Trap Alarm's Trap OID and Trap Value parameters are used differently when defining rules for SNMPv2c/SNMPv3 traps. For vendor-defined notifications, set the Trap ID as "1.3.6.1.6.3.1.1.4.1.0" to target the snmpTrapOID.0 varbind, and enter the trap's notification OID (e.g., "1.3.6.1.2.1.33.2.0.1" for upsTrapOnBattery) as the Trap Value. Together, these identify a vendor-defined SNMPv2c/SNMPv3 event, the v2c/v3 equivalent of an SNMPv1 Enterprise Specific trap.



Trap Alarm On/Off (SNMPv2c/SNMPv3): SNMP Version: SNMPv2c/SNMPv3

Trap Alarm On: ☑ Enable SNMP Trap to Turn On the Relay

1. SNMP Version: SNMPv2c/SNMPv3
2. Source IP: Enter source ip address
3. Generic Trap Type: Enterprise Specific
4. Special OID: Enter Special OID
5. Trap OID: Enter Trap OID (optional)
6. Trap Value: Enter trap values or varbinds (optional)

Trap Alarm Off: ☑ Enable SNMP Trap to Turn Off the Relay

1. SNMP Version: SNMPv2c/SNMPv3
2. Source IP: Enter source ip address
3. Generic Trap Type: Enterprise Specific
4. Special OID: Enter Special OID
5. Trap OID: Enter Trap OID (optional)
6. Trap Value: Enter trap values or varbinds (optional)

Trap Alarm On/Off (SNMPv2c/SNMPv3) Configuration Windows

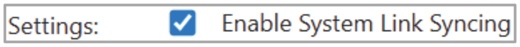
Items	Parameter	Description
1	`SNMP Version`	Specifies the SNMP Version (SNMPv1, or SNMPv2c/SNMPv3) this rule expects for incoming traps. SNMPv1 uniquely includes the Enterprise OID and Agent Address parameters. By default, this field is set to SNMPv1.
2	`Source IP`	The rule's permitted source IP address, corresponding to the IP header of a data packet carrying the trap. Usually identical to the Agent Address, unless the packet is forwarded through an SNMP proxy agent or translated by NAT.
3	`Generic Trap Type`	Provides the same Generic Trap Type selections as in SNMPv1, converting each to the equivalent SNMPv2c/SNMPv3 notification OID. When the Trap Value parameters to identify a vendor-defined notification.
4	`Special OID`	Specifies a varbind OID that the trap must contain for the rule to trigger. When Enterprise Specific is the Generic Trap Type, this is configured as the vendor-specific notification ID of the trap.
5	`Trap OID`	Specifies a varbind OID that the trap must contain for the rule to trigger. When Enterprise Specific is the Generic Trap Type, this is typically set to the OID of the snmpTrapOID.0 varbind ("1.3.6.1.6.3.1.1.4.1.0") so the rule interprets the Trap Value as the vendor-defined notification OID. If the Trap Value is blank, the rule will accept any varbind value for this OID.
6	`Trap Value`	Specifies a varbind OID that the trap must contain for the rule to trigger. When Enterprise Specific is the Generic Trap Type, this is configured as the vendor-specific notification ID of the trap.

System Pairing

System Pairing establishes a persistent TCP session between Smart 8 Input Sensor and Smart 8 Relay Output units, enabling Digital Input state changes to energize or de-energize mapped relays.

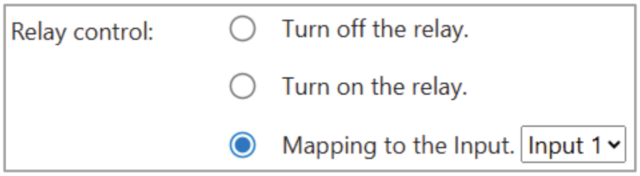
I/O Channel Participation

All Digital Input channels participate in an active System Pairing connection by default. Digital Inputs may alternatively be excluded a System Pairing connection by disabling the Enable System Link Syncing setting on the individual Digital Input channel:



Settings: ☑ Enable System Link Syncing

Similarly, all Relay Output channels are configured by default to participate in an active System Pairing connection, due to their initial setup in a "Mapped" Relay control scheme. This "Mapped" control scheme associates each Relay Output channel with the same enumerated Digital Input channel, such that Relay 1 will sync to Input 1, Relay 2 will sync to Input 2, and so on. These associations may be re-defined by the user.



Relay control:
○ Turn off the relay.
○ Turn on the relay.
● Mapping to the Input. Input 1

Client / Server Roles

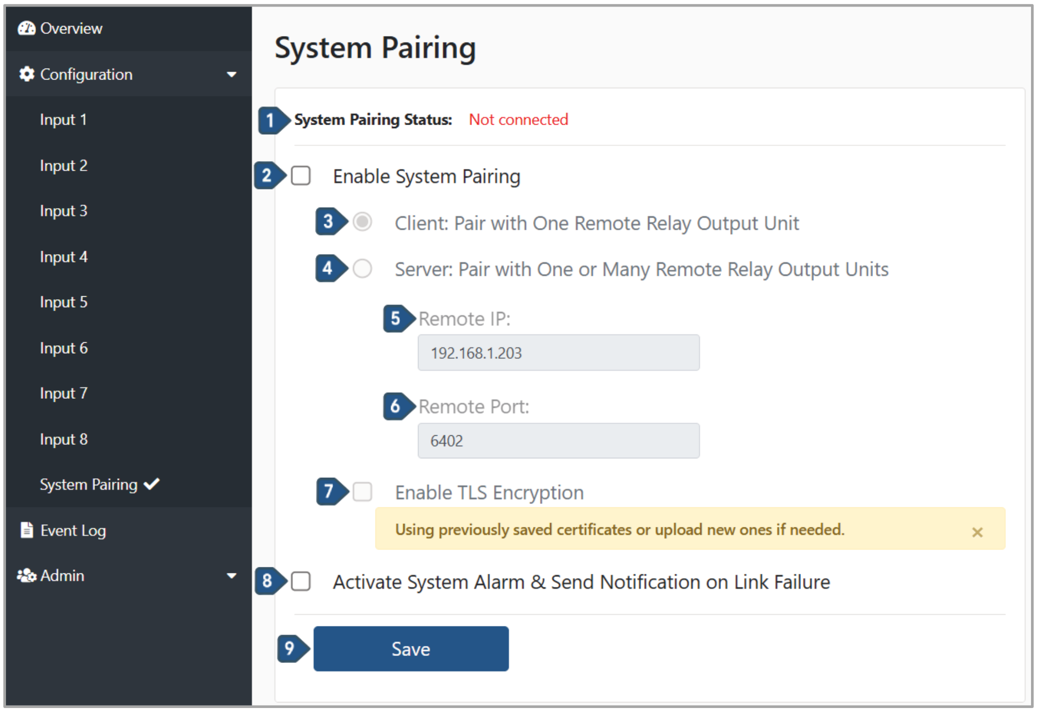
System Pairing links Smart 8 Input Sensor and Smart 8 Relay Output units together through a standard TCP client–server relationship. At least one unit within the relationship will initiate the session as the Client(s), while one unit listens for inbound connections as the Server. Both the Input Sensor and Relay Output systems may function as a Client, or Server, depending on the nature of the System Pairing topology (One-to-One, One-to-Many, Many-to-One) implemented:

Topology	Input Sensor	Relay Output	Description
One-to-One	`Client`	`Server`	The Relay Output listens for state changes from a single Input Sensor, and updates its' mapped relays in response.
One-to-Many	`Server`	`Clients`	The Input Sensor fans out state changes to all connected Relay Outputs; each unit updates its own mapped relays.
Many-to-One	`Clients`	`Server`	The Relay Output listens for state changes from multiple Input Sensors, and updates its' mapped relays accordingly.

Aside from the Client/Server role and its default presentation in the System Pairing window, the layout and overall functionality are identical on the Smart 8 Input Sensor and Smart 8 Relay Output. The following sections present each model's System Pairing window individually and highlight their Client/Server role defaults, provide topology guidance, and outline any model-specific details.

System Pairing (Smart 8 Input Sensor) Configuration

System Pairing is disabled by default on the Smart 8 Input Sensor, while each Digital Input channel is preconfigured to participate in System Pairing. When System Pairing is enabled and the connection is active, the unit distributes its Digital Input states across the session's connected Smart 8 Relay Output(s). Among all Smart Series models, the Smart 8 Input Sensor can only pair with the Smart 8 Relay Output.



System Pairing

System Pairing Status: Not connected

☐ Enable System Pairing

● Client: Pair with One Remote Relay Output Unit

○ Server: Pair with One or Many Remote Relay Output Units

Remote IP: 192.168.1.203

Remote Port: 6402

☐ Enable TLS Encryption

Using previously saved certificates or upload new ones if needed. ×

☐ Activate System Alarm & Send Notification on Link Failure

System Pairing (Smart 8 Input Sensor)

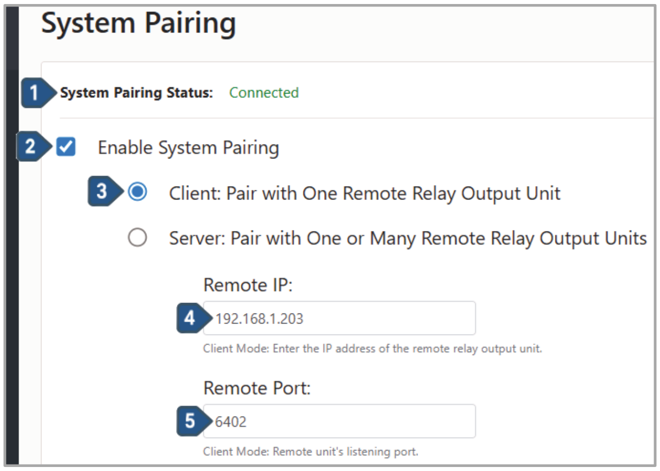
Item	Parameter	Description
1	`System Pairing Status`	Displays the session status for this unit as "Connected" or "Not connected". Not updated in real time; refresh the webpage for the current session status.
2	`Enable System Pairing`	Enables or disables the System Pairing service. Disabled by default.
3	`Client`	Selects "Client Mode" to initiate a TCP session over the Remote Port with
4	`Server`	Selects "Server Mode" to listen on the Remote Port for incoming connections from one (Many-to-One) or multiple (One-to-Many) Smart 8 Relay Outputs.
5	`Remote IP`	Specifies the destination IP address of the Smart 8 Relay Output in the System Pairing connection. Enter "0.0.0.0" when pairing with multiple units.
6	`Remote Port`	The TCP port used for either initiating the System Pairing session as a Client, or listening on as a Server. By default, this is TCP port 6402.
7	`Enable TLS Encryption`	Enables TLS 1.3 for the System Pairing session using TLS/SSL certificates uploaded to or generated by the unit. When enabled, all units participating in the session must enable TLS Encryption and use compatible certificates.
8	`Active System Alarm & Send Notification on Link Failure`	When enabled, the unit energizes its alarm relay if the System Pairing Status changes from "Connected" to "Not connected". If Email Notifications are enabled, an Email Alert is also sent per the configured SMTP parameters.
9	`Save`	Commits and immediately applies all System Pairing configuration changes.

System Pairing (Smart 8 Input Sensor) Topologies

The configurations outlined below express the System Pairing settings required on behalf of the Smart 8 Input Sensor to facilitate a One-to-One, One-to-Many, or Many-to-One System Pairing topology:

Input Sensor One-to-One:

Transmits Digital Inputs changes to one Relay Output unit



System Pairing

1 System Pairing Status: Connected

2 ☑ Enable System Pairing

3 ● Client: Pair with One Remote Relay Output Unit

○ Server: Pair with One or Many Remote Relay Output Units

Remote IP:

4 192.168.1.203

Client Mode: Enter the IP address of the remote relay output unit.

Remote Port:

5 6402

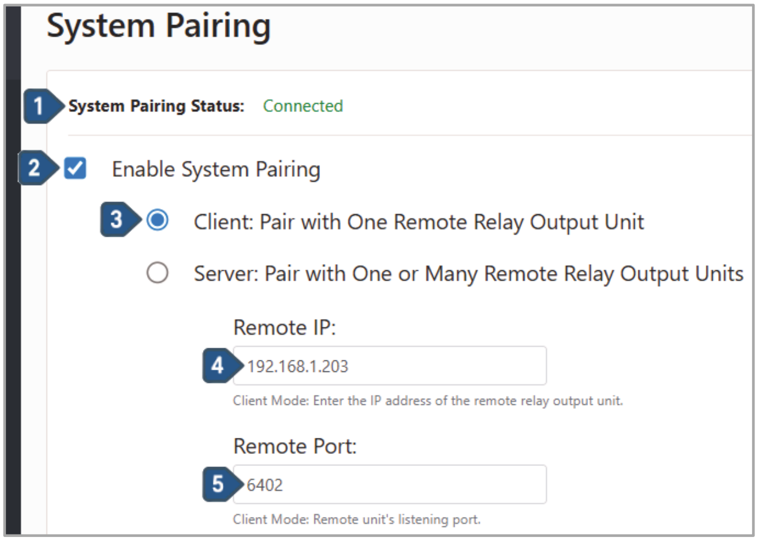
Client Mode: Remote unit's listening port.

1x Smart 8 Input Sensor (Client) to 1x Smart 8 Relay Output (Server)

Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Default (Client)
4	`Remote IP`	The Relay Output's IP address RJ45 Default: 192.168.1.203 SFP Default: 192.168.1.204
5	`Remote Port`	Default (6402)

Input Sensor One-to-Many:

Broadcasts Digital Input changes across multiple Relay Output units



System Pairing

1 System Pairing Status: Connected

2 ☑ Enable System Pairing

3 ● Client: Pair with One Remote Relay Output Unit

○ Server: Pair with One or Many Remote Relay Output Units

Remote IP:

4 192.168.1.203

Client Mode: Enter the IP address of the remote relay output unit.

Remote Port:

5 6402

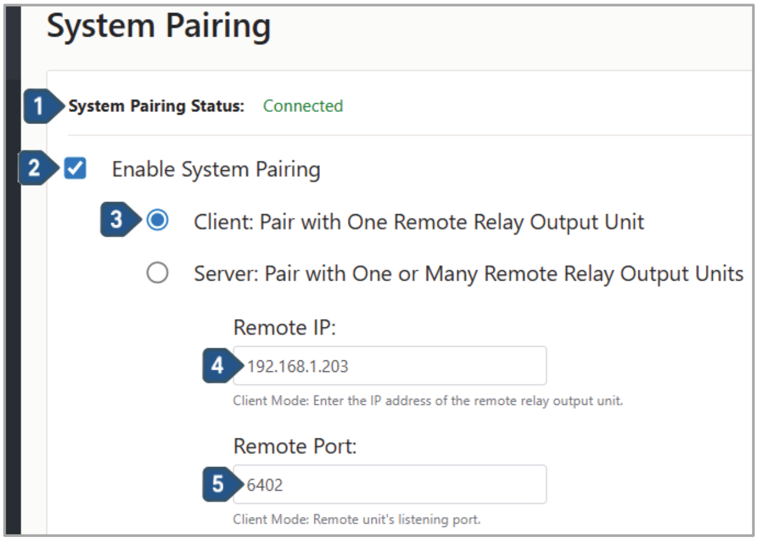
Client Mode: Remote unit's listening port.

1x Smart 8 Input Sensor (Server) to >1x Smart 8 Relay Outputs (Clients)

Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Set to Server
4	`Remote IP`	Enter "0.0.0.0" to allow multiple Relay Output units as Clients
5	`Remote Port`	Default (6402)

Input Sensor Many-to-One:

Contributes Digital Input changes to one Relay Output unit in parallel with other Input Sensors



System Pairing

1 System Pairing Status: Connected

2 ☑ Enable System Pairing

3 ● Client: Pair with One Remote Relay Output Unit

○ Server: Pair with One or Many Remote Relay Output Units

Remote IP:

4 192.168.1.203

Client Mode: Enter the IP address of the remote relay output unit.

Remote Port:

5 6402

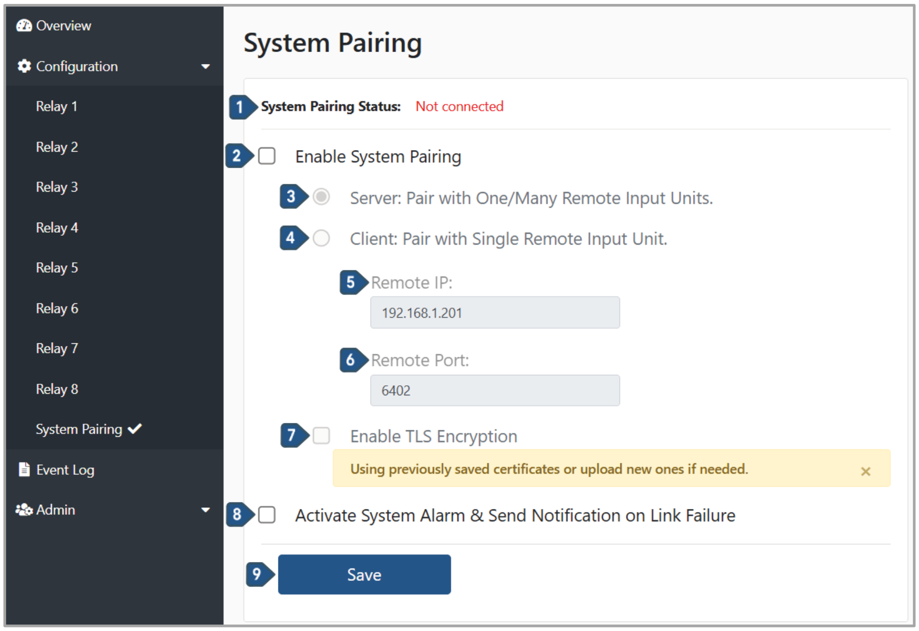
Client Mode: Remote unit's listening port.

>1x Smart 8 Input Sensors (Clients) to 1x Smart 8 Relay Output (Server)

Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Default (Client)
4	`Remote IP`	The Relay Output's IP address RJ45 Default: 192.168.1.203 SFP Default: 192.168.1.204
5	`Remote Port`	Default (6402)

System Pairing (Smart 8 Relay Output) Configuration

System Pairing is disabled by default on the Smart 8 Relay Output, while each Relay Output channel is preconfigured to participate in System Pairing and mapped sequentially to a corresponding Digital Input. When System Pairing is enabled and the connection is active, the unit drives each Relay Output in response to the Digital Input states distributed by the session's connected Smart 8 Input Sensor(s). Among all Smart Series models, the Smart 8 Relay Output can only pair with the Smart 8 Input Sensor.



System Pairing

1 System Pairing Status: Not connected

2 ☐ Enable System Pairing

3 ● Server: Pair with One/Many Remote Input Units.

4 ○ Client: Pair with Single Remote Input Unit.

5 Remote IP: 192.168.1.201

6 Remote Port: 6402

7 ☐ Enable TLS Encryption

Using previously saved certificates or upload new ones if needed. ×

8 ☐ Activate System Alarm & Send Notification on Link Failure

9 Save

System Pairing (Smart 8 Relay Output)

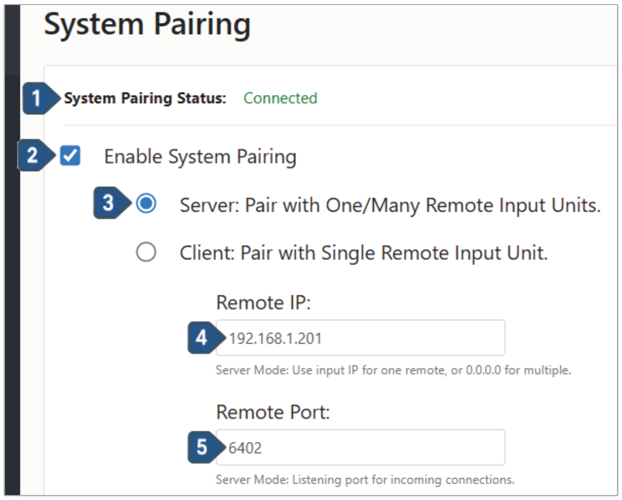
Item	Parameter	Description
1	`System Pairing Status`	Displays the session status for this unit as "Connected" or "Not connected". Not updated in real time; refresh the webpage for the current session status.
2	`Enable System Pairing`	Enables or disables the System Pairing service. Disabled by default.
3	`Server`	Selects "Server Mode" to listen on the Remote Port for incoming connections
4	`Client`	Selects "Client Mode" to initiate a TCP session over the Remote Port with one Smart 8 Input Sensor (Remote IP), in a One-to-Many pairing topology.
5	`Remote IP`	Specifies the destination IP address of the Smart 8 Input Sensor in the System Pairing connection. Enter "0.0.0.0" when pairing with multiple units.
6	`Remote Port`	The TCP port used for either initiating the System Pairing session as a Client, or listening on as a Server. By default, this is TCP port 6402.
7	`Enable TLS Encryption`	Enables TLS 1.3 for the System Pairing session using TLS/SSL certificates uploaded to or generated by the unit. When enabled, all units participating in the session must enable TLS Encryption and use compatible certificates.
8	`Active System Alarm & Send Notification on Link Failure`	When enabled, the unit energizes its alarm relay if the System Pairing Status changes from "Connected" to "Not connected". If Email Notifications are enabled, an Email Alert is also sent per the configured SMTP parameters.
9	`Save`	Commits and immediately applies all System Pairing configuration changes.

System Pairing (Smart 8 Relay Output) Topologies

The configurations outlined below express the System Pairing settings required on behalf of the Smart 8 Relay Output to facilitate a One-to-One, One-to-Many, or Many-to-One System Pairing topology:

Relay Output One-to-One:

Receives Digital Input changes from one Input Sensor



System Pairing

System Pairing Status: Connected

☑ Enable System Pairing

● Server: Pair with One/Many Remote Input Units.

○ Client: Pair with Single Remote Input Unit.

Remote IP:

192.168.1.201

Server Mode: Use input IP for one remote, or 0.0.0.0 for multiple.

Remote Port:

6402

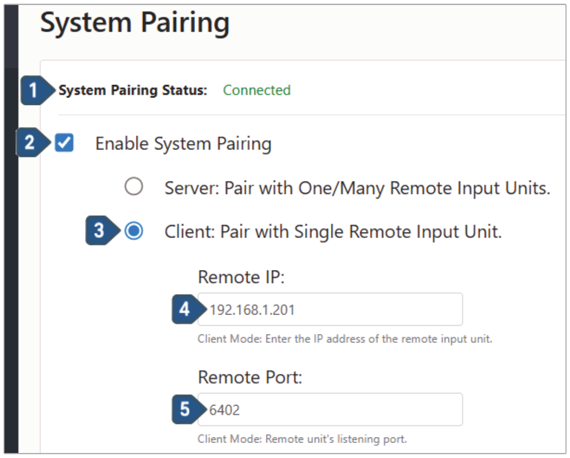
Server Mode: Listening port for incoming connections.

1x Smart 8 Input Sensor (Client) to 1x Smart 8 Relay Output (Server)

Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Default (Server)
4	`Remote IP`	The Input Sensor's IP address RJ45 Default: 192.168.1.203 SFP Default: 192.168.1.204
5	`Remote Port`	Default (6402)

Relay Output One-to-Many:

Mirrors a single Input Sensor's Digital Input changes in parallel with other Relay Output units



System Pairing

System Pairing Status: Connected

☑ Enable System Pairing

○ Server: Pair with One/Many Remote Input Units.

● Client: Pair with Single Remote Input Unit.

Remote IP:

192.168.1.201

Client Mode: Enter the IP address of the remote input unit.

Remote Port:

6402

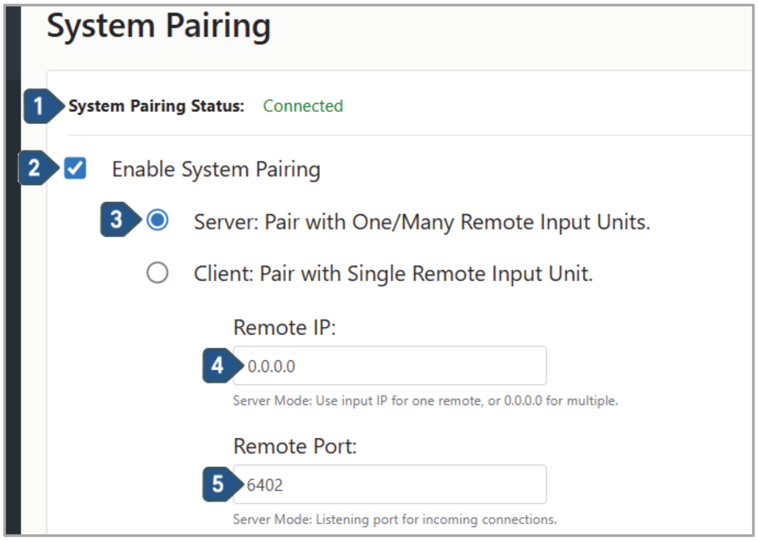
Client Mode: Remote unit's listening port.

1x Smart 8 Input Sensor (Server) to >1x Smart 8 Relay Outputs (Clients)

Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Set to Client
4	`Remote IP`	The Input Sensor's IP address RJ45 Default: 192.168.1.201 SFP Default: 192.168.1.202
5	`Remote Port`	Default (6402)

Relay Output Many-to-One:

Consolidates Digital Input changes across multiple Input Sensors



System Pairing

1 System Pairing Status: Connected

2 ☑ Enable System Pairing

3 ● Server: Pair with One/Many Remote Input Units.

○ Client: Pair with Single Remote Input Unit.

Remote IP:

4 0.0.0.0

Server Mode: Use input IP for one remote, or 0.0.0.0 for multiple.

Remote Port:

5 6402

Server Mode: Listening port for incoming connections.

>1x Smart 8 Input Sensors (Clients) to 1x Smart 8 Relay Output (Server)

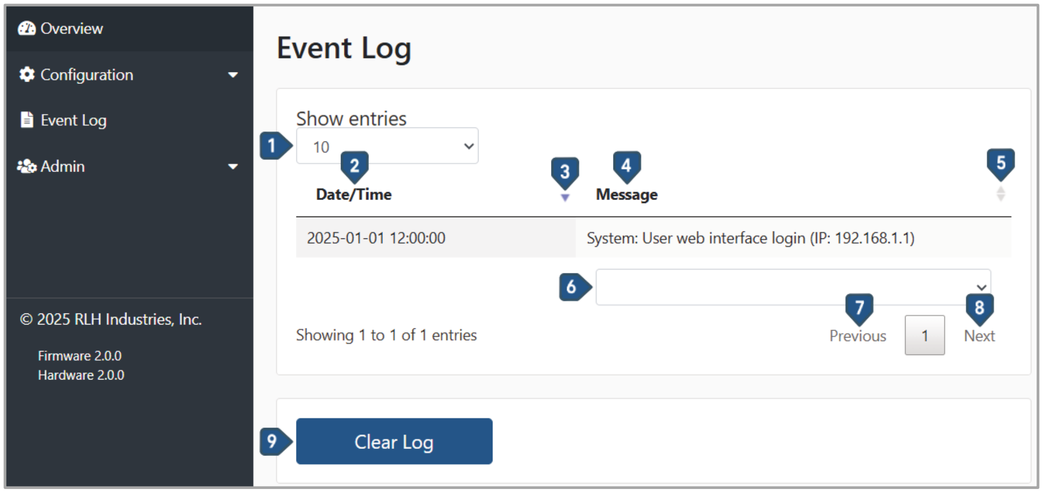
Item	Parameter	Description
1	`System Pairing Status`	Connected (refresh to update)
2	`Enable System Pairing`	Set to Enabled
3	`Client/Server Mode`	Set to Client
4	`Remote IP`	Enter "0.0.0.0" to allow multiple Input Sensor units as Clients
5	`Remote Port`	Default (6402)

Event Log

Overview

The Event Log, identified by a Document icon, provides a timestamped audit of system activity showcasing Digital Input/Relay Output state changes, user log-ins, configuration updates, and other system notices. Event Log entries may be sorted by their timestamp or event description, filtered by the recorded events, or collectively purged from the Event Log.

Use this page to review the system's activity over time, and reference its most recent events. Timestamps follow the system's clock, which is configured on the Date & Time page (p.51). This feature functions identically on both the Smart 8 Input Sensor and Smart 8 Relay Output models.



© 2025 RLH Industries, Inc.

Firmware 2.0.0
Hardware 2.0.0

Date/Time	Message
2025-01-01 12:00:00	System: User web interface login (IP: 192.168.1.1)

Showing 1 to 1 of 1 entries

Event Log Window

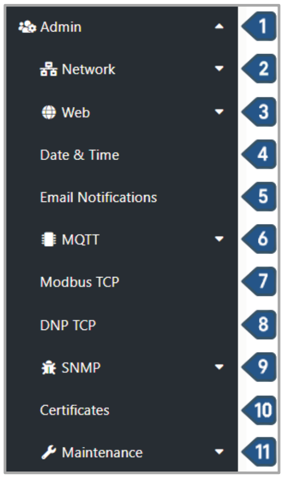
Item	Parameter	Description
1	`Show entries`	Sets the number of Event Log entry rows, per page, offering the following options: 5, 10, 25, 50, 100, 250, 500. (Default: 10)
2	`Date/Time`	Displays the timestamp associated with an event in the below format: [Year-Month-Day Hour:Minute:Second] / [YYYY-MM-DD HH:MM:SS]
3	`Date/Time sort`	Toggles the Date/Time column by ascending or descending order.
4	`Message`	Displays the event's description (e.g., logins, I/O status, configuration).
5	`Message sort`	Toggles the Message column by ascending or descending order.
6	`Message filter`	Filters the Message column by specific events already captured in the Log. Example: "Relay 1 status changed by Input mapping."
7	`Previous`	Opens the previous page of entries (page size determined by Show entries).
8	`Next`	Opens the next page of entries (page size determined by Show entries).
9	`Clear Log`	Purges all entries from the Event Log. This action cannot be undone.

Admin Panel

Overview

The Admin Panel, identified by the Users icon, provides centralized access to all system-wide configuration areas that govern device operation, network connectivity, protocol services, and security. Each item in this panel opens a dedicated configuration window for its respective subsystem, ranging from Ethernet and web access settings to time synchronization, alarm notifications, and certificate management.

These features enable administrators to provision network interfaces, authenticate users, enable and configure communication services (Modbus TCP, DNP3, MQTT, SNMP), and perform firmware or maintenance operations, providing full administrative control over the Smart 8 Input Sensor and Smart 8 Relay Output.



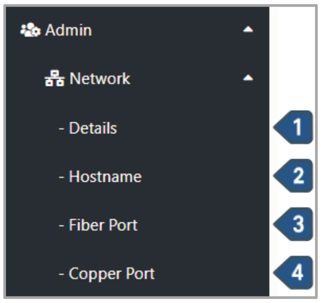
Admin Panel

Item	Parameter	Description
1	Admin	Expands the Admin Panel for system-wide configuration: networking, web access/auth, timekeeping, notifications, protocols, certificates, and maintenance
2	Network	Configures RJ45/SFP interface addressing and 802.1X integration, sets the hostname, and offers a quick read-only interface view (e.g., speed, IP, MAC)
3	Web	Configures HTTP/HTTPS and REST API/token, manages local users (Admin, Guest) or RADIUS, assigns the management portal's access method
4	Date & Time	Sets the system's clock manually or via NTP, and selects the time zone
5	Email Notifications	Configures the SMTP server settings used for sending system Email Alerts
6	MQTT	Configures an MQTT broker on both models, an MQTT publisher for the Smart 8 Input Sensor, and an MQTT Subscriber for the Smart 8 Relay Output
7	Modbus TCP	Enables the Modbus TCP slave service. This maps eight points to Coil, Discrete Input, and Holding/Input Register address blocks for ICS/SCADA integration
8	DNP TCP	Enables the DNP3/TCP outstation service. The Smart 8 Input Sensor publishes Binary Inputs, while the Smart 8 Relay Output publishes Binary Output Statuses and supports Binary Output control (CROB/Select-Operate).
9	SNMP	Enables SNMPv1/v2c/v3, defines views/communities/users, configures Trap Notifications, and hosts a Trap Receiver (Smart 8 Relay Output only)
10	Certificates	Manages TLS/SSL certificates: download or delete existing certificates, generate self-signed certificates, or upload organizational certificates.
11	Maintenance	Upload or reset firmware, and initiate manual system reboots/shutdowns

Network Panel

Overview

The Network provides configuration access towards all Ethernet interface parameters, including hostname assignment, per-port addressing for of the system's copper (RJ45) and fiber (SFP) interfaces, and the optional implementation of 802.1X authentication.

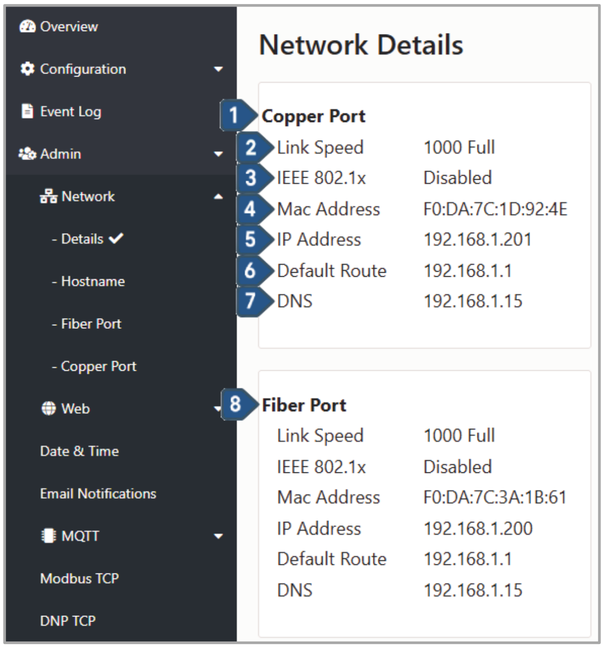


Network Sub-Panel

Item	Parameter	Description
1	`Details`	Displays current link, addressing, and DNS information for both Ethernet interfaces.
2	`Hostname`	Sets a DNS-compliant system hostname
3	`Fiber Port`	Configures IP addressing, gateway, DNS, and 802.1X settings for the SFP interface.
4	`Copper Port`	Configures IP addressing, gateway, DNS, and 802.1X settings for the RJ45 interface.

Network Details

The Network Details page provides a read-only summary of each Ethernet interface's current operating and addressing parameters. Items referenced below as #1-#7 display the Ethernet link, authentication, and IPv4 configuration data for the copper (RJ45) port, which is functionally identical to the sections listed under the Fiber Port section (#8) below.



Network Details

Copper Port
Link Speed 1000 Full
IEEE 802.1x Disabled
Mac Address F0:DA:7C:1D:92:4E
IP Address 192.168.1.201
Default Route 192.168.1.1
DNS 192.168.1.15

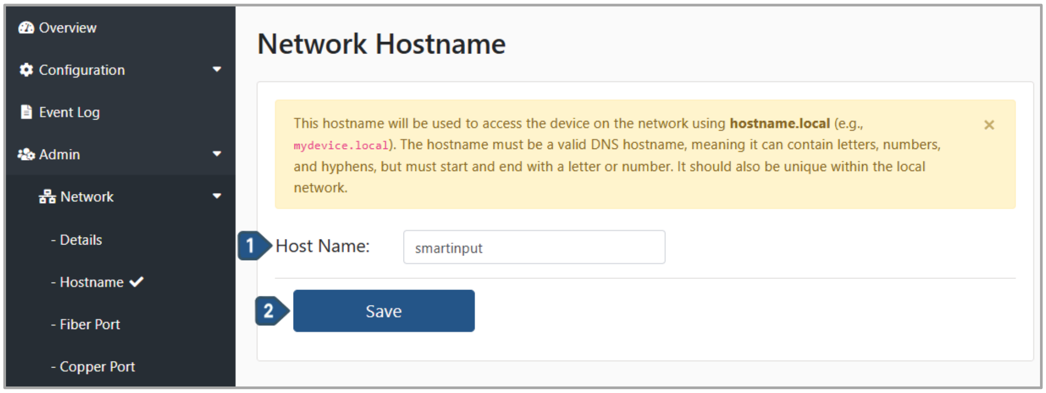
Fiber Port
Link Speed 1000 Full
IEEE 802.1x Disabled
Mac Address F0:DA:7C:3A:1B:61
IP Address 192.168.1.200
Default Route 192.168.1.1
DNS 192.168.1.15

Network Details Window

Item	Parameter	Description
1	`Copper Port`	Displays operational and addressing information for the copper RJ45 interface
2	`Link Speed`	The link's negotiated data rate/duplex mode
3	`IEEE 802.1x`	Indicates whether port-based authentication (via IEEE 802.1X) is enabled or not
4	`Mac Address`	The interface's unique hardware address
5	`IP Address`	The interface's assigned IPv4 address
6	`Default Route`	The IPv4 address of the network gateway used for routing outbound traffic
7	`DNS`	The IPv4 address of the DNS server performing hostname resolution
8	`Fiber Port`	Displays operational and addressing information for the SFP transceiver interface

Network Hostname

The Network Hostname page enables administrators to assign a DNS-compliant hostname for identifying this device on a local network. It can be used in place of an IP address for browser-based access. By default, the Smart 8 Input Sensor's hostname is smartinput, and the Smart 8 Relay Output's hostname is smartoutput.



This hostname will be used to access the device on the network using **hostname.local** (e.g., `mydevice.local`). The hostname must be a valid DNS hostname, meaning it can contain letters, numbers, and hyphens, but must start and end with a letter or number. It should also be unique within the local network.

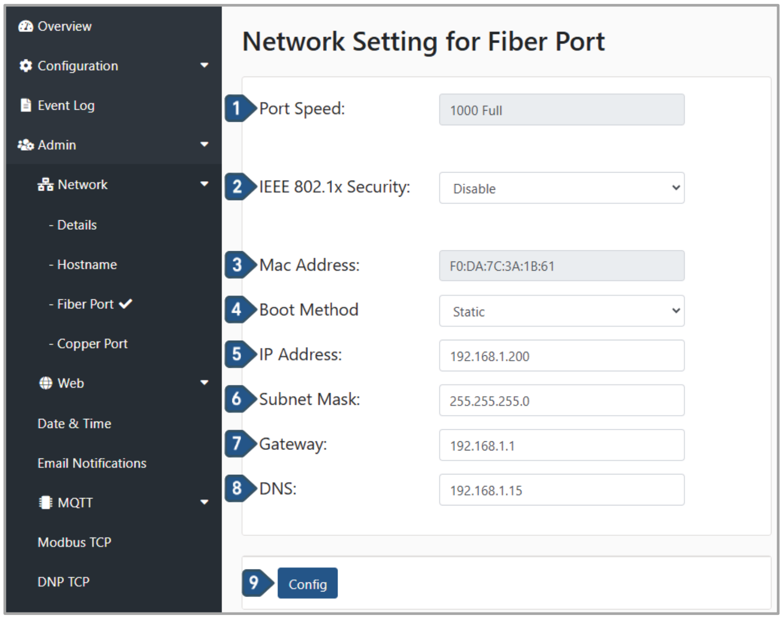
Host Name: smartinput

Network Hostname Window

Item	Parameter	Description
1	`Host Name`	Defines the system's DNS-compliant hostname used to identify the device on the network (e.g., mydevice.local). The hostname must begin and end with a letter or number, may include hyphens, and must be unique within the local network.
2	`Source IP`	Commits the entered hostname to the system configuration.

Network Fiber Port

The Fiber Port configuration page enables administrators to define the IP addressing and security parameters of the SFP transceiver Ethernet interface. These settings determine how the port communicates on the network, derives its IPv4 address, and implements IEEE 802.1X authentication for secure deployments.



Network Setting for Fiber Port

1 Port Speed: 1000 Full

2 IEEE 802.1x Security: Disable

3 Mac Address: F0:DA:7C:3A:1B:61

4 Boot Method: Static

5 IP Address: 192.168.1.200

6 Subnet Mask: 255.255.255.0

7 Gateway: 192.168.1.1

8 DNS: 192.168.1.15

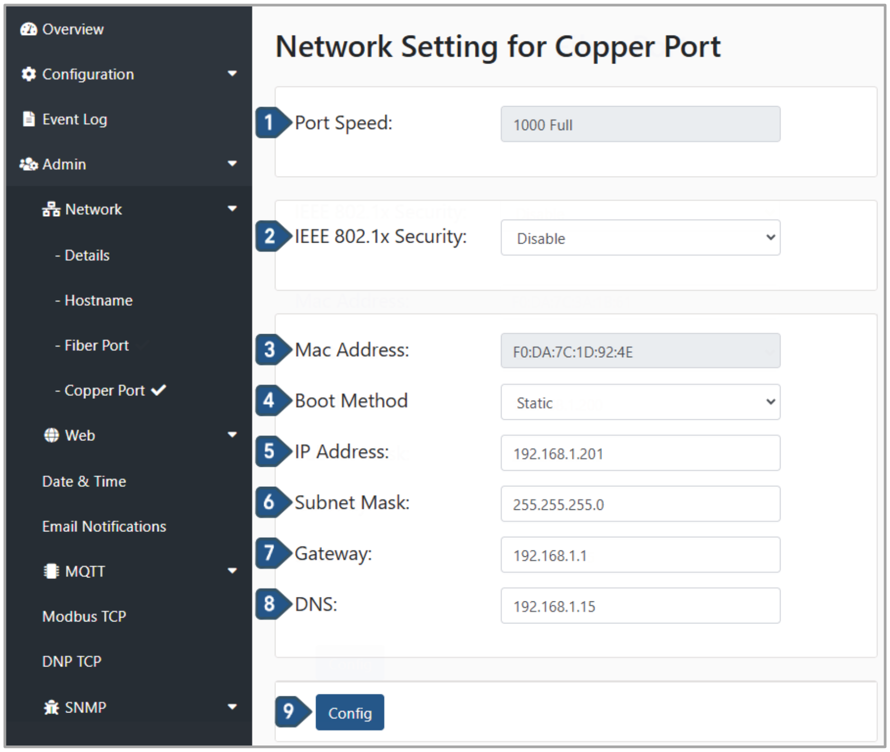
9 Config

Fiber Port Configuration Window

Item	Parameter	Description
1	`Port Speed`	The auto-negotiated data rate and duplex mode of the Ethernet link (read-only)
2	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control
3	`Mac Address`	The unique hardware address assigned to the SFP interface (read-only)
4	`Boot Method`	Selects the port's IP address assignment method (Static / DHCP)
5	`IP Address`	Assigns the SFP interface's static IPv4 address (read-only if DHCP is selected)
6	`Subnet Mask`	Assigns the subnet boundary for the local network (read-only if DHCP is selected)
7	`Gateway`	Assigns the network gateway's IPv4 address (read-only if DHCP is selected)
8	`DNS`	Assigns the DNS server's IPv4 address (read-only if DHCP is selected)
9	`Config`	Applies and saves all parameter changes to the SFP interface configuration. Connectivity to the device may be temporarily interrupted when modifying the IP parameters or Boot Method.

Network Copper Port

The Copper Port configuration page provides identical functionality to the Fiber Port section, but instead applies to the system's RJ45 (Copper) interface. Administrators can define static or DHCP addressing schemes, configure network gateway and DNS parameters, and optionally enable IEEE 802.1X authentication.



Network Setting for Copper Port

1 Port Speed: 1000 Full

2 IEEE 802.1x Security: Disable

3 Mac Address: F0:DA:7C:1D:92:4E

4 Boot Method Static

5 IP Address: 192.168.1.201

6 Subnet Mask: 255.255.255.0

7 Gateway: 192.168.1.1

8 DNS: 192.168.1.15

9 Config

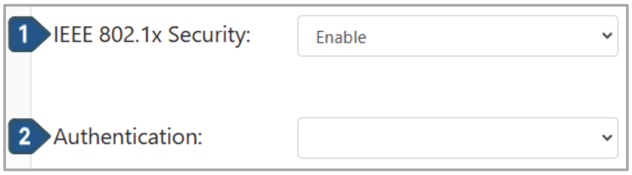
Copper Port Configuration Window

Item	Parameter	Description
1	`Port Speed`	The auto-negotiated data rate and duplex mode of the Ethernet link (read-only)
2	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control
3	`Mac Address`	The unique hardware address assigned to the SFP interface (read-only)
4	`Boot Method`	Selects the port's IP address assignment method (Static / DHCP)
5	`IP Address`	Assigns the SFP interface's static IPv4 address (read-only if DHCP is selected)
6	`Subnet Mask`	Assigns the subnet boundary for the local network (read-only if DHCP is selected)
7	`Gateway`	Assigns the network gateway's IPv4 address (read-only if DHCP is selected)
8	`DNS`	Assigns the DNS server's IPv4 address (read-only if DHCP is selected)
9	`Config`	Applies and saves all parameter changes to the SFP interface configuration. Connectivity to the device may be temporarily interrupted when modifying the IP parameters or Boot Method.

Network Fiber/Copper Port - IEEE 802.1X Configuration

The IEEE 802.1X Security setting parameters define port-based authentication for the Fiber Port and/or Copper Port, using the Extensible Authentication Protocol (EAP) to validate user credentials and/or certificates with an organization's RADIUS server. EAP provides a flexible framework for defining how credentials are securely exchanged from within an authentication tunnel, using either stored credentials or digital certificates (typically X.509-based).

IEEE 802.1X is disabled by default, but when enabled, it propagates an additional "Authentication" drop-down field onto the webpage for selecting a supported EAP authentication framework: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, and EAP-LEAP. Selecting an EAP method populates additional fields onto the webpage that are specific to that EAP method's configuration. Each EAP method's implementation is described in detail over the next few subsequent pages.



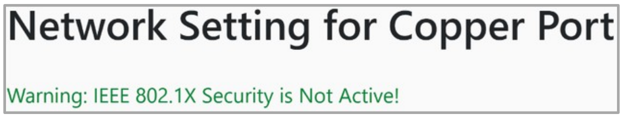
1 IEEE 802.1x Security: Enable

2 Authentication:

IEEE 802.1X - Enabled

Item	Parameter	Description
1	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control. This parameter must be set as Enable for the port to require RADIUS-based authentication before network access is granted.
2	`Authentication`	Specifies the EAP method used for verifying client credentials with a RADIUS server. The following EAP methods may be selected: TLS, TTLS (Tunneled TLS), PEAP (Protected EAP), MD5, and LEAP.

IEEE 802.1X status indicators will be listed at the top of the webpage, listing "Warning: IEEE 802.1X Security is Not Active!" for when the IEEE 802.1x Security field is set to Enable, but the connection has not been established.



Network Setting for Copper Port

Warning: IEEE 802.1X Security is Not Active!

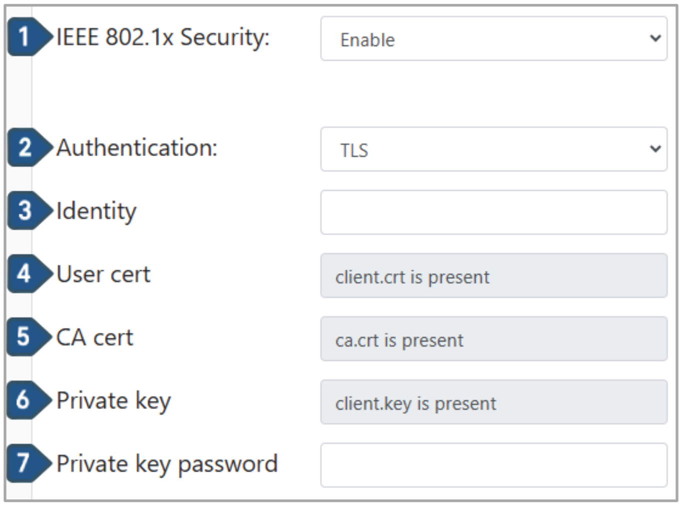
Conversely, for when the connection is successful, the IEEE 802.1X status indicator will list, "Connected and authenticated."

Note that the port's network link will remain inactive until it successfully authenticates with the configured RADIUS server using the selected EAP method and associated credentials.

During the initial provisioning of an IEEE 802.1X-enabled port for this system, it is recommended that the end user temporarily connects both the Fiber and Copper ports to an accessible network before selecting the Config button. This fail-safe procedure ensures continued access to the system's web management portal in the event that IEEE 802.1X authentication fails on the configured port.

Network Fiber/Copper Port - IEEE 802.1X: EAP-TLS Configuration

EAP-TLS employs mutual certificate-based authentication between the client and RADIUS server. This method requires specifying a client certificate, private key, and CA certificate. TLS offers the highest security level, and is recommended when an organizational public-key infrastructure (PKI) is available. By default, the systems will use self-signed certificates to encrypt the TLS tunnel. To upload organization-specific certificates, go to the Admin->Certificates sub-section.



1 IEEE 802.1x Security: Enable

2 Authentication: TLS

3 Identity

4 User cert: client.crt is present

5 CA cert: ca.crt is present

6 Private key: client.key is present

7 Private key password

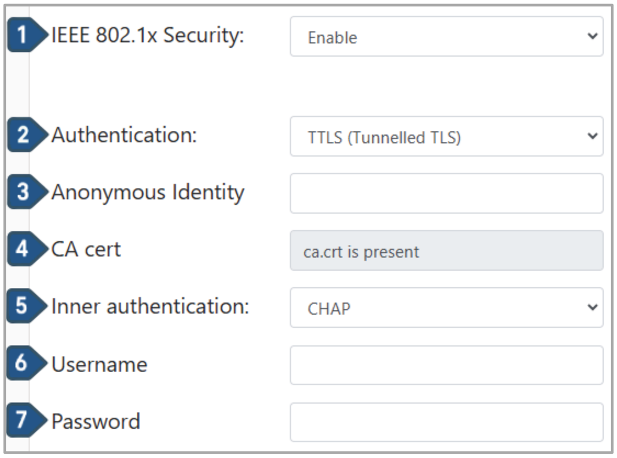
Network (Fiber/Copper Port) - IEEE 802.1X: EAP-TLS

Item	Parameter	Description
1	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control. This parameter must be set as Enable for the port to require RADIUS-based authentication before network access is granted.
2	`Authentication`	Specifies the EAP method used for verifying client credentials with a RADIUS server. Selecting TLS enables certificate-based mutual authentication between the client and RADIUS server.
3	`Identity`	Defines the client's identification string used during the TLS handshake. This parameter typically corresponds to the device or user identity registered on the RADIUS server that the Smart 8 Input Sensor / Smart 8 Relay Output is attempting to authenticate as.
4	`User cert`	Displays the current client certificate (client.crt) as a read-only field. When "client. crt is present" (default) is shown, a valid client certificate exists on the device's 802.1X supplicant certificate store. When "client.crt is not present" is displayed, it has been deleted at some point from the certificate store, which may be remediated by generating or uploading another client certificate.
5	`CA cert`	Displays the trusted Certificate Authority certificate (ca.crt) used to validate the RADIUS server's certificate. Shows "ca.crt is present" (default) when a valid CA certificate exists on the device's 802.1X supplicant certificate store, and "ca.crt is not present" when it has been deleted from the certificate store. This may be remediated by generating or uploading another CA certificate.
6	`Private key`	Displays the client's private key (client.key) associated with the uploaded user certificate. Shows "client.key is present" when valid, and "client.key is not present" when the key has been deleted from the 802.1x supplicant certificate store. A new key may be generated or uploaded.
7	`Private key password`	Specifies a varbind value that the trap must contain for the rule to trigger. If the Trap OID is blank, the rule will accept any varbind OID with this value.

Network Fiber/Copper Port - IEEE 802.1X: EAP-TTLS Configuration

EAP-TTLS (Tunneled TLS) and EAP-PEAP (Protected EAP) both implement an encrypted outer TLS tunnel to protect the exchange of authentication credentials. Once the TLS session is established, each protocol defines an "inner" authentication method that determines how user credentials are verified within the secure tunnel.

EAP-TTLS offers broader compatibility than EAP-PEAP by supporting multiple inner authentication formats, which includes both password-based methods (MD5, PAP) and challenge-response methods (CHAP, MSCHAPv2) for credential verification within the TLS tunnel. While MD5, PAP, and CHAP remain supported for backwards compatibility with legacy security implementations, it is advised to use MSCHAPv2 as the inner authentication format.



1 IEEE 802.1x Security: Enable

2 Authentication: TTLS (Tunnelled TLS)

3 Anonymous Identity

4 CA cert: ca.crt is present

5 Inner authentication: CHAP

6 Username

7 Password

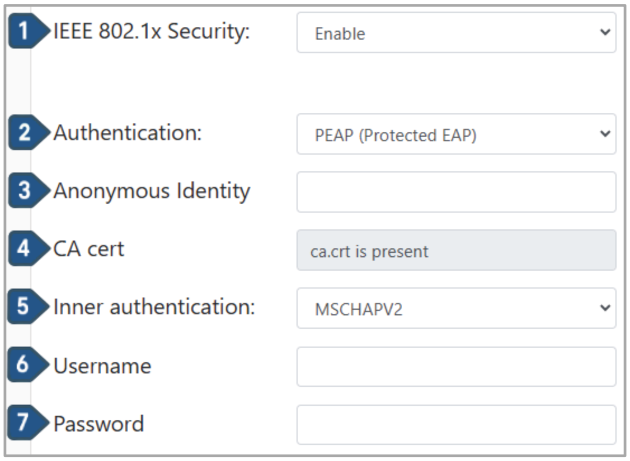
Network (Fiber/Copper Port) - IEEE 802.1X: EAP-TTLS

Item	Parameter	Description
1	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control. This parameter must be set as Enable for the port to require RADIUS-based authentication before network access is granted.
2	`Authentication`	Specifies the EAP method used for verifying client credentials with a RADIUS server. Selecting TTLS (Tunneled TLS) establishes an encrypted outer TLS tunnel to protect credential exchange between the client and RADIUS server.
3	`Anonymous Identity`	Defines an optional outer-identity string sent in the initial (unencrypted) EAP-Identity Request message. This is typically a placeholder (e.g., "anonymous"@domain) used to obscure the actual user identity until the TLS tunnel is established.
4	`CA cert`	Displays the trusted Certificate Authority certificate (ca.crt) used to validate the RADIUS server's certificate. Shows "ca.crt is present" (default) when a valid CA certificate exists on the device's 802.1X supplicant certificate store, and "ca.crt is not present" when it has been deleted from the certificate store. This may be remediated by generating or uploading another CA certificate.
5	`Inner Authentication`	Specifies the credential-based authentication method used inside the TLS tunnel for user verification. EAP-TTLS supports MSCHAPv2, PAP, CHAP, and MD5. The chosen method must match the RADIUS server's configured inner-authentication policy.
6	`Username`	Defines the user or device identity used during the inner authentication stage of the EAP-TTLS process. This parameter must correspond to an existing account that is recognized as valid by the RADIUS server.
7	`Password`	Defines the password associated with the configured Username. The password is encrypted within the secure TLS tunnel during transmission.

Network (Fiber/Copper Port) IEEE 802.1X: EAP-PEAP Configuration

EAP-PEAP (Protected EAP) implements an encrypted outer TLS tunnel similarly to EAP-TTLS, but it is designed primarily for integration with Microsoft Active Directory, or other credential-based authentication domains. After a secure TLS session is established, PEAP performs inner authentication using a secondary method.

In this system's implementation of EAP-PEAP, two inner authentication methods are supported: MSCHAPv2, which provides mutual authentication with a username and password, and GTC, which supports token-based or one-time-password (OTP) authentication.



1 IEEE 802.1x Security: Enable

2 Authentication: PEAP (Protected EAP)

3 Anonymous Identity

4 CA cert: ca.crt is present

5 Inner authentication: MSCHAPV2

6 Username

7 Password

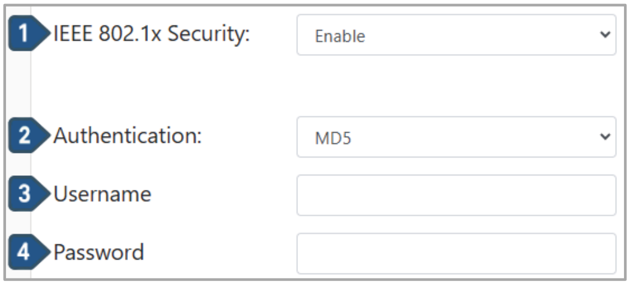
Network (Fiber/Copper Port) - IEEE 802.1X: EAP-PEAP

Item	Parameter	Description
1	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control. This parameter must be set as Enable for the port to require RADIUS-based authentication before network access is granted.
2	`Authentication`	Specifies the EAP method used for verifying client credentials with a RADIUS server. Selecting TTLS (Tunneled TLS) establishes an encrypted outer TLS tunnel to protect credential exchange between the client and RADIUS server.
3	`Anonymous Identity`	Defines an optional outer-identity string sent in the initial (unencrypted) EAP-Identity Request message. This is typically a placeholder (e.g., "anonymous"@domain) used to obscure the actual user identity until the TLS tunnel is established.
4	`CA cert`	Displays the trusted Certificate Authority certificate (ca.crt) used to validate the RADIUS server's certificate. Shows "ca.crt is present" (default) when a valid CA certificate exists on the device's 802.1X supplicant certificate store, and "ca.crt is not present" when it has been deleted from the certificate store. This may be remediated by generating or uploading another CA certificate.
5	`Inner Authentication`	Specifies the credential-based authentication method used inside the TLS tunnel for user verification. EAP-TTLS supports MSCHAPv2, PAP, CHAP, and MD5. The chosen method must match the RADIUS server's configured inner-authentication policy.
6	`Username`	Defines the user or device identity used during the inner authentication stage of the EAP-TTLS process. This parameter must correspond to an existing account that is recognized as valid by the RADIUS server.
7	`Password`	Defines the password associated with the configured Username. The password is encrypted within the secure TLS tunnel during transmission.

Network (Fiber/Copper Port) IEEE 802.1X: EAP-MD5 Configuration

EAP-MD5 and EAP-LEAP are both credential-based EAP authentication methods that rely on a username and password combination for identity verification. Both EAP methods transmit authentication data through a RADIUS server, require no certificates, and are considered obsolete. These methods are included solely for ensuring compatibility with older RADIUS implementations, and legacy network environments. Due to how they share identical configuration parameters and similar characteristics, they are presented together in this section.

EAP-MD5 is the simplest EAP method type, using a one-way challenge-response mechanism to validate user credentials. It does not provide mutual authentication or session encryption, and the underlying MD5 cryptography is deprecated.



1 IEEE 802.1x Security: Enable

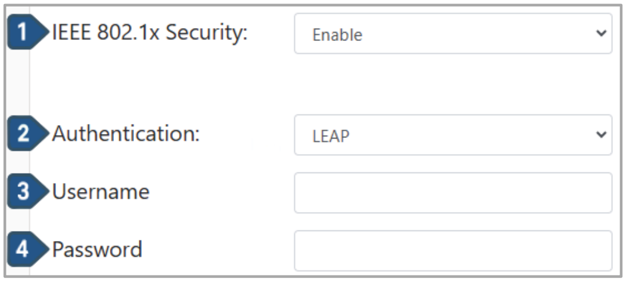
2 Authentication: MD5

3 Username

4 Password

Network (Fiber/Copper Port) - IEEE 802.1X: EAP-MD5

EAP-LEAP (Lightweight EAP) was developed by Cisco Systems to provide mutual authentication between an 802.1X client and RADIUS server. While it offers more protection than EAP-MD5, it is still considered deprecated and obsolete due to known security vulnerabilities in its underlying authentication protocol (MSCHAPv1).



1 IEEE 802.1x Security: Enable

2 Authentication: LEAP

3 Username

4 Password

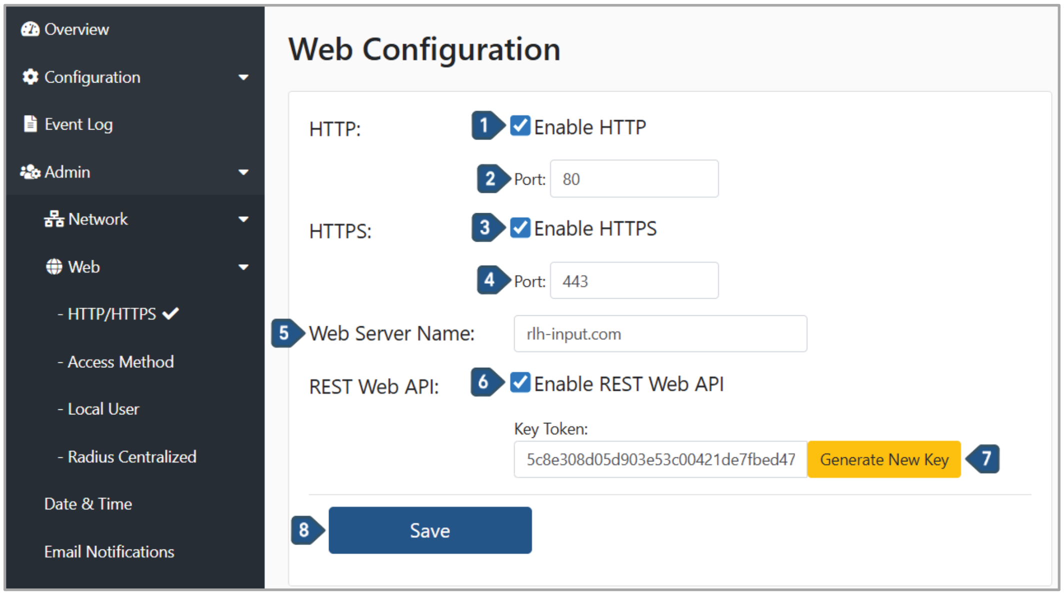
Network (Fiber/Copper Port) - IEEE 802.1X: EAP-LEAP

Item	Parameter	Description
1	`IEEE 802.1x Security`	Enables or disables IEEE 802.1X port-based authentication/access control. This parameter must be set as Enable for the port to require RADIUS-based authentication before network access is granted.
2	`Authentication`	Specifies the EAP method used for verifying client credentials with a RADIUS server. Selecting TTLS (Tunneled TLS) establishes an encrypted outer TLS tunnel to protect credential exchange between the client and RADIUS server.
3	`Username`	Defines the user or device identity that is sent to the RADIUS server for authentication. This value must correspond to a valid account on the RADIUS server or authentication database.
4	`Password`	Specifies the password associated with the configured Username. The password is transmitted to the RADIUS server for verification during the authentication exchange.

Web (HTTP/HTTPS) Configuration

The Web Configuration page defines how the system's embedded web server is accessed over the network. Both HTTP (insecure, unencrypted) and HTTPS (secure, encrypted) protocols can be independently enabled or disabled. Both HTTP and HTTPS are enabled by default, with HTTPS using the latest, most secure version of TLS (1.3).

The system also supports a REST API, which allows external applications and monitoring tools that can interpret the REST architecture to securely exchange I/O channel configuration and status data using HTTP or HTTPS. This REST API uses a randomly generated Key Token for authorization, which may be reviewed or re-generated through this webpage.



Web Configuration

HTTP: ☑ Enable HTTP

Port: 80

HTTPS: ☑ Enable HTTPS

Port: 443

Web Server Name: rlh-input.com

REST Web API: ☑ Enable REST Web API

Key Token: 5c8e308d05d903e53c00421de7fbed47

Web (HTTP/HTTPS) - Web Configuration

Item	Parameter	Description
1	`Enable HTTP`	Enables or disables access to the system's web interface through HTTP (Hypertext Transfer Protocol). When enabled, users can connect with an unencrypted HTTP connection (e.g., http://192.168.1.201)
2	`Port (HTTP)`	Defines the TCP port used for HTTP communication. The default port is 80.
3	`Enable HTTPS`	Enables or disables access to the system's web interface through HTTPS (Hypertext Transfer Protocol Secure). When enabled, users can connect with an encrypted HTTPS connection (e.g., https://192.168.1.201). This implementation of HTTPS uses the latest version of TLS (1.3).
4	`Port (HTTPS)`	Defines the TCP port used for HTTPS communication. The default port is 443.
5	`Web Server Name`	Specifies the Common Name used when generating self-signed TLS certificates for the HTTPS web server in the Certificates menu.
6	`Enable REST WEB API`	Enables the system's REST API interface, which may be used with HTTP and/or HTTPS.
7	`Generate New Key`	Generates a new 128-bit bearer token used in the "Authorization: Bearer <token>" header of REST API authentication requests. Generating a new token invalidates previous tokens from further use.
8	`Save`	Commits and applies all Web Configuration parameter setting changes.

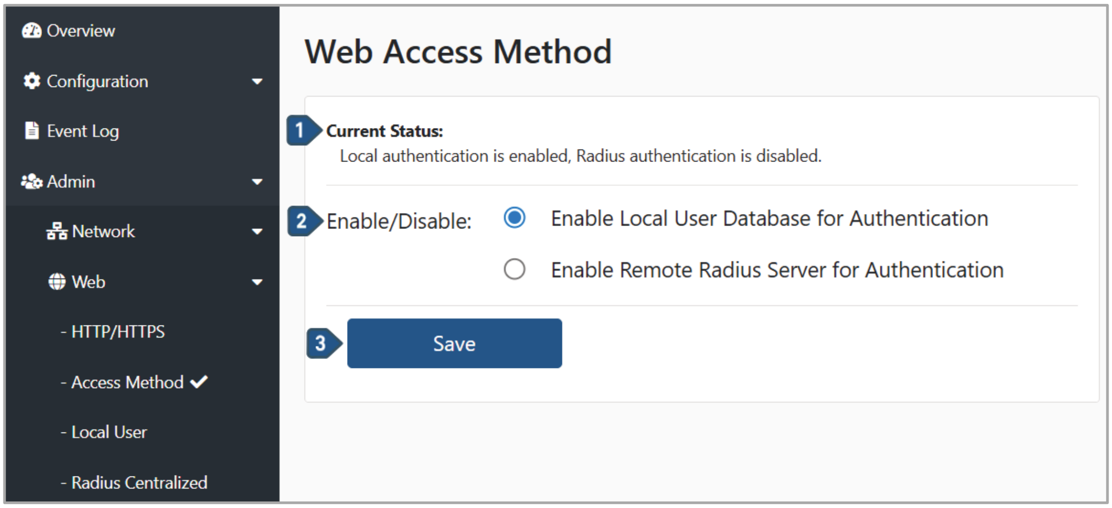
Web (Access Method) Configuration

The Web Access Method page defines how administrative users are authenticated when accessing the system's web management interface. The system supports two primary Web Access authentication methods:

1. **Local User Database Authentication:** Uses two locally-stored and configurable user accounts ("Admin", and optionally "Guest")
2. **Remote RADIUS Server Authentication:** Delegates login verification to a centralized RADIUS server for enterprise-managed user access and authentication

Only one authentication method may be active at a time. When switching between modes, existing login sessions will be terminated, and users must re-authenticate according to the newly-selected access method.

It is imperative that when enabling RADIUS authentication the RADIUS server parameters are correctly configured under Web (Radius Centralized). Otherwise, if the RADIUS server parameters are incorrect and Remote RADIUS Server Authentication is enabled, user access to the system will become locked.



Current Status:
Local authentication is enabled, Radius authentication is disabled.

Enable/Disable: ● Enable Local User Database for Authentication
○ Enable Remote Radius Server for Authentication

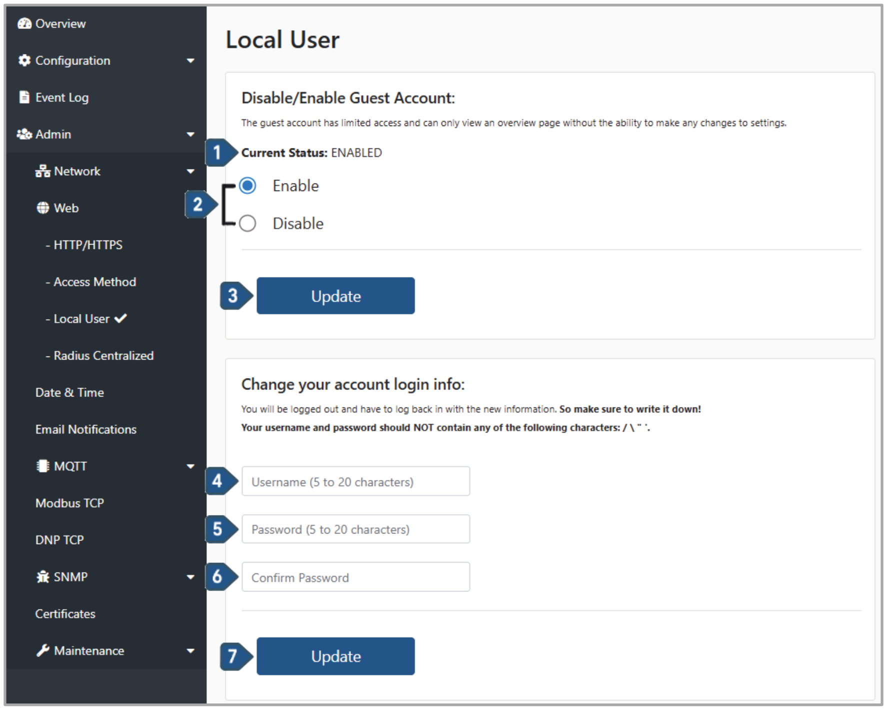
Web (Access Method) - Web Access Method Configuration

Item	Parameter	Description
1	`Current Status`	Displays the currently active Web Access authentication method. This status updates automatically when configuration changes are made to the authentication method, and saved. Only one Web Access authentication method will be enabled at once.
2	`Enable/Disable`	Toggles between the two available Web Access authentication methods: Enable Local User Database for Authentication for using local user accounts (Admin/Guest) Enable Remote Radius Server for Authentication for using a RADIUS server
3	`Save`	Applies and stores the selected Web Access authentication method. The web service restarts its authentication module to activate a new configuration; users will need to log in again after saving, when the current session's authentication method has changed.

Web (Local User) Accounts Configuration

The Local User page allows administrators to manage local login credentials for the device's web management interface.

When Local User Database Authentication is active (Admin -> Web -> Access Method), the settings contained on this page will determine whether the Guest account is enabled, and enable users to modify current passwords for either the Admin account, or the Guest account.



Local User

Disable/Enable Guest Account:

The guest account has limited access and can only view an overview page without the ability to make any changes to settings.

Current Status: ENABLED

● Enable
○ Disable

Change your account login info:

You will be logged out and have to log back in with the new information. **So make sure to write it down!**

Your username and password should NOT contain any of the following characters: / \ " `.

Username (5 to 20 characters)

Password (5 to 20 characters)

Confirm Password

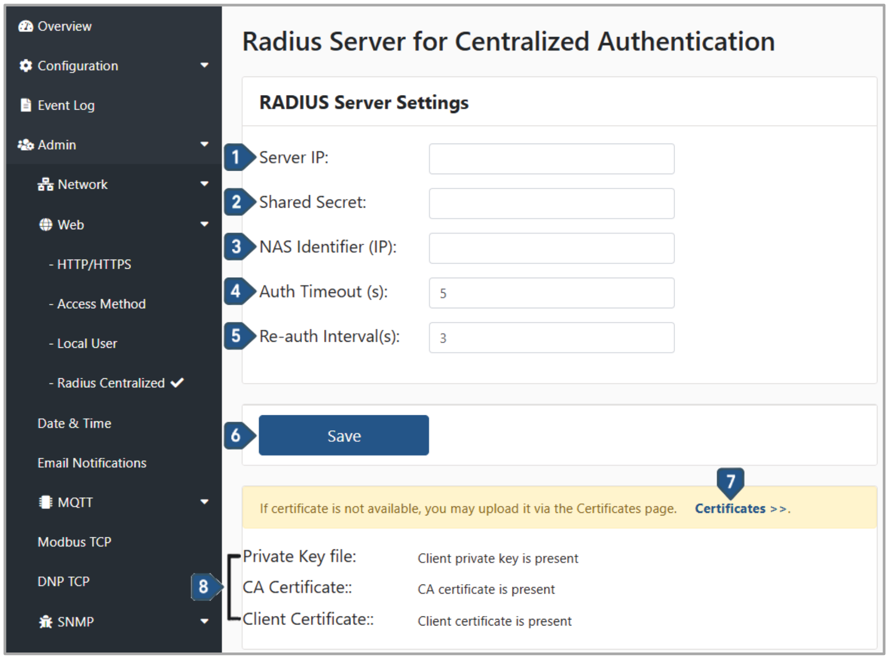
Web (Local User) - Local User Accounts Configuration

Item	Parameter	Description
1	`Current Status`	Displays whether the Guest account is currently Enabled or Disabled.
2	`Enable/Disable`	A Radio button selection for enabling or disabling the Guest account. This is set to Disable by default.
3	`Update (Guest Account)`	Saves the currently-toggled Enable/Disable radio button setting for the Guest account.
4	`Username`	Defines a new Username (5-20 characters) for the account that is currently logged in and committing the change. The Admin account can only update its own Username, and the Guest account can only update its own Username. The Username must not include special characters such as /, \, ", or '.
5	`Password`	Defines a new Password (5-20 characters) for the account that is currently logged in and committing the change. The Admin account can only update its own Password, and the Guest account can only update its own Password. The Password must not include special characters such as /, \, ", or '.
6	`Confirm Password`	Confirms the Password entry by reviewing the text string entered into this field, and the Password field
7	`Update (Account Login)`	Applies and commits the updated account credentials to either the Admin account, or the Guest account, depending on which of the two accounts issued the update.

Web (Radius Centralized) RADIUS Server Client Configuration

The Radius Centralized page defines the parameters required to connect the device to a RADIUS server for user authentication. This configuration works in conjunction with the Web Access Method page for enabling web-based authentication through an organization's RADIUS server, instead of the device's local user database.

If the RADIUS server requires mutual authentication, the corresponding Client Certificate, CA Certificate, and Private Key must be uploaded through the Certificates page. A direct link to the Certificates page is provided on this page.



Radius Server for Centralized Authentication

RADIUS Server Settings

Server IP:

Shared Secret:

NAS Identifier (IP):

Auth Timeout (s): 5

Re-auth Interval(s): 3

If certificate is not available, you may upload it via the Certificates page. Certificates >>.

Private Key file: Client private key is present

CA Certificate:: CA certificate is present

Client Certificate:: Client certificate is present

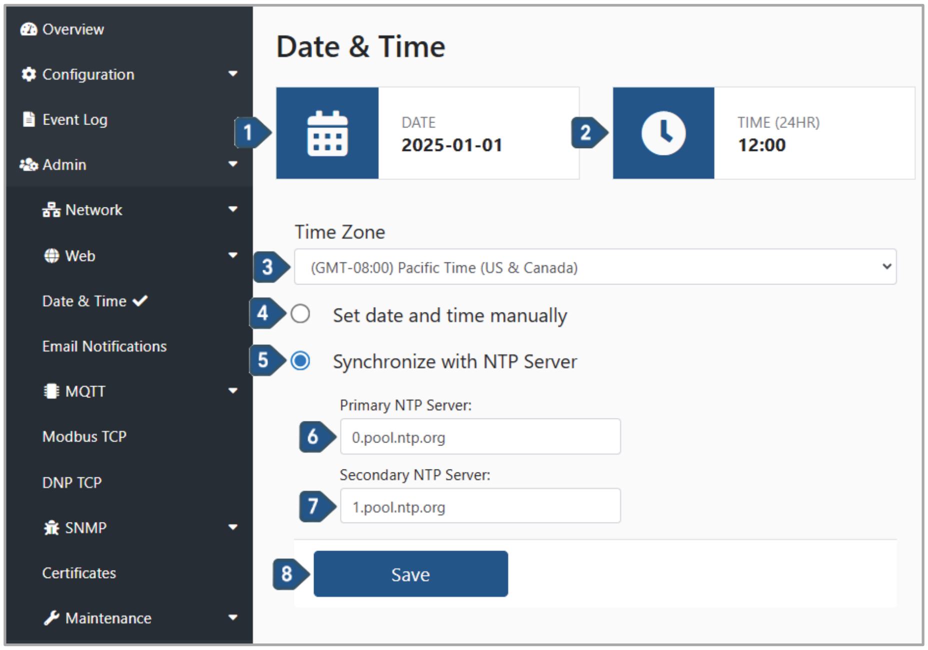
Web (Radius Centralized) - RADIUS Server Client Configuration

Item	Parameter	Description
1	Server IP	Specifies the IP address of the RADIUS server used for centralized authentication. The device communicates with this server to validate user credentials during login attempts.
2	Shared Secret	Defines the shared secret (authentication key) used between the device and the RADIUS server. This value must match the secret configured on the RADIUS server to establish a trusted connection.
3	NAS Identifier (IP)	Optionally specifies the Network Access Server (NAS) identifier, expressed as an IPv4 address, sent to the RADIUS server in each Access-Request message for identifying the device as a RADIUS client.
4	Auth Timeout(s)	Sets the number of seconds the device waits for a response from the RADIUS server before timing out an authentication request. The default is set as "5", for establishing 5 seconds as the timeout period.
5	Re-auth Interval(s)	Defines how frequently the device attempts to re-authenticate with the RADIUS server to maintain an active session. The default is set as "3", for establishing 3 seconds as the interval period.
6	Save	Applies and stores the current RADIUS Server Settings. These settings will take effect upon saving.
7	Certificates > >	Provides a shortcut link to the Certificates page, where administrators can generate (self-signed) or upload the Client Certificate, CA Certificate, and Private Key used for TLS-based RADIUS authentication.
8	Certificate/Key Status	Displays the presence of TLS certificates (Client, CA) and a private key file inside the device's Radius Client certificate store. These files are required for establishing secure RADIUS authentication.

Web (Date & Time) System Clock Configuration

The Date & Time page allows administrators to configure the device's internal system clock, and time synchronization method. The system clock affects the accuracy of time-stamped data reported internally, and to external platforms such as Network Management Systems (NMS/SNMP), email notification services (SMTP), and SCADA systems using DNP3.

Administrators can either manually set the date and time or configure automatic synchronization using Network Time Protocol (NTP) servers. When NTP synchronization is enabled, the device periodically contacts the configured NTP server(s) to maintain system clock accuracy.



Date & Time

1 DATE 2025-01-01

2 TIME (24HR) 12:00

Time Zone

3 (GMT-08:00) Pacific Time (US & Canada)

4 ○ Set date and time manually

5 ● Synchronize with NTP Server

Primary NTP Server:

6 0.pool.ntp.org

Secondary NTP Server:

7 1.pool.ntp.org

8 Save

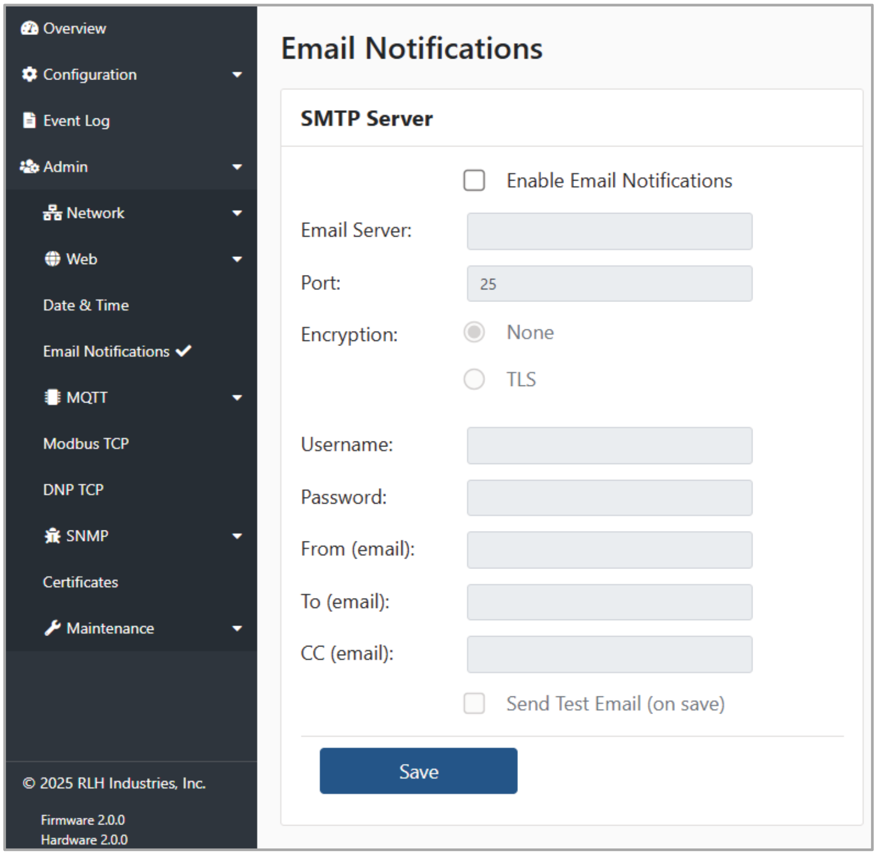
Date & Time - System Clock Configuration

Item	Parameter	Description
1	`Date`	Displays the device's current calendar date (YYYY-MM-DD) as a read-only field, referencing the date this is either manually configured locally, or automatically retrieved via an NTP server.
2	`Time (24HR)`	Displays the device's system clock time in a 24-hour format (HH:MM) as a read-only field.
3	`Time Zone`	Selects the local time zone applied to the system clock. Options include all IANA-defined time zones.
4	`Set date and time manually`	Enables manual entry of date and time values. When selected, a "Date" and "Time" field will propagate.
5	`Sychronize with NTP Server`	Enables automatic time synchronization by using Network Time Protocol (NTP). When selected, the device periodically contacts one or more NTP servers to maintain an accurate system clock.
6	`Primary NTP Server`	Defines the primary NTP server (hostname or IP address). The device attempts to synchronize with this server first. This parameter's default value, 0.pool.ntp.org, is a public NTP server.
7	`Secondary NTP Server`	Defines an optional backup NTP server (hostname or IP address. The device uses this server if the primary NTP server is unavailable. This parameter's default value, 1.pool.ntp.org, is a public NTP server.
8	`Save`	Saves all modified date, time, and NTP server parameters. The new settings are applied immediately.

Web (Email Notifications) SMTP Server Configuration

The Email Notifications page defines the parameters used by the system to send automated email alerts for I/O event changes or System Pairing faults, when enabled. The system supports standard email delivery by connecting to external servers that use Simple Mail Transfer Protocol (SMTP), and can operate with either unencrypted (plaintext) or encrypted (TLS 1.3) forms of mail delivery.

When email notifications are enabled, messages are sent automatically to the configured recipient addresses when system-defined events (I/O changes, System Pairing faults, test emails) occur. Administrators must configure the email server address, authentication credentials, and sender/recipient addresses. TLS encryption should be enabled, when supported by the email server, to ensure secure email transmission.



Email Notifications

SMTP Server

□ Enable Email Notifications

Email Server:

Port: 25

Encryption: ● None ○ TLS

Username:

Password:

From (email):

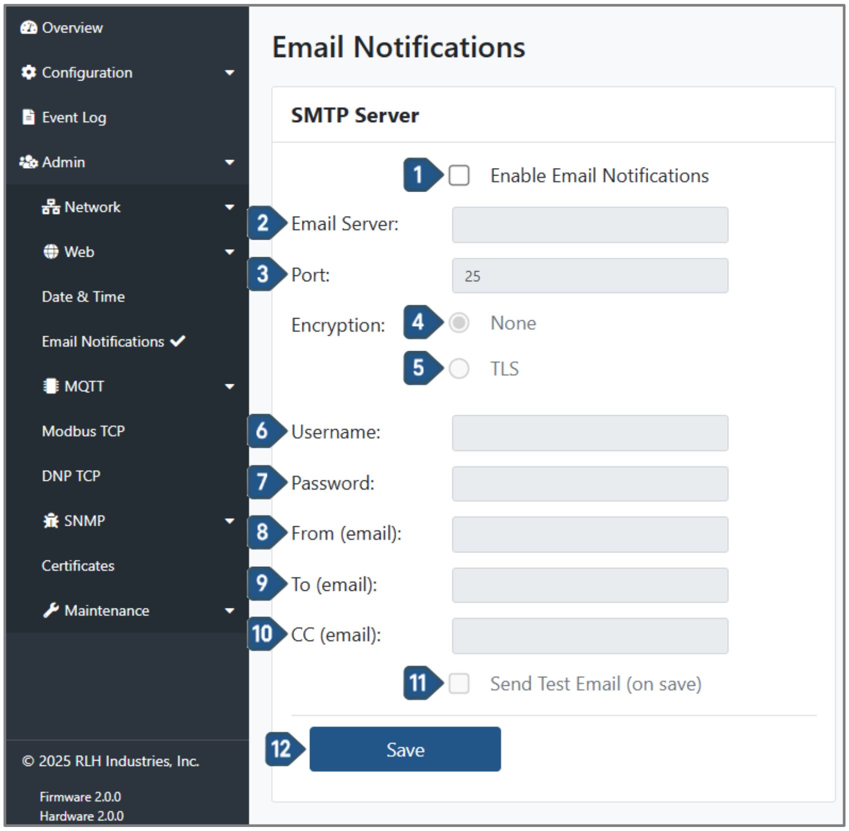
To (email):

CC (email):

□ Send Test Email (on save)

Email Notifications - SMTP Server Configuration

Web (Email Notifications) SMTP Server Configuration



Email Notifications

SMTP Server

1 □ Enable Email Notifications

2 Email Server:

3 Port: 25

Encryption: 4 ● None

5 ○ TLS

6 Username:

7 Password:

8 From (email):

9 To (email):

10 CC (email):

11 □ Send Test Email (on save)

12 Save

Email Notifications - SMTP Server Configuration

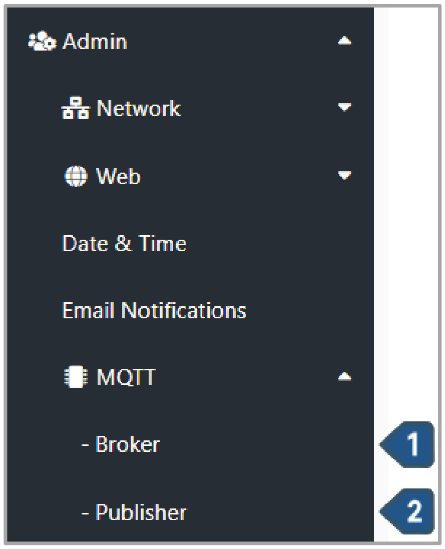
Item	Parameter	Description
1	`Enable Email Notifications`	Activates or deactivates the system's email notification service.
2	`Email Server`	Specifies the hostname or IP address of the SMTP mail server used for outgoing emails.
3	`Port`	Defines the SMTP server port used for sending emails. The default value is 25, for unencrypted SMTP traffic. For TLS-encrypted traffic, typically port 465 or 587 is used.
4	`Encryption (None)`	Selects unencrypted email transmission.
5	`Encryption (TLS)`	Enables Transport Layer Security (TLS) encryption for SMTP communication with the outbound email server. TLS must be supported by the configured email server for this setting to apply successfully.
6	`Username`	Defines the account username used to authenticate with the configured SMTP server.
7	`Password`	Defines the password associated with the configured SMTP username.
8	`From (email)`	Defines the sender address that will appear in outgoing email notifications.
9	`To (email)`	Defines the primary recipient email address for system notifications. Only one email address may be entered.
10	`CC (email)`	Specifies an additional recipient email address to receive system notifications. Only address may be entered.
11	`Send Test Email (on save)`	When enabled, selecting Save sends a test email to the recipient addresses specified in the To (email) and CC (email) fields. After saving, this field returns to a disabled state.
12	`Save`	Applies and stores all SMTP configuration parameters. If Send Test Email (on save) is enabled, a test message is sent to the configured recipients immediately after saving.

MQTT (Navigation Panel) Overview

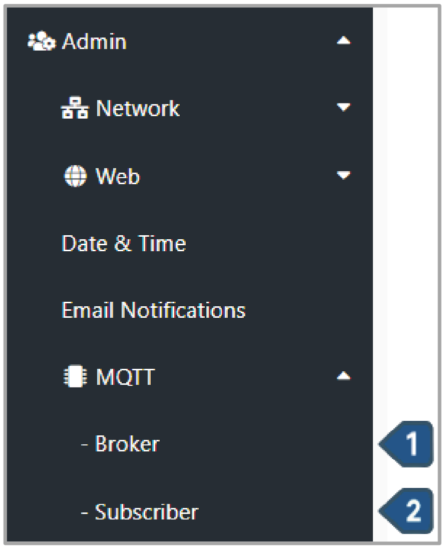
The MQTT Navigation Panel provides access to configuration pages for the systems' implementation of Message Queuing Telemetry Transport (MQTT), a protocol widely used in IoT and automation systems. This primarily enables I/O monitoring and control through external IoT dashboards.

In addition to IoT dashboard integration, MQTT allows Smart 8 Input Sensors to control Smart 8 Relay Outputs through the same system topology formats supported by System Pairing ("One-to-One", "One-to-Many", "Many-to-One"). MQTT's lightweight publish/subscribe architecture also enables multiple Smart 8 Input Sensors to publish I/O updates across multiple Smart 8 Relay Outputs in a scalable, "Many-to-Many", control relationship.

Both the Smart 8 Input Sensor and Smart 8 Relay Output include a configurable Broker page for hosting an embedded MQTT broker to distribute messages. Otherwise, an external broker may be used. The Smart 8 Input Sensor uniquely includes a Publisher page for configuring how Digital Input states are published to MQTT topics, while the Smart 8 Relay Output uniquely includes a Subscriber page for defining how the device subscribes to MQTT topics published by other MQTT publisher clients (i.e., Smart 8 Input Sensors, third-party MQTT publishers).



MQTT - Navigation Panel (Smart 8 Input Sensor)



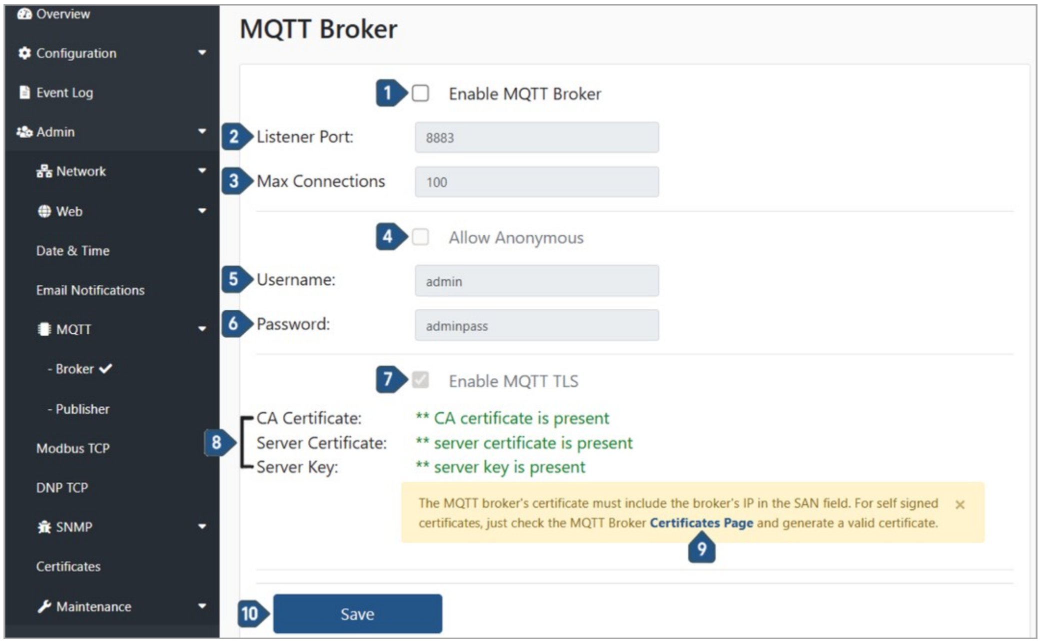
MQTT- Navigation Panel (Smart 8 Relay Output)

Item	Parameter	Description
1	`Broker`	Opens the MQTT Broker configuration page, where the device can enable and configure an embedded MQTT broker for message distribution.
2	`Publisher (Smart 8 Input Sensor)`	Opens the MQTT Publisher configuration page, where the Smart 8 Input Sensor can publish Digital Input states to defined MQTT topics through a connected MQTT broker.
2	`Subscriber (Smart 8 Relay Output)`	Opens the MQTT Subscriber configuration page, where the Smart 8 Relay Output subscribes to MQTT topics with messages published by Smart 8 Input Sensors and/or third-party publishers.

MQTT (Broker) Configuration

The MQTT Broker page allows the device to operate its own embedded MQTT broker for facilitating message distribution between MQTT publishers and subscribers, without the need for connecting to an external broker.

The broker can operate in an anonymous or authenticated mode, and supports TLS encryption for secure message transportation when certificates are present.



MQTT Broker

1 □ Enable MQTT Broker

2 Listener Port: 8883

3 Max Connections 100

4 □ Allow Anonymous

5 Username: admin

6 Password: adminpass

7 ☑ Enable MQTT TLS

8 CA Certificate: ** CA certificate is present

Server Certificate: ** server certificate is present

Server Key: ** server key is present

The MQTT broker's certificate must include the broker's IP in the SAN field. For self signed certificates, just check the MQTT Broker **Certificates Page** and generate a valid certificate. ×

MQTT Broker Configuration

Item	Parameter	Description
1	`Enable MQTT Broker`	Activates the embedded MQTT broker service. When enabled, the devices begin listening for MQTT client connections on the configured listener port.
2	`Listener Port`	Defines the TCP port the broker uses to accept inbound MQTT client connections. Standard listener ports for MQTT are 1883 for unencrypted connections, and 8883 for encrypted (TLS) connections.
3	`Max Connections`	Sets the maximum number of concurrent MQTT clients that may connect to the broker.
4	`Allow Anonymous`	When enabled, the broker allows clients to connect without a username or password. When disabled, the Username and Password parameters are automatically removed from the webpage.
5	`Username`	Defines the username required for MQTT clients when Allow Anonymous authentication is disabled.
6	`Password`	Defines the password associated with the configured MQTT broker username.
7	`Enable MQTT TLS`	Enables Transport Layer Security (TLS) encryption for MQTT communication through the broker. When active, the broker encrypts all message between itself and connected clients using the certificates and private key present in the device's MQTT Broker certificate store.
8	`Certificate Status`	Displays the presence of TLS certificates (Client, CA) and private key file inside the device's MQTT Broker certificate store. These files are required for establishing secure MQTT communication.
9	`Certificate Page`	Provides a shortcut link to the Certificates page, where administrators can generate (self-signed) or upload the Client Certificate, CA Certificate, and Private Key used for TLS-based MQTT communication.
10	`Save`	Saves all MQTT Broker parameters, and applies the configuration changes immediately.

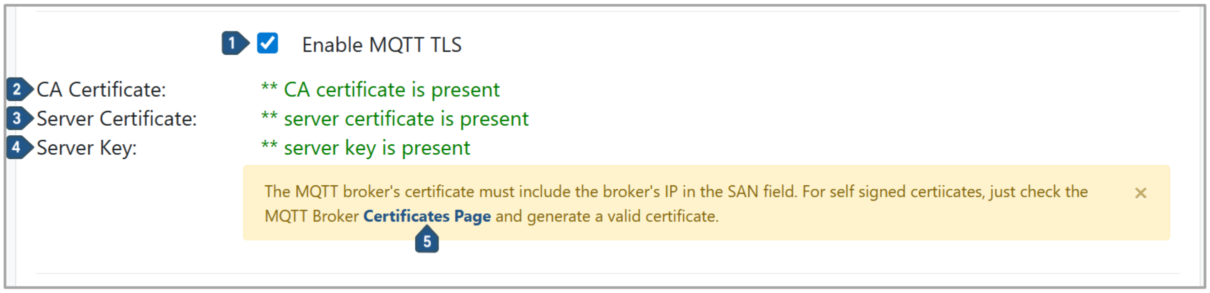
[Admin] MQTT (Broker) - MQTT over TLS (MQTTS) Broker Configuration

Enabling MQTT over TLS (MQTTS) encrypts all MQTT communications between connected MQTT clients (publishers, subscribers) and the MQTT broker using TLS/SSL certificates.

When "Enable MQTT TLS" is enabled, the broker listens for secure connections on the configured Listener Port (default 8883 for MQTTS), and requires valid X.509 certificates for authentication and session encryption

The Certificates page may be accessed directly from this screen via the highlighted shortcut link present on

Ref #5 of the below screenshot. In this page, administrators can upload existing certificates, generate self signed certificates, or download the default configuration file (broker-server.cnf) used when creating a broker's server certificate (server.crt).



1 ☑ Enable MQTT TLS

2 CA Certificate: ** CA certificate is present

3 Server Certificate: ** server certificate is present

4 Server Key: ** server key is present

The MQTT broker's certificate must include the broker's IP in the SAN field. For self signed certiicates, just check the MQTT Broker **Certificates Page** and generate a valid certificate. ×

5

Item	Parameter	Description
1	`Enable MQTT Broker`	Enables Transport Layer Security (TLS) encryption for MQTT communication through the broker. When active, the broker encrypts all message between itself and connected clients using the certificates (server, CA) and private key (server) present in the device's MQTT Broker certificate store.
2	`CA Certificate`	Indicates whether a trusted Certificate Authority (CA) certificate (ca.crt) is present on the device. The CA must be the issuer (or within the trust chain) of the broker's server certificate, which contains the broker's IP address, to allow MQTT clients to validate the broker during the TLS handshake.
3	`Server Certificate`	Displays the presence of the broker's signed server certificate (server.crt). This certificate identifies the broker to MQTT clients, and must include the broker's IP address in the Subject Alternative Name (SAN) field for MQTT clients to confirm they are connecting to the intended broker.
4	`Server Key`	Indicates the presence of the broker's private key (server.key) associated with the server certificate (server.crt). This key remains stored securely on the device's MQTT Broker certificate store for completing the TLS handshake.
5	`Certificates Page`	A shortcut link to the Certificates page, where administrators can upload organization-issued certificates, or generate self-signed CA certificates, server certificates and private keys for the MQTT Broker certificate store. The Certificates page also provides a downloadable broker-server.cnf configuration file, which may be used for generating self-signed broker server certificates signed by a designated CA.

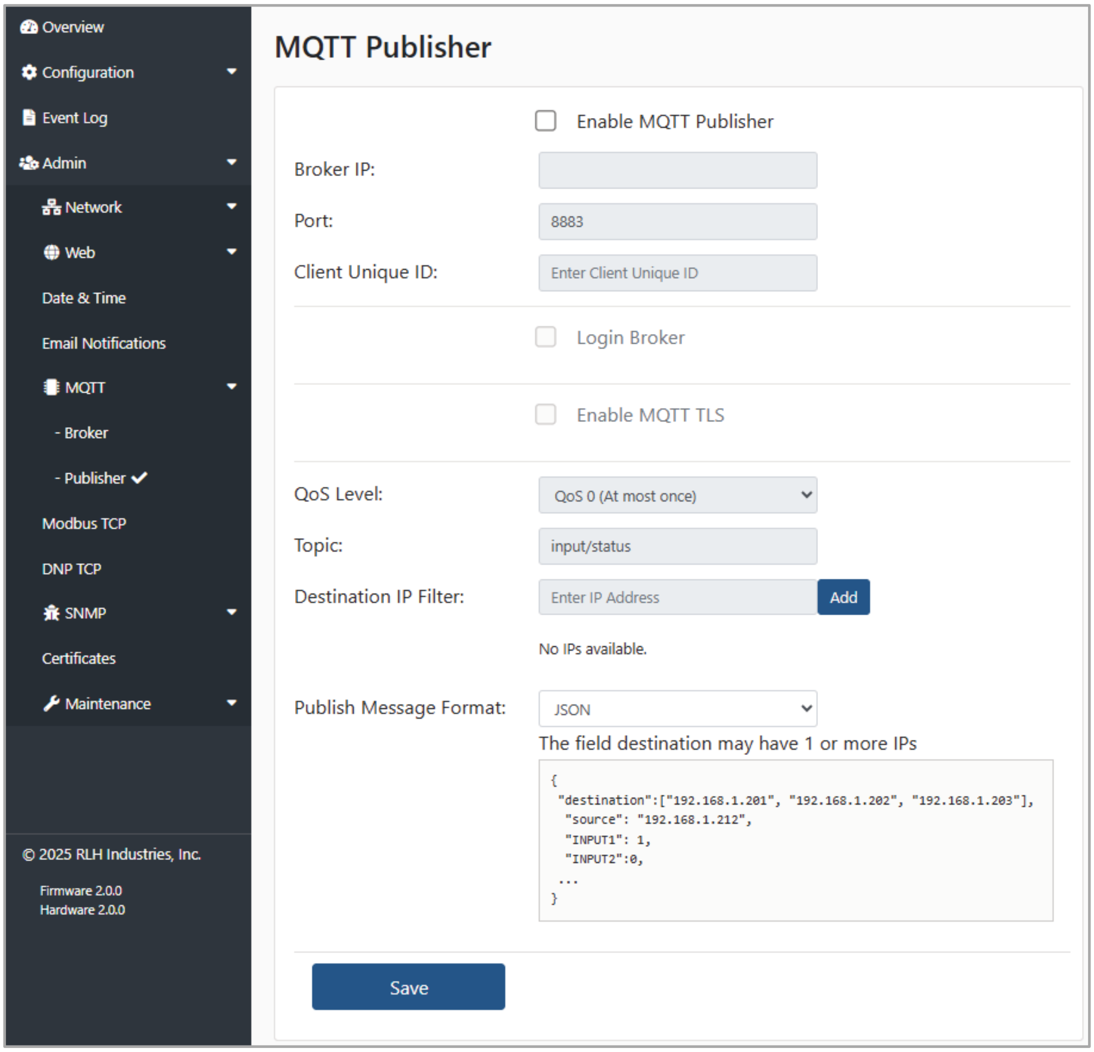
The Certificates page may be accessed directly from this screen via the highlighted shortcut link present on Ref #5 of the below screenshot. In this page, administrators can upload existing certificates, generate self signed certificates, or download the default configuration file (broker-server.cnf) used when creating a broker's server certificate (server.crt).

MQTT (Publisher) Configuration

The MQTT Publisher page allows the Smart 8 Input Sensor to act as an MQTT client, publishing Digital Input to a specified MQTT broker. Digital Input state changes are transmitted to user-specified MQTT topics that other devices (e.g., Smart 8 Relay Output) or services (e.g., IoT dashboards) may subscribe to.

This page defines the parameters for establishing a connection to the MQTT broker, including its IP address, port, client ID, authentication credentials, and TLS encryption. It also specifies how message payloads are formatted (JSON or Plain Text), and to which whitelisted IP addresses the Smart 8 Input Sensor will publish.

System Pairing is not required for MQTT publishing; however, only Digital Inputs with "Enable System Link Syncing" enabled on their channel's configuration page are reported in the MQTT payload.



MQTT Publisher

□ Enable MQTT Publisher

Broker IP:

Port: 8883

Client Unique ID: Enter Client Unique ID

□ Login Broker

□ Enable MQTT TLS

QoS Level: QoS 0 (At most once)

Topic: input/status

Destination IP Filter: Enter IP Address [Add]

No IPs available.

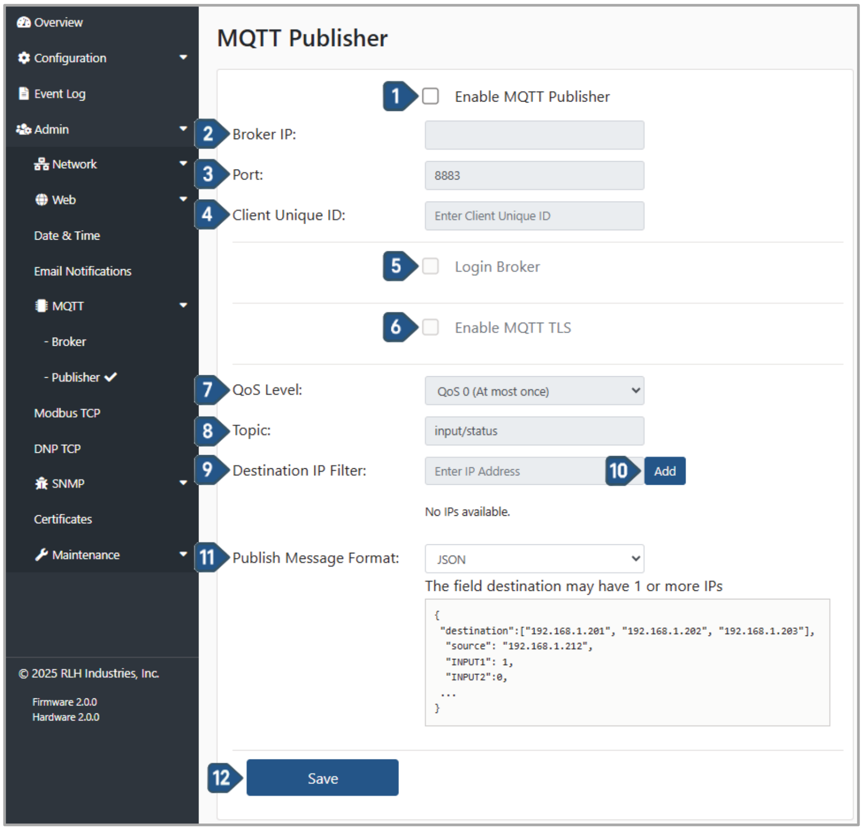
Publish Message Format: JSON

The field destination may have 1 or more IPs

```
{
 "destination":["192.168.1.201", "192.168.1.202", "192.168.1.203"],
  "source": "192.168.1.212",
  "INPUT1": 1,
  "INPUT2":0,
 ...
}
```

MQTT (Publisher) - MQTT Publisher Configuration

MQTT (Publisher) Configuration



MQTT Publisher

□ Enable MQTT Publisher

Broker IP:

Port: 8883

Client Unique ID: Enter Client Unique ID

□ Login Broker

□ Enable MQTT TLS

QoS Level: QoS 0 (At most once)

Topic: input/status

Destination IP Filter: Enter IP Address

No IPs available.

Publish Message Format: JSON

The field destination may have 1 or more IPs

```
{
 "destination":["192.168.1.201", "192.168.1.202", "192.168.1.203"],
  "source": "192.168.1.212",
  "INPUT1": 1,
  "INPUT2":0,
 ...
}
```

MQTT Publisher Configuration

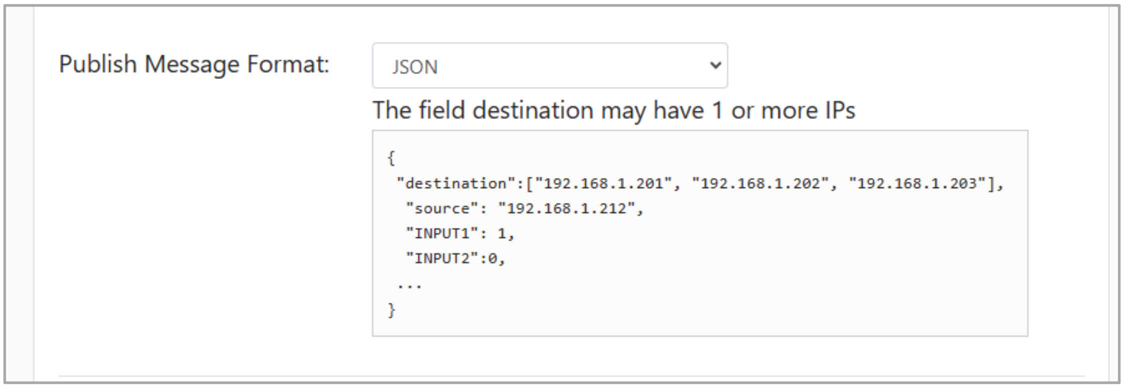
Item	Parameter	Description
1	`Enable MQTT Publisher`	Activates or deactivates the system's email notification service.
2	`Broker IP`	Specifies the hostname or IP address of the SMTP mail server used for outgoing emails.
3	`Port`	Defines the SMTP server port used for sending emails. The default value is 25, for unencrypted SMTP traffic. For TLS-encrypted traffic, typically port 465 or 587 is used.
4	`Client Unique ID`	Selects unencrypted email transmission.
5	`Login Broker`	Enables Transport Layer Security (TLS) encryption for SMTP communication with the outbound email server. TLS must be supported by the configured email server for this setting to apply successfully.
6	`Enable MQTT TLS`	Defines the account username used to authenticate with the configured SMTP server.
7	`QoS Level`	Defines the password associated with the configured SMTP username.
8	`Topic`	Defines the sender address that will appear in outgoing email notifications.
9	`Destination IP Filter`	Defines the primary recipient email address for system notifications. Only one email address may be entered.
10	`Add`	Specifies an additional recipient email address to receive system notifications. Only one email address may be entered.
11	`Publish Message Format`	When enabled, selecting Save sends a test email to the recipient addresses specified in the To (email) and CC (email) fields. After saving, this field returns to a disabled state.
12	`Save`	Applies and stores all SMTP configuration parameters. If Send Test Email (on save) is enabled, a test message is sent to the configured recipients immediately after saving.

MQTT (Publisher) Publish Message Format Configuration

The Publish Message Format parameter defines how the MQTT publisher service (Smart 8 Input Sensor) structures each MQTT payload before transmitting it to broker, for its reception by the underlying subscriber clients (e.g., Smart 8 Relay Output). The Smart 8 Relay Output, when enabling the MQTT subscriber service, automatically accepts either payload format.

Two message formats are supported: JSON, and Plain Text. JSON is the default configured message format.

MQTT (Publisher) - Publish Message Format (Plain Text)When JSON is selected, each MQTT payload is formatted as a JavaScript Object Notation (JSON) string. This representation is preferred for use with modern IoT dashboards, SCADA middleware, and Cloud services are designed to parse JSON key/value pairs.



Publish Message Format: JSON

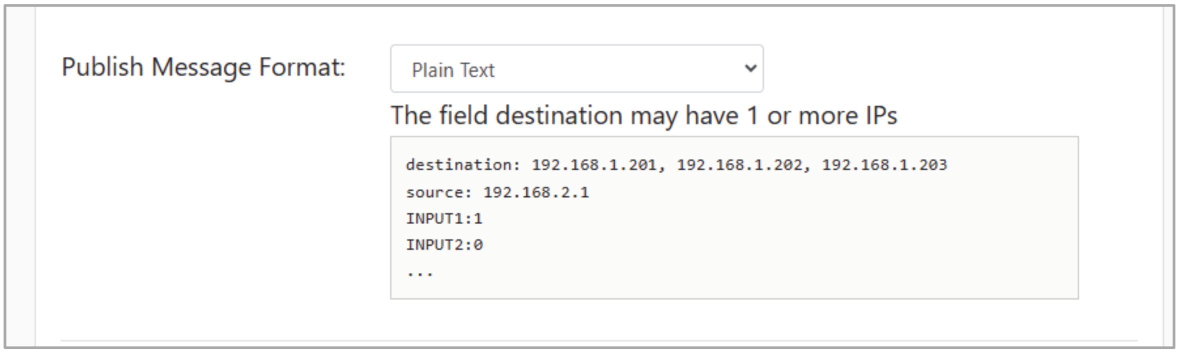
The field destination may have 1 or more IPs

```
{
 "destination":["192.168.1.201", "192.168.1.202", "192.168.1.203"],
  "source": "192.168.1.212",
  "INPUT1": 1,
  "INPUT2":0,
 ...
}
```

MQTT Publisher Configuration: Publish Message Format (JSON)

JSON Key	Description
`destination`	Lists the MQTT subscriber IP address(es) authorized to receive this update, as defined in the Destination IP Filter.
`source`	Identifies the Smart 8 Input Sensor's IP address as the MQTT publishing source that generated the payload.
`INPUT[#]`	Reports the ON/OFF state (1 = ON, 0 = OFF) of each Digital Input channel at the time of the message publication.

When Plain Text is selected, MQTT messages are delivered as simple ASCII strings separated by newline characters. This format is advantageous for legacy integration scenarios or basic clients that cannot parse JSON, such as terminal monitors or constrained, embedded subscriber clients.



Publish Message Format: Plain Text

The field destination may have 1 or more IPs

```
destination: 192.168.1.201, 192.168.1.202, 192.168.1.203
source: 192.168.2.1
INPUT1:1
INPUT2:0
...
```

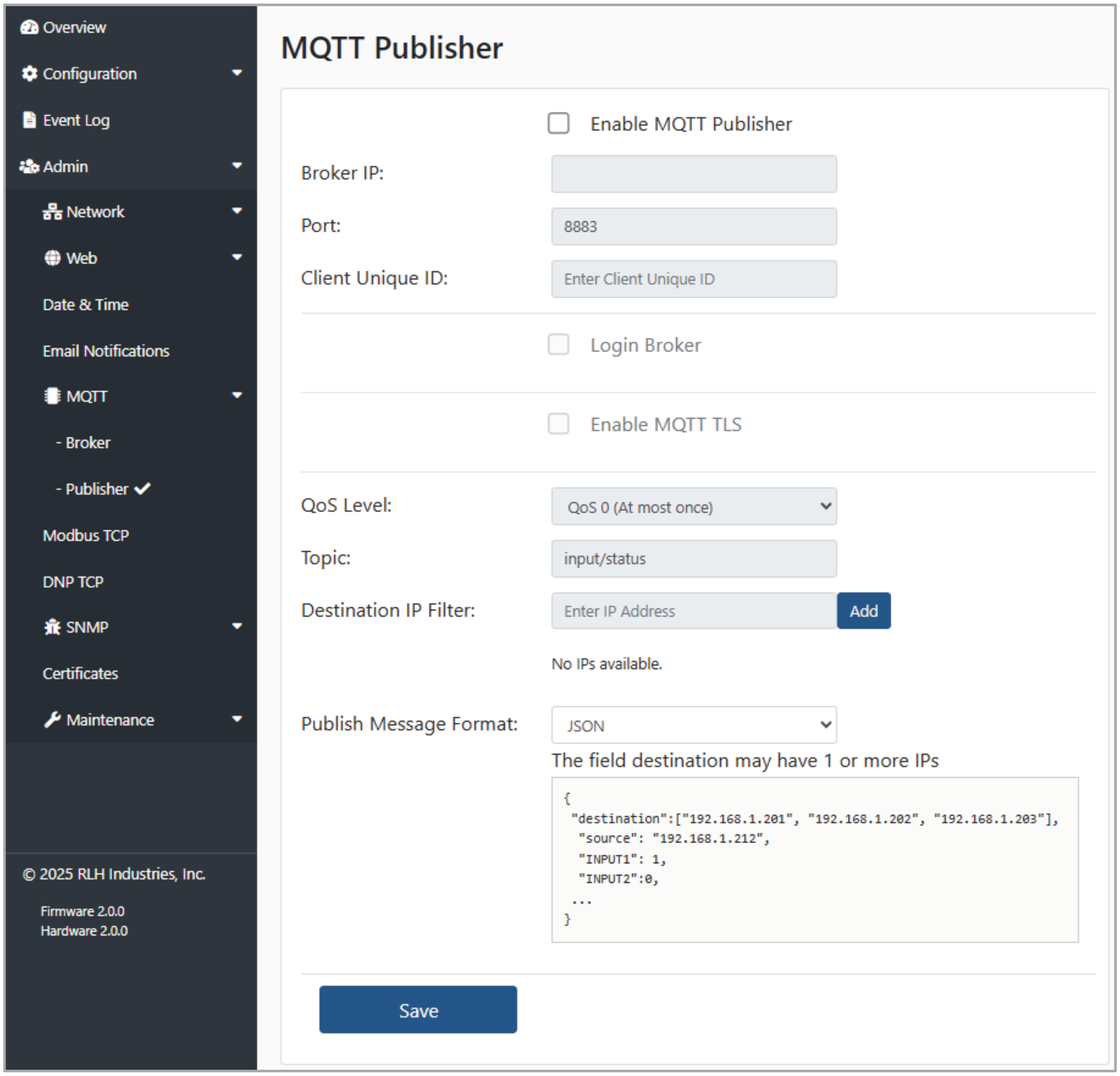
MQTT Publisher Configuration: Publish Message Format (Plain Text)

MQTT (Subscriber) Overview

The MQTT Subscriber page allows the Smart 8 Relay Output to act as an MQTT client, subscribing to Digital Input topics published by a Smart 8 Input Sensor acting as an MQTT publisher, or a third-party MQTT publisher that structures its payload in a compatible format. When the MQTT subscriber service is enabled, and a subscribed receives a message, Relay Outputs may be updated in accordance with the payload contents.

This page defines the parameters for establishing a connection to the MQTT broker, including its IP address, port, client ID, authentication credentials, and TLS encryption. It also specifies how incoming message payloads are interpreted (JSON or plaintext) for controlling Relay Outputs, and form whitelisted IP addresses the Smart 9 Relay Output may accept messages from.

The MQTT subscriber service operates independently of System Pairing, but only Relay Outputs with a "Mapping to the Input." Relay control parameter selected will act on the received payloads.



MQTT Publisher

□ Enable MQTT Publisher

Broker IP:

Port: 8883

Client Unique ID: Enter Client Unique ID

□ Login Broker

□ Enable MQTT TLS

QoS Level: QoS 0 (At most once)

Topic: input/status

Destination IP Filter: Enter IP Address

No IPs available.

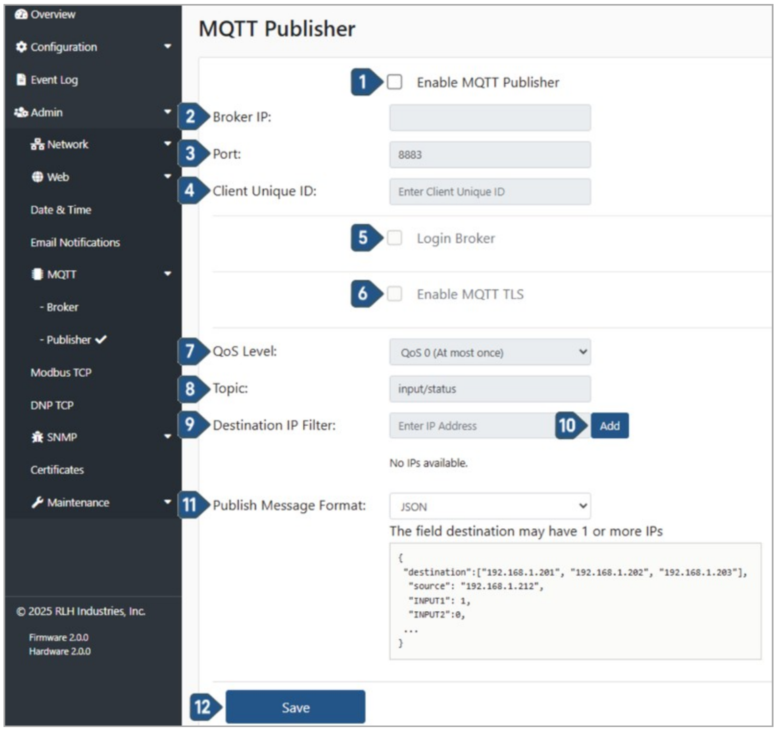
Publish Message Format: JSON

The field destination may have 1 or more IPs

```
{
 "destination":["192.168.1.201", "192.168.1.202", "192.168.1.203"],
  "source": "192.168.1.212",
  "INPUT1": 1,
  "INPUT2":0,
 ...
}
```

MQTT Subscriber Overview

MQTT (Subscriber) Configuration



MQTT Publisher

□ Enable MQTT Publisher

Broker IP:

Port: 8883

Client Unique ID: Enter Client Unique ID

□ Login Broker

□ Enable MQTT TLS

QoS Level: QoS 0 (At most once)

Topic: input/status

Destination IP Filter: Enter IP Address Add

No IPs available.

Publish Message Format: JSON

The field destination may have 1 or more IPs

```
{
 "destination":["192.168.1.201", "192.168.1.202", "192.168.1.203"],
  "source": "192.168.1.212",
  "INPUT1": 1,
  "INPUT2":0,
 ...
}
```

Save

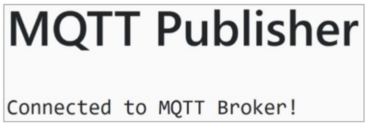
MQTT Subscriber Configuration

Item	Parameter	Description
1	`Enable MQTT Publisher`	Activates the MQTT Publisher service, allowing the Smart 8 Input Sensor to transmit Digital Input state changes to the configured MQTT broker.
2	`Broker IP`	Specifies the IP address or hostname of the MQTT broker to which the Smart 8 Input Sensor will publish.
3	`Port`	Specifies the TCP port used to connect to the MQTT broker. Port 1883 is typically used for unencrypted communcication, while port 8883 is used for MQTT with TLS.
4	`Client Unique ID`	Identifies the Smart 8 Input Sensor as a unique MQTT client on the network. This ID must be distinct than other MQTT clients to avoid connection conflicts.
5	`Login Broker`	When enabled, the Smart 8 Input Sensor uses a configured username and password to authenticate with the broker. If disabled, the connection is attempted anonymously. If enabled, a Username and Password field will populate onto the webpage.
6	`Enable MQTT TLS`	Enables Transport Layer Security (TLS) encryption for publishing messages securely to the MQTT broker. This requires a valid CA certificate in the Smart 8 Input Sensor's MQTT Publisher certificate store. Enabling this parameter populates a field for the CA certificate's status, and instructions for generating CA certificates used with MQTT TLS.
7	`QoS Level`	Sets the MQTT Quality of Service (QoS) level for message delivery. Options include QoS 0 (At most once), QoS 1 (At least once), and QoS 2 (Exactly once).
8	`Topic`	Defines the MQTT topic to which the Smart 8 Input Sensor will publish messages (e.g., "input/status"). The MQTT publisher and subscriber clients must use identical topic names for messages to be exchanged successfully.
9	`Destination IP Filter`	Specifies a list of MQTT subscriber client(s) the Smart 8 Input Sensor may publish to, per their IP addresses. Enter an IP address, and select Add, to add it to the list.
10	`Add`	Adds an IP address into the Destination IP Filter list.
11	`Publish Message Format`	Specifies the data format used for published MQTT payloads. Options include JSON (structured data) or Plain Text (simplified message body).
12	`Save`	Stores and immediately applies all MQTT Publisher settings.

MQTT (Publisher/Subscriber) Debug Messages Overview

When the MQTT publisher or subscriber service is enabled, the MQTT Publisher (Smart 8 Input Sensor) and MQTT Subscriber (Smart 8 Relay Output) pages will display debug messages beneath the title header pertaining to its connection status with the specified MQTT broker. Debug messages are updated dynamically, in real-time.

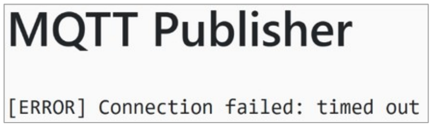
The examples below illustrate common debug messages that appear on both the MQTT Publisher and MQTT Subscriber pages, with the MQTT Publisher page shown as the reference example.



MQTT Publisher

```
Connected to MQTT Broker!
```

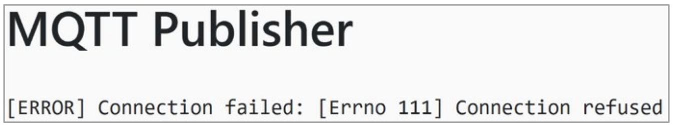
Debug Message: Connected to MQTT Broker!



MQTT Publisher

```
[ERROR] Connection failed: timed out
```

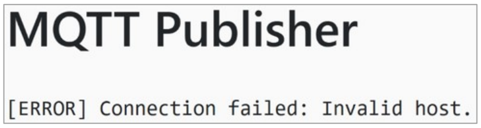
Debug Message: timed out



MQTT Publisher

```
[ERROR] Connection failed: [Errno 111] Connection refused
```

Debug Message: [Errno 111] Connection Refused



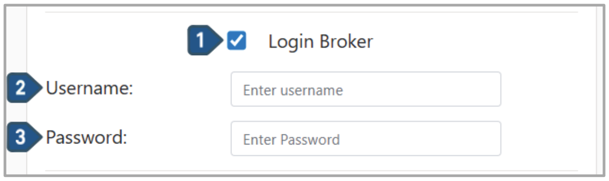
MQTT Publisher

```
[ERROR] Connection failed: Invalid host.
```

Debug Message: Invalid host.

Debug Message	Description
Connected to MQTT Broker!	Indicates a successful connection to the specified MQTT broker. MQTT communication is active; messages may be published or subscribed to now as configured.
Connection failed: timed out	The device attempted to connect to the specified MQTT broker, but did not receive a response. This error typically occurs when the broker's IP address is unreachable, or the configured port is closed or incorrect. To troubleshoot this error, verify that the specified MQTT broker is online, accessible across the network, and the specified port number is correct.
[Errno 111] Connection Refused	The MQTT broker actively rejected the connection attempt. This error typically occurs when the broker…
Connection failed: Invalid host.	Specifies the password used in conjunction with the configured Username for broker authentication.

The Login Broker parameter defines the authentication settings applied to the MQTT publisher (Smart 8 Input Sensor) or MQTT subscriber (Smart 8 Relay Output) when a connection attempt is made to the specified MQTT broker. When the Login Broker is enabled, a Username and Password field will populate onto the page.



1 ☑ Login Broker

2 Username: Enter username

3 Password: Enter Password

MQTT (Publisher/Subscriber) Login Broker Configuration

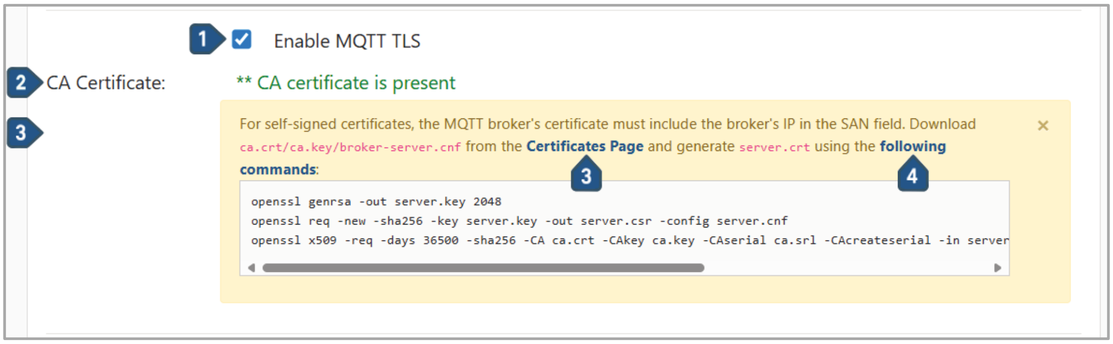
Item	Parameter	Description
1	Login Broker	Enables or disables authentication when connecting to the MQTT broker. If disabled, the MQTT publisher (Smart 8 Input Sensor) or subscriber (Smart 8 Relay Output) connects anonymously.
2	User Name	Defines the username used by the MQTT publisher/subscriber to authenticate with the broker.
3	Password	Specifies the password used in conjunction with the configured Username for broker authentication.

MQTT (Publisher/Subscriber) MQTTS Configuration

The MQTT TLS section enables encrypted message exchange as the MQTT over TLS (MQTTS) protocol. When MQTT TLS is enabled, the Smart 8 Input Sensor requires valid TLS/SSL certificates to secure communication between the MQTT broker and connected publisher or subscriber MQTT clients.

MQTTS requires the broker's IP address to be included inside the Subject Alternative Name (SAN) field of the server certificate for MQTT clients to verify the broker's identity. To fulfill this unique requirement for MQTTS, administrators may upload their own predefined organization-specific certificates (CA, server, private key) that include this information.

Alternatively, for administrators that desire to use self-signed certificates, the server certificate must be generated manually by using the device's self-signed CA certificate



☑ Enable MQTT TLS

CA Certificate: ** CA certificate is present

For self-signed certificates, the MQTT broker's certificate must include the broker's IP in the SAN field. Download ca.crt/ca.key/broker-server.cnf from the **Certificates Page** and generate server.crt using the **following commands**:

```
openssl genrsa -out server.key 2048
openssl req -new -sha256 -key server.key -out server.csr -config server.cnf
openssl x509 -req -days 36500 -sha256 -CA ca.crt -CAkey ca.key -CAserial ca.srl -CAcreateserial -in server
```

MQTT (Publisher) - MQTT Publisher Configuration : MQTT TLS (MQTTS)

Ref #	Parameter	Description
1	`Enable MQTT TLS`	Enables MQTT over TLS (MQTTS) for either the Smart 8 Input Sensor (MQTT publisher) or the Smart 8 Relay Output (MQTT subscriber). When enabled, the publisher or subscriber requires a trusted CA certificate to validate the broker's server certificate, and establish an encrypted connection.
2	`CA Certificate`	Indicates whether a CA certificate is present on the Smart 8 Input Sensor's MQTT Publisher CA certificate store, or the Smart 8 Relay Output's MQTT Subscriber CA certificate store. This CA certificate must be the issuer (or part of the trust chain) of the broker's server.crt certificate.
3	`Certificates Page`	Shortcut reference to the Certificates section, where administrators can upload organization-issued CA certificates, or generate self-signed CA certificates for using the MQTT publisher (Smart 8 Input Sensor) or MQTT subscriber (Smart 8 Relay Output) services over TLS.
4	`OpenSSL Commands ("following commands")`	Provides example commands for creating a broker's server key, Certificate Signing Request (CSR), and server certificate signed by a CA. This ensures that the broker's IP address appears in the SAN field for client validation. This process applies only when hosting a self-signed MQTTS broker, and no existing organizational TLS/SSL certificates are available.

The OpenSSL commands referenced in **Ref #4** of the above table are outlined further below, which are used when generating a self-signed certificate for a self-hosted MQTT broker:

openssl genrsa -out server.key 2048

Generates a new 2048-bit RSA private key for the MQTT broker.

openssl req -new -sha256 -key server.key -out server.csr -config server.cnf

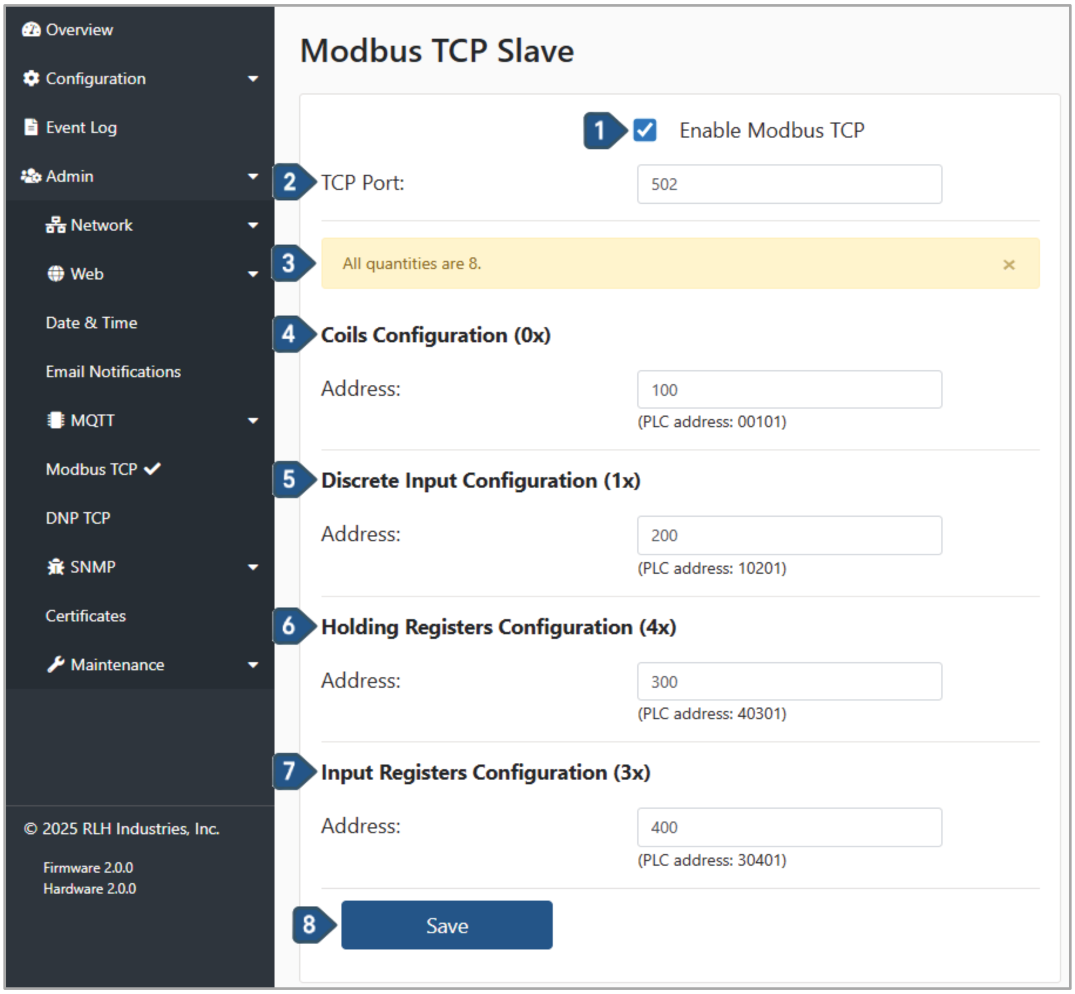
Creates a Certificate Signing Request (CSR) using the broker's private key. The configuration file (server.cnf) defines certificate attributes, including the broker's IP address in the Subject Alternative Name (SAN) field, when configured.

openssl x509 -req -days 36500 -sha256 -CA ca.crt -CAkey ca.key -CAserial -in server.csr -out server.crt -extensions req_ext -extfile broker-server.cnf

Uses the CA certificate and CA private key to sign the CSR, producing the broker's server certificate (server.crt). This certificate will include the broker's IP address in the SAN field, and be correctly presented to clients during MQTT over TLS (MQTTS) authentication

Modbus TCP Slave Overview

The Smart 8 Input Sensor and Smart 8 Relay Output both may operate as Modbus TCP slaves (servers), allowing other Modbus TCP masters (clients) to read or write I/O data across the network. Both devices expose their local I/O channels as standard Modbus data types: Coils (0x), Discrete Inputs (1x), Holding Registers (4x), and Input Registers (3x) to support wide compatibility across different SCADA systems and instruments (PLCs, HMIs, RTUs).



Modbus TCP Slave

1 ☑ Enable Modbus TCP

2 TCP Port: 502

3 All quantities are 8.

4 Coils Configuration (0x)

Address: 100
(PLC address: 00101)

5 Discrete Input Configuration (1x)

Address: 200
(PLC address: 10201)

6 Holding Registers Configuration (4x)

Address: 300
(PLC address: 40301)

7 Input Registers Configuration (3x)

Address: 400
(PLC address: 30401)

8 Save

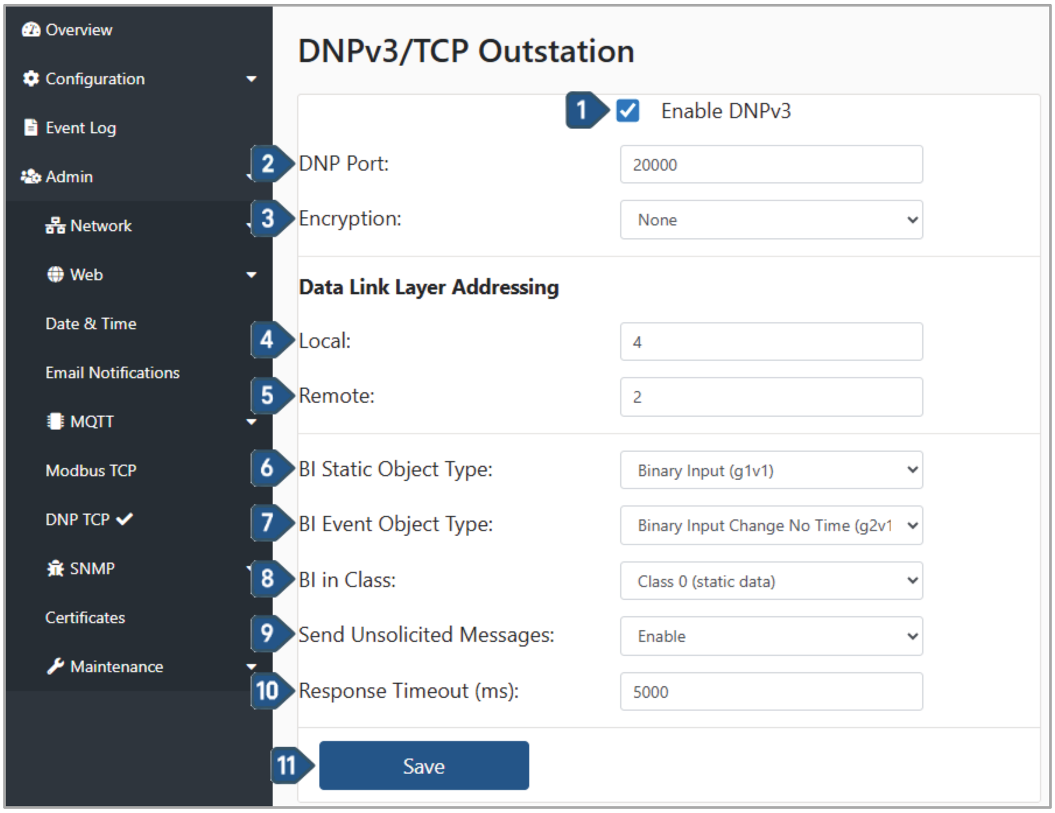
MQTT Modbus TCP Slave Overview

The Smart 8 Input Sensor presents all eight Digital Inputs as read-only Modbus values. For ensuring compatibility with Modbus TCP masters that are unable to read Discrete Input or Input Register values, the Digital Input states are mirrored in a read-only state across the Coils (0x) and Holding Register (4x) addresses.

By contrast, the Smart 8 Relay Output supports full read/write access onto its eight Relay Output channels; Relay Output values are mirrored in a read-only format across Discrete Input (1x) and Input Register (3x) addresses, while Relay Outputs may be configured by either sending write requests to either the Coils (0x) address, or Holding Registers (4x) address.

Each Modbus TCP data block is published in a contiguous, user-configurable address space on the Modbus TCP Slave Configuration page. Integrators may align the address layout with the conventions of the existing Modbus environment.

Modbus TCP Slave Configuration



DNPv3/TCP Outstation

1 ☑ Enable DNPv3

2 DNP Port: 20000

3 Encryption: None

Data Link Layer Addressing

4 Local: 4

5 Remote: 2

6 BI Static Object Type: Binary Input (g1v1)

7 BI Event Object Type: Binary Input Change No Time (g2v1

8 BI in Class: Class 0 (static data)

9 Send Unsolicited Messages: Enable

10 Response Timeout (ms): 5000

11 Save

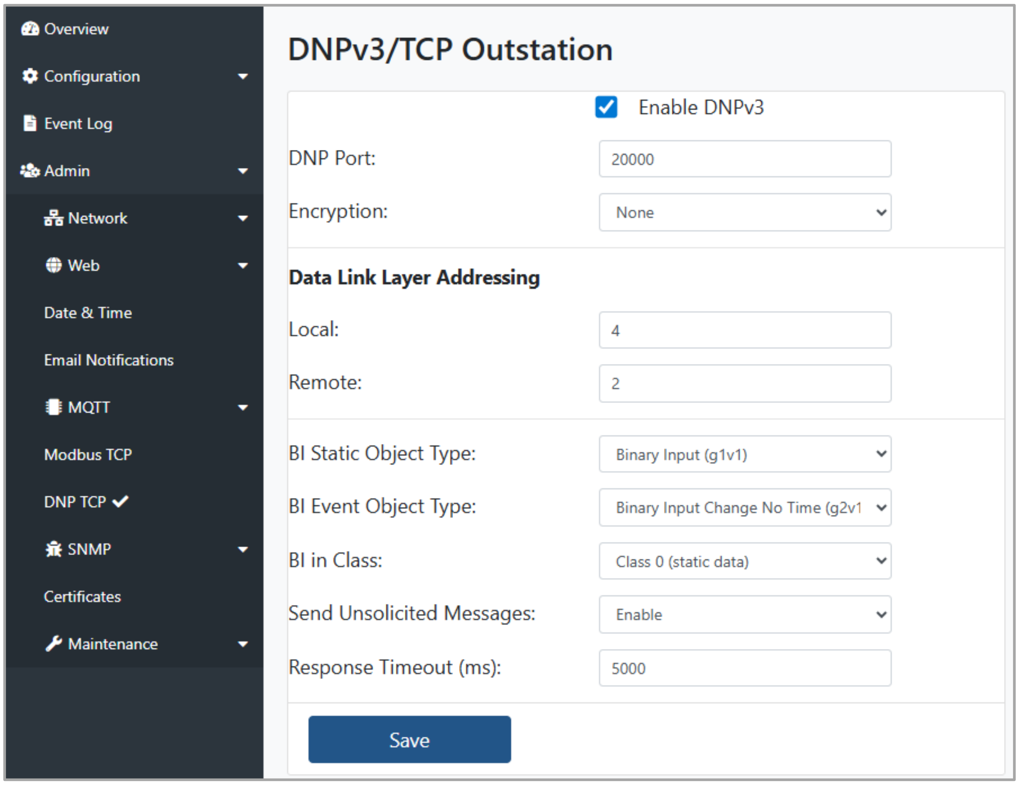
Modbus TCP - Modbus TCP Slave Configuration

Ref #	Parameter	Description
1	`Enable Modbus TCP`	Activates the Modbus TCP Slave service. When enabled, the unit listens for incoming Modbus TCP master (client) requests on the configured TCP port.
2	`TCP Port`	Defines the TCP port that the Modbus TCP Slave service will bind to. The default and standard Modbus TCP port is 502, but this value may be reconfigured.
3	`All quantities are 8. (Note)`	Displays an informational reminder that each Modbus data block contains exactly 8 I/O points, corresponding to either the device's eight Digital Inputs (Smart 8 Input Sensor) or eight Relay Outputs (Smart 8 Relay Output).
4	`Coils Configuration (0x)`	Defines the starting Modbus address for the device's Coil data block (0xxxx). On the Smart 8 Input Sensor, Coils represent read-only mirrors of Discrete Inputs. On the Smart 8 Relay Output, Coils support both read and write operations to control Relay Output energization.
5	`Discrete Input Configuration (1x)`	Defines the starting Modbus address for the device's Discrete Input (1xxxx) data block. On the Smart 8 Input Sensor, these represent native Digital Input states and are read-only. On the Smart 8 Relay Output, these represent read-only mirrors of Coils.
6	`Holding Registers Configuration (4x)`	Defines the starting Modbus address for the device's Holding Register (4xxxx) data block. On the Smart 8 Input Sensor, these represent read-only mirrors of Input Registers. On the Smart 8 Relay Output, these offer a 16-bit register-based presentation of Coils/Relay Output states.
7	`Input Registers Configuration (3x)`	Defines the starting Modbus address for the device's Input Register (3xxxx) data block. On the Smart 8 Input Sensor, these offer a 16-bit register-based presentation of Discrete Input/Digital Input states. On the Smart 8 Relay Output, these represent read-only mirrors of Holding Registers.
8	`Save`	Applies and immediately stores all Modbus TCP Slave service configuration changes.

DNP TCP (DNP3 Outstation) Overview: Smart 8 Relay Output

The Smart 8 Input Sensor includes a built-in DNP3/TCP Outstation service, allowing SCADA hosts that function as DNP3 masters to poll or receive event-driven updates from Digital Inputs using the DNP3/TCP protocol. When DNP3/TCP is enabled, the Smart 8 Input Sensor operates as a DNP3/TCP outstation (server), listening on the configured TCP port and responding to requests from a DNP3 master (client).

Through the DNP3 data model, all eight Digital Inputs are published as Binary Inputs (BI) points. Their current states may be retrieved through static polls, and their change-of-state events may be assigned to an event class (Class 1/2/3). Unsolicited reporting is supported, allowing these



DNPv3/TCP Outstation

☑ Enable DNPv3

DNP Port: 20000

Encryption: None

Data Link Layer Addressing

Local: 4

Remote: 2

BI Static Object Type: Binary Input (g1v1)

BI Event Object Type: Binary Input Change No Time (g2v1

BI in Class: Class 0 (static data)

Send Unsolicited Messages: Enable

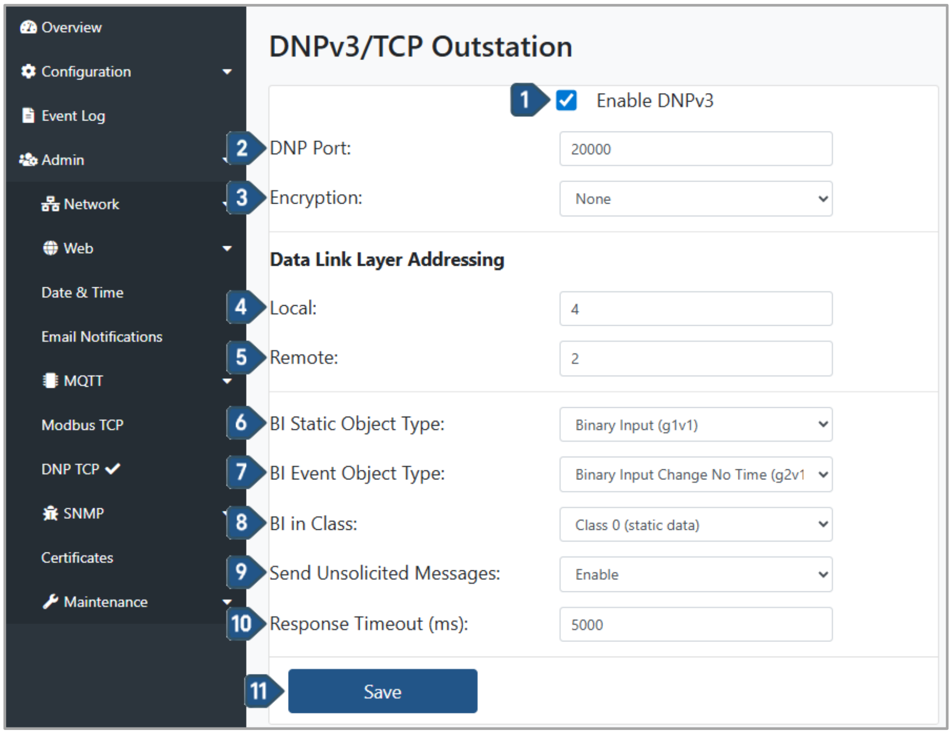
Response Timeout (ms): 5000

DNP TCP - DNP3 Outstation Configuration: Smart 8 Input Sensor

The table below illustrates each Digital Input's corresponding Binary Input (BI) point, and the status flag bits used by Binary Input - with Status (Group 1, Variation 2) and Binary Input Event (Group 2) objects when the point is in an OFF or ON state:

Binary Input Point Assignment		Binary Input - with Status (OFF)		Binary Input - with Status (ON)	
Digital Input	Binary Input	Point State	Status Flags	Point State	Status Flags
Input 1 Input 2 Input 3 Input 4 Input 5 Input 6 Input 7 Input 8	0 (000000) 1 (000001) 2 (000002) 3 (000003) 4 (000004) 5 (000005) 6 (000006) 7 (000007)	OFF - 0 (0x01)	State [MSB]: 0 Reserved: 0 Chatter Filter: 0 Local Forced: 0 Remote Forced: 0 Comm Fail: 0 Restart: 0 Online [LSB]: 1	ON - 1 (0x81)	State [MSB]: 1 Reserved: 0 Chatter Filter: 0 Local Forced: 0 Remote Forced: 0 Comm Fail: 0 Restart: 0 Online [LSB]: 1

DNP TCP (DNPv3 Outstation) Smart 8 Relay Output Configuration



DNPv3/TCP Outstation

☑ Enable DNPv3

DNP Port: 20000

Encryption: None

Data Link Layer Addressing

Local: 4

Remote: 2

BI Static Object Type: Binary Input (g1v1)

BI Event Object Type: Binary Input Change No Time (g2v1

BI in Class: Class 0 (static data)

Send Unsolicited Messages: Enable

Response Timeout (ms): 5000

Save

DNP TCP - DNP3 Outstation Configuration: Smart 8 Input Sensor

Ref #	Parameter	Description
1	`Enable DNPv3`	Activates the DNP3/TCP Outstation service. When enabled, the device listens on the configured DNP port and responds to requests for static and event-driven Binary Input data.
2	`DNP Port`	Specifies the TCP port the Outstation service listens on for incoming DNP3/TCP connections. The default value, 20000, is the standard port assignment for DNP3 over TCP.
3	`Encryption`	Selects whether the DNP/TCP session uses TLS transport encryption. "None" disables encryption, while "TLS" secures the DNP3 connection using certificate-based TLS.
4	`Local`	Defines the Outstation service's DNP3 Link Layer address, which uniquely identifies the Smart 8 Input Sensor in DNP3 request/respond exchanges. This must match the address expected by the DNP3 master, and be between 0 - 65535.
5	`Remote`	Specifies the DNP3 Link Layer address of the DNP3 master device. This must match the master's Link Layer address for proper communication, and be between 0 - 65535.
6	`BI Static Object Type`	Selects the Object Group/Variation used to report static Binary Inputs during Class 0 (static data) polls. Options include g1v1 (packed format), and g1v2 (with status flags).
7	`BI Event Object Type`	Selects the Object Group/Variation used to report Binary Input change-of-state events. Options include g2v1 (without timestamp), g2v2 (with timestamp / absolute), and g2v3 (with timestamp / relative).
8	`BI in Class`	Assigns Binary Inputs to a DNP3 event class: Class 0 (static only), Class 1, Class 2, or Class 3. Event classes determine whether unsolicited and Class integrity polls will include these Digital Inputs as points.
9	`Send Unsolicited Messages`	Enables or disables unsolicited DNP3 event reporting. When enabled, the Outstation service pushes Binary Input change-of-state events to the master as they occur.
10	`Response Timeout (ms)`	Defines how long the Outstation service waits for a complete DNP3 request or response exchange before timing out. It is recommended to increase this setting from its default value (5000ms) in high-latency networks.
11	`Save`	Applies all DNP3/TCP parameters, and restarts the Outstation service's DNP3 session. Once the Outstation service is online, a DNP3 master may perform an integrity poll to re-synchronize its view of static (Class 0) and pending event (Class 1/2/3) object data.

DNP3/TCP Object Implementation Table - Smart 8 Input Sensor

The following DNP3/TCP Object Implementation Table provides a consolidated view of the specific DNP3 Object Groups, Variations, Function Codes, and Qualifiers incorporated by the Smart 8 Input Sensor's outstation service when reporting Digital Input states and responding to requests from a DNP3 master.

All eight Digital Inputs are exposed as Binary Input points. Their static states are reported using Binary Input objects (Group 1), either in a packed format (Variation 1) or with status flags (Variation 2), depending on the configured BI Static Object Type parameter field. These static objects are returned during Group 1 requests, or Class 0 integrity polls.

Change-of-state activity is generated using Binary Input Event objects (Group 2), with the event-reporting format selected by the BI Event Object Type parameter field. Events may be sent without a timestamp (Variation 1), with an absolute timestamp (Variation 2), or with a relative timestamp (Variation 3). When "Send Unsolicited Messages" is enabled, the outstation service can deliver these Group 2 events to the DNP3 master as unsolicited responses, in addition to responding to normal class integrity polls.

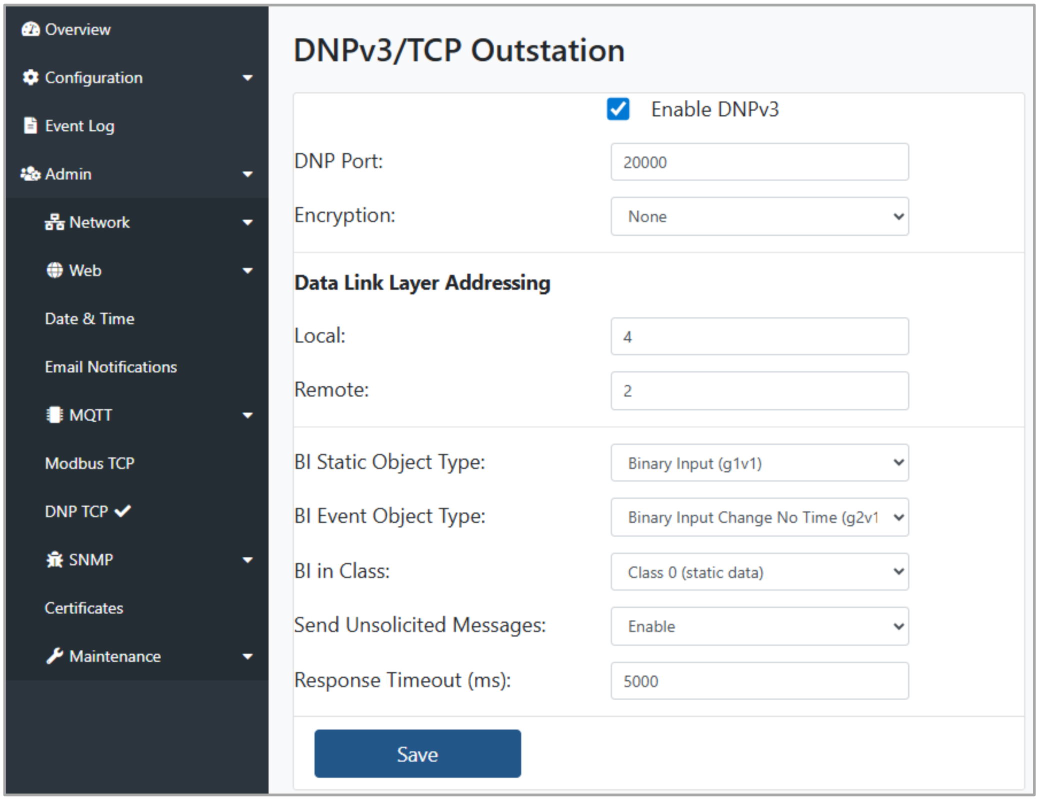
Binary Input points may collectively be assigned to an event class (Class 0, 1, 2, or 3). Class 0 polls return the current static Binary Input point values, while Class 1, 2, or 3 polls return Binary Event data for points mapped to the corresponding class. If a Class poll is issued for a class that currently has no pending events, the outstation acknowledges the request and sets the appropriate Event Data Is Available IIN bit to identify the class of queued events, indicating that the master should perform another Class event poll to retrieve them. If the BI in Class parameter field is set to Class 0, event reporting does not occur.

Object			Request		Response	
Group	Variation	Description	Function Code	Qualifiers (Hex)	Function Code	Qualifier (Hex)
1	1	Binary Input - Packed Format	1 (0x01) - Read	0x06 - All Points 0x00 - 8-Bit Start/Stop 0x01 - 16-Bit Start/Stop	129 (0x81) - Response	0x00 - 8-Bit Start/Stop
1	2	Binary Input - with Status	1 (0x01) - Read	0x06 - All Points 0x00 - 8-Bit Start/Stop 0x01 - 16-Bit Start/Stop	129 (0x81) - Response	0x00 - 8-Bit Start/Stop
2	1	Binary Input Event - without Timestamp	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
2	2	Binary Input Event - with Timestamp	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
2	3	Binary Input Event - with Relative Time (used with CTO)	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
50	1	Time and Date - Absolute Time	2 (0x02) - Write	0x07 - 8-Bit Limited Qty	129 (0x81) - Response	N/A
50	3	Time and Date - Absolute Time with Last Recorded Time (LAN Sync)	2 (0x02) - Write	0x07 - 8-Bit Limited Qty	129 (0x81) - Response	N/A
51	1	Time and Date CTO - Synchronized	N/A	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
51	2	Time and Date CTO - Unsynchronized	N/A	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
52	2	Time Delay - Fine (milliseconds)	23 (0x17) - Delay Measurement	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
60	1	Class Poll Request - Class 0 Data	1 (0x01) - Read	0x06 - All Points	129 (0x81) - Response	N/A
60	2	Class Poll Request - Class 1 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A
60	3	Class Poll Request - Class 2 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A
60	4	Class Poll Request - Class 3 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A

DNP TCP - DNP3 Outstation Configuration: Smart 8 Relay Output

The Smart 8 Relay Output includes a built-in DNP3/TCP Outstation service, allowing SCADA hosts that function as DNP3 masters to both command and monitor Relay Outputs using the DNP3/TCP protocol. When DNP3/TCP is enabled, the Smart 8 Relay Output operates as a DNP3/TCP outstation (server), listening on the configured TCP port and responding to control or status requests from a DNP3 master (client).

Through the DNP3 data model, all eight Relay Outputs are published as Binary Outputs (BO) points. Their current states are retrievable as Binary Output Status objects, and may be controlled via Control Relay Output (CROB) commands. This Outstation service supports the following CROB commands: Latch On, Latch Off, Pulse On, and Pulse Off.



DNPv3/TCP Outstation

☑ Enable DNPv3

DNP Port: 20000

Encryption: None

Data Link Layer Addressing

Local: 4

Remote: 2

BI Static Object Type: Binary Input (g1v1)

BI Event Object Type: Binary Input Change No Time (g2v1

BI in Class: Class 0 (static data)

Send Unsolicited Messages: Enable

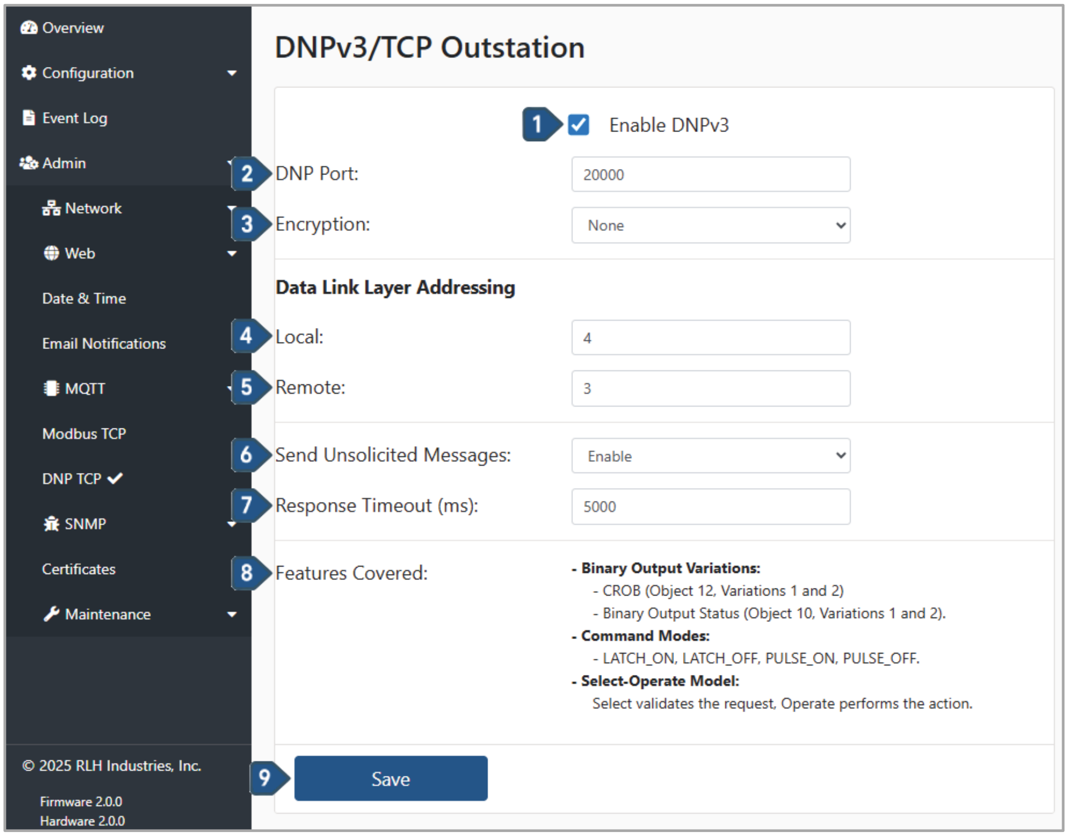
Response Timeout (ms): 5000

DNP TCP - DNP3 Outstation Overview: Smart 8 Relay Output

The table below illustrates each Relay Output's corresponding Binary Output (BO) point, and the status flag bits used by Binary Output Status (Group 10, Variation 2) and Binary Output Status Event (Group 11, Variation 2) objects when the point is in an OFF or ON state:

Binary Input Point Assignment		Binary Input - with Status (OFF)		Binary Input - with Status (ON)	
Digital Input	Binary Input	Point State	Status Flags	Point State	Status Flags
Input 1 Input 2 Input 3 Input 4 Input 5 Input 6 Input 7 Input 8	0 (000000) 1 (000001) 2 (000002) 3 (000003) 4 (000004) 5 (000005) 6 (000006) 7 (000007)	OFF - 0 (0x01)	State [MSB]: 0 Reserved: 0 Chatter Filter: 0 Local Forced: 0 Remote Forced: 0 Comm Fail: 0 Restart: 0 Online [LSB]: 1	ON - 1 (0x81)	State [MSB]: 1 Reserved: 0 Chatter Filter: 0 Local Forced: 0 Remote Forced: 0 Comm Fail: 0 Restart: 0 Online [LSB]: 1

MQTT (DNP TCP) DNPv3 Outstation Configuration: Smart 8 Relay Output



DNPv3/TCP Outstation

☑ Enable DNPv3

DNP Port: 20000

Encryption: None

Data Link Layer Addressing

Local: 4

Remote: 3

Send Unsolicited Messages: Enable

Response Timeout (ms): 5000

Features Covered:

- **Binary Output Variations:**
  - CROB (Object 12, Variations 1 and 2)
  - Binary Output Status (Object 10, Variations 1 and 2).
- **Command Modes:**
  - LATCH_ON, LATCH_OFF, PULSE_ON, PULSE_OFF.
- **Select-Operate Model:**
  Select validates the request, Operate performs the action.

Save

DNP TCP - DNP3 Outstation Configuration: Smart 8 Relay Output

Ref #	Parameter	Description
1	`Enable DNPv3`	Activates the DNP3/TCP Outstation service. When enabled, the device listens on the configured DNP port and responds to requests for static and event-driven Binary Input data.
2	`DNP Port`	Specifies the TCP port the Outstation service listens on for incoming DNP3/TCP connections. The default value, 20000, is the standard port assignment for DNP3 over TCP.
3	`Encryption`	Selects whether the DNP/TCP session uses TLS transport encryption. "None" disables encryption, while "TLS" secures the DNP3 connection using certificate-based TLS.
4	`Local`	Defines the Outstation service's DNP3 Link Layer address, which uniquely identifies the Smart 8 Input Sensor in DNP3 request/respond exchanges. This must match the address expected by the DNP3 master, and be between 0 - 65535.
5	`Remote`	Specifies the DNP3 Link Layer address of the DNP3 master device. This must match the master's Link Layer address for proper communication, and be between 0 - 65535.
6	`BI Static Object Type`	Selects the Object Group/Variation used to report static Binary Inputs during Class 0 (static data) polls. Options include g1v1 (packed format), and g1v2 (with status flags).
7	`BI Event Object Type`	Selects the Object Group/Variation used to report Binary Input change-of-state events. Options include g2v1 (without timestamp), g2v2 (with timestamp / absolute), and g2v3 (with timestamp / relative).
8	`BI in Class`	Assigns Binary Inputs to a DNP3 event class: Class 0 (static only), Class 1, Class 2, or Class 3. Event classes determine whether unsolicited and Class integrity polls will include these Digital Inputs as points.
9	`Send Unsolicited Messages`	Enables or disables unsolicited DNP3 event reporting. When enabled, the Outstation service pushes Binary Input change-of-state events to the master as they occur.
10	`Response Timeout (ms)`	Defines how long the Outstation service waits for a complete DNP3 request or response exchange before timing out. It is recommended to increase this setting from its default value (5000ms) in high-latency networks.
11	`Save`	Applies all DNP3/TCP parameters, and restarts the Outstation service's DNP3 session. Once the Outstation service is online, a DNP3 master may perform an integrity poll to re-synchronize its view of static (Class 0) and pending event (Class 1/2/3) object data.

DNP3/TCP Object Implementation Table - Smart 8 Relay Output

The following DNP3/TCP Object Implementation Table provides a consolidated view of the specific DNP3 Object Groups, Variations, Function Codes, and Qualifiers incorporated by the Smart 8 Relay Output's outstation service when reporting Relay Output states and responding to requests from a DNP3 master.

All eight Relay Outputs are exposed as Binary Output Status points, and mirrored onto Binary Input points in a read-only state that reference the same point indices (0-7). These static objects (Groups 1 and 10) are returned during Class 0 integrity polls, while timestamped Binary Output Status event objects (Group 11) are generated during Relay Output state changes. When "Send Unsolicited Messages" is enabled, all available Group 11 event objects are delivered to the DNP3 master as unsolicited responses. These objects may also be retrieved at any time via Class 1 event polling.

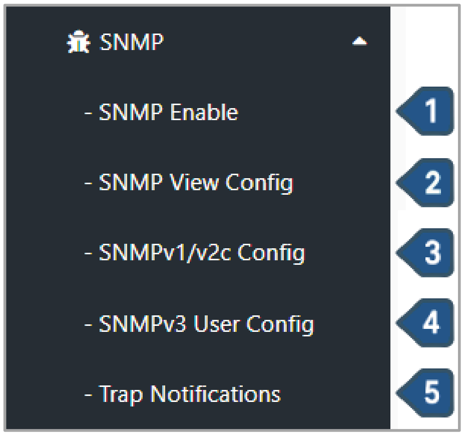
All Binary Output Status and Binary Input points are assigned to Class 1 for event reporting. Class 0 (static) and Class 1(event) polls therefore return point data, while Class 2 and 3 polls are accepted but return no objects. When a Class 2 or Class 3 poll is issued, the outstation service acknowledges the request; if Class 1 events are present, it also sets the Class 1 Event Data is Available IIN bit, indicating that the master should perform a Class 1 event poll to retrieve queued event objects

Object			Request		Response	
Group	Variation	Description	Function Code	Qualifiers (Hex)	Function Code	Qualifier (Hex)
1	1	Binary Input - Packed Format	1 (0x01) - Read	0x06 - All Points 0x00 - 8-Bit Start/Stop 0x01 - 16-Bit Start/Stop	129 (0x81) - Response	0x00 - 8-Bit Start/Stop
1	2	Binary Input - with Status	1 (0x01) - Read	0x06 - All Points 0x00 - 8-Bit Start/Stop 0x01 - 16-Bit Start/Stop	129 (0x81) - Response	0x00 - 8-Bit Start/Stop
2	1	Binary Input Event - without Timestamp	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
2	2	Binary Input Event - with Timestamp	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
2	3	Binary Input Event - with Relative Time (used with CTO)	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response 130 (0x82) - Unsolicited Response	0x28 - 16-Bit Index
50	1	Time and Date - Absolute Time	2 (0x02) - Write	0x07 - 8-Bit Limited Qty	129 (0x81) - Response	N/A
50	3	Time and Date - Absolute Time with Last Recorded Time (LAN Sync)	2 (0x02) - Write	0x07 - 8-Bit Limited Qty	129 (0x81) - Response	N/A
51	1	Time and Date CTO - Synchronized	N/A	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
51	2	Time and Date CTO - Unsynchronized	N/A	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
52	2	Time Delay - Fine (milliseconds)	23 (0x17) - Delay Measurement	N/A	129 (0x81) - Response	0x07 - 8-Bit Limited Qty
60	1	Class Poll Request - Class 0 Data	1 (0x01) - Read	0x06 - All Points	129 (0x81) - Response	N/A
60	2	Class Poll Request - Class 1 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A
60	3	Class Poll Request - Class 2 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A
60	4	Class Poll Request - Class 3 Data	1 (0x01) - Read	0x06 - All Points 0x07 - 8-Bit Limited Qty 0x08 - 16-Bit Limited Qty	129 (0x81) - Response	N/A

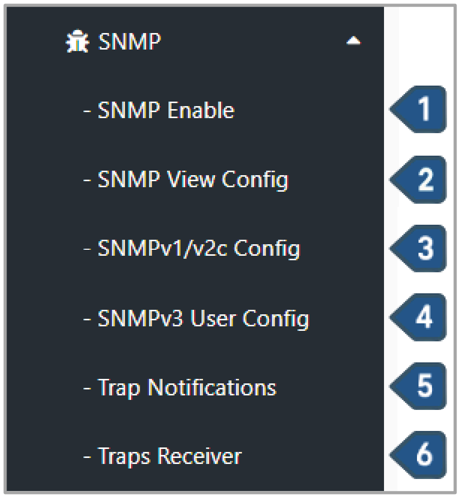
SNMP (Navigation Panel) Overview

The SNMP Navigation Panel organizes all SNMP (Simple Network Management Protocol) configuration options available for allowing administrators to enable SNMPv1/v2c/v3 agent services, define MIB view access, configure SNMPv1/v2c communities, set SNMPv3 user credentials, and specific trap-delivery and/or reception behavior.

Both the Smart 8 Input Sensor and Smart 8 Relay Output modules share the same core SNMP features; however, the Smart 8 Relay Output uniquely includes a Traps Receiver window for establishing an SNMPv1/v2c/v3 trap receiver service. This service may be used in conjunction with Relay channels to actuate Relay Outputs based on the reception of an SNMP trap with user-defined parameters.



SNMP - Navigation Panel (Smart 8 Input Sensor)



SNMP - Navigation Panel (Smart 8 Relay Output)

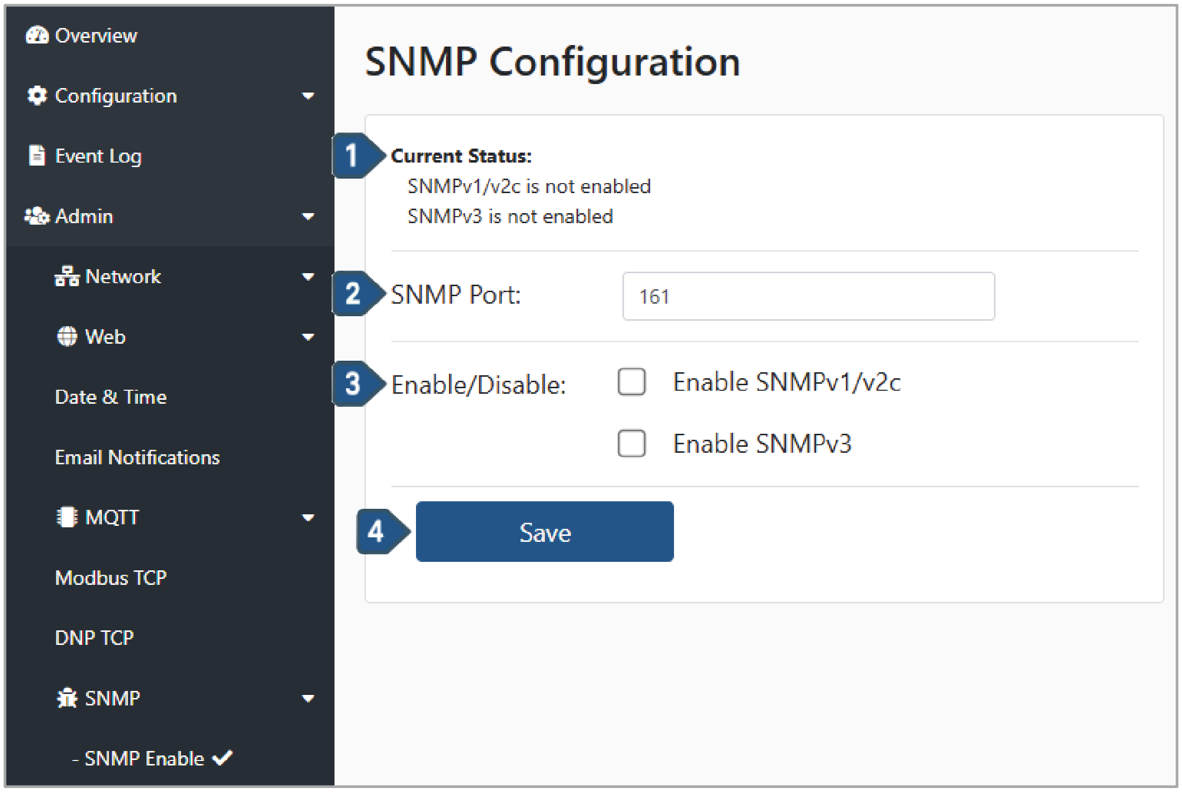
Ref #	Parameter	Description
1	`SNMP Enable`	Opens the SNMP Configuration window for toggling SNMP agent services on or off, and selecting the version(s) permitted for remote management.
2	`SNMP View Config`	Opens the SNMP View Configuration window for defining MIB view scopes ("included" vs. "excluded" OIDs) used commonly by community strings, or SNMPv3 users.
3	`SNMPv1/v2c Config`	Opens the SNMPv1/v2c Configuration window for defining community strings, and adding or removing associated views.
4	`SNMPv3 User Config`	Opens the SNMPv3 User Configuration window for creating and removing USM users.
5	`Trap Notifications`	Opens the SNMP Traps Notification window for configuring up to two outbound SNMPv1/v2c trap destinations, and/or one SNMPv3 trap destination, to receive SNMP traps during I/O state changes.

6	`Traps Receiver`
	`(Smart 8 Relay Output only)`
		Opens the SNMP Traps Receiver window for toggling SNMP trap receiver services on or off, and selecting the version(s) permitted for trap reception.

SNMP (SNMP Enable) Configuration

The SNMP Configuration webpage presents a unified interface for activating the device's SNMP agent service, specifying the protocol version, UDP port, and the current service status overview.

The SNMP agent service supports all SNMP protocol versions, consolidated into either SNMPv1/v2c or SNMPv3, selections. Both selections may be enabled simultaneously.



SNMP Configuration

1 **Current Status:**
SNMPv1/v2c is not enabled
SNMPv3 is not enabled

2 SNMP Port: 161

3 Enable/Disable: □ Enable SNMPv1/v2c
□ Enable SNMPv3

SNMP (SNMP Enable) - SNMPv1/v2c/v3 Enable

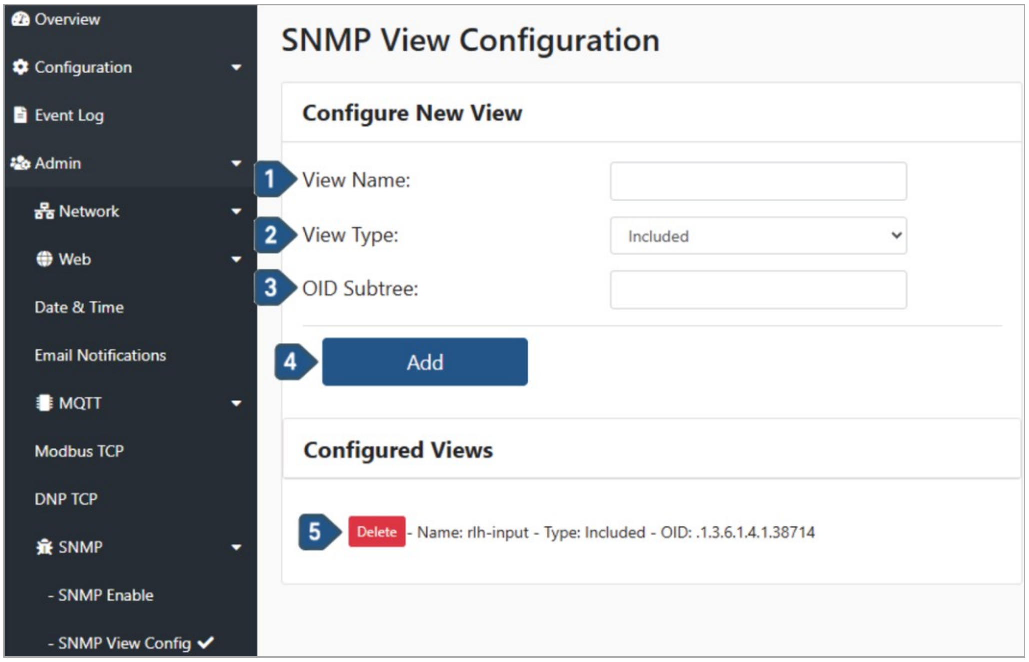
Item	Parameter	Description
1	`Current Status`	Displays the live state of the device's SNMP agent service, indicating whether SNMPv1/v2c and/or SNMPv3 are currently enabled.
2	`SNMP Port`	Specifies the UDP port used by the SNMP agent service to receive inbound requests. By default, the port is configured as 161.
3	`Enable/Disable (Enable SNMPv1/v2c/v3)`	Two independent checkboxes that allow administrators to activate one or both protocol versions: SNMPv1/v2c (Enable SNMPv1/v2c) or SNMPv3 (Enable SNMPv3).
4	`Save`	Commits the SNMP configuration changes, and restarts the SNMP agent service.

SNMP (SNMP View Config) Configuration

The SNMP View Configuration webpage defines which portions of the device's MIB tree are visible to SNMPv1, SNMPv2c, and SNMPv3 clients. Each entry consists of a named View that marks an OID subtree as either included or excluded. SNMP Views are applied on the SNMPv1/v2c Configuration and SNMPv3 User Configuration webpages.

The SNMP View feature uses the same View mechanism across all SNMP versions; however, note that its viewmatching behavior contrasts with the full VACM (View-based Access Control Model) specification found in SNMPv3. Prefix lengths are not considered for "Excluded" rules in this SNMP View implementation, which can cause nested OIDs to still appear when shorter-prefix OIDs are explicitly assigned as "Included" rules. Administrators should therefore always validate the Configured Views section with real SNMP queries, to avoid unintentionally exposing nested objects.

By default, the SNMP View "rlh-input" is defined as an Included View containing the RLH Industries enterprise OID prefix.



SNMP View Configuration

Configure New View

View Name:

View Type: Included

OID Subtree:

Configured Views

- Name: rlh-input - Type: Included - OID: .1.3.6.1.4.1.38714

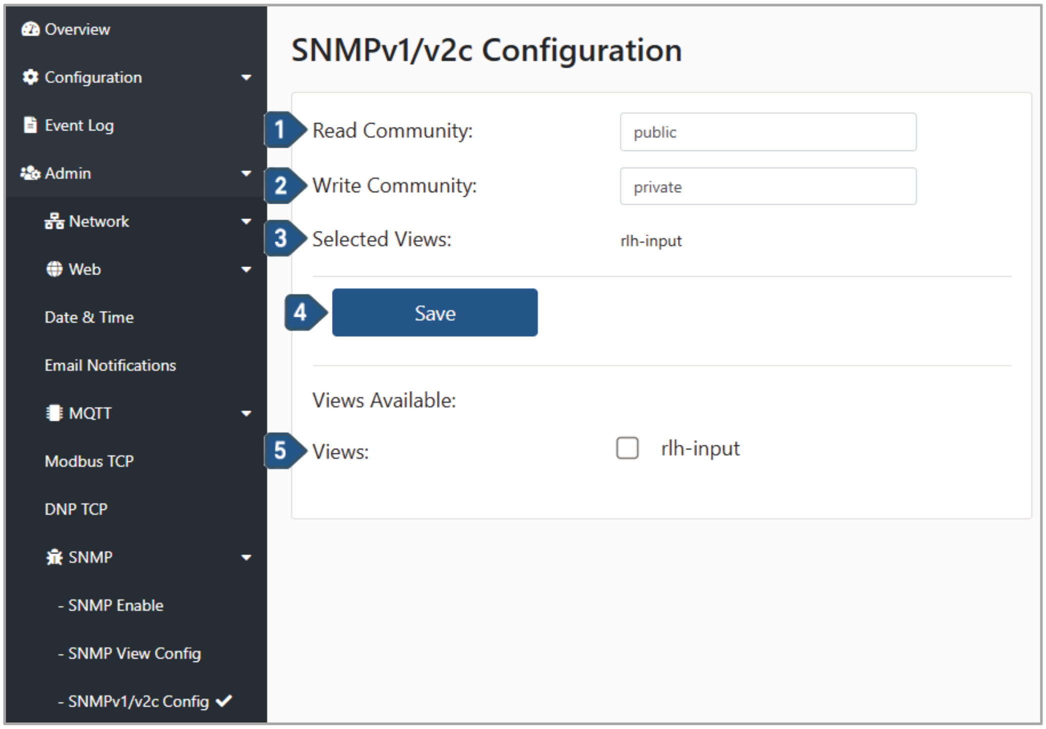
SNMP (SNMP View Config) - SNMP View Configuration

Items	Parameter	
1	`View Name`	Configures the label used by the SNMP View entry.
2	`View Type`	Defines whether the OID subtree is Included or Excluded from the resulting SNMP View. If "Included" is selected, the specified OID subtree is visible to SNMP queries. If "Excluded" is selected, the specified OID subtree is hidden from SNMP queries.
3	`OID Subtree`	Defines the root OID applied to the SNMP View. The device interprets this as the base of the OID subtree that will be included or excluded, depending on the View Type.
4	`Add`	Creates a new SNMP View entry using the parameters configured in Items 1-3. Once added, the entry appears in the Configured Views list.
5	`Delete`	Deletes the selected SNMP View entry.

SNMP (SNMPv1/v2c Config) Configuration

The SNMPv1/v2c Configuration webpage establishes the community-based access credentials used by legacy SNMP management systems. The Read and Write communities used for SNMPv1 and SNMPv2c authentication are configurable, for integrating the device's SNMP agent service with NMSes that do not support SNMPv3.

Administrators may also assign selected SNMP Views to the SNMPv1/v2c configuration. This determines which portions of the MIB tree are accessible when polling or modifying device objects through SNMPv1 or SNMPv2c.



Read Community: public

Write Community: private

Selected Views: rlh-input

Views: □ rlh-input

SNMP (SNMPv1/v2c Config) - SNMPv1/v2c Configuration

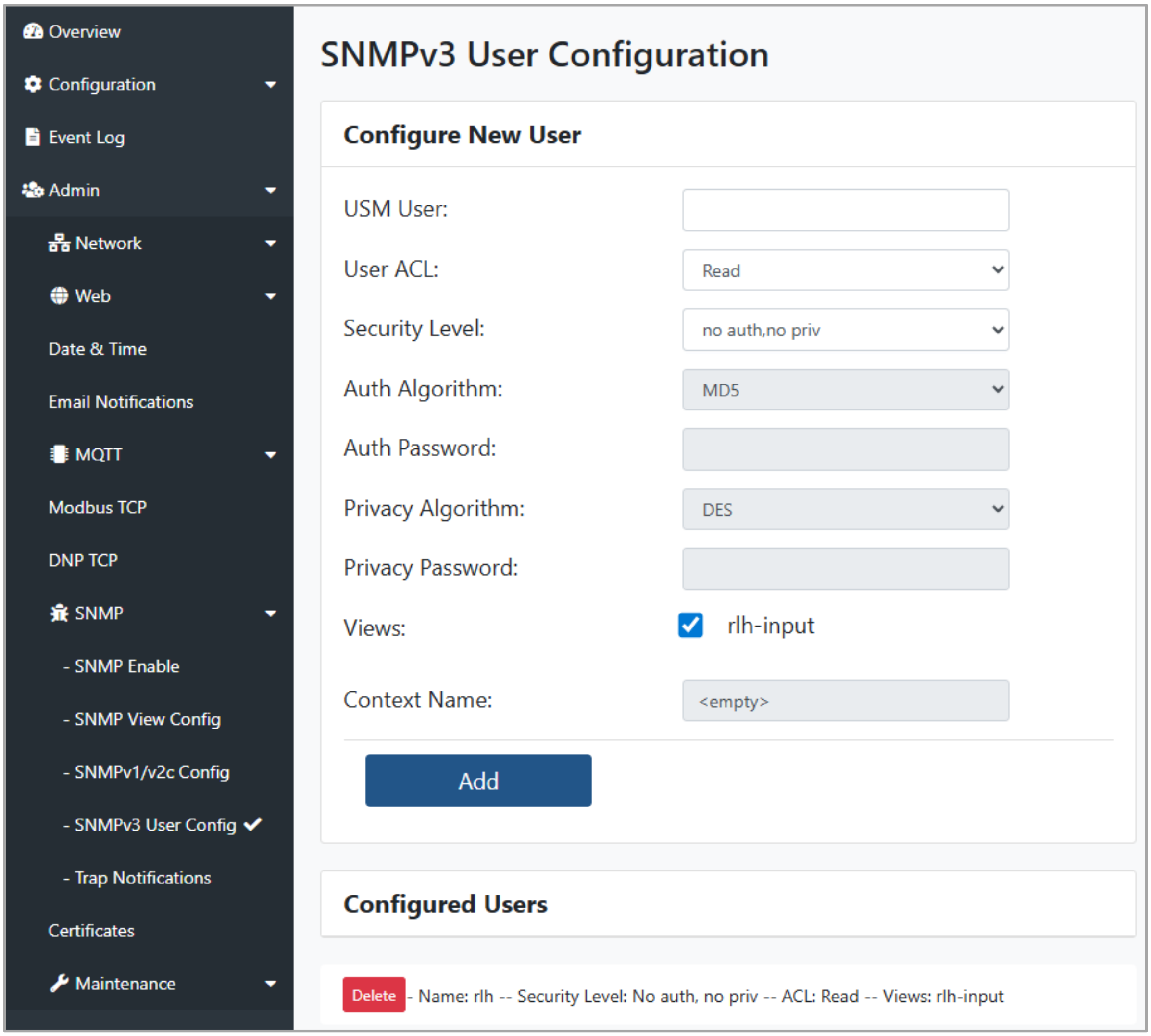
Items	Parameter	Description
1	`Read Community`	Specifies the plaintext community string used for read-only SNMP operations (e.g, GET, GETNEXT, GETBULK). By default, "public" is used. This field can't be blank.
2	`Write Community`	Specifies the plaintext community string used for read/write SNMO operations (e.g, SET requests). By default, "private" is used. This field can't be blank.
3	`Selected Views`	Displays which SNMP View(s) are currently assigned to the community strings. These views define which OID subtrees are visible through SNMPv1/v2c.
4	`Save`	Commits and immediately applies community and View assignments to the device. Note that Views are reassigned when the Save parameter is selected; when intending to update only community strings, ensure the proper Views are also selected prior to saving.
5	`Views`	Lists all SNMP Views present in the SNMP View Configuration webpage. Administrators may select one or more Views, which are applied upon saving. Only OIDs permitted by the chosen View(s) will be accessible through the specified community strings.

SNMP (SNMPv3 User Config) Overview

The SNMPv3 User Configuration webpage presents a secure, standards-based method for defining user accounts under the SNMPv3 User-based Security Model (USM). SNMPv3 offers authentication, optional data encryption, per-user access control, and granular visibility management via configurable SNMP Views.

Administrators may create multiple SNMPv3 users and assing read-only or read-write permissions, authentication and privacy algorithms, and SNMP Views. These controls provide significantly stronger security than community based SNMPv1/v2c access.

When using the SNMP features present on the Smart 8 Input Sensor and Smart 8 Relay Output, it is recommended to use SNMPv3 as the protocol version medium for security purposes..



SNMPv3 User Configuration

Configure New User

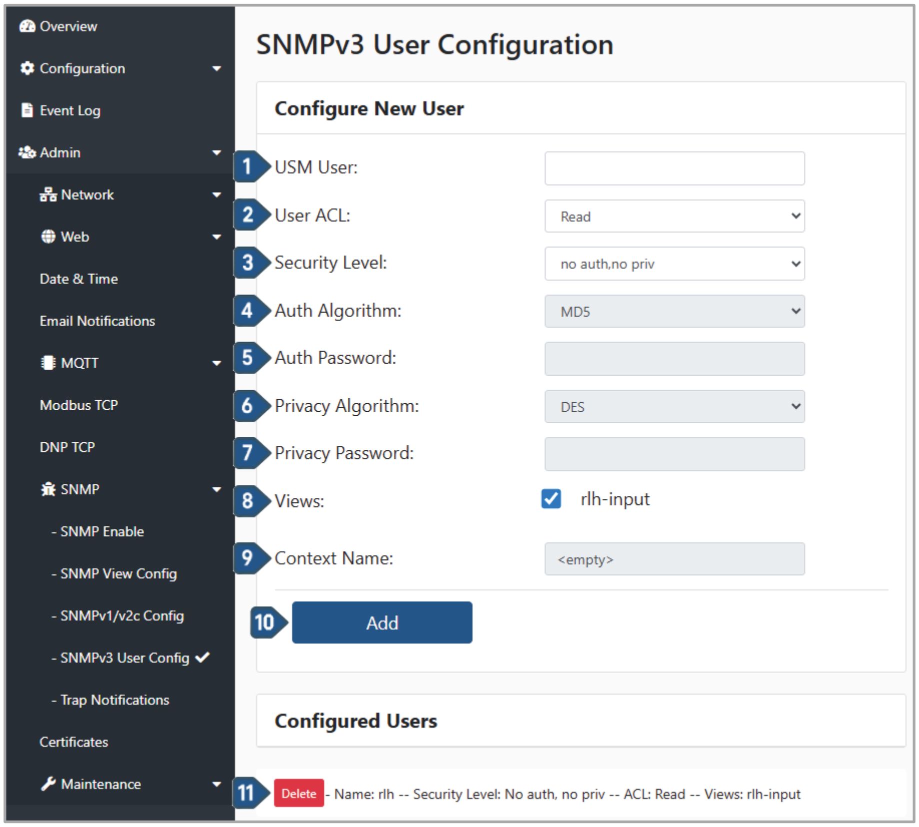
USM User:	
User ACL:	Read
Security Level:	no auth,no priv
Auth Algorithm:	MD5
Auth Password:	
Privacy Algorithm:	DES
Privacy Password:	
Views:	☑ rlh-input
Context Name:	<empty>

Configured Users

Delete - Name: rlh -- Security Level: No auth, no priv -- ACL: Read -- Views: rlh-input

SNMP (SNMPv3 User Config) - SNMPv3 User Overview

SNMP (SNMPv3 User Config) Configuration



SNMPv3 User Configuration

Configure New User

1 USM User:

2 User ACL: Read

3 Security Level: no auth,no priv

4 Auth Algorithm: MD5

5 Auth Password:

6 Privacy Algorithm: DES

7 Privacy Password:

8 Views: ☑ rlh-input

9 Context Name: <empty>

Configured Users

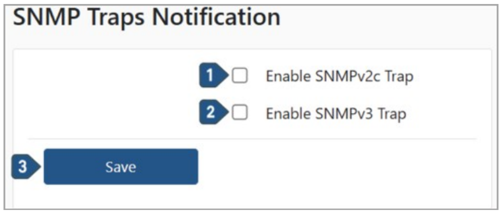
11 Delete - Name: rlh -- Security Level: No auth, no priv -- ACL: Read -- Views: rlh-input

SNMP (SNMPv3 User Config) - SNMPv3 User Configuration

Items	Parameter	Description
1	USM User	Specifies the username for the SNMPv3 account. This value is is authenticated and optionally encrypted depending on the selected Security Level parameter.
2	User ACL	Defines the access permissions assigned to the SNMPv3 account. Options include "Read" (e.g., GET operations) and "Read & Write" (e.g., GET, SET operations).
3	Security Level	Determines the SNMPv3 account's security profile based on whether authentication and/or encryption are required. Options include "no auth,no priv", "auth,no priv", and "auth,priv".
4	Auth Algorithm	Specifies the authentication algorithm used when the Security Level parameter requires authentication. Options include MD5 and SHA.
5	Auth Password	Defines the password used for the selected authentication algorithm. The minimum password length is 8 characters.
6	Privacy Algorithm	Specifies the encryption algorithm used when the Security Level parameter requires encryption, protecting SNMP payloads while in transit. Options include DES and AES.
7	Privacy Password	Defines the password used to generate the data-encryption key for the selected encryption algorithm. The minimum password length is 8 characters.
8	Views	Lists all SNMP Views present in the SNMP View Configuration webpage. The selected Views determine which OIDs are visible or hidden for this SNMPv3 account.
9	Context Name	Identifies the account's SNMPv3 data context. This device only supports the default (empty) context, and only lists this parameter as a reference. It is a read-only field.
10	Add	Creates an SNMPv3 account, using the specified parameters.
11	Delete	Removes SNMPv3 accounts from the device. This section also displays each SNMPv3 account currently defined on the device, including their username ("Name"), Security Level, ACL permissions, and assigned SNMP Views.

SNMP (Trap Notifications) Configuration: SNMPv2c

The SNMP Traps Notification webpage activates outbound trap reporting using either SNMPv2c, or SNMPv3, for transmitting I/O state change alerts to an external NMS solution. Selecting either "Enable SNMPv2c Trap" or "Enable SNMPv3 Trap" will reveal additional configuration fields on the webpage that correspond to that particular SNMP protocol version. Both may be used simultaneously.



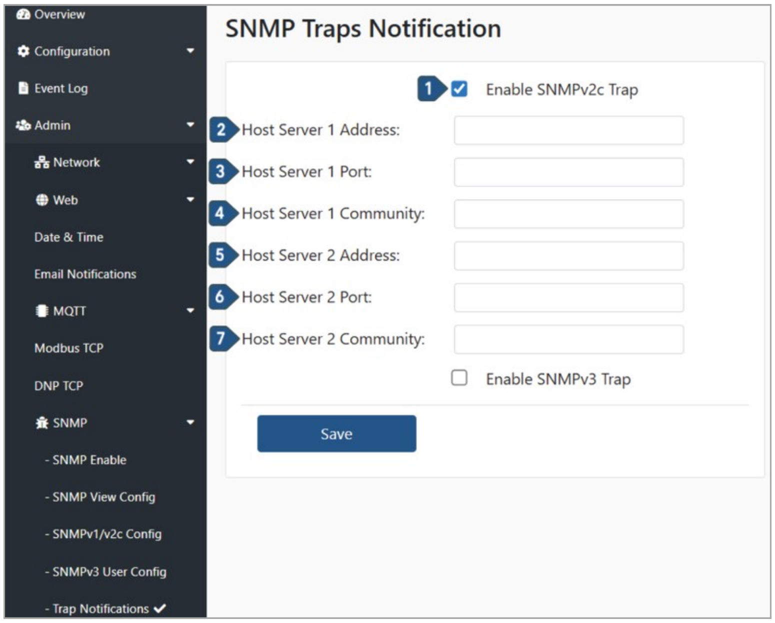
SNMP Traps Notification

1 □ Enable SNMPv2c Trap

2 □ Enable SNMPv3 Trap

SNMP (Trap Notifications) - SNMPv2c/v3 Trap Configuration

Item	Parameter	Description
1	`Enable SNMPv2c Trap`	Enables SNMP trap delivery using SNMPv2c
2	`Enable SNMPv3 Trap`	Enables SNMP trap delivery using SNMPv3
3	`Save`	Commits all SNMP Traps Notification settings, including the underlying configuration parameters present when Enable SNMPv2c Trap or Enable SNMPv3 Trap is selected



SNMP Traps Notification

1 ☑ Enable SNMPv2c Trap

2 Host Server 1 Address:

3 Host Server 1 Port:

4 Host Server 1 Community:

5 Host Server 2 Address:

6 Host Server 2 Port:

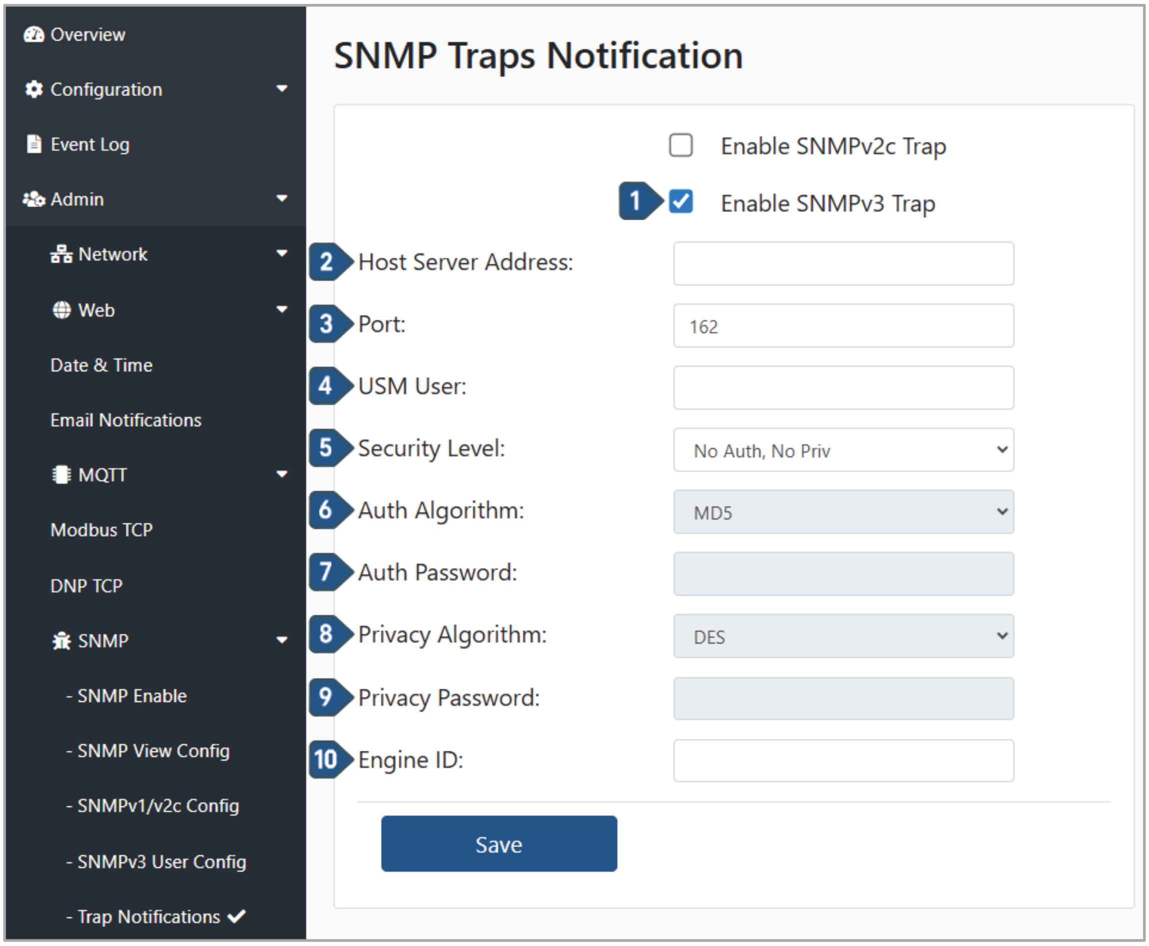
7 Host Server 2 Community:

□ Enable SNMPv3 Trap

SNMP (Trap Notifications) - SNMP Traps Notification: SNMPv2c

Ref #	Parameter	Description
1	`Enable SNMPv2c Trap`	Activates SNMPv2c trap delivery for the device.
2	`Host Server 1 Address`	Specifies the IP address of the first SNMPv2c trap receiver platform (e.g., NMS).
3	`Host Server 1 Port`	Specifies the UDP port for the first SNMPv2c trap receiver platform (e.g., NMS).
4	`Host Server 1 Community`	Defines the trap community string used when transmitting SNMPv2c traps to Host Server 1.
5	`Host Server 2 Address`	Specifies the IP address for a second SNMPv2c trap receiver platform.
6	`Host Server 2 Port`	Specifies the UDP port for a second SNMPv2c trap receiver platform.
7	`Host Server 2 Community`	Defines the trap community string used when transmitting SNMPv2c traps to Host Server 2.

SNMP Traps Configuration: SNMPv3



SNMP Traps Notification

□ Enable SNMPv2c Trap

1 ☑ Enable SNMPv3 Trap

2 Host Server Address:

3 Port: 162

4 USM User:

5 Security Level: No Auth, No Priv

6 Auth Algorithm: MD5

7 Auth Password:

8 Privacy Algorithm: DES

9 Privacy Password:

10 Engine ID:

SNMP (Trap Notifications) - SNMP Traps Notification: Enable SNMPv3 Trap

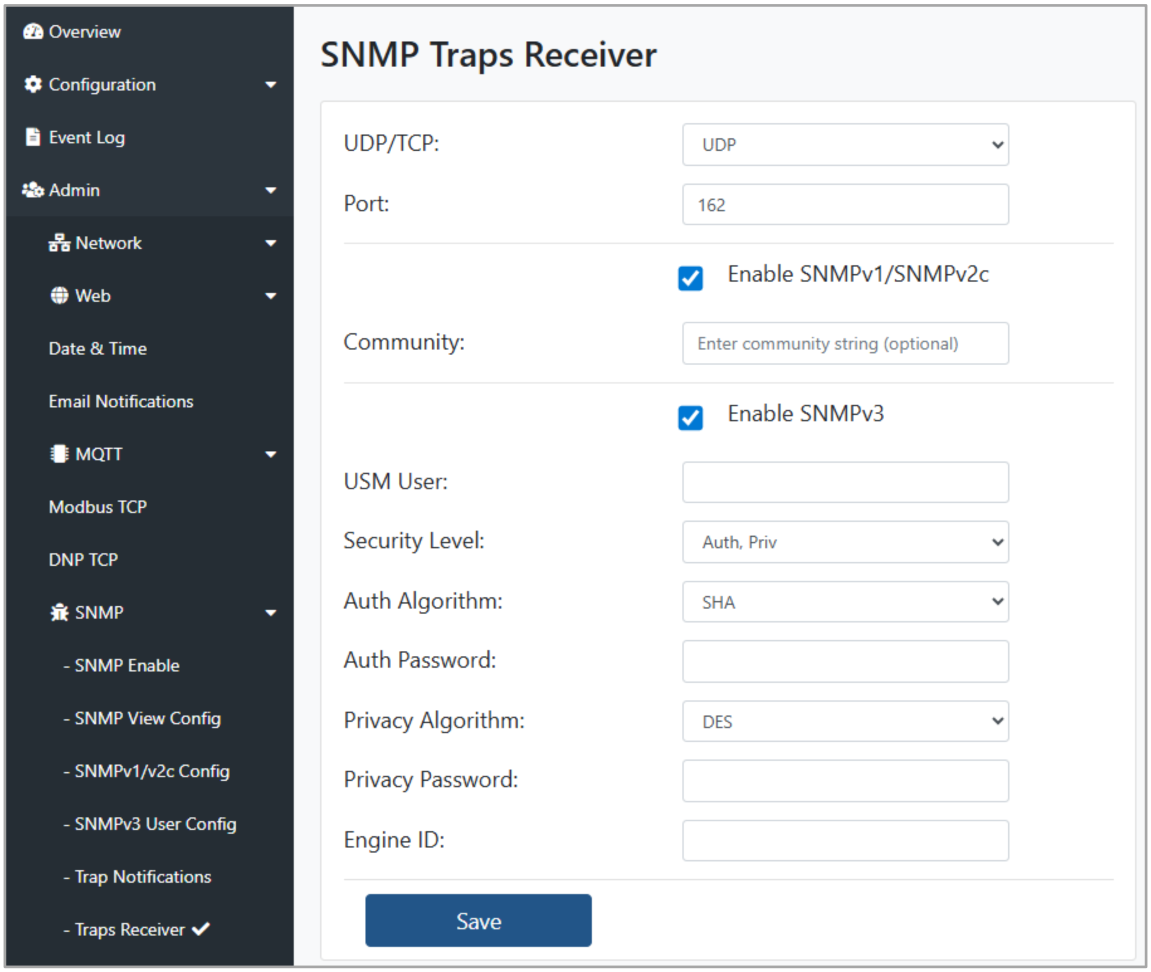
Ref #	Parameter	Description
1	`Enable SNMPv3 Trap`	Activates SNMPv2c trap delivery for the device.
2	`Host Server Address`	Specifies the IP address of the SNMPv3 trap receiver platform (e.g., NMS).
3	`Port`	Specifies the UDP port for the first SNMPv2c trap receiver platform (e.g., NMS).
4	`USM User`	Specifies the SNMPv3 account username that the trap receiving platform expects for inbound traps. This must match an SNMPv3 account defined on the trap receiver.
5	`Security Level`	Specifies the SNMPv3 account's security profile based on whether authentication and/or encryption are required. Options include "no auth,no priv", "auth,no priv", and "auth,priv".
6	`Auth Algorithm`	Specifies the SNMPv3 account's authentication algorithm, when the Security Level parameter is "auth,no priv" or "auth,priv". Options include MD5 and SHA.
7	`Auth Password`	Specifies the SNMPv3 account's password used for the selected authentication algorithm. The minimum password length is 8 characters.
8	`Privacy Algorithm`	Specifies the SNMPv3 account's encryption algorithm, when the Security Level parameter is "no auth,priv" or "auth,priv". Options include DES and AES.
9	`Privacy Password`	Specifies the SNMPv3 account's password used to generate the data-encryption key for the selected encryption algorithm. The minimum password length is 8 characters.
10	`Engine ID`	Specifies the SNMPv3 Engine ID of the trap receiver platform. The Engine ID parameter must match the Engine ID configured on the SNMPv3 management system.

SNMPv1/v2c/v3 Traps Receiver Overview

The SNMP Traps Receiver webpage allows the Smart 8 Relay Output module to operate as an SNMP trap receiver platform, listening for inbound SNMP traps transmitted by external sources, and actuating Relay Outputs in response to specific SNMP traps defined by the user.

The SNMP Traps Receiver supports both community-based (SNMPv1/v2c) and USM-secured (SNMPv3) trap formats, with configuration parameters populating onto the webpage dynamically based on which protocol versions are enabled.

This implementation also supports both UDP and TCP transportation formats, although only one of the two may be specified at once.



SNMP Traps Receiver

UDP/TCP: UDP

Port: 162

☑ Enable SNMPv1/SNMPv2c

Community: Enter community string (optional)

☑ Enable SNMPv3

USM User:

Security Level: Auth, Priv

Auth Algorithm: SHA

Auth Password:

Privacy Algorithm: DES

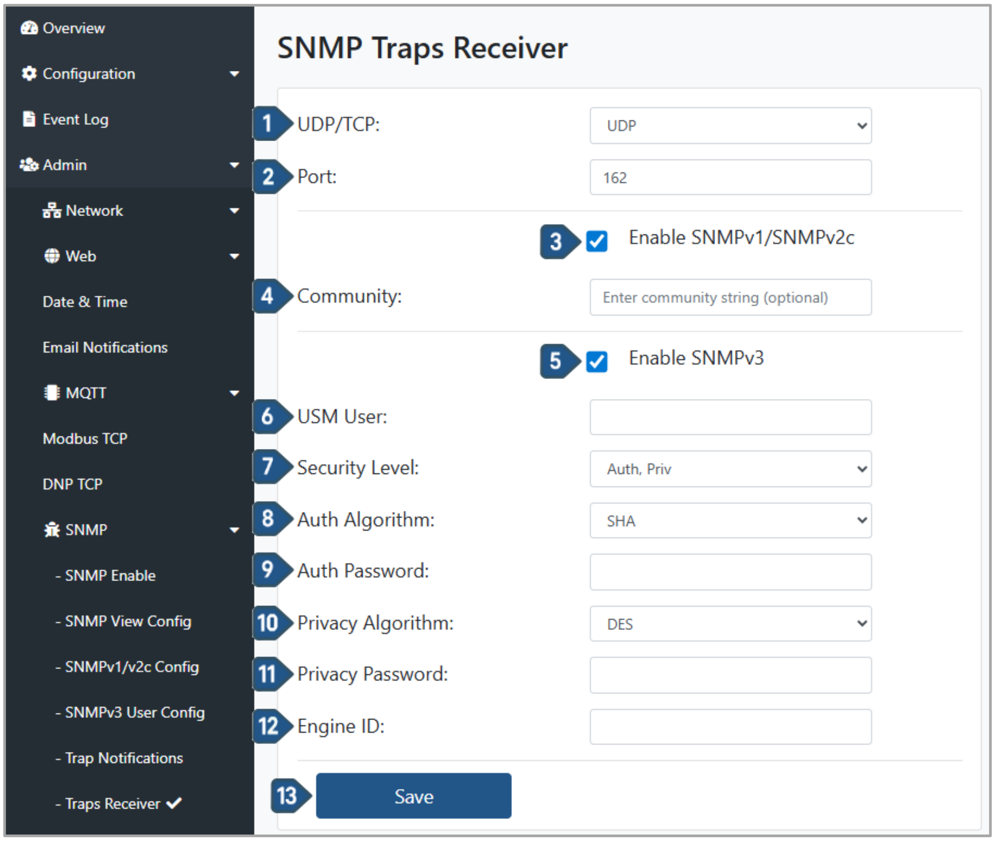
Privacy Password:

Engine ID:

Save

SNMP (Traps Receiver) - SNMPv1/v2c/v3 Traps Receiver Overview

SNMPv1/v2c/v3 Traps Receiver Configuration



SNMP Traps Receiver

1 UDP/TCP: UDP

2 Port: 162

3 ☑ Enable SNMPv1/SNMPv2c

4 Community: Enter community string (optional)

5 ☑ Enable SNMPv3

6 USM User:

7 Security Level: Auth, Priv

8 Auth Algorithm: SHA

9 Auth Password:

10 Privacy Algorithm: DES

11 Privacy Password:

12 Engine ID:

13 Save

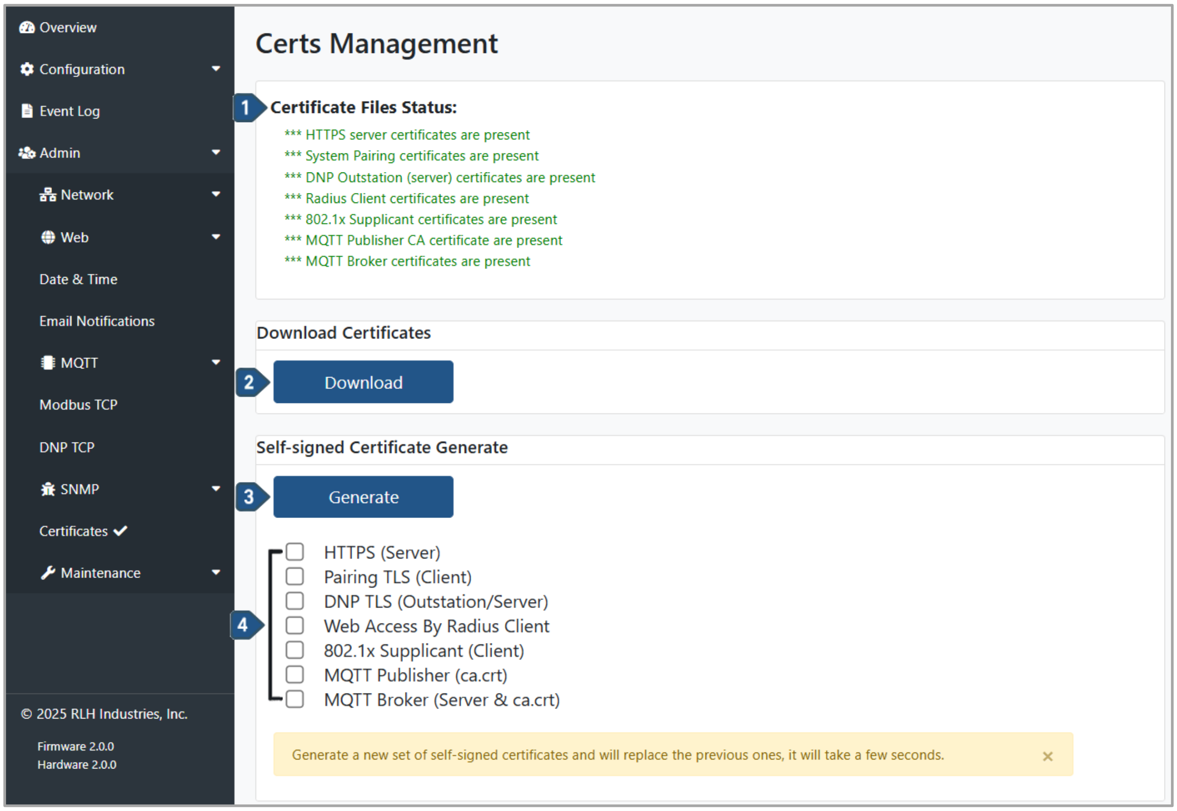
SNMP (Traps Receiver) - SNMPv1/v2c/v3 Traps Receiver Configuration

Ref #	Parameter	Description
1	`UDP/TCP`	Specifies the transport protocol (UDP or TCP) chosen. By default, UDP is selected.
2	`Port`	Defines the port on which the Smart 8 Relay Output listens for incoming traps. By default, this Port parameter is configured as 162.
3	`Enable SNMPv1/SNMPv2c`	Activates the SNMP Traps Receiver for community-based traps, using SNMPv1/v2c. When selected, the Community parameter becomes visible on the webpage.
4	`Community`	Identifies a specific trap community string expected from inbound traps. This is only for a user's reference; inbound SNMPv1/v2c traps are accepted regardless of the community string.
5	`Enable SNMPv3`	Activates the SNMP Traps Receiver for USM-facilitated traps, using SNMPv3. When selected, USM account parameters will become visible on the webpage.
6	`USM User`	Specifies the SNMPv3 account username that the SNMP Traps Receiver expects for inbound traps. This must match an SNMPv3 account defined on the trap sender platform.
7	`Security Level`	Specifies the SNMPv3 account's security profile based on whether authentication and/or encryption are required. Options include "no auth,no priv", "auth,no priv", and "auth,priv".
8	`Auth Algorithm`	Specifies the SNMPv3 account's authentication algorithm, when the Security Level parameter is "auth,no priv" or "auth,priv". Options include MD5 and SHA.
9	`Auth Password`	Specifies the SNMPv3 account's password used for the selected authentication algorithm. The minimum password length is 8 characters.
10	`Privacy Algorithm`	Specifies the SNMPv3 account's encryption algorithm, when the Security Level parameter is "no auth,priv" or "auth,priv". Options include DES and AES.
11	`Privacy Password`	Specifies the SNMPv3 account's password used to generate the data-encryption key for the selected encryption algorithm. The minimum password length is 8 characters.
12	`Engine ID`	Specifies the SNMPv3 Engine ID of the trap receiver platform. The Engine ID parameter must match the Engine ID configured on the SNMPv3 management system.
13	`Save`	Commits all SNMP Traps Receiver settings, including the underlying configuration parameters present when Enable SNMPv2c Trap or Enable SNMPv3 Trap is selected.

Certificates - Certs Management

The Certs Management webpage presents a centralized TLS/SSL certificate management interface for generating self-signed certificates, uploading certificates, or deleting certificates on the Smart 8 Input Sensor and Smart 8 Relay Output. Platform services that incorporate TLS/SSL certificates include the systems':

- HTTPS web server (server certificates)
- System Pairing TLS client (client certificate)
- DNP3/TCP outstation server (server certificates)
- RADIUS client (client certificate)
- IEEE 802.1X supplicant client (EAP-TLS client certificate)
- MQTT Publisher client (Smart 8 Input Sensor only; uses CA certificate for broker authentication)
- MQTT Subscriber client (Smart 8 Relay Output only; uses CA certificate for broker authentication)
- MQTT Broker server (CA and server certificate)



Certs Management

1 Certificate Files Status:

*** HTTPS server certificates are present
*** System Pairing certificates are present
*** DNP Outstation (server) certificates are present
*** Radius Client certificates are present
*** 802.1x Supplicant certificates are present
*** MQTT Publisher CA certificate are present
*** MQTT Broker certificates are present

Download Certificates

Self-signed Certificate Generate

□ HTTPS (Server)
□ Pairing TLS (Client)
□ DNP TLS (Outstation/Server)
□ Web Access By Radius Client
□ 802.1x Supplicant (Client)
□ MQTT Publisher (ca.crt)
□ MQTT Broker (Server & ca.crt)

Generate a new set of self-signed certificates and will replace the previous ones, it will take a few seconds. ×

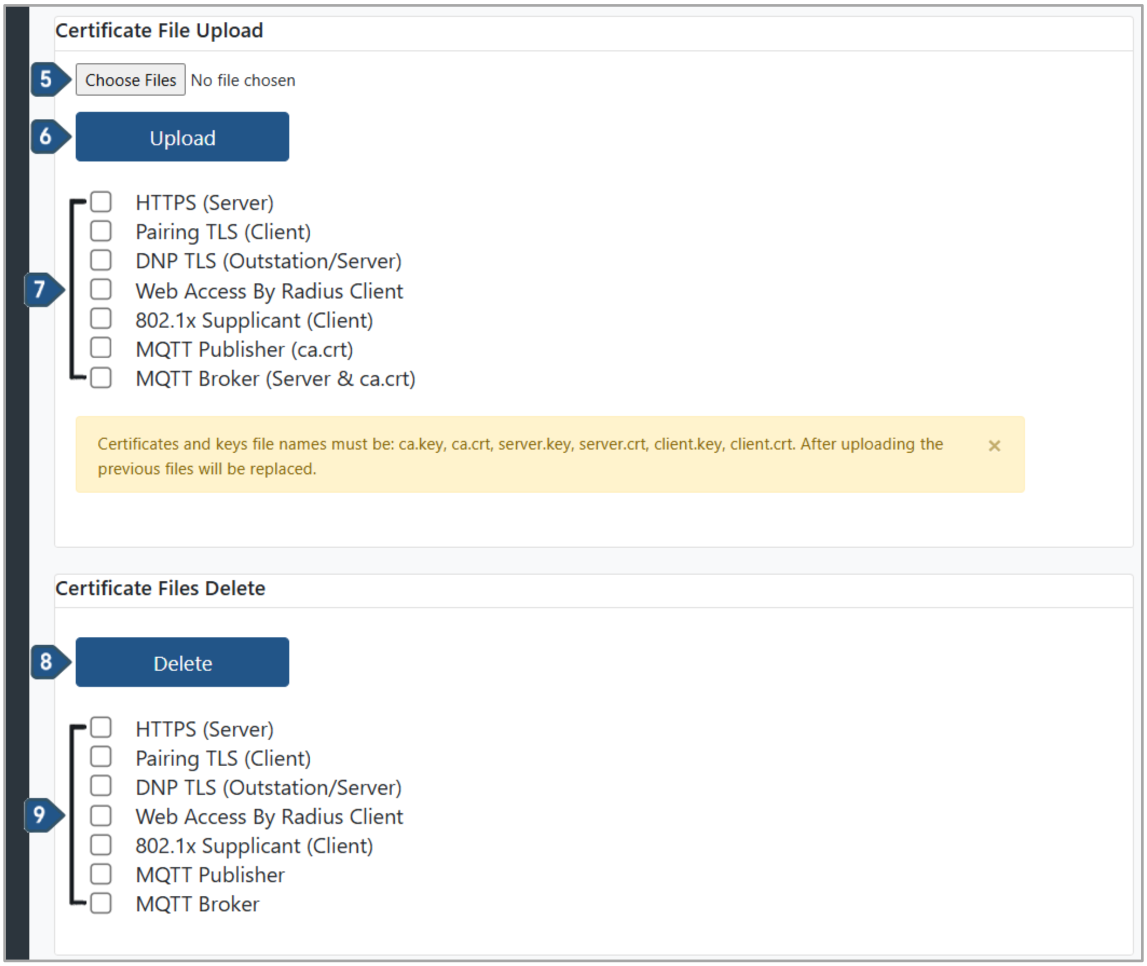
Certificates - Certs Management

Ref #	Parameter	Description
1	`Certificate Files Status`	This section provides a summary of all TLS/SSL certificate stores present across the platform. Each certificate is identified as either "present" (green text) or "not present" (red text) for the corresponding server or client service.
2	`Download`	Opens the Download Configuration Files webpage used for downloading the device's factory-default certificates, keys, MQTT broker server configuration, and SNMP MIB file.
3	`Generate`	Replaces the current TLS/SSL certificates and private keys with factory-default, self-generated versions. Select the Download button to view these factory-default files.
4	`TLS/SSL Certificate Store (Generate)`	Specifies which platform service(s) will receive self-signed certificates upon the generation. When selections are finalized, selecting the Generate button will generate the certificates. If the selected services already have certificates present, they will be overwritten with self-signed certificates.

Certificates - TLS/SSL Certificate Management Store

Administrators may upload CA-issued certificates, server/client certificates, and private keys onto the TLS/SSL certificate management store used by various platform features. Certificates and private keys may also be removed entirely from the existing certificate management store.

When uploading TLS/SSL certificates, note that the certificate file's maximum file size should not exceed 3KB, and that the webpage must be refreshed for the Certificate File Status to update. Supported file extensions include .crt for certificates, and .key for private keys.



Certificate File Upload

Choose Files No file chosen

Upload

□ HTTPS (Server)
□ Pairing TLS (Client)
□ DNP TLS (Outstation/Server)
□ Web Access By Radius Client
□ 802.1x Supplicant (Client)
□ MQTT Publisher (ca.crt)
□ MQTT Broker (Server & ca.crt)

Certificates and keys file names must be: ca.key, ca.crt, server.key, server.crt, client.key, client.crt. After uploading the previous files will be replaced. ×

Certificate Files Delete

Delete

□ HTTPS (Server)
□ Pairing TLS (Client)
□ DNP TLS (Outstation/Server)
□ Web Access By Radius Client
□ 802.1x Supplicant (Client)
□ MQTT Publisher
□ MQTT Broker

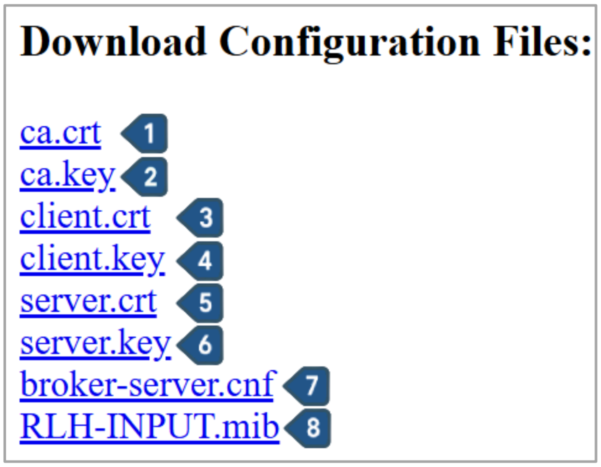
Certificates - Certs Management

Ref #	Parameter	Description
5	`Choose Files`	Opens a window to select one or more certificate files for uploading.
6	`Upload`	Initiates the certificate upload process. Uploaded certificates will replace any existing certificates present on the selected TLS/SSL Certificate Store(s).
7	`TLS/SSL Certificate Store (Upload)`	Specifies which platform service(s) the uploaded certificate files belong to. Each service expects a specific subset of certificate files (e.g., "Server" for server.crt).
8	`Delete`	Initiates the certificate deletion process. All certificate files associated with the selected platform service(s) will be removed. Upon deletion, the associated Certificate Files Status will be updated to "not present".
9	`TLS/SSL Certificate Store (Delete)`	Specifies which platform service(s) will have their certificate files removed.

TLS/SSL Certificate Management Store - Download

The Download Configuration Files webpage is initiated by selecting the "Download" button, and provides administrators with direct access to all factory-default, self-generated TLS/SSL certificate files: CA certificate, client certificate, server certificate, an each certificate's private key file.

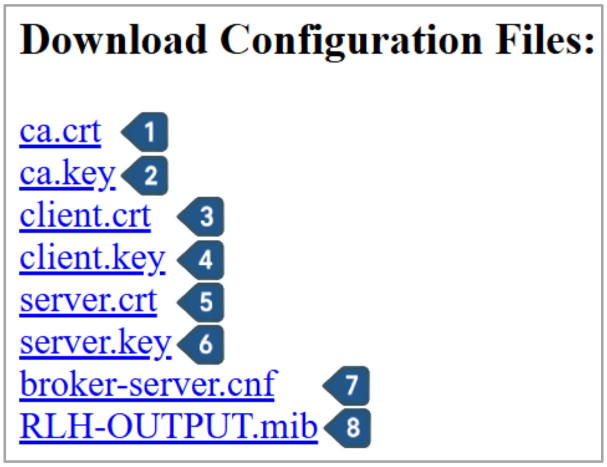
Also included is the default OpenSSL configuration file used for generating self-signed certificates with an MQTT TLS (MQTTS) broker, and the device's SNMP MIB file. The MIB file will appropriately reflect the device model, for either the Smart 8 Input Sensor (RLH-INPUT.mib) or Smart 8 Relay Output (RLH-OUTPUT.mib).



Download Configuration Files:

ca.crt
ca.key
client.crt
client.key
server.crt
server.key
broker-server.cnf
RLH-INPUT.mib

Certificates - Download (Smart 8 Input Sensor)



Download Configuration Files:

ca.crt
ca.key
client.crt
client.key
server.crt
server.key
broker-server.cnf
RLH-OUTPUT.mib

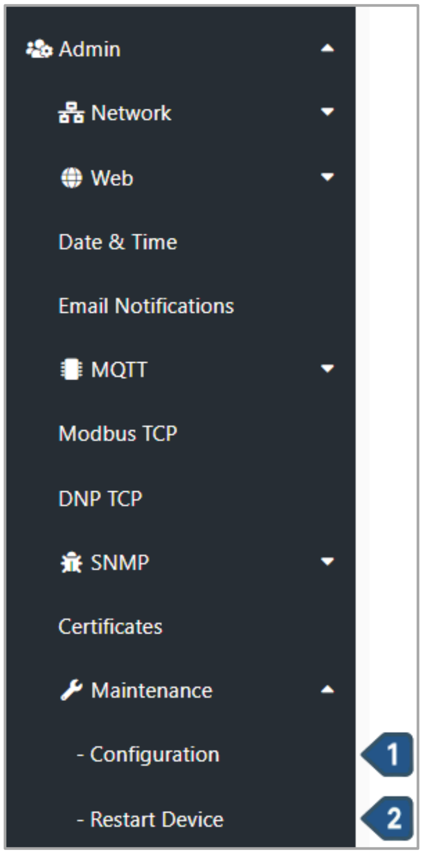
Certificates - Download (Smart 8 Relay Output)

Ref #	Parameter	Description
1	`ca.crt`	Downloads the factory-default Certificate Authority (CA) certificate used for validating remote TLS servers. This is required for verifying HTTPS servers, secure MQTT TLS (MQTTS) brokers, RADIUS servers, and DNP3/TLS peers.
2	`ca.key`	Downloads the factory-default private key paired with the CA certificate.
3	`client.crt`	Downloads the factory-default client certificate used when the Smart 8 Input Sensor or Smart 8 Relay Output authenticates itself to remote TLS servers. This is required for using System Pairing with TLS encryption when functioning in Client Mode. It is also required for RADIUS (web access) and IEEE 802.1X authentication when EAP-TLS is used as the EAP method.
4	`client.key`	Downloads the factory-default private key paired with the client certificate.
5	`server.crt`	Downloads the factory-default server certificate used when the Smart 8 Input Sensor or Smart 8 Relay Output is hosting an HTTPS server, DNP3 TLS server, secure MQTT TLS (MQTTS) broker, or is using System Pairing with TLS encryption when functioning in Server Mode.
6	`server.key`	Downloads the factory-default private key paired with the server certificate.
7	`broker-server.cnf`	Downloads the factory-default OpenSSL configuration file used to regenerate or customize the TLS server certificate used for the embedded MQTT broker, when MQTT TLS (MQTTS) is enabled.
8	`RLH-INPUT.mib / RLH-OUTPUT.mib`	Downloads the SNMP Management Information Base (MIB) file for either the Smart 8 Input Sensor ("RLH-INPUT.mib") or Smart 8 Relay Output ("RLH-OUTPUT.mib").

Maintenance (Navigation Panel) Overview

The Maintenance Navigation Panel presents access to system-level tools for device configuration administration, and remotely performing a system power cycle.

This Navigation Panel will only contain two drop-down options: Configuration, and Restart Device



Maintenance - Navigation Panel

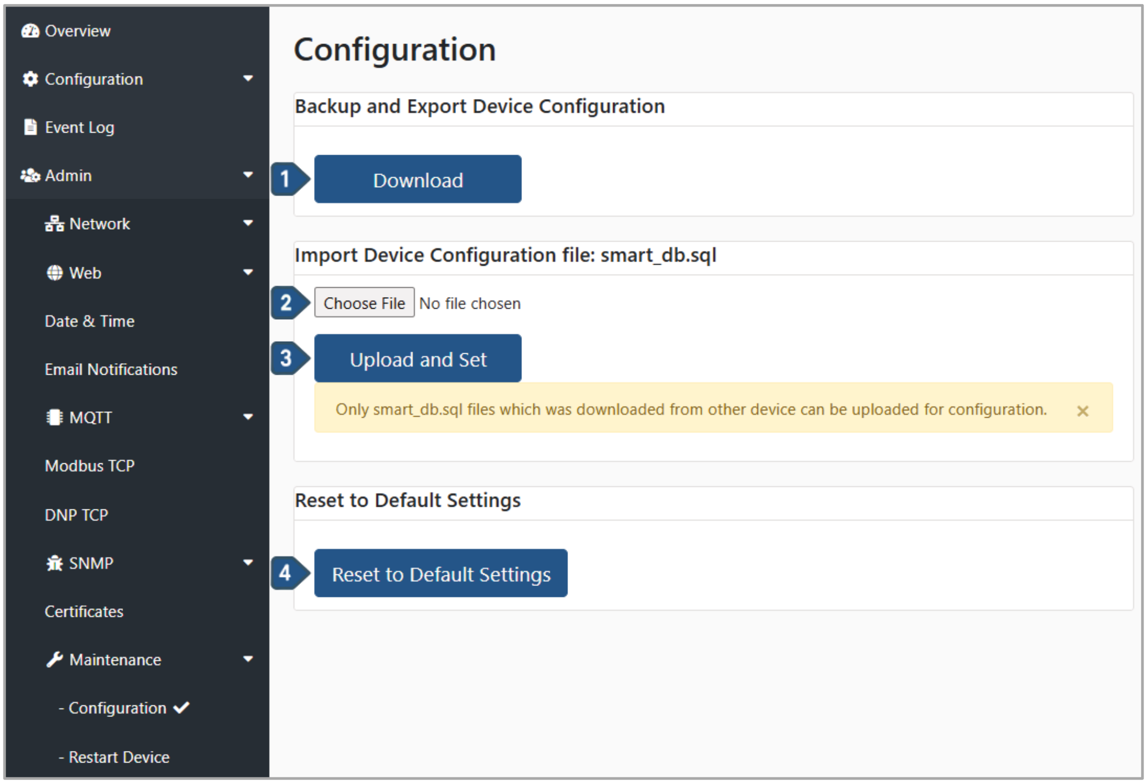
Ref #	Parameter	Description
1	`Configuration`	Opens the Configuration webpage for saving, exporting, importing, or restoring all configuration settings.
2	`Restart Device`	Opens the Restart webpage for securely, and remotely, initiating a system power cycle.

Maintenance (Configuration) Management

The Configuration webpage provides tools for backing up, restoring, and resetting the Smart 8 Input Sensor or Smart 8 Relay Output's system configuration.

Administrators may download the current configuration settings as a .sql database file ("smart_db.sql"), and import it on another Smart 8 Input Sensor or Smart 8 Relay Output device.

When importing a Device Configuration file, please ensure that the device does not remain on the same network, or shares the imported IP addresses with another device on the network. Otherwise, IP address conflicts will arise.



Configuration

Backup and Export Device Configuration

Import Device Configuration file: smart_db.sql

Only smart_db.sql files which was downloaded from other device can be uploaded for configuration.

Reset to Default Settings

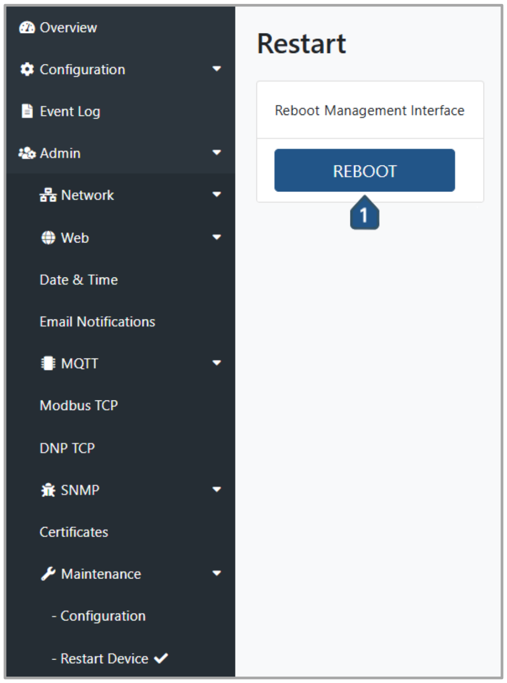
Maintenance - Configuration Management

Ref #	Parameter	Description
1	`Download`	Creates and downloads a complete backup of the device's configuration database. The downloaded file ("smart_db.sql") contains all saved system settings, and may be imported onto other devices.
2	`Choose File`	Opens a window to select a Device Configuration file for uploading.
3	`Upload and Set`	Uploads the selected Device Configuration, and applies all configuration settings contained within it.
4	`Reset to Default Settings`	Restores all system configuration parameters to their factory-default state.

Maintenance (Restart Device) - Restart

The Restart webpage provides a safe and controlled method for rebooting the Smart 8 Input Sensor, or Smart 8 Relay Output.

The REBOOT command offered will ensure that all system services safely shut down, prior to the system performing a power cycle. This power cycle may take one to two minutes before the device may be accessed.



Maintenance (Restart Device) - Restart

Ref #	Parameter	Description
1	`Reboot`	Initiates a full power cycle of the Smart 8 Input Sensor, or Smart 8 Relay Output.