

Stellaris Web-Client Reference Manual

Release: 4.1.1-a5443afe

Date: 2025-10-29

Copyright: RNX Ltd Switzerland

Applies to products: RNX UPDU, RNX SPDU, Bachmann BN Essential

Contents

0.1	Glossary	3
1	Introduction	4
1.1	Logging in	4
1.2	IP address via local UI	5
2	Home	6
2.1	Summary	6
2.2	Support	6
2.3	Changing the password	7
2.4	Logging out	7
3	Analyzer	8
3.1	Objects	8
3.2	Identify feature	8
3.3	Monitoring rules	9
3.4	Outlet Switching	10
4	Environment	11
4.1	Monitoring rules	11
5	Settings	12
5.1	General	12
5.2	Network	14
5.3	Services	16
5.4	Authentication	20
5.5	Certificates	23
6	Maintenance	26
6.1	Support	26
6.2	Device Overview	26
6.3	Licenses	27
6.4	Firmware update	27
6.5	Reboot the device	28
6.6	Configuration Management	28
6.7	Diagnostics	29
6.8	Factory Reset	29
7	User Management	31
7.1	Create a new user	31
7.2	Create a new role	31
7.3	Editing an existing user	31
8	Log	32
9	Legal	33

0.1 Glossary

API	Application Programming Interface
AUX	AUXiliary
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MIB	Management Information Base (SNMP)
NTP	Network Time Protocol
PC	Personal Computer
PDU	Power Distribution Unit
PoE	Power over Ethernet
REST	REpresentational State Transfer
RSTP	Rapid Spanning Tree Protocol
SNTP	Simple Network Time Protocol
SNMP	Simple Network Management Protocol
SSH	Secure SHell
STP	Spanning Tree Protocol
TCP	Transfer Control Protocol
UTC	Coordinated Universal Time

1 Introduction

Thank you for purchasing a Power Distribution Unit from RNX.

Each PDU of the family can be accessed, read and configured via a simple web interface and this document describes how to use this interface.

Please refer to the *Hardware User Manual* for details on how to use and install the hardware which can be found the the vendor's support page.

The web interface allows configuration the most common features of the product. More advanced options are available on the command-line interface (CLI). For more information regarding the CLI, refer to the *CLI Reference Manual*.

1.1 Logging in

The web-interface is served on all the available network interfaces.

- By default, the device is configured to get an IP address via DHCP.
- All Ethernet ports also support Auto-IP.

The web interface can be accessed via any of the below mentioned browsers by simply typing `https://` followed by the IP address (e.g. `https://192.168.1.57`).

Note: Supported browser versions:

- Chrome version 67 or newer
- Edge version 80 or newer
- Firefox version 58 or newer
- Safari version 12.1 or newer

As by default an IP address can not be assigned a valid TLS certificate, a warning message such as the following will likely appear.

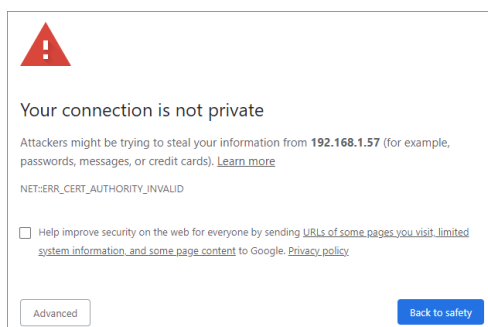


Figure 1: HTTPS connection warning message

This can usually be bypassed by clicking on `Advanced` and `Proceed to ...` (or similar depending browser). The connection should now be established and the login screen appears:

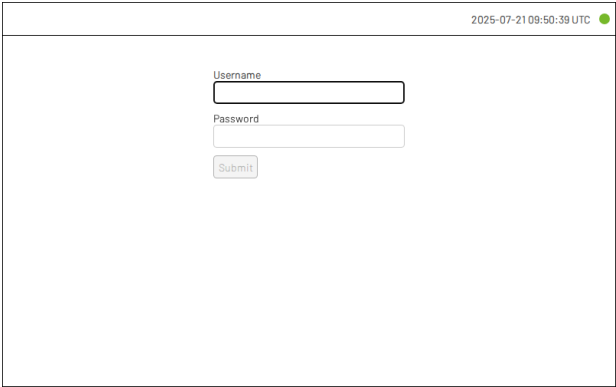


Figure 2: Login dialog box

Warning: Factory defaults - Change password!

The default username is “admin” and the default password is “admin”. It is crucial to change the default password immediately after completing the initial configuration.

1.2 IP address via local UI

The current IP address can be obtained from the local user-interface by using the following sequence on the controller.

hostname

L1 L2 L3
0.0A 0.0A 0.0A

5 W

1.0mA RMS
0.1mA DC

INFO 1/4

FW 4.1.0-DEV (af92638c)
Model PDU
P/N 100-0001-1
S/N 100499
Date 2025-07-21
Time 07:17:46 UTC
Uptime 0h05:56

INFO 2/4

Network port ETH1
MAC d4:66:a8:10:0b:6a
Link UP
IPv4 DHCP 10.2.18.138
IPv6 SLAAC n/a

Note that depending on the device model, additional button clicks may be required to land on the information page.

2 Home

After logging on, the main page with a context menu on the left is shown.

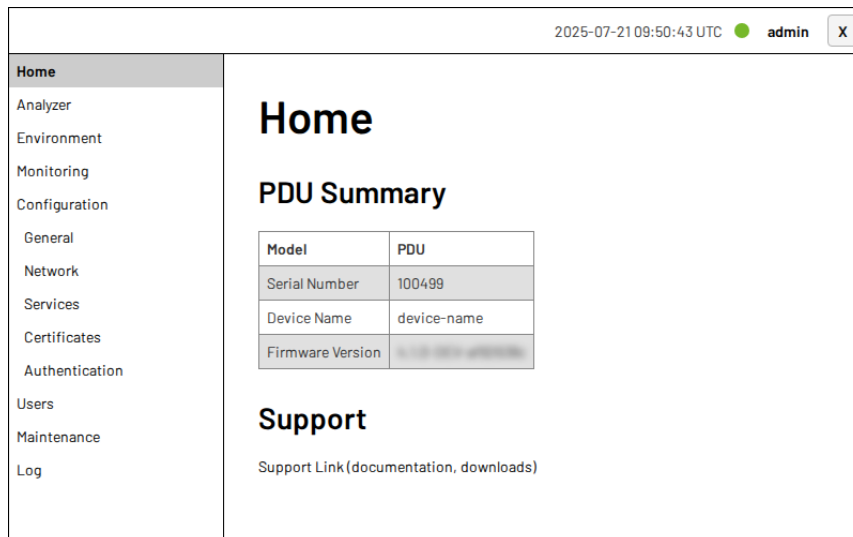


Figure 3: Landing page after login

2.1 Summary

A summary of the device's most important details is shown on the landing page.

PDU Summary

Model	PDU
Serial Number	100499
Device Name	device-name
Firmware Version	1.0.0-2023-08-08-10:00:00

Figure 4: Device summary

2.2 Support

Additionally, a link to the most important documents, new firmware and other support material is provided on the landing page.

2.3 Changing the password

By clicking on the logged in username (e.g. `admin`) a user would see its own profile information along with the option to configure `SSH Keys` and change the password. As opposed to most other settings, the new password is immediately stored persistently.

2.4 Logging out

Clicking the `x` button in the top-right corner of the web-client allows to immediately logout the current user.

Warning

A user session may remain active for a while even after closing a browser window. Using the logout button is highly recommended especially on shared clients.

3 Analyzer

The analyzer page shows real-time measurement values taken by the device. The values are automatically updated every second.

The tables, their size and the values shown depend on the hardware configuration of the device.

	P(W)	Q(var)	S(VA)	U(V)	I(A)	RCM RMS (mA)	RCM DC (mA)	Energy (kWh)
Total	4.9	-2.9	10.6	235.5	0.045	1.0	0.0	80.433
Phase L1	4.9	-2.9	10.6	235.5	0.045	-	-	79.587
Phase L2	0.0	0.0	0.0	235.5	0.000	-	-	0.698
Phase L3	0.0	0.0	0.0	235.0	0.000	-	-	0.148

Module	Phase	P(W)	Q(var)	S(VA)	U(V)	I(A)	Energy (kWh)

Figure 5: The analyzer page

3.1 Objects

By clicking on the name of an object it is possible to edit its and add a description. If no name has been set "n/a" is displayed.

By hovering the mouse over the name the description is shown.

3.2 Identify feature

The UID function (short for unit identification) is useful to help an on-site engineer to find a device, a module or an outlet by blinking the outlet LEDs of the selected object. In a typical setup with multiple devices next to each other, this helps to avoid wiring issues.

It is activated by clicking the indication light symbol next to the object name.

	P(W)	Q(var)	S(VA)	U(V)	I(A)	RCM RMS (mA)	RCM DC (mA)	Energy (kWh)
Total	4.9	-2.9	10.6	235.7	0.045	1.0	0.1	80.433
Phase L1	4.9	-2.9	10.6	235.6	0.045	-	-	79.587
Phase L2	0.0	0.0	0.0	235.7	0.000	-	-	0.698
Phase L3	0.0	0.0	0.0	235.2	0.000	-	-	0.148

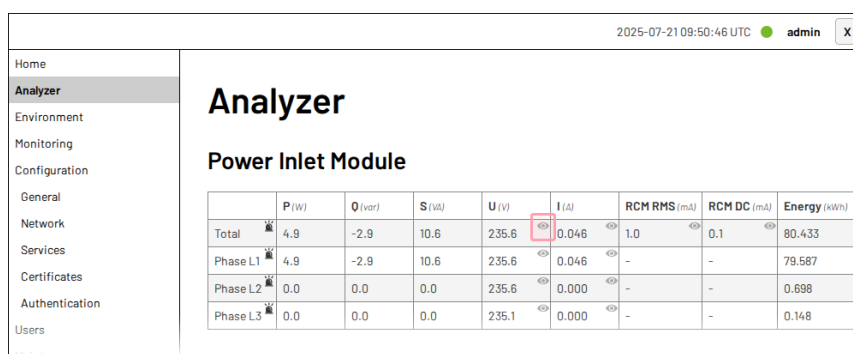
Figure 6: Identify button

By default, the UID function is active for 5 minutes. It can also be stopped from the web-client or locally on the device.

3.3 Monitoring rules

Rules define conditions which are monitored. If a condition is not satisfied, an alert message is logged locally and remotely if configured (see Syslog Logging), and notifications can be sent if configured (see SNMP Service Configuration).

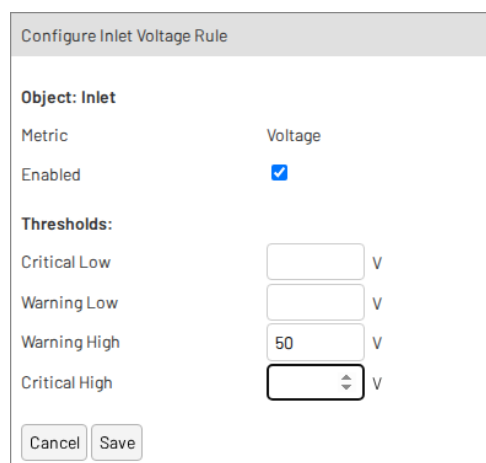
Rules are configured by clicking on the eye-shaped symbol within a value cell and support multiple thresholds.



	P (W)	Q (var)	S (VA)	U (V)	I (A)	RCM RMS (mA)	RCM DC (mA)	Energy (kWh)
Total	4.9	-2.9	10.6	235.6	0.046	1.0	0.1	80.433
Phase L1	4.9	-2.9	10.6	235.6	0.046	-	-	79.587
Phase L2	0.0	0.0	0.0	235.6	0.000	-	-	0.698
Phase L3	0.0	0.0	0.0	235.1	0.000	-	-	0.148

Figure 7: Monitoring watch button

Once a rule is enabled for a certain metric, messages may immediately be sent. This can be used to test the messaging sent by different rules by setting a threshold below or above the current measurement value. The following example configuration should trigger a warning message upon saving the rule. Note that the device must be connected to mains for the threshold to trigger.



Configure Inlet Voltage Rule

Object: Inlet

Metric: Voltage

Enabled: ☒

Thresholds:

Critical Low: V

Warning Low: V

Warning High: 50 V

Critical High: V

Cancel Save

Figure 8: Monitoring watch test configuration

Note that the monitoring messages are also shown in the Log section as well as in the Monitoring section.

3.4 Outlet Switching

Outlets equipped with relays can be switched on and off individually. Outlets are identified using the module label and the outlet number printed on the PDU. Buttons to control switchable outlets are shown in the **Switch** column of the module table.













Object	Name	P (W)	Q (var)	S (VA)	U (V)	I (A)	PF	Energy (kWh)	Switch
Outlet1.1	asdf	0.0	0.0	0.0	235.6	0.000	0.00	0.029	 cycle 
Outlet1.2	n/a	0.0	0.0	0.0	235.6	0.000	0.00	0.022	 cycle 
Outlet1.3	n/a	0.0	0.0	0.0	235.6	0.000	0.00	0.022	 cycle 
Outlet1.4	n/a	0.0	0.0	0.0	235.6	0.000	0.00	0.022	 cycle 
Outlet1.5	n/a	0.0	0.0	0.0	235.6	0.000	0.00	0.023	 cycle 
Outlet1.6	n/a	0.0	0.0	0.0	235.6	0.000	0.00	0.021	 cycle 

Figure 9: Table of a device with a switchable outlets

The outlets of a module with switching function can be individually switched on and off by clicking on the red or green button, provided that the user has enough privileges. If the button is red the outlet is off; if it's green it's on. A pop-up window asks for confirmation before the outlet is switched.

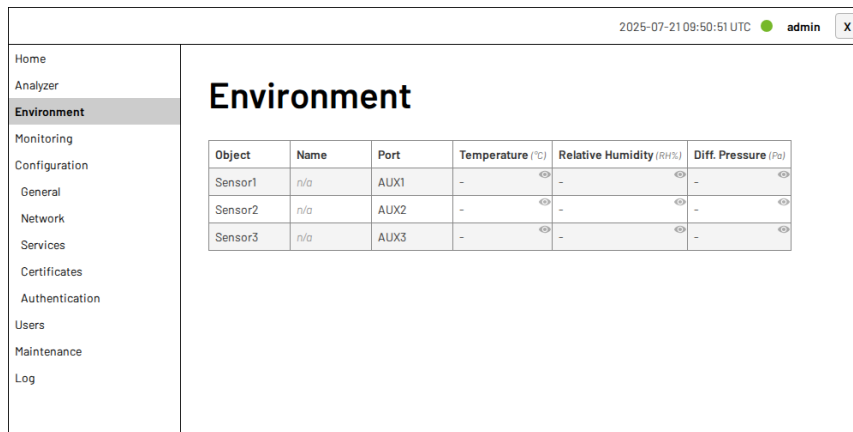
Outlet can also be automatically cycled off and back on automatically after a certain delay. This allows power-cycling an equipment even if the connection to this device depends on the equipment itself.

Warning

When remotely switching a relay, the operator must be sure that the load connected to the outlet being remotely switched, will not generate a dangerous situation. A such example would be starting a dangerous machine.

4 Environment

In the environment page, the temperature and humidity values are displayed according to the type of sensors connected to AUX ports of the Controller.



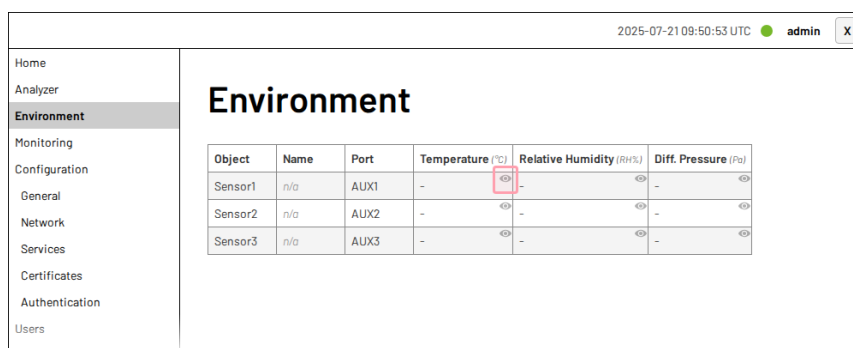
Object	Name	Port	Temperature (°C)	Relative Humidity (RH%)	Diff. Pressure (Pa)
Sensor1	n/a	AUX1	-	-	-
Sensor2	n/a	AUX2	-	-	-
Sensor3	n/a	AUX3	-	-	-

Figure 10: Environment values table

4.1 Monitoring rules

Rules define conditions which are monitored. If a condition is not satisfied, an alert message is logged locally and remotely if configured (see Syslog Logging), and notifications can be sent if configured (see SMTP Service Configuration).

Rules are configured by clicking on the eye-shaped symbol within a value cell and support multiple thresholds.



Object	Name	Port	Temperature (°C)	Relative Humidity (RH%)	Diff. Pressure (Pa)
Sensor1	n/a	AUX1	-	-	-
Sensor2	n/a	AUX2	-	-	-
Sensor3	n/a	AUX3	-	-	-

Figure 11: Environment watch button

Refer to *Monitoring rules* for more information about the configuration of watches on measurement values.

5 Settings

Settings can be directly configured in the different **Settings** pages. The most common settings are configurable from the web-client. Note however that some of the settings can only be configured via the command-line interface.

Unless documented otherwise, changes to settings are effective immediately but are not persisted until the **Save configuration** button is clicked.

Note

It is important to persist the settings as a restart of the device will revert the configuration to the last persisted state.

5.1 General

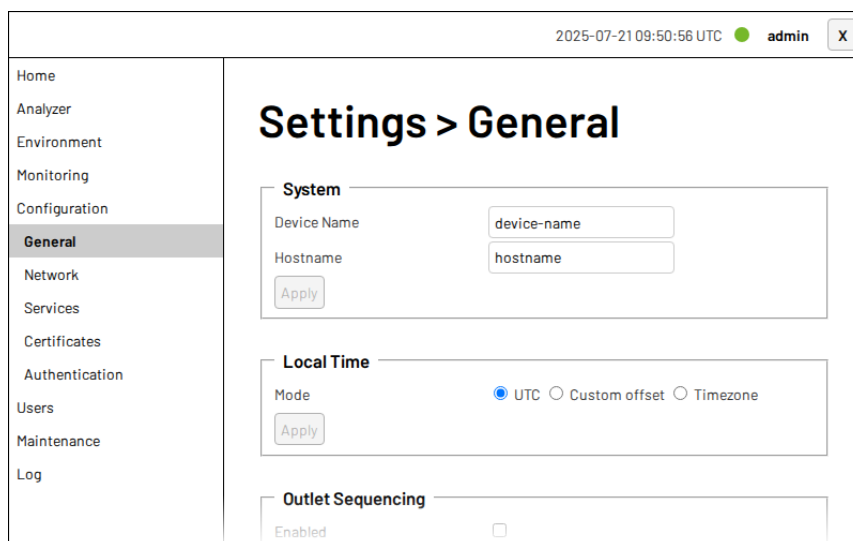


Figure 12: General settings page

5.1.1 System settings

The **System** settings allow to change the device's hostname and device name. The hostname is used in DHCP requests and the device name is used as **sysName** in the standardized SNMP MIB-II System Group.

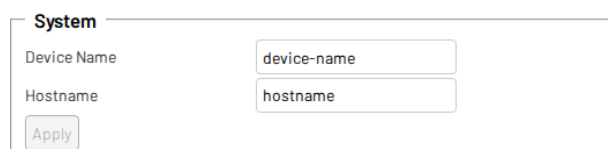


Figure 13: Device and hostname configuration dialog.

The hostname is also shown on the device's local user-interface.

5.1.2 Time settings

By default the PDU is configured to use UTC time. It is possible to select a local time zone either by entering a custom offset or by selecting a time zone from a list.

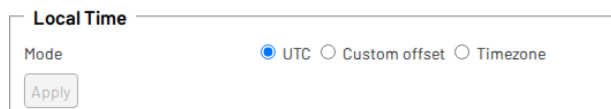


Figure 14: UTC timezone is used by default

By selecting a custom offset, it is possible to enter the offset in hours and minutes. The format to use is indicated next to the input field, e.g. `+7:00`, and is an offset from `UTC`.

5.1.3 Outlet sequencing

Products with switchable outlets can be configured for autonomous outlet sequencing. Upon a power-loss all outlets are switched off and gradually switched on once power is restored. This mechanism helps to reduce inrush currents.

Latching relays are used for switching outlets. Latching relays are not dependent on power to maintain their state. The relays thus have to be explicitly opened when a power outage is detected. Therefore, in order for the outlet sequencing feature to work, it is crucial that the device is powered by Power over Ethernet (PoE), even during a power outage. Should the PoE supply also be affected by the power outage, it is important to enable the PoE supply at least one minute before the mains power.

When `outlet-sequencing` is enabled and a power outage is detected, the device immediately switches off all affected outlets which are currently switched on. This happens in a couple of seconds.

Afterwards, once power is restored and deemed stable, outlets which were automatically switched off are switched on again.

Certain earlier switchable devices do not support the outlet sequencing functionality. This limitation will be addressed in a future firmware version. Upon enabling this feature on a currently unsupported PDU, a warning message is shown.

Important: The Interface and Controller Module (ICM) needs backup PoE power in order to switch outlets during a power outage or at least one minute before the mains power is restored.

Outlet Sequencing

Enabled ☐

Power-On Stable-Time seconds

Power-On Delay seconds

Figure 15: Outlet sequencing

Global Parameters

The following parameters are applied system-wide (globally) when the outlet sequencing feature is enabled. Some of these parameters can be overridden individually per outlet.

Two global parameters allow to fine-tune the power on behaviour:

- **Power-On Stable-Time** defines the time in seconds during which the restored power has to be stable before outlets are switched on again. Each power event happening during this time will restart the timer and further delay switching on the outlets.
- **Power-On Delay** defines the interval in which individual outlets are switched on once power is restored. After each outlet, the system waits for the specified number of seconds before proceeding with the next outlet. When **delay** is set to **disabled**, outlets are switched on as fast as possible.

5.2 Network

2025-07-21 09:50:57 UTC ● admin X

Home
Analyzer
Environment
Monitoring
Configuration
General
Network
Services
Certificates
Authentication
Users
Maintenance
Log

Settings > Network

General

Outgoing Interface

ETH1

Enabled ☒

MAC Address

Link state

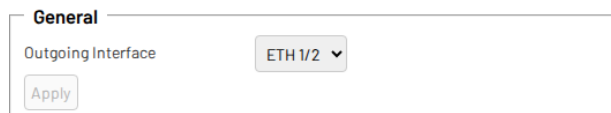
DHCP hostname

IPv4

Figure 16: Networking settings page

5.2.1 General settings

The default outgoing interface is the interface used by the device initiated outgoing traffic. Any network traffic initiated from the device, such as DNS requests, syslog events, NTP updates etc. are solely sent via the default outgoing interface.



The screenshot shows a 'General' settings panel. It contains a label 'Outgoing Interface' next to a dropdown menu currently set to 'ETH 1/2'. Below the dropdown is an 'Apply' button.

Figure 17: Setting the default outgoing interface

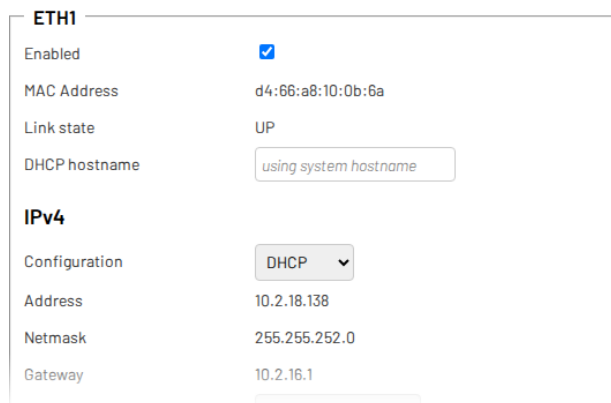
DNS Lookups

DNS Lookups are done using the DNS servers configured on the default outgoing network interface. If the default outbound network interface has IPv6 active, the device first does IPv6 lookups. If that lookup fails, it falls back to IPv4 lookups.

5.2.2 ETH1 and ETH2

ETH1 and ETH2 are switched (or bridged), thus act as a single interface above layer two. The physical ports (link) can be individually enabled or disabled, but any higher level configuration (IP, ..) is always applied to both ports.

By default, the device uses DHCP for IPv4 address configuration and falls back to Auto-IP setup after failing to obtain a valid address. SLAAC is used for IPv6 address configuration by default.



The screenshot shows the 'ETH1' settings panel. It includes a table of settings:

Enabled	<input checked="" type="checkbox"/>
MAC Address	d4:66:a8:10:0b:6a
Link state	UP
DHCP hostname	using system hostname
IPv4	
Configuration	DHCP
Address	10.2.18.138
Netmask	255.255.252.0
Gateway	10.2.16.1

Figure 18: ETH1 port network settings

As mentioned above, ETH2 is bridged to ETH1 and thus only the link layer can be configured.

ETH2

Enabled

☒ (bridged to ETH1)

Link state

DOWN

Apply

Figure 19: ETH2 port network settings

5.2.3 ETH3

ETH3 is an independent port on a dedicated network interface and has the same settings as ETH1. ETH3 cannot be bridged to ETH1/2.

ETH3

Enabled

☒

MAC Address

d4:66:a8:10:0b:69

Link state

DOWN

DHCP hostname

using system hostname

IPv4

Configuration

DHCP

Address

n/a

Netmask

n/a

Gateway

n/a

Figure 20: ETH3 port network settings

5.3 Services

The service settings allow the configuration of the important services and protocols operating on the device.

Home
Analyzer
Environment
Monitoring
Configuration
General
Network
Services
Certificates
Authentication
Users
Maintenance
Log

2025-07-21 09:50:59 UTC ● admin X

Settings > Services

Webserver

HTTP Enabled

☒

HTTPS Enabled

☒

Redirect to HTTPS

☐

HTTP Strict Transport Security

☐

TLS certificate

built-in: generic built-in certificate

Apply

STP

Enabled

☐

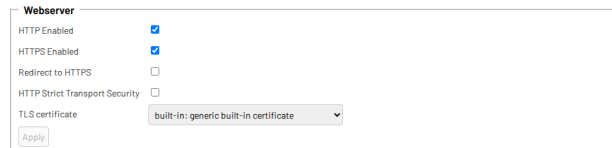
Version

☐ STP(Classic)
☒ RSTP(Rapid)

Figure 21: Services settings page

5.3.1 Webserver

The Webserver configuration configures the different options to access the web-client and the device's REST API.



The Webserver settings panel includes the following options:

Option	Value
HTTP Enabled	<input checked="" type="checkbox"/>
HTTPS Enabled	<input checked="" type="checkbox"/>
Redirect to HTTPS	<input type="checkbox"/>
HTTP Strict Transport Security	<input type="checkbox"/>
TLS certificate	built-in: generic built-in certificate

An 'Apply' button is located at the bottom left of the panel.

Figure 22: Webserver settings

5.3.2 SSH

The SSH protocol can be used to securely connect to the command line interface of the device.



The SSH settings panel includes the following options:

Option	Value
Enabled	<input type="checkbox"/>

An 'Apply' button is located at the bottom left of the panel.

Figure 23: SSH settings

5.3.3 Telnet

The Telnet protocol can be used to connect to the command line interface of the device. It is kept for legacy reasons and is disabled by default. Due to the missing transport encryption of login details, it is highly suggested to use the secure SSH protocol instead.



The Telnet settings panel includes the following options:

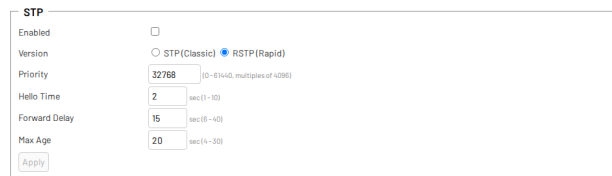
Option	Value
Enabled	<input type="checkbox"/>

An 'Apply' button is located at the bottom left of the panel.

Figure 24: STNP settings

5.3.4 STP/RSTP

The spanning-tree configuration can be used to modify spanning tree protocol settings. The spanning tree protocol is applied to the bridged ETH1 and ETH2 ports.



STP

Enabled ☐

Version ☐ STP(Classic) ☒ RSTP(Rapid)

Priority (0-65535, multiples of 4096)

Hello Time sec (1-10)

Forward Delay sec (16-40)

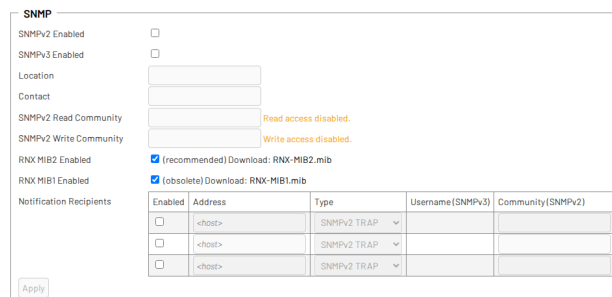
Max Age sec (6-300)

Figure 25: STP/RSTP settings

The STP/RSTP protocol allows connecting devices in a network loop to create a redundant connection in case one link fails. The protocol takes care of automatically breaking the loop and reconnect in case of a fault. RSTP is used by default.

5.3.5 SNMP

The industry standard protocol to remotely obtain measurement and monitoring values is by using the Simple Network Management Protocol (SNMP).



SNMP

SNMPv2 Enabled ☐

SNMPv3 Enabled ☐

Location

Contact

SNMPv2 Read Community Read access disabled.

SNMPv2 Write Community Write access disabled.

RNX MIB2 Enabled ☒ (recommended) Download: RNX-MIB2.mib

RNX MIB1 Enabled ☒ (obsolete) Download: RNX-MIB1.mib

Notification Recipients

Enabled	Address	Type	Username(SNMPv3)	Community(SNMPv2)
<input type="checkbox"/>	<host>	SNMPv2 TRAP		
<input type="checkbox"/>	<host>	SNMPv2 TRAP		
<input type="checkbox"/>	<host>	SNMPv2 TRAP		

Figure 26: SNMP settings

Multiple data structures can be activated but only the most recent should be used in new deployments. Others are kept for legacy reasons and may be retired at some point. The standardized data structure file (MIB) can be downloaded from the device itself.

This device supports both SNMP version 2 and version 3 setups with the later being known for its significantly improved authentication mechanism. Both protocol versions can be enabled or disabled individually.

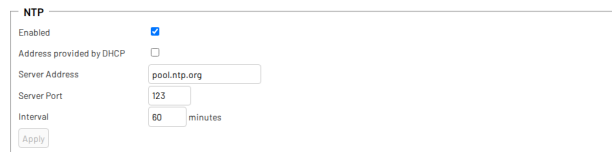
To use SNMP v2, a password in **Read Community** and/or **Write Community** is required. If no password is given, that respective access is disabled.

SNMP v3 access rights are configured as user roles in the user management section.

The **Location** and **Contact** information are optional descriptors.

5.3.6 NTP

To synchronize the internal clock of the PDU the NTP protocol is used. By default the publicly reachable **pool.ntp.org** servers are used and polled upon reboot and subsequently every hour.



SNTP

Enabled ☒

Address provided by DHCP ☐

Server Address

Server Port

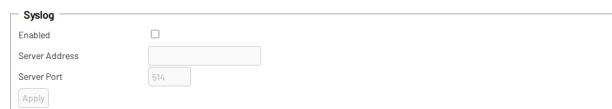
Interval minutes

Figure 27: SNTP settings

Note that certain services may not operate correctly if the time has not been set. Thus, it is suggested to operate an internal SNTP server or relay for setups without WAN access.

5.3.7 Syslog

Centralized logging of all devices in a network is usually achieved with a Syslog server. Upon configuration, the device will send all logging messages to the configured server.



Syslog

Enabled ☐

Server Address

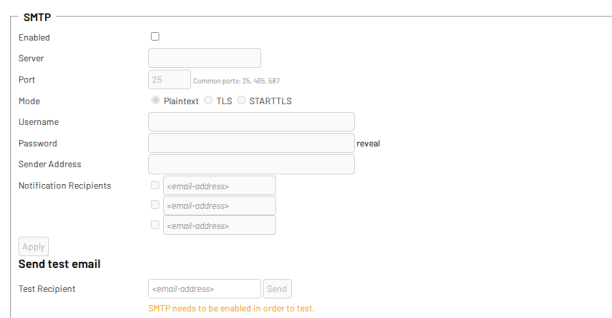
Server Port

Figure 28: Syslog settings

5.3.8 SMTP

The device can be configured to send notifications by email using the Simple Mail Transfer Protocol (SMTP). The following connection methods are available:

- Plain: Unencrypted TCP connections, typically to ports 25 or 587.
- TLS: Encrypted TLS connections, typically to port 465.
- STARTTLS: Also called opportunistic TLS connections, are plain TCP connections which are upgraded to TLS after the connection is established. Typically used on ports 25 or 587.



SMTP

Enabled ☐

Server

Port Common ports: 25, 465, 587

Mode ☒ Plaintext ☐ TLS ☐ STARTTLS

Username

Password

Sender Address

Notification Recipients ☐
☐
☐

Send test email

Test Recipient

SMTP needs to be enabled in order to test.

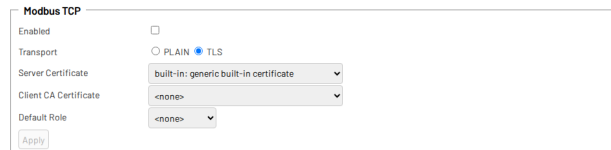
Figure 29: SMTP settings

The configuration can be verified by sending a test email.

5.3.9 Modbus/TCP

Modbus/TCP authorizes connections using roles embedded in x.509 client certificates used for authentication. The role transmitted to the device corresponds to the configured roles. In order to read Modbus/TCP registers, the `modbus-read` permission is required.

If no client authentication is configured, the role configured with the `Default Role` command is used.



The image shows a 'Modbus TCP' configuration form. It includes a checkbox for 'Enabled', a radio button for 'Transport' (with 'PLAIN' and 'TLS' options, where 'TLS' is selected), a dropdown for 'Server Certificate' (set to 'built-in: generic built-in certificate'), a dropdown for 'Client CA Certificate' (set to '<none>'), and a dropdown for 'Default Role' (set to '<none>'). An 'Apply' button is at the bottom left.

Figure 30: Modbus/TCP settings

To make client authorization mandatory (i.e. only grant access to authenticated clients having a role with the `modbus-read` permission in the client certificate), set the default role to `<none>`:

The Modbus/TCP server supports two transport modes:

- **PLAIN** : Connections without encryption or authentication
- **TLS** : Modbus/TCP over TLS (also known as Modbus Security or MBAPS)

With **PLAIN** transport mode, all connections use the configured `Default Role`. It is not recommended to use **PLAIN** transport mode except in fully isolated networks. In **PLAIN** mode the server listens on port 502.

With **TLS** transport mode, all communication with the Modbus/TCP server is encrypted. The server identifies itself using the certificate configured with as `Server Certificate`, allowing clients to make sure they are communicating with the correct server. In **TLS** mode, the server listens on port 802.

If client authentication is configured, clients have to identify themselves with a certificate signed with one of the certificates configured in `Client CA Certificate`. Other connections are refused. Depending on the `Default Role` setting, client certificates have to specify the role of the client in an x.509v3 certificate extension (OID Role: 1.3.6.1.4.1.50316.802.1, refer to section 8.4 within the *Modbus/TCP Security Protocol Specification V36*).

5.4 Authentication

Multiple remote authentication methods may exist. Depending on the device model and make and installed licenses, some of the following methods may not be available.

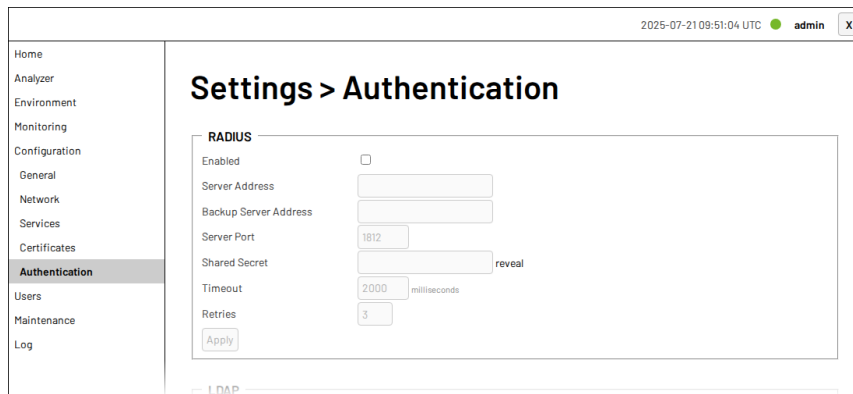


Figure 31: Authentication settings page

5.4.1 RADIUS

RADIUS (short for Remote Authentication Dial In User Service) allows to authenticate users on a RADIUS server without having to create them locally. When RADIUS is enabled and configured, the username and password of users trying to log in is sent to the RADIUS server which verifies if the user has access and which then responds with the roles of that user.



Figure 32: Radius settings

Server Setup

In order to transmit user roles to the device, a vendor specific attribute called “RNx-UPDU-Roles” consisting of a string with a comma-separated list of roles which must be configured for each user.

For FreeRADIUS, this can be achieved with this setting in the `dictionary` configuration file:

```
VENDOR RNx 55108
ATTRIBUTE RNx-UPDU-Roles 1 string RNx
```

Users can now be configured as follows:

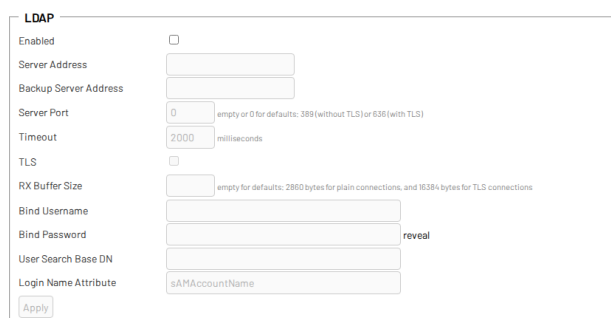
```
bob      Cleartext-Password := "bobspassword"
         RNx-UPDU-Roles = "admin"
```

To mitigate the Blast-RADIUS vulnerability (CVE-2024-3596), the RADIUS client sends the `Message-Authenticator` attribute along with all request packets.

By default, responses from the server are required to contain a valid `Message-Authenticator` attribute. If your server does not support sending this attribute, the RADIUS client can be configured to ignore this requirement. Note that this setting can only be changed via the command-line interface.

5.4.2 LDAP

LDAP (short for Lightweight Directory Access Protocol) allows a device to authenticate users on a authentication server providing LDAP interface without having to create them locally. When LDAP is enabled and configured, the username and password of users trying to log in is sent to the LDAP authentication server which verifies if the user has access and which then responds with the groups the user is member of.



The image shows a web-based configuration form for LDAP settings. The form is titled 'LDAP' and contains the following fields and controls:

- Enabled:** A checkbox that is currently unchecked.
- Server Address:** A text input field.
- Backup Server Address:** A text input field.
- Server Port:** A text input field with the value '0'. A tooltip below it reads: 'empty or 0 for default: 389 (without TLS) or 636 (with TLS)'.
- Timeout:** A text input field with the value '2000'. A tooltip below it reads: 'milliseconds'.
- TLS:** A checkbox that is currently unchecked.
- RX Buffer Size:** A text input field. A tooltip below it reads: 'empty for default: 2860 bytes for plain connections, and 16384 bytes for TLS connections'.
- Bind Username:** A text input field.
- Bind Password:** A text input field with a 'reveal' button to its right.
- User Search Base DN:** A text input field.
- Login Name Attribute:** A text input field with the value 'sAMAccountName'.
- Apply:** A button at the bottom left of the form.

Figure 33: LDAP settings

In some installations, e.g. when users are members of many groups, LDAP responses can grow very large and cause authentication problems. In this case, the size of the receive buffer may need to be tuned using the optional `RX Buffer Size` parameter. By default, buffer size is 2860 bytes for plain connections, and 16384 bytes for TLS connections.

Currently supported authentication server is Microsoft Active Directory.

Configuration of a Microsoft Active Directory User

In order to authenticate a user with certain roles, it is necessary for the user to be member of at least one group with the name `RNX-UPDU-[role]`.

Example : User bob is member of groups `RNX-UPDU-admin` and `RNX-UPDU-snmp-read`.

5.4.3 TACACS+

TACACS+ (short for Terminal Access Controller Access-Control System Plus) is a protocol allowing user authentication through an external server. When configured and enabled, the device sends credentials of users trying to log in to the configured server which checks if that user should be granted access and what roles it is member of.

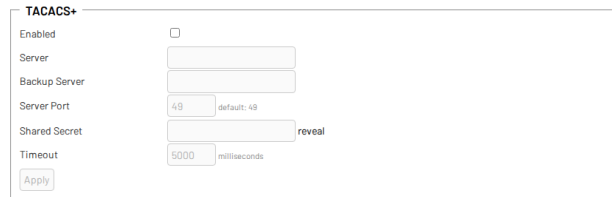


Figure 34: TACACS settings

The hostname or IP address of up to two TACACS+ servers can be configured. The backup server is used when the connection to first server fails.

The TACACS+ timeout option controls how long the device waits for a response from TACACS+ servers until it considers the request failed. The default timeout is 5 seconds.

Server Setup

Users are configured as follows on the TACACS+ server:

```
user = <USERNAME> {
  login = <PASSWORD-SPEC>
  service = rnx-updu {
    roles="<ROLES>"
  }
}
```

Where `<USERNAME>` is the username allowed to log in, `<PASSWORD-SPEC>` is a specification of the password (see the documentation of your TACACS+ server for more information) and `<ROLES>` is a comma-separated list of roles which are configured on the device in question. The user logging in will have the combined set of permissions of all the specified roles. Note that whitespace is not stripped from the list of roles.

5.5 Certificates

Certificates are used for a variety of services whenever a TLS connection is used to authenticate and/or encrypt the communication channel.

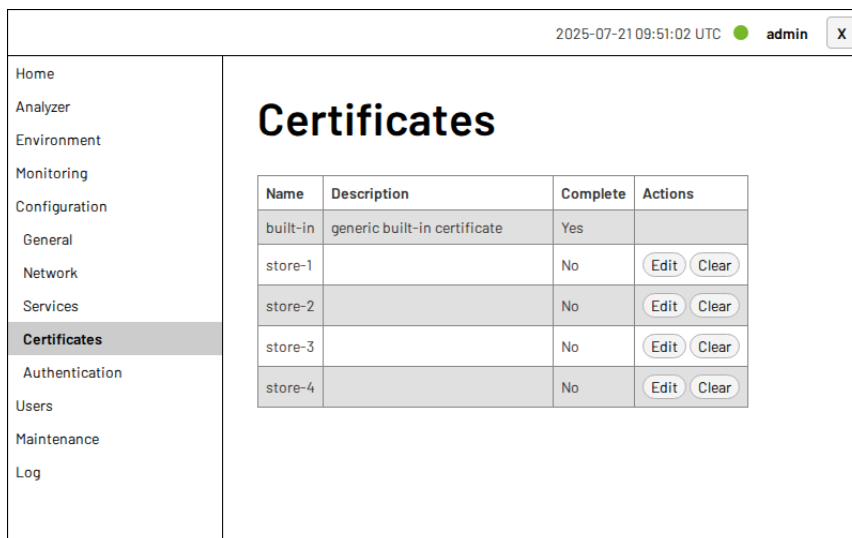


Figure 35: Certificates settings page

5.5.1 SSL/TLS Certificates Configuration

In addition to the built-in SSL/TLS certificate, up to four custom certificates, stored in the certificate stores `store-1` to `store-4` can be configured by the user.

To configure a certificate, two text files containing PEM formatted data are needed:

- A private key (e.g. pdu.domain.key), with a format as follows:

```
-----BEGIN PRIVATE KEY-----
<base64 data>
-----END PRIVATE KEY-----
```

- A certificate (e.g. pdu.domain.crt), with a format as follows:

```
-----BEGIN CERTIFICATE-----
<base64 data>
-----END CERTIFICATE-----
```

The certificate can contain intermediate certificates, in which case multiple `BEGIN/END CERTIFICATE` lines are present.

5.5.2 Using the rnx.io Certificate

The device comes with an embedded certificate which can be used to access the device securely and without browser warnings. A special DNS resolver is operated which allows to use the rnx.io domain to access the device via HTTPS.

This works as followed: If your device is configured to have the IP address 10.10.0.33 , the host-name to access the device would be 10-10-0-33.rnx.io . For this to work, the client (e.g. PC) which

connects to the device must have internet access. The device itself is not required to have internet access because the DNS lookup happens on the client.

Given that the rnx.io certificate is signed and trusted by all major browsers, there will not be any warning message when accessing the web-interface.

6 Maintenance

The maintenance page allows upgrading the firmware and rebooting the device. The relevant data is shown per module.

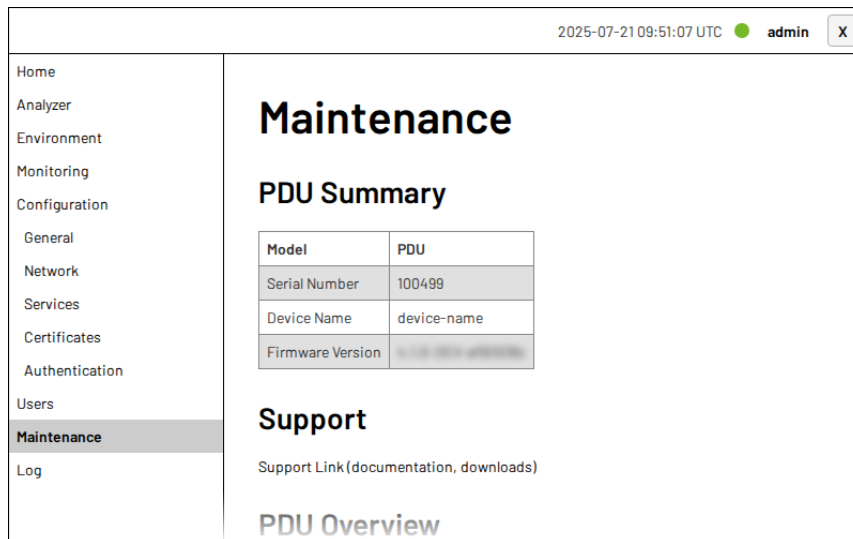


Figure 36: Maintenance page

6.1 Support

Use the provided link to open the support website for:

- Documentation
- Firmware Updates
- Software Tools

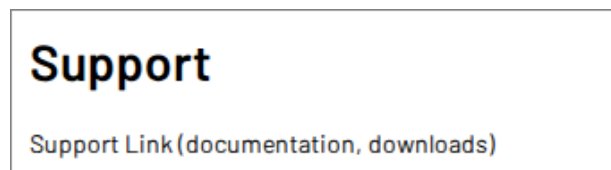


Figure 37: Support link

6.2 Device Overview

The device overview shows a list of all installed modules along with the most important details of the modules.

PDU Overview							
Phase	Module	# Outlets	Part Number	Serial Number	Revision	Firmware	Firmware Standby
-	PIM	-	100-0579	1006010	1	3.76.1-00014-000	3.76.2-00014-000
L1	POM	6	100-0508	1035128	2	3.76.1-00014-000	3.76.2-00014-000
L2	POM	8	100-0290	1001267	2	3.76.1-00014-000	3.76.2-00014-000
-	ICM	-	100-0141	1009549	1	3.76.1-00014-000	3.76.2-00014-000
L3	POM	8	100-0290	1001274	2	3.76.1-00014-000	3.76.2-00014-000

Figure 38: Device overview

6.3 Licenses

A list of all installed licenses along with the option to add new licenses. To obtain new licenses, refer for the support or vendor of the device.

Licensed Features			
Feature ID	License S/N	Status	Description
1	523	Active	Feature Set V1
100	523	Active	Feature Outlet Metering

[Add Licenses](#)

Figure 39: List of licensed features

6.4 Firmware update

The firmware running on the device can be downloaded from the support link provided above. Once the archive has been downloaded and the containing files extracted, the [Release Notes](#) shall be consulted to make sure the device will still work as before within a given environment.

Firmware update

No file chosen

Figure 40: Firmware update

Once the documentation has been consulted, the firmware can be updated by selecting **Choose File** and clicking **Update**.

The update should complete within a minute after which a notification will confirm the update. The update is fail-safe, thus in case of problems or errors during the update, the previously installed firmware is booted.

Note

When upgrading from older firmware revisions (2.5.x or earlier), the confirmation message and certain error messages may be missing or not show all details. It may be required to manually verify the installation of the new version.

Reverting back to the previous image firmware is possible via the command-line interface.

6.5 Reboot the device

The **Reboot now** button will simply ask for confirmation and reboot the device. As soon as the device has restarted, a new login is required.

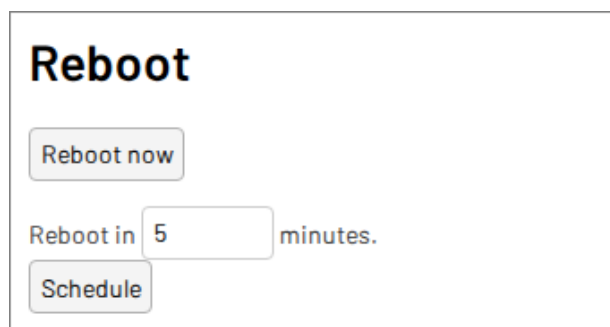


Figure 41: Reboot device

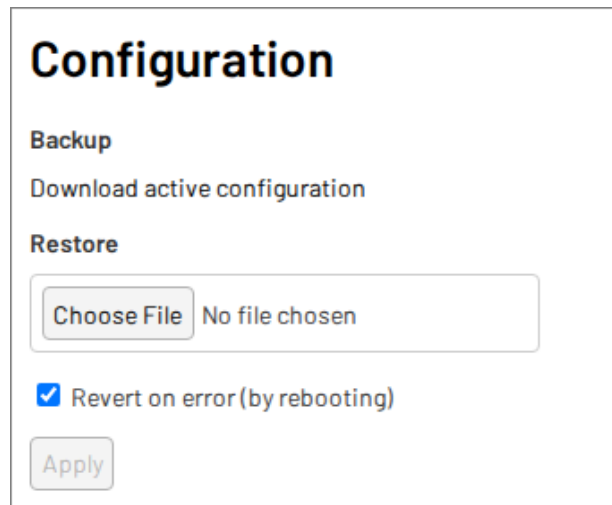
A reboot can be scheduled with **Reboot in <minutes>**. Note that this can be very helpful when remotely changing the configuration, especially networking and service related settings. One would schedule a reboot and start changing the configuration. Should for some reason the connection been lost (e.g. wrong IP settings, disable HTTPS), the device reboots after a certain period and restores the last persisted (**Save Configuration**) configuration.

Note

Rebooting the device will not reset the internal network switch on ETH1 and ETH2 which will continue to operate. Thus rebooting a PDU will not break the network daisy-chain one may have built with these ports.

6.6 Configuration Management

The currently active configuration can be exported by clicking on **Download active configuration**. This configuration can later be restored if needed.



Configuration

Backup

Download active configuration

Restore

Choose File No file chosen

☒ Revert on error (by rebooting)

Apply

Figure 42: Configuration backup and restore

Note

The configuration backup is a plain-text file which can be modified with a text editor. This allows for example to prepare configurations for a fleet of devices. Refer to the command-line interface manual for more details on how to configure by using this textual structure.

6.7 Diagnostics

The support team may ask to provide diagnostics information to identify possible issues with a given device. In this case, the file downloaded by clicking on **Download diagnostics information** shall be transmitted.



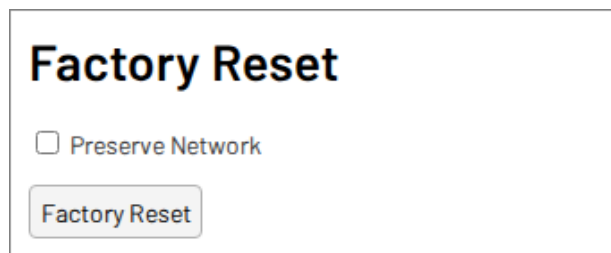
Diagnostics

Download diagnostic information

Figure 43: Device diagnostics

6.8 Factory Reset

The **Factory Reset** resets settings to their factory defaults and reboots the device. If requested, network settings (interface configuration and spanning-tree protocol settings) can be preserved in order not to lose connectivity when the factory reset is initiated remotely.



The screenshot shows a dialog box titled "Factory Reset" in a large, bold, black font. Below the title, there is a checkbox labeled "Preserve Network". At the bottom of the dialog, there is a button labeled "Factory Reset".

Figure 44: Factory reset

7 User Management

Users with a role containing the `Configure` permission have access to the user management menu.

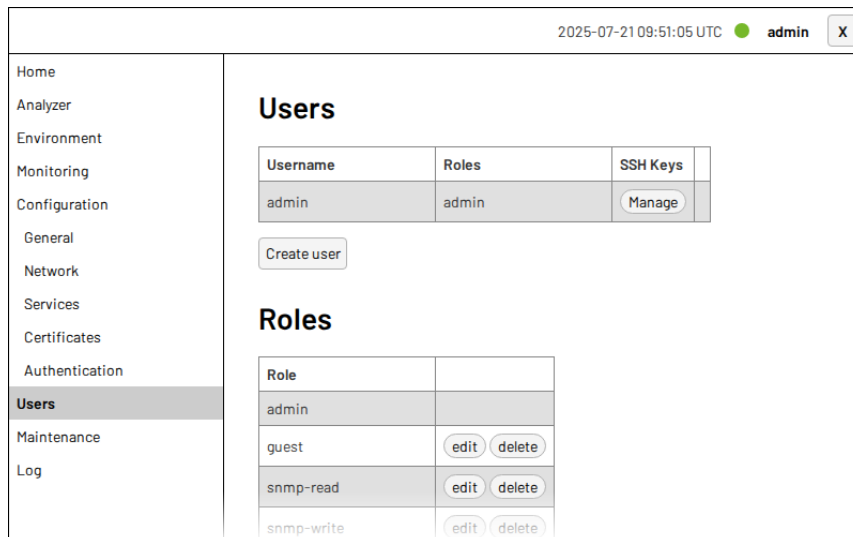


Figure 45: User management

7.1 Create a new user

A new user is created by clicking on `Create user` and selecting the desired Username, Roles, Password and whether this user would be allowed to authenticate against the device's SNMPv3 server.

7.2 Create a new role

A new role is created by clicking on `Create role`. Fine grained permissions can be configured by creating roles and assigning these to users.

7.3 Editing an existing user

Editing a user allows changing its role(s) and its password in pretty much the same way the user was created. Note that a logged in user could not modify its own settings other than password and SSH Keys by clicking on the username at the top-right of the page.

Note

Once created, the username cannot be edited. The user must be deleted and a new user with the correct username can be created.

8 Log

The Log page prints the log messages of the device. The timestamp can be chosen.

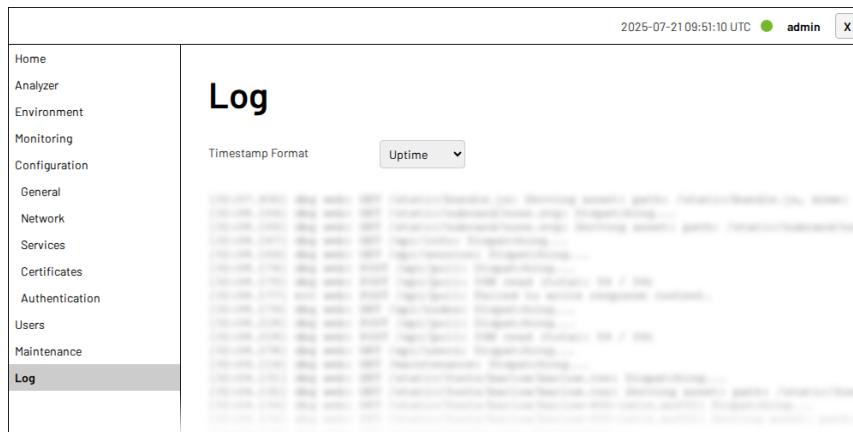


Figure 46: Log page

9 Legal

Electronics and Stellaris™ Firmware Copyright by RNX™ (Riedo Networks Ltd, Switzerland).

Stellaris™ and RNX™ are registered trademarks of Riedo Networks Ltd, Switzerland.